

CISCO MICROSOFT PRIVATE CLOUD FAST TRACK 3.0 SOLUTION FOR EMC VSPEX WITH SYSTEM CENTER 2012 SP1 FOR 250 VMS

DEPLOYMENT GUIDE

July 2013

Table of Contents

About the Authors **8**
Acknowledgements **8**
About Cisco Validated Design (CVD) Program **8**

1 Introduction **10**
1.1 Private Cloud Fast Track Program Description **10**
Business Value 10
Technical Benefits 11
Program Requirements and Validation 11
1.2 Design Patterns Overview **11**
Design Pattern #3: Converged Infrastructure 12

2 Core Fast Track Infrastructure **12**
2.1 Architecture **13**
2.2 Software Revisions **15**
2.3 Configuration Guidelines **19**
2.4 Configuration Workstation **20**
2.5 Deployment **21**
2.6 Cabling Information **22**

3 EMC VNX5500 Deployment: Part 1 ..... **24**
3.1 VNX Worksheets **25**
Creation of Storage Pools 29
Create Support for Hot Spares and Clone Private LUNs 29
Configure VNX5500 iSCSI Connections 30

4 Cisco Nexus 5548 Deployment: Part 1 ..... **32**
4.1 Set Up Initial Cisco Nexus 5548 Switch **32**
Enable Appropriate Cisco Nexus Features 33
Configure Fibre Channel Ports 34
Create Necessary VLANs 34
Add Individual Port Descriptions for Troubleshooting 35
Create Necessary Port Channels 36
Add Port Channel Configurations 37
Configure Virtual Port Channels 39
Configure Fibre Channel Ports 40
Link into Existing Network Infrastructure 40
4.2 Configure Cisco Unified Computing System Fabric Interconnects **40**
Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects 41
Log into Cisco UCS Manager 41
Add a Block of IP Addresses for KVM Access 42
Synchronize Cisco Unified Computing System to NTP 43
Edit the Chassis Discovery Policy 44
Enable Server and Uplink Ports 45
Configure Unified Ports for Fibre Channel 46
Acknowledge the Cisco UCS Chassis 47
Create Uplink PortChannels to the Cisco Nexus 5548 Switches 48
4.3 Configure Service Profiles **50**
Create an Organization 50
Create a MAC Address Pool 50
Create WWNN Pools 52
Create WWPN Pools 53
Create UUID Suffix Pools 55

Create Server Pools 56
Create VLANs 57
Configure Appliance Ports for iSCSI (optional SMB) 58
Create Host Firmware Package Policy 59
Enable Quality of Service in Cisco UCS Fabric 60
Create a Power Control Policy 61
Create a Local Disk Configuration Policy 62
Create a Server Pool Qualification Policy 63
Create a Server BIOS Policy 64
Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts 64
Create vNIC Templates 65
Create vHBA Templates for Fabric A and B 72
Create Boot Policies 73
Cisco UCS Manager for Fabric A 75
Cisco UCS Manager for Fabric B 79
Create Service Profile Templates 81
Create Service Profiles 88

5 EMC VNX5500 Deployment: Part 2 89
5.1 Create VNX LUNs for Private Cloud Environment 89
Mask Boot LUN with EMC Unisphere 91
5.2 Cisco Nexus 5548 Switch: Configure for SAN Boot 95
Gather Necessary Information 95
Create Device Aliases and Create Zone for First Server 95

6 First Installation Windows Server 2012 Datacenter Edition 96
6.1 Local Configuration Tasks 105
Initial Network Configuration 105
Common Configuration Tasks 109
Run Windows Update 109
Install Microsoft Hotfixes 109
Install Windows Roles and Features 109
Configure Paging File 109
Configure MPIO 112
EMC VNX5500 112
6.2 Sysprep the Image 114
6.3 Removal of Source Master Image 114
6.4 Create Clones of Sysprep Image 115
Create Clones with ESI 115
Create Clones through Unisphere 118
6.5 Booting from Sysprepped LUNs 122
Zone the Network 122
Mask the Boot LUNs to Service Profiles 123
6.6 Complete the Image Builds from Sysprepped Images 123
Configure Networks 125
Configure NIC Teaming 125
Configure Hyper-V Virtual Switches 127
Unconfigure DNS Registration 128
Binding Order 130
Install EMC PowerPath 131
Install Unisphere Host Agent 133
6.7 Create Hyper-V Cluster 137
Hyper-V Network Configuration 137
Create Shared Storage 139
Run Cluster Validation Wizard 142
Create Fabric Management Cluster 143

7 Fabric Management 150
7.1 Fabric Management Host and Guest Installation 150
Provisioning Fabric Management Hosts 150
Create Fabric Management Virtual Guests 151
7.2 Create Required User Accounts and Security Groups 155
Active Directory Domain User Accounts 155
Active Directory Domain Security Groups 156

8 Microsoft SQL Server 2012 SP1 Cluster Installation 157
8.1 Overview 158
8.2 Prerequisites 159
Accounts 159
Groups 160
Required Networks 160
Establish the SQL Server Guest Cluster 160
8.3 Installation 170
Install the SQL Named Instances on the Guest Cluster (Node 1) 170
Install the SQL Named Instances on the Guest Cluster (Additional Nodes) 183
Post-Installation Tasks 188
Configure Windows Firewall Setting for SQL Named Instances 188
Assign Preferred Owners for SQL Instances in Failover Cluster Manager 201

9 System Center Virtual Machine Manager 204
9.1 Overview 205
9.2 Prerequisites 206
Accounts 206
Groups 206
Required Networks 207
Install the Windows Assessment and Deployment Kit 207
Install the Prerequisite Windows Server Roles and Features 209
Install the SQL Server 2012 SP1 Command Line Utilities 213
Configure Failover Clustering with SMB 3.0 Shared Storage 219
Create the Virtual Machine Manager Distributed Key Management Container in Active Directory Domain Services 222
9.3 Installation – SCVMM Management Server 227
Install the Virtual Machine Manager Failover Cluster 227
9.4 Creating Virtual Machine Manager Library Share on the VNX5500 244
9.5 Add Hyper-V Hosts to VMM 254
9.6 Configure Logical Networks 256
9.7 Configure Library Subdirectories (optional) 257
9.8 Configure Constrained Delegation (optional) 258

10 System Center Operations Manager 259
10.1 Overview 260
10.2 Prerequisites 261
Accounts 261
Groups 261
Required Networks 262
Add the .NET Framework 3.5 Feature 262
Install the SQL Server Reporting Services and Analysis Services (Split Configuration) 264
Install Microsoft Report Viewer 2010 SP1 280
Configuration of Operations Manager SQL Server Prerequisites 282
10.3 Installation 285
Install the Operations Manager Management Server 285
Install the Second Operations Manager Management Server 292
Install the Operations Manager Reporting Server 293

10.4 Post-Installation Tasks 297
Register Service Principal Names for the Operations Manager Management Servers 297
Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Servers 298
Install Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server 302
Install Operations Manager Console on the VMM Management Server 303
Download and Import the Prerequisite Operations Manager Management Packs in Operations Manager 306
Install SQL Analysis Management Objects 310
Perform Virtual Machine Manager and Operations Manager Integration 314

11 System Center Service Manager 317
11.1 Overview 318
11.2 Prerequisites 319
Accounts 320
Groups 321
Required Networks 321
Add the .NET Framework 3.5 Feature on all Server Manager Servers 321
Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers 325
Install SQL Server 2012 Native Client on the on the Management and Data Warehouse Servers 326
Install SQL Server 2012 SP1 Analysis Management Objects 328
Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server 330
Install SharePoint Foundation 2010 Service Pack 1 on the Self-Service Portal Server 343
Install .NET Framework 4 on the Self-Service Portal Server 352
Request and Install an SSL Certificate on the Self-Service Portal Server 354
Configuration of Service Manager Environmental Prerequisites 356
11.3 Installation 360
Installation – Management Server 360
Installation – Second Management Server 369
Installation – Data Warehouse Server 370
Install the Silverlight Runtime 386
Installation – Self-Service Portal Server 387

12 System Center Orchestrator 394
12.1 Overview 395
12.2 Prerequisites 396
Accounts 396
Groups 396
Required Networks 396
Add the .NET Framework 3.5 Feature 396
Install the Silverlight Runtime 399
12.3 Installation – Orchestrator Runbook, Web Service, and Designer Server 400
12.4 Install an Additional Orchestrator Runbook Server 411
12.5 Post-Installation Tasks 418
Install the Virtual Machine Manager Console 418
Install the Microsoft Report Viewer 2010 SP1 422
Install the Operations Manager Console 423
Install Integration Packs 426
Deploy Integration Packs 430

13 System Center App Controller 436
13.1 Overview 437

13.2 Prerequisites ... **438**
Accounts ... 438
Groups ... 438
Required Networks ... 438
Add the .NET Framework 3.5 Feature ... 438
Install Silverlight Runtime ... 441
Install the Virtual Machine Manager Console ... 442
13.3 Installation ... **445**
Install the App Controller Portal Server ... 445

14 System Center Cloud Services Process Pack ... **453**
14.1 Overview ... **454**
14.2 Prerequisites ... **455**
Deploy Chargeback Report Files on the Operations Manager Management Server ... 455
Deploy Chargeback Report Files on the Service Manager Management Server ... 456
Create the System Center Operations Manager Connector ... 458
Create the OrchestratorUsersGroup local group on the Orchestrator Server ... 461
14.3 Installation ... **462**
Install the Cloud Services Process Pack ... 462
Install the Cloud Services Process Pack Runbooks ... 465

15 Cisco Integration Components ... **468**
15.1 Cisco UCS PowerTool ... **468**
Before You Begin ... 468
Install PowerTool ... 469
15.2 System Center 2012 SP1 Operations Manager Management Pack ... **471**
Install the Management Pack ... 472
Add Cisco UCS Domains to Operations Manager ... 474
Configure Administrator Account ... 477
Configure Fault Acknowledgement ... 479
Configure Cisco UCS Management Service ... 481
15.3 System Center 2012 SP1 Orchestrator Integration Pack ... **482**
Register the Cisco UCS OIP ... 482
Deploy the Cisco UCS OIP ... 483
Configure the Cisco UCS OIP ... 486
15.4 System Center 2012 SP1 Virtual Machine Manager UI Extension ... **487**
Importing the Add-in ... 487
Configure and Use the Cisco UCS Add-in ... 488
15.5 Cisco Nexus 1000V ... **489**
Create Two Virtual Supervisor Module VMs ... 489
Configure the VSM ... 492
Configure Virtual Switch Extension Manager in VMM ... 497
Copy Virtual Ethernet Module Installation Packager to the VMM Virtual Machines ... 500
Configure a Logical Switch in VMM ... 500
Create the Logical Switch on the Hyper-V Hosts ... 504
Create a VM Network ... 506
Configure the Virtual Machine Manager Virtual Machine Properties ... 507

16 EMC Integration Components ... **512**
16.1 EMC Software Installation Locations ... **512**
16.2 Install and Configure the EMC Storage Integrator Management Pack for System Center Operations Manager ... **512**
16.3 Install the ESI Service and ESI Service PowerShell Toolkit ... **513**
Register the VNX with the ESI Service ... 514
Create an ESI Service User for the SCOM Management Pack Run As Account ... 515
16.4 Install the ESI SCOM Management Packs ... **515**

Import the ESI SCOM Management Packs 517
Create ESI Run As Account and Associate with a Profile 519
Setting Overrides for the EMC SI Service Discovery 523
16.5 Install and Configure the EMC SMI-S Provider for System Center Virtual Machine Manager integration 524
Install the EMC SMI-S Provider 525
Register the VNX with the Provider 526
Create the SMI-S User for the SCVMM Run As Account 528
Create the Run As Account within SCVMM 530
Register the EMC SMI-S provider with SCVMM 531
Allocate Storage Pools to Host Groups 533
16.6 Configure the Library Server 534
16.7 Create a SAN Copy Capable Template 538
16.8 Select the Rapid Provisioning Deployment Method 540

17 Appendix A: SQL Cluster Named Instance Worksheet 542

18 Appendix B: Sample PowerShell Scripts 543
18.1 Populate Domain Accounts and Security Groups 543
Add-FTUsers.ps1 543
AddFTUsers.csv 543
Add-FTGroups.ps1 544
AddFTGroups.csv 544
18.2 Add-UcsHyperVFeatures.ps1 545
18.3 Create-UcsFtVms.ps1 546
18.4 Set-UcsHyperVAdapters.ps1 548
18.5 Set-UcsHyperVRemoteMgmt.ps1 550
18.6 Fast Track Software Download 552
FastTrackDownloadSoftware.ps1 552
FastTrackDownloads.xml 553
18.7 PowerShell Scripts for VNX5500 Management 557
Create-EMCHyperVSparesClones.ps1 557
PrepMasterBoot-AddViaWWPN.ps1 558
ProcessStorageRequests.ps1 560
ProcessClones.ps1 562
PostClone_AddViaWWPN.ps1 565

19 Appendix C: VNX5500 SMB 3.0 Configuration 568
19.1 Configure DNS and NTP 568
19.2 Configure Network Services 569
19.3 Configure Interfaces 570
19.4 Configure Storage 570
19.5 Configure SMB File Systems and Mounts 572
19.6 Configure VNX CIFS Servers and Associated Shares 574

20 Appendix D: Sample SMB Cluster Configuration 576
20.1 Overview 576
20.2 Create the Cluster 577
20.3 VNX5500 Share Preparation 577
20.4 Set Share Permissions 579
20.5 Complete the Cluster 581

About the Authors

Tim Cerling, Technical Marketing Engineer, Cisco

Tim Cerling is a Technical Marketing Engineer with Cisco's Datacenter Group, focusing on delivering customer-driven solutions on Microsoft Hyper-V and System Center products. Tim has been in the IT business since 1979. He started working with Windows NT 3.5 on the DEC Alpha product line during his 19 year tenure with DEC, and he has continued working with Windows Server technologies since then with Compaq, Microsoft, and now Cisco. During his twelve years as a Windows Server specialist at Microsoft, he co-authored a book on Microsoft virtualization technologies - Mastering Microsoft Virtualization. Tim holds a BA in Computer Science from the University of Iowa.

Mike McGhee, EMC

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, we would like to thank:

- Mike Mankovsky – Cisco
- Txomin Barturen – EMC

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx,

and the WebEx logo are registered trademarks of Cisco Systems, Inc. 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. (0809R)
© 2013 Cisco Systems, Inc. All rights reserved

1 Introduction

The Microsoft Private Cloud Fast Track program is a joint effort between Microsoft and its hardware partners such as Cisco and EMC. The goal of the program is to help organizations develop and implement private clouds quickly while reducing both complexity and risk. The program provides a reference architecture that combines Microsoft software, consolidated guidance, and validated configurations with partner technology such as compute, network, and storage architectures, in addition to value-added software components.

The private cloud model provides much of the efficiency and agility of cloud computing, along with the increased control and customization that are achieved through dedicated private resources. With Private Cloud Fast Track, Microsoft and its hardware partners can help provide organizations both the control and the flexibility that are required to reap the potential benefits of the private cloud.

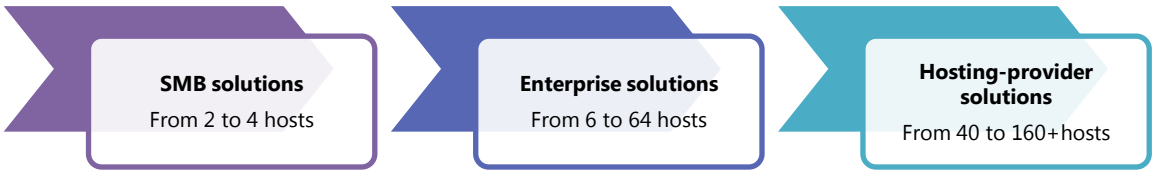
Private Cloud Fast Track utilizes the core capabilities of the Windows Server (OS), Hyper-V, and System Center to deliver a private cloud infrastructure as a service offering. These are also key software components that are used for every reference implementation.

1.1 Private Cloud Fast Track Program Description

Each Private Cloud Fast Track program outlines the high-level architectural vision that is intended to help partners rapidly develop end-to-end, integrated, and tested virtualization or private cloud solutions for small- and medium-size businesses and for the enterprise and data center that meet or exceed the Microsoft validation standards.

The Fast Track program has three main branches, as shown in the following figure. This guide will focus exclusively on the Enterprise Solutions branch.

Figure 1 Branches of the Microsoft Private Cloud Fast Track Program



Each branch in the Fast Track program uses a reference architecture that defines the requirements that are necessary to design, build, and deliver virtualization and private cloud solutions for small-, medium-, and large-size enterprise implementations.

Each reference architecture in the Fast Track program combines concise guidance with validated configurations for the compute, network, storage, and virtualization layers. Each architecture presents multiple design patterns for enabling the architecture, and each design pattern describes the minimum requirements for validating each Fast Track solution.

The Cisco and EMC Fast Track Solution presented here is an Enterprise solution. The Cisco and EMC with Microsoft Private Cloud Fast Track solution utilizes the core capabilities of Windows Server 2012, Hyper-V and System Center 2012 SP1 to deliver a Private Cloud - Infrastructure as a Service offering. The key software components of every Reference Implementation are Windows Server 2012, Hyper-V, and System Center 2012 SP1. The solution also includes software from Cisco and EMC to form a complete solution that is ready for your enterprise.

Business Value

The Cisco and EMC with Microsoft Private Cloud Fast Track solution provides a reference architecture for building private clouds on each organization's unique terms. Each Fast-Track

solution helps organizations implement private clouds with increased ease and confidence. Among the benefits of the Microsoft Private Cloud Fast Track Program are faster deployment, reduced risk, and a lower cost of ownership.

Reduced risk:

- Tested, end-to-end interoperability of compute, storage, and network
- Predefined, out-of-box solutions based on a common cloud architecture that has already been tested and validated
- High degree of service availability through automated load balancing

Lower cost of ownership:

- A cost-optimized, platform and software-independent solution for rack system integration
- High performance and scalability with Windows Server 2012 operating system and Hyper-V
- Minimized backup times and fulfilled recovery time objectives for each business critical environment

Technical Benefits

The Microsoft Private Cloud Fast Track Program integrates best-in-class hardware implementations with Microsoft's software to create a Reference Implementation. This solution has been co-developed by Cisco, EMC, and Microsoft and has gone through a validation process. As a Reference Implementation, Cisco, EMC, and Microsoft have taken the work of building a private cloud that is ready to meet a customer's needs.

Faster deployment:

- End-to-end architectural and deployment guidance
- Streamlined infrastructure planning due to predefined capacity
- Enhanced functionality and automation through deep knowledge of infrastructure
- Integrated management for virtual machine (VM) and infrastructure deployment
- Self-service portal for rapid and simplified provisioning of resources

Program Requirements and Validation

The Microsoft Private Cloud Fast Track program is comprised of three pillars; Engineering, Marketing and Enablement. These three pillars drive the creation of Reference Implementations, making them public and finally making them available for customers to purchase. This Reference Architecture is one step in the "Engineering" phase of the program and towards the validation of a Reference Implementation.

1.2 Design Patterns Overview

As the Microsoft Private Cloud Fast Track program has multiple solutions, it also presents multiple design patterns that its partners can choose from to show the partners best solutions. The following table lists the three design patterns that Microsoft offers.

Table 1 Design Pattern Summary

Design Pattern	Key Features
Continuous Availability over SMB	• File-based Storage Networking via SMB3 • Deep guidance for using Windows as the storage platform i.e. Storage Spaces, SMB Direct, etc.

Non-Converged	• Dedicated Ethernet NICs and Storage HBAs • iSCSI, FCoE, or Fibre Channel storage networking
Converged	• Converged Networking • iSCSI or FCoE storage networking

The Cisco and EMC solution is a converged solution.

Design Pattern #3: Converged Infrastructure

Converged Infrastructure in this context is the sharing of network topology between network and storage network traffic. This typically implies an Ethernet network devices and network controllers with particular features to provide segregation, quality of service (performance), and scalability. The result is a network fabric with less physical complexity, greater agility and lower costs than those associated with traditional Fiber-based storage networks.

In this topology, many storage designs are supported including traditional SANs, SMB3-enabled SANs, and Windows-based Scale-Out File Servers. The main point in a converged infrastructure is that all storage connectivity is network-based using a single media such as copper. SFP+ adapters are most commonly used.

Key drivers for convergence include cost savings and operational efficiency of a single common Ethernet network vs. multiple physical networks and HBAs for storage traffic. Benefits often include higher utilization levels of datacenter infrastructure with reduced equipment and management costs of the network.

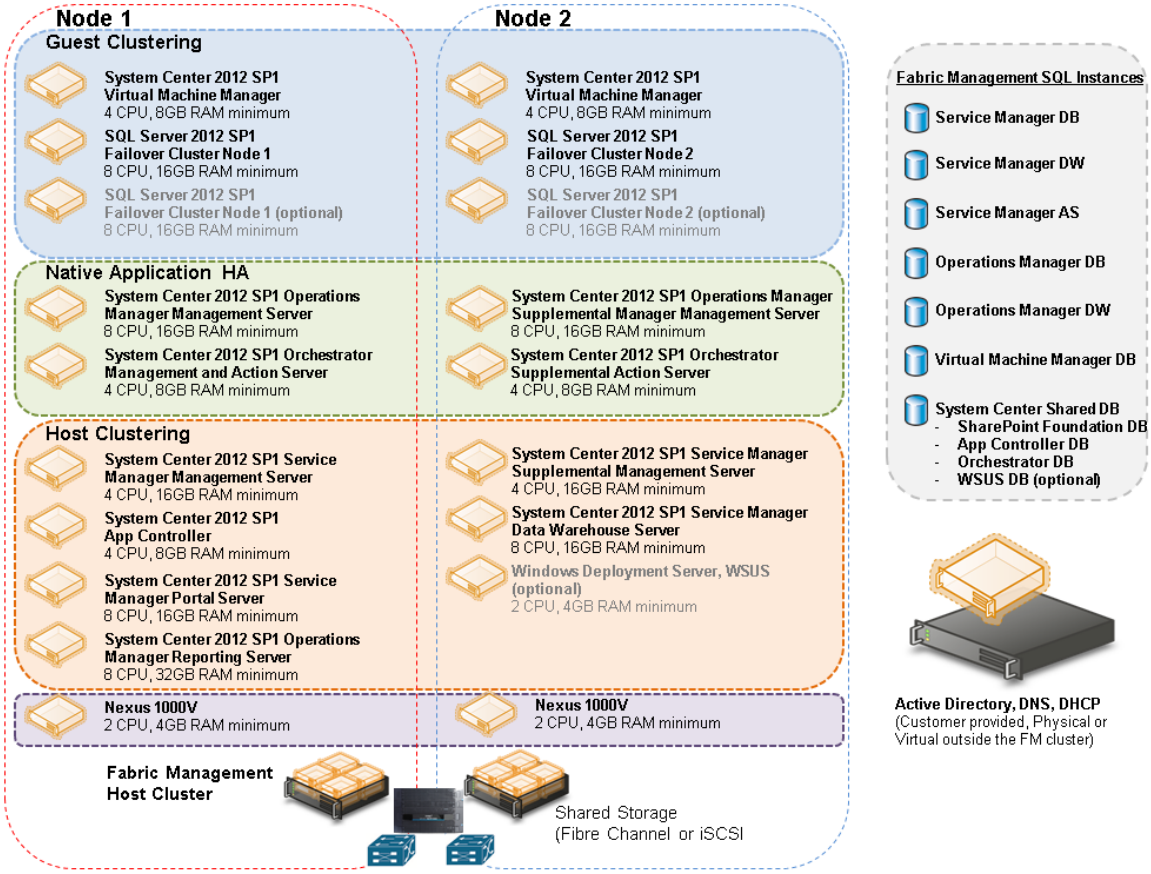
2 Core Fast Track Infrastructure

The Cisco and EMC solution is based on Design Pattern 3 – Converged Infrastructure. In Design Pattern 3 the fabric management VMs are hosted directly on a compute fabric cluster along with other workload VMs. Additionally, Pattern 2 leverages the minimal number of System Center component servers recommended in order to provide full functionality in a production environment. This document will cover the steps for installing Design Pattern 2. Design Pattern 2 is outlined in the diagram below.

A single design pattern is introduced for Fabric Management which includes a dedicated two-to-four node Hyper-V failover cluster to host the fabric management virtual machines. This design pattern utilizes both scaled-out and highly available deployments of the System Center components to provide full functionality in a production environment.

In addition to the System Center components running as virtual machines, Cisco deploys a pair of Nexus 1000V virtual machines to handle network management for the VMs.

Figure 1 Design Pattern 2 – Private Cloud Fabric Management Infrastructure

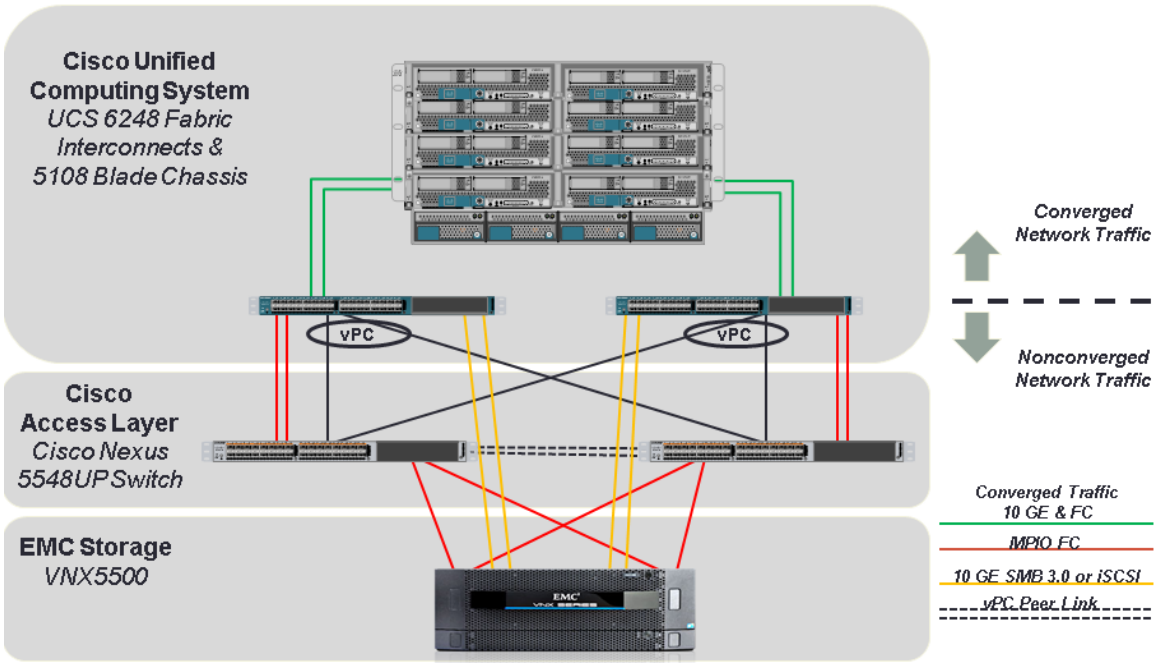


2.1 Architecture

The Cisco and EMC architecture is highly modular. Although each customer's components might vary in its exact configuration, after a Cisco and EMC configuration is built, it can easily be scaled as requirements and demands change. This includes both scaling up (adding additional resources within a Cisco UCS chassis and/or EMC VNX array) and scaling out (adding additional Cisco UCS chassis and/or EMC VNX array).

The Cisco UCS solution validated with Microsoft Private Cloud includes EMC VNX5500 storage, Cisco Nexus 5500 Series network switches, the Cisco Unified Computing Systems (Cisco UCS) platforms, and Microsoft virtualization software in a single package. The computing and storage can fit in one data center rack with networking residing in a separate rack or deployed according to a customer's data center design. Due to port density, the networking components can accommodate multiple configurations of this kind.

Figure 2 Implementation Diagram



The above reference configuration contains the following components:

- 5108 chassis each with eight Cisco UCS B200 M3 Blade servers, dual Intel E5-2640 2.50 GHz processors, 256 GB memory, 1240 Virtual Interface Card
- Two Cisco UCS 2108 fabric extenders per chassis
- Two Cisco UCS 6248UP Fabric Interconnects
- Two Cisco Nexus 5548UP Switches
- 10 GE and 8 Gb FC connections
- EMC VNX5500 Unified Platform
- 115 x 600 GB 15k rpm 3.5-inch SAS disks
- 6 x 200 GB EFDs
- 4 x 300 GB 15k rmp 3.5-inch SAS drives as hot spares
- 1 x 200 GB EFD as hot spare
- EMC SnapView

Storage is provided by an EMC VNX5500 storage array with accompanying disk shelves. All systems and fabric links feature redundancy, providing for end-to-end high availability (HA configuration within a single chassis). For server virtualization, the deployment includes Microsoft Hyper-V. While this is the default base design, each of the components can be scaled flexibly to support the specific business requirements in question. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves or SSDs could be deployed to improve I/O capacity and throughput, or special hardware or software features could be added to introduce new features.

The remainder of this document provides guidance through the low-level steps of deploying the base architecture, as shown in the above figure. This includes everything from physical cabling, to

compute and storage configuration, to configuring virtualization with Microsoft Windows Server 2012 Hyper-V.

2.2 Software Revisions

It is important to note the software versions used in this document. The following table details the software revisions used throughout this document.

Appendix B contains a sample PowerShell script, FastTrackDownloadSoftware.ps1, that automates the download of many of these pieces of software. Not all pieces can be downloaded automatically as some require login information to be provided to access them. The PowerShell script reads an XML file, FastTrackDownloads.xml, to define which software packages to download.

Table 2 Software Revisions

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect	2.1(1b)	http://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821
	Cisco UCS B-200-M3	2.1(1b)	http://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821
Network	Nexus Fabric Switch	5.0(3)N2(2a)	Operating system version
Storage	EMC VNX5500 Block	05.32.000.5.201	Operating system version
	EMC VNX5500 File (Optional)	7.1.65.8	Operating system version
Software	Cisco UCS Hosts	2012	Microsoft Windows Server Datacenter Edition + Hyper-V Role
	.NET Framework	3.5.1	Feature enabled within Windows Server 2012 (Required for SQL installations)
	.NET Framework	4.0	http://download.microsoft.com/download/9/5/A/95A9616B-7A37-4AF6-BC36-D6EA96C8DAAE/dotNetFx40_Full_x86_x64.exe
	Windows MPIO software		Feature within Windows Server 2012
	Microsoft Hotfixes		http://support.microsoft.com/kb/2796995 - ODX failure
			http://support.microsoft.com/kb/2785638 - SR-IOV failure
			List of additional hotfixes that should be checked: http://social.technet.microsoft.com/wiki/contents/articles/15576.hyper-v-update-list-for-windows-server-2012.aspx
	Cisco UCS Management Pack 2012	2.6.1	http://developer.cisco.com/web/unifiedcomputing/systemcenter
	Cisco UCS Power Tools	1.0.0	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1

			.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest
	Cisco UCS Integration Pack	1.0	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574013&release=1.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest
	Cisco Nexus 1000V	1.0	http://software.cisco.com/download/release.html?mdfid=284786025&softwareid=282088129&release=5.2(1)SM1(5.1)&relind=AVAILABLE&rellifecycle=&reltype=latest&i=rm
	Cisco UCS SCVMM Extension	1.0	http://developer.cisco.com/web/unifiedcomputing/systemcenter/vmm
	EMC PowerPath	5.7	EMC integration within Windows operating system
	EMC Storage Integrator (ESI)	2.1.812.5137	EMC Storage Integrator with EMC PowerShell
	EMC Management Pack	2.1.812.5137	Systems Center Operations Manager Management Pack
	EMC SMI-S Provider	4.5.1	Provider for Systems Center Virtual Machine Manager Integration.
	EMC Unisphere Host Agent	1.2.25.1.0163	Automated host registration with VNX
VM Software	Windows Server Datacenter Edition	2012	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/6/D/A/6DAB58BA-F939-451D-9101-7DE07DC09C03/9200.16384.WIN8_RTM.120725-1247_X64FRE_SERVER_EVAL_EN-US-HRM_SSS_X64FREE_EN-US_DV5.ISO
	Windows Server Datacenter Edition	2008 R2 SP1	Evaluation software – can be upgraded. http://www.microsoft.com/en-us/download/details.aspx?id=11093
	MS SQL Server (2 VMs in HA cluster)	2012 SP1	Evaluation software – can be upgraded http://download.microsoft.com/download/3/B/D/3BD9DD65-D3E3-43C3-BB50-0ED850A82AD5/SQLServer2012SP1-FullSlipstream-ENU-x64.iso
	Operations Manager Management Server	2012 SP1	Evaluation software – can be upgraded http://care.dlservice.microsoft.com/dl/download/0/3/F/03F1B876-E7D7-45BE-8B0B-0BDBD02DD800/SC2012_SP1_SCOM_EN.exe
	Operations Manager Supplemental Management Server	2012 SP1	Same as above

	Operations Manager Reporting Server	2012 SP1	Same as above.
	Virtual Machine Manager (2 VMs in HA configuration)	2012 SP1	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/4/8/5/485D6D85-5811-4E7E-83F5-84F9492D3234/SC2012_SP1_SCVMM.exe
	Orchestrator Management and Action Server	2012 SP1	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/9/9/4/99473D48-B8E2-453D-9B34-33FEA42038F7/SC2012_SP1_SCO.exe
	Orchestrator Supplemental Action Server	2012 SP1	Same as above.
	Service Manager Management Server	2012 SP1	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/B/F/5/BF5B6A61-D12C-41F3-B220-6A127E24C57F/SC2012_SP1_SCSM.exe
	Service Manager Supplemental Management Server	2012 SP1	Same as above.
	Service Manager Data Warehouse	2012 SP1	Same as above.
	Service Manager Self-Service Portal	2012 SP1	Same as above.
	App Controller	2012 SP1	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/F/9/1/F916020F-CCFF-427C-BF88-30318B72582F/SC2012_SP1_SCAC.exe
	Windows Deployment Server	2012	Optional: Enabled role within Windows Server 2012
	Windows Assessment and Deployment Kit (ADK) for Windows	1.0	http://download.microsoft.com/download/9/9/F/99F5E440-5EB5-4952-9935-B99662C3DF70/adk/adksetup.exe
	System Center Cloud Services Process Pack	2012	http://download.microsoft.com/download/2/A/4/2A495A01-6016-4058-BC41-CD07FE4D8C0A/System_Center_Cloud_Services_Process_Pack.zip

	System Center 2012 SP1 Integration Packs	2012 SP1	http://download.microsoft.com/download/1/6/5/16536A3A-DD03-4FE8-AD32-6DDA091FDC03/System_Center_2012_SP1_Integration_Packs.exe
	System Center 2012 Operations Manager management packs	2012	http://download.microsoft.com/download/f/7/b/f7b960c9-7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.Library.mp http://download.microsoft.com/download/f/7/b/f7b960c9-7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.2008.Discovery.mp http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.CommonLibrary.mp http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2003.mp http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2008.mp http://download.microsoft.com/download/0/7/7/07714012-3B7C-4691-9F2B-7ADE4188E552/Microsoft.SQLServer.Library.mp
	SQL Server 2012 Analysis Management Objects	2012	http://download.microsoft.com/download/4/B/1/4B1E9B0E-A4F3-4715-B417-31C82302A70A/ENU/x64/SQL_AS_AMO.msi
	SQL Server 2008 R2 SP1 Analysis Management Objects	2008	http://download.microsoft.com/download/9/1/3/9138773A-505D-43E2-AC08-9A77E1E0490B/1033/IA64/SQLSERVER2008_ASAMO10.msi
	Microsoft Report Viewer 2010 SP1	2010	http://download.microsoft.com/download/5/B/9/5B95F704-F7E3-440D-8C68-A88635EA4F87/ReportViewer.exe
	Microsoft Report Viewer 2008 SP1	2008 SP1	http://download.microsoft.com/download/0/4/F/04F99ADD-9E02-4C40-838E-76A95BCEFB8B/ReportViewer.exe
	SQL Server 2012 SP1 Native Client	2012	http://download.microsoft.com/download/4/B/1/4B1E9B0E-A4F3-4715-B417-31C82302A70A/ENU/x64/sqlncli.msi
	Microsoft SharePoint Foundation 2010	2010	http://download.microsoft.com/download/3/5/C/35C62B58-0C29-4A8F-BC6B-D28CD1A6EEDD/SharePointFoundation.exe

	Microsoft SharePoint Foundation 2010 SP1	2010 SP1	http://download.microsoft.com/download/7/0/0/7002DFA1-831C-414A-AE71-A5D18BEF1E32/sharepointfoundation2010sp1-kb2460058-x64-fullfile-en-us.exe
	Silverlight		http://download.microsoft.com/download/5/A/C/5AC56802-B26B-4876-8872-7303C8F27072/20125.00/runtime/Silverlight_x64.exe
Miscellaneous	Java	7.0 or later	http://java.com/en/download/ie_manual.jsp?locale=en
	PuTTy	0.62	http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
	PL-2303 USB-to-Serial driver	1.7.0	https://s3.amazonaws.com/plugable/bin/PL2303_Prolific_DriverInstaller_v1.7.0.zip

2.3 Configuration Guidelines

This document provides details for configuring a fully redundant, highly-available configuration. As such, references are made as to which component is being configured with each step whether that be A or B. For example, Storage Processor A (SP A) and Storage Processor B (SP B), are used to identify the two EMC storage controllers that are provisioned with this document while Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are configured likewise. Additionally, this document details steps for provisioning multiple UCS hosts and these are identified sequentially, F3-Infra01 and F3-Infra02, and so on. Finally, when indicating that the reader should include information pertinent to their environment in a given step, this is indicated with the inclusion of <*italicized text*> as part of the command structure. See the example below for the vlan create command:

controller A> vlan create

Usage:

vlan create [-g {on|off}] <*ifname*> <*vlanid_list*>

vlan add <*ifname*> <*vlanid_list*>

vlan delete -q <*ifname*> [<*vlanid_list*>]

vlan modify -g {on|off} <*ifname*>

vlan stat <*ifname*> [<*vlanid_list*>]

Example:

controller A> vlan create vif0 177

The Cisco UCS PowerTool allows configuration and modification of the UCS environment by using Microsoft PowerShell. The same conventions for entering parameters shown above are followed for entering commands, parameters, and variables within PowerShell. One thing to note with UCS PowerTool is that many of its parameters are case sensitive, whereas parameters in PowerShell are not case sensitive. For example, a parameter value of 'enabled' in PowerShell can be represented as either 'enabled' or 'Enabled' (without the single quotes). With the UCS PowerTool cmdlets, 'enabled' is different from 'Enabled'.

This document is intended to allow the reader to fully configure the customer environment. In order to do so, there are various steps which will require you to insert your own naming conventions, IP address and VLAN schemes as well as record appropriate WWPN, WWNN, or MAC addresses. The following table details the list of VLANs necessary for deployment as outlined in this guide. Note that in this document the VMaccess VLAN is used for virtual machine access. The Mgmt VLAN is used for

management interfaces of the Hyper-V hosts. A Layer-3 route must exist between the Mgmt and VMaccess VLANs.

Table 3 VLAN Names and IDs Used in this Document

VLAN Name	VLAN Purpose	VLAN ID
Default	VLAN to which untagged frames are assigned	1
VMaccess	VM access	10
LiveMigration	Hyper-V Live Migration	11
CSV	Cluster Shared Volume	12
ClusComm	VM guest cluster communication	13
	Unused	14
VEM	Virtual Ethernet Module for Nexus 1000V	15
SMB-A	SMB traffic on Fabric A	16
SMB-B	SMB traffic on Fabric B	17
iSCSI-A	iSCSI traffic on Fabric A	18
iSCSI-B	iSCSI traffic on Fabric B	19
Mgmt	Host management interface	177

Note: This configuration can be configured with iSCSI shared storage access for the virtual machines, with the option to use SMB 3.0. Both SMB 3.0 and iSCSI traverse directly from the fabric interconnect to the VNX.

2.4 Configuration Workstation

It is recommended to have a Windows 8 or Windows Server 2012 workstation configured with certain pre-requisite software and joined to the same domain as the Hyper-V servers will be joined. Using a properly configured workstation makes the job of installing the solution easier. Here is the recommendation for software to be installed on the workstation.

- Windows 8 workstation
  - Install .NET Framework 3.5 by issuing the following command from an elevated command prompt: `Enable-WindowsOptionalFeature -Online -FeatureName NetFx3 -Source D:\sources\sxs`. This assumes the drive D: is the location of your Windows distribution media.
  - Install the Remote Server Administration Tools. This is found at http://www.microsoft.com/en-us/download/details.aspx?id=28972. This is available in both a 32-bit and 64-bit distribution. Ensure you select the copy that matches your Windows 8 installation.
  - After installing the Remote Server Administration Tools, install specific management tools.
    - Hyper-V Management Tools – issue the following command from an elevated command prompt: `dism /online /enable-feature /all /featurename:Microsoft-Hyper-V-Tools-All`
    - Failover Clustering Tools – issue the following command from an elevated command prompt: `dism /online /enable-feature /featurename:RemoteServerAdministrationTools-Features-Clustering`
- Windows Server 2012 system

    - Install .NET Framework 3.5 by issuing the following command from an elevated command prompt: `Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs`. This assumes the drive D: is the location of your Windows distribution media.
    - Install the Hyper-V Management Tools by issuing this PowerShell cmdlet: `Install-WindowsFeature –Name RSAT-Hyper-V-Tools`
    - Install the Windows Failover Clustering Tools by issuing this PowerShell cmdlet: `Install-WindowsFeature –Name RSAT-Clustering`
- Naviseccli – Navisphere Secure Command Line Interface
- ESI (EMC Storage Integrator) – EMC PowerShell library
- Java 7 – required for running UCS Manager. Installed from the web.
- Cisco UCS PowerTool for UCSM, version 1.0. Installation instructions are found in section on Cisco Integration Components.
- PuTTY – an SSH and Telnet client helpful in initial configuration of the Cisco UCS 6248UP Fabric Interconnects. This program just needs to be copied to the system.
- PL-2303 USB-to-Serial driver – used to connect to the Cisco UCS 6248UP Fabric Interconnects via a serial cable connected to a USB port on the workstation. The download is a .zip file. Extract the executable from the .zip file and load it on the system.

You can download all the software listed in the revision table to this workstation. Some of the software, such as distribution media, can be placed into a file share for access by other systems.

There are several PowerShell scripts contained in Appendix B of this document. These are sample scripts. They have been tested, but they are not warranted against errors. They are provided as is, and no support is assumed. But they assist greatly in getting the Hyper-V implementation configured properly and quickly. Some of the scripts will require editing to reflect customer-specific configurations. It is best to create a file share on the configuration workstation and place all the PowerShell scripts on that file share. Most of the scripts will run from the configuration workstation, but there may be some that have to be run locally on the server being configured. Having them available on a file share makes it easier to access them.

For each of the PowerShell scripts contained in Appendix B, do the following.

- Open Notepad (or Windows PowerShell ISE or your editor of choice)
- Copy the contents of a section in Appendix B
- Paste into Notepad
- Save the file using as the name of the file the name of the section in Appendix B. While saving, ensure to set the “Save as type:” field to “All files (*)”. For example, section Create-UcsHyperVFastTrack.ps1 should be saved as “Create-UcsHyperVFastTrack.ps1”.

2.5 Deployment

This document details the necessary steps to deploy base infrastructure components as well as provisioning Microsoft Private Cloud as the foundation for virtualized workloads. At the end of these deployment steps, you will be prepared to provision your applications on top of a Microsoft Private Cloud virtualized infrastructure. The outlined procedure includes:

- Initial EMC VNX array configuration
- Initial Cisco UCS configuration
- Initial Cisco Nexus configuration

- Creation of necessary VLANs for management, basic functionality, and specific to the Microsoft virtualized infrastructure
- Creation of necessary vPCs to provide HA among devices
- Creation of necessary service profile pools: WWPN, world-wide node name (WWNN), MAC, server, and so forth
- Creation of necessary service profile policies: adapter, boot, and so forth
- Creation of two service profile templates from the created pools and policies: one each for fabric A and B
- Provisioning of two servers from the created service profiles in preparation for OS installation
- Initial configuration of the infrastructure components residing on the EMC Controller
- Deployment of Microsoft Hyper-V
- Deployment of Microsoft System Center
- Deployment of the Cisco Plug-ins
- Deployment of the EMC Plug-ins

The Microsoft Private Cloud Solution validated with the Cisco and EMC architecture is flexible; therefore, the exact configuration detailed in this section might vary for customer implementations depending on specific requirements. Although customer implementations might deviate from the information that follows, the best practices, features, and configurations listed in this section should still be used as a reference for building a customized Cisco and EMC with Microsoft Private Cloud solution.

2.6 Cabling Information

The following information is provided as a reference for cabling the physical equipment in a Cisco and EMC environment. The tables include both local and remote device and port locations in order to simplify cabling requirements.

The tables in this section contain details for the prescribed and supported configuration of the EMC VNX5500. This configuration leverages 10 GE adapters for iSCSI data access by the virtual machines as well as the native 8Gb FC target ports for the host UCS servers.

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

Be sure to follow the cable directions in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned.

It is possible to order an EMC VNX5500 system in a different configuration from what is described in the tables in this section. Before starting, be sure the configuration matches what is described in the tables and diagrams in this section.

Note: Fibre Channel connections to the EMC VNX5500 are assumed to be connected to the first and second onboard IO ports. The onboard ports used for these connections are numbered 2 -5.

Table 4 Cisco Nexus 5548 A Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Cisco Nexus 5548 B	Eth 1/1
Eth 1/2	10 GE	Cisco Nexus 5548 B	Eth 1/2

Eth 1/17	10 GE	Cisco 6248 A	Eth 1/17
Eth 1/18	10 GE	Cisco 6248 B	Eth 1/17
Eth 1/29	10 GE	EMC SPA	A2
Eth 1/30	10 GE	EMC SPB	B2
FC 1/31	FC	Cisco 6248 A	FC 1/31
FC 1/32	FC	Cisco 6248 A	FC 1/32

Table 5 Cisco Nexus B Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Cisco Nexus 5548 A	Eth 1/1
Eth 1/2	10 GE	Cisco Nexus 5548 A	Eth 1/2
Eth 1/17	10 GE	Cisco 6248 B	Eth 1/18
Eth 1/18	10 GE	Cisco 6248 A	Eth 1/18
Eth 1/29	10 GE	EMC SPA	A3
Eth 1/30	10 GE	EMC SPB	B3
FC 1/31	FC	Cisco 6248 B	FC 1/31
FC 1/32	FC	Cisco 6248 B	FC 1/32

Table 6 Cisco 6248 Fabric Interconnect A Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Chassis 1 FEX A	Port 1
Eth 1/2	10 GE	Chassis 1 FEX B	Port 1
Eth 1/17	10 GE	Cisco 5548 A	Eth 1/17
Eth 1/18	10 GE	Cisco 5548 B	Eth 1/17
Eth 1/23 (optional)	10 GE	EMC SMB-A (server_2)	Fxg-1-0
Eth 1/24 (optional)	10 GE	EMC SMB-B (server_2)	Fxg-1-0
Eth 1/25	10 GE	EMC iSCSI A0	Slot A1, Port0
Eth 1/26	10 GE	EMC iSCSI B0	Slot B1, Port0
FC 1/31	FC	Cisco 5548 A	FC 1/31
FC 1/32	FC	Cisco 5548 A	FC 1/32

Table 7 Cisco 6248 Fabric Interconnect B Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Chassis 1 FEX A	Port 2
Eth 1/2	10 GE	Chassis 1 FEX B	Port 2

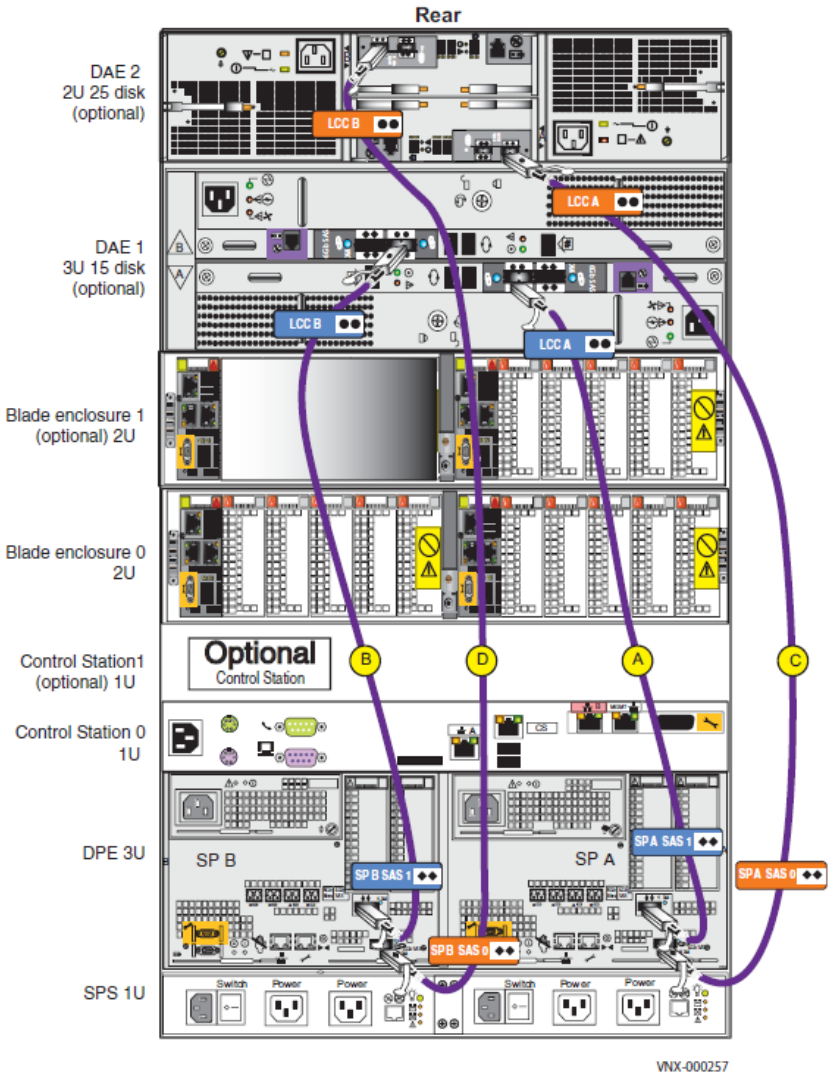
Eth 1/17	10 GE	Cisco 5548 B	Eth 1/18
Eth 1/18	10 GE	Cisco 5548 A	Eth 1/18
Eth 1/23 (optional)	10 GE	EMC SMB-A (server_2)	Fxg-1-1
Eth 1/24 (optional)	10 GE	EMC SMB-B (server_2)	Fxg-1-1
Eth 1/25	10 GE	EMC iSCSI A1	Slot A1, Port1
Eth 1/26	10 GE	EMC iSCSI B1	Slot B1, Port1
FC 1/31	FC	Cisco 5548 B	FC 1/31
FC 1/32	FC	Cisco 5548 B	FC 1/32

3 EMC VNX5500 Deployment: Part 1

Initial configuration and implementation of an EMC VNX5500 is covered in detail from the EMC documentation library. This is accessible at https://mydocs.emc.com/VNX/ and select Install VNX, using the VNX5500 series as the installation type. Installation documentation covers all areas from unpacking VNX storage components, installing in rack, provisioning power requirements and physical cabling.

When physically installed, the VNX should include the Disk Processing Enclosure (DPE) and two additional Disk Array Enclosures (DAEs), cabled as shown in Figure 3.

Figure 3 Cabling Diagram for VNX5500 with 2 DAE



To complete software setup of the VNX array, it will be necessary to configure system connectivity including the creation of an Administrative user for the VNX array. The following worksheets (also found in the Installation documentation) list all required information, and can be used to facilitate the initial installation.

3.1 VNX Worksheets

With your network administrator, determine the IP addresses and network parameters you plan to use with the storage system, and record the information on the following worksheet. You must have this information to set up and initialize the system. The VNX5500 array is managed through a dedicated LAN port on the Control Station and each storage processor. These ports must share a subnet with the host you use to initialize the system. After initialization, any host on the same network and with a supported browser can manage the system through the management ports. This information can be recorded in the following table.

Table 8 IPV4 Management Port Information

	IP Address	Subnet Mask	Gateway
CSO (optional)			
SP A			
SP B			

Note: Do not use 128.221.1.248 through 128.221.1.255, 192.168.1.1, or 192.168.1.2 for an IPv4 IP Address.

While it is possible to implement IPv6 settings for the VNX array, the Fast Track implementation does not require it, and it is not implemented.

It is possible to more fully configure management IP addresses for the VNX5500 array. The following table lists some of the addresses you can optionally configure.

Table 9 Optional Control Station LAN Settings

Field	Value	Comments
CSO Primary hostname		
DNS domain		
Primary DNS Server		
Secondary DNS Server		
NTP Server		
Time Zone		

An administrative user account is required to be set for the array, and this account can be later utilized for executing NaviSecCLI commands, as well as for the ESI PowerShell environment used to provision LUNs from storage pools, and map those LUNs to hosts. Information required is outlined in the following table.

Table 10 Login Information for the Storage System Administrator

Field	Description	Value
Username	nasadmin (default)	Passwords are default and should be changed during installation or from within Unisphere.
Password	nasadmin (default)	

Within the Fast Track environment, iSCSI connectivity is provided to Virtual Machine clusters, specifically for SQL Server instances. Two 10 Gbps iSCSI I/O modules are implemented within the VNX5500 array, where each I/O module implements two physical connections. The following worksheet allows you to record the required configuration details.

Table 11 IPv4 Addresses for iSCSI Targets

SP, slot and port	IP address	Subnet Mask	Gateway
SPA, slot 1, port0			
SPA, slot 1, port1			
SPB, slot 1, port0			
SPB, slot 1, port1			

The VNX 5500 can optionally include one blade enclosure with 2 Blades (a.k.a. Datamovers) to support file-based protocol access, specifically SMB 3.0. The Blades will be configured in a Primary/Standby configuration where Blade2 will be used for SMB 3.0 access with Blade3 used for redundancy. In the event of a failure to Blade2, the SMB services will fail over and be provided from Blade3. The base configuration will include 2 x 10Gb connections to both Blade2 and Blade3 for performance and redundancy.

The VNX SMB physical ports can be configured with IP addresses either individually, or combined as a single IP address via "Link Aggregation." Windows Server 2012 and Windows 8, with SMB 3.0 support, have a feature called Multichannel. Multichannel automatically combines multiple SMB connections for increased throughput and fault tolerance. The base VNX configuration will utilize SMB 3.0 Multichannel to provide enhanced performance and redundancy across the two active "interfaces." Therefore two VNX interfaces will be created to represent the two active physical ports. The two IP addresses representing the interfaces can be documented below.

Should non-Windows 2012/Windows 8 operating systems, which do not support SMB 3.0, be planned for use against VNX SMB based storage, link aggregation should be used to provide fault tolerance and increased throughput for clients that only support SMB 2.1 or earlier versions of the protocol.

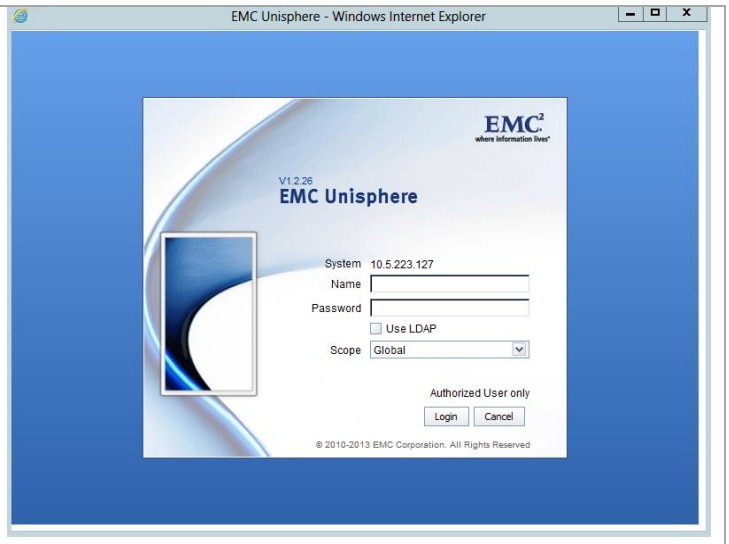
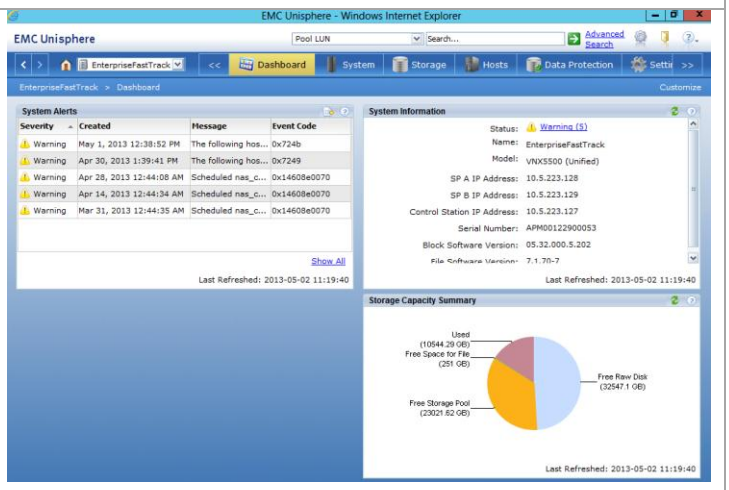
The following worksheet allows you to record the required configuration details.

Table 12 IPv4 Addresses for SMB 3.0 (optional)

Field	IP Address	Subnet Mask	Gateway
Server_2/3 Slot 1, Port0			
Server_2/3 Slot 1, Port1			

It is also necessary at this time to install the NaviSecCli command line interface from a supported Windows client environment. The client should have network access to the VNX5500 array for both HTTP/HTTPS access and for remote NaviSecCli command execution.

Installation media for the NaviSecCli utility, as well as ESI, are available by download at http://support.emc.com. The current version of the media should always be utilized. Installation of the utility is implemented through the typical application installation process for Windows-based systems.

After array installation, it will also be possible to connect to the VNX5500 array via the Unisphere graphical user interface at the IP address assigned to either SP-A or SP-B, or the control station in the event that a Unified version of the VNX is being implemented.	
After entering appropriate login credentials, the Unisphere home page will be presented, providing an overview of the VNX5500 storage array. Summary alerts and errors will be visible as well as full management capabilities for all array features.	

The following configuration details assume the VNX5500 array as defined, will be configured with 75 x SAS drives across the DPE and two DAEs. It is also assumed that the array has been configured with IP address assignments to the Control Station and both SP-A and SP-B as previously indicated in Part 1. It is also necessary to have appropriately configured a Windows-based management system with network connectivity to the VNX array that has an appropriate version of the NaviCLI software installed.

The following configuration also assumes that the array has been configured with:

DPE – BUS 0 / Enclosure 0	25 drives
DAE – BUS 0 / Enclosure 1	25 drives
DAE – BUS 1 / Enclosure 0	25 drives

In the event that the physical configuration of the system differs in regards to the DAE placements, then modifications to the Bus Enclosure naming used subsequently will need to be appropriately altered.

Creation of Storage Pools

A number of storage pools are utilized in the Private Cloud configuration. LUNs are subsequently created within the pools to satisfy the requirements of the Management Infrastructure, the Virtual Machines, and the applications and services which run within the environment.

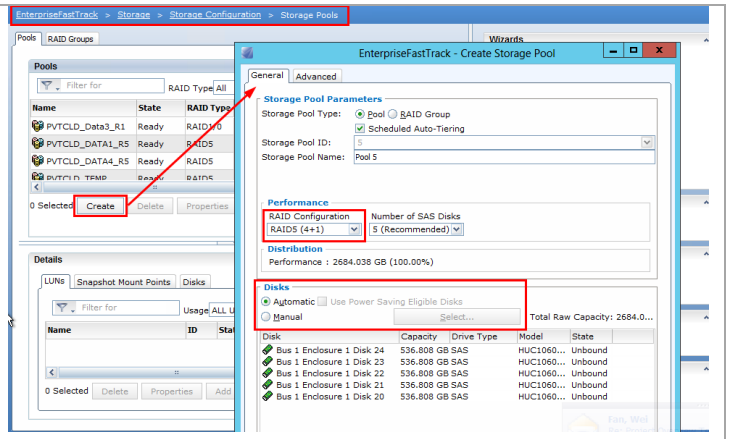
When newly created, a VNX array will not contain usable Storage Pools, from which LUNs can be created and used by the hosts connected to the system. As much of the configuration of the required LUNs and masking operation through EMC Storage Integrator require named pools, the following commands, when run from PowerShell, will create the required Storage Pools.

The first command defines the IP address for the array, and should be modified as necessary for the implementation.

```
#Enter VNX management IP address in the next line
$VNX="10.5.223.128"
naviseccli -h $VNX storagepool -create -disks 0_0_4 0_0_5 0_0_6 0_0_7 0_0_8 0_0_9 0_0_10 0_0_11 0_0_12 0_0_13 0_0_14 0_0_15 0_0_16 0_0_17 0_0_18 0_0_19 0_0_20 0_0_21 0_0_22 0_0_23 -rtype r_5 -name PVTCLD_DATA1_R5
naviseccli -h $VNX storagepool -create -disks 1_0_0 1_0_1 1_0_2 1_0_3 1_0_4 1_0_5 1_0_6 1_0_7 1_0_8 1_0_9 1_0_10 1_0_11 1_0_12 1_0_13 1_0_14 1_0_15 1_0_16 1_0_17 1_0_18 1_0_19 1_0_20 1_0_21 1_0_22 1_0_23 1_0_24 -rtype r_5 -name PVTCLD_DATA2_R5
naviseccli -h $VNX storagepool -create -disks 0_1_0 0_1_1 0_1_2 0_1_3 0_1_4 0_1_5 0_1_6 0_1_7 -rtype r_10 -name PVTCLD_Data3_R1
naviseccli -h $VNX storagepool -create -disks 0_1_8 0_1_9 0_1_10 0_1_11 0_1_12 0_1_13 0_1_14 0_1_15 0_1_16 0_1_17 0_1_18 0_1_19 0_1_20 0_1_21 0_1_22 -rtype r_5 -name PVTCLD_DATA4_R5
```

Alternatively, the desired pools can be created from the Unisphere GUI.

From within the S**torage > Storage Configuration > Storage Pools** menu in Unisphere, select **Create**. The RAID configuration, desired number of drives and specific drive locations (by choosing **Manual**) can be selected from the **Create Storage Pool** menu as outlined in the Figure below.

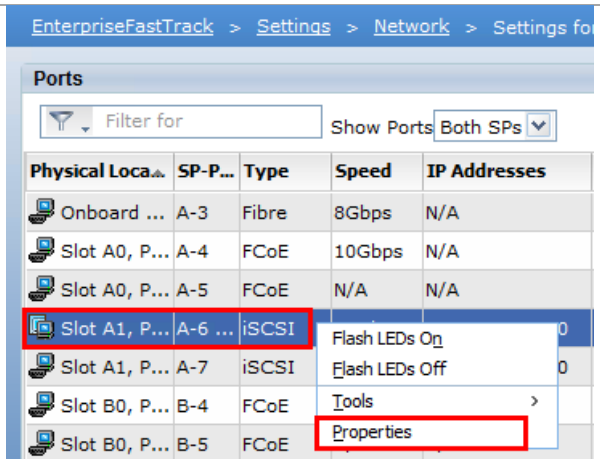
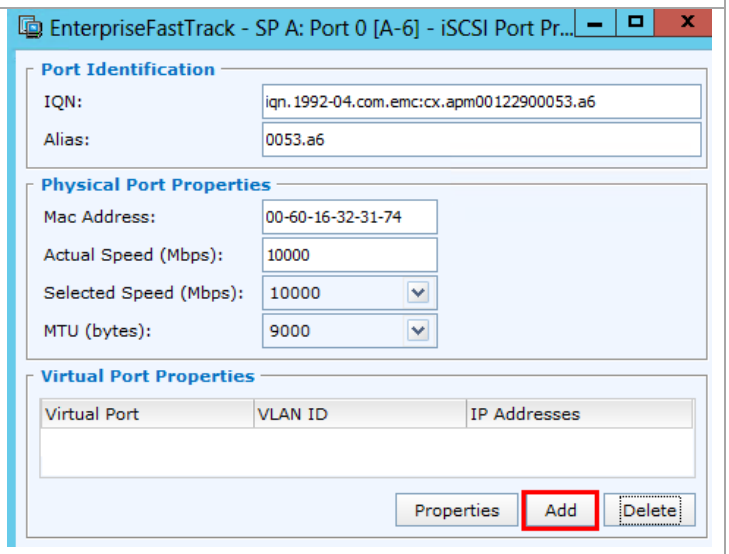


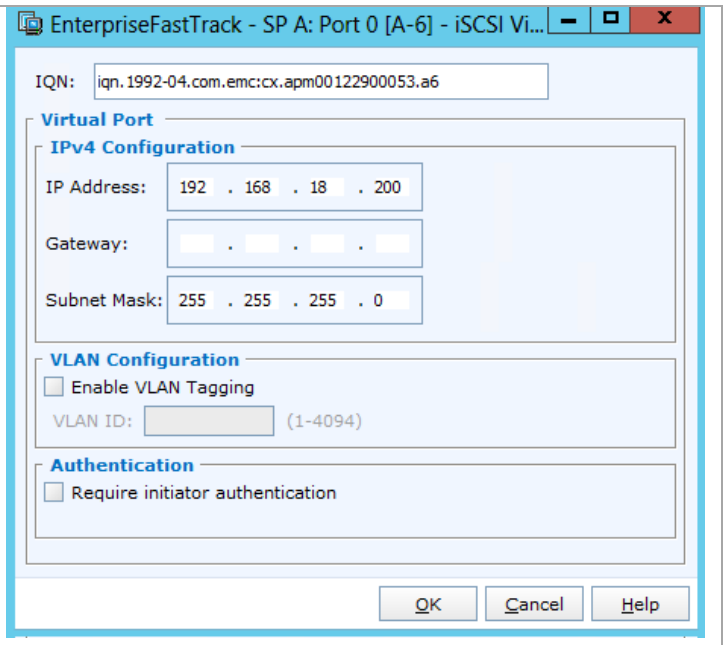
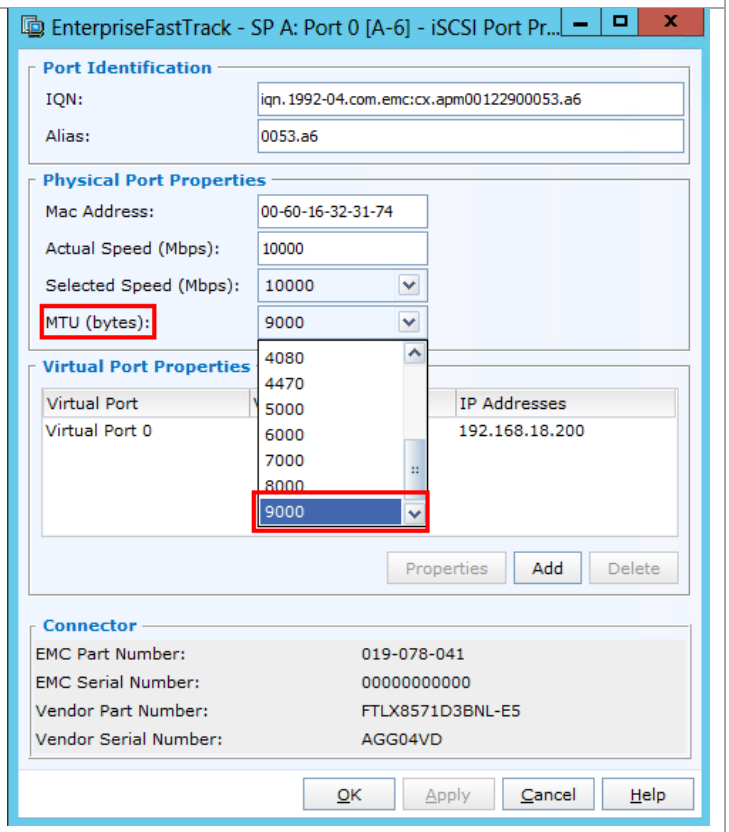
Create Support for Hot Spares and Clone Private LUNs

In the previous step Storage pools were defined on the VNX array based on disks within the chassis. Additional RAID Group based LUNs are required to support hot spares as well as clone private LUNs in the system. As part of the automation of Virtual Machine deployments, SnapView Clones are utilized both through scripting and also through the SMI-S integration of System Center Virtual Machine Manager.

The example PowerShell script found in Appendix B, Create-EMCHyperVSparesClones.ps1, can be used to create the RAID Groups and LUNs that will be used to facilitate the hot spares and clone private LUNs. Ensure that it is modified to reflect the customer environment.

Configure VNX5500 iSCSI Connections

In Unisphere, go to **Settings > Network > Settings for Block** Find the **iSCSI** connection in the **Type** column. Right click on the A Port 0 connection and select **Properties**	
From the properties window select **Add**	

Enter the appropriate IP and subnet information for the iSCSI connection and select **OK.** Select **Yes** at the following confirmation screen.	
Ensure the MTU size is set to **9000** Select **Apply** to change the MTU and select **Yes** at the following confirmation screen. Select **OK** to exit the properties window. Repeat the iSCSI configuration procedure for the three remaining connections.	

4 Cisco Nexus 5548 Deployment: Part 1

The following section provides a detailed procedure for configuring the Cisco Nexus 5548 switches for use in a Cisco and EMC with Microsoft Private Cloud environment. Follow these steps precisely because failure to do so could result in an improper configuration.

Note: You will need to have the following information identified before you begin.

Table 13 Nexus Management Information

Item	Value
Nexus A Switch name	
Nexus B Switch name	
Nexus A mgmt0 IP / netmask	
Nexus B mgmt0 IP / netmask	
Mgmt 0 gateway	
NTP Server IP	
vPC domain ID	

4.1 Set Up Initial Cisco Nexus 5548 Switch

These steps provide details for the initial Cisco Nexus 5548 Switch setup.

Cisco Nexus 5548 A

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.

1. Enter **`yes`** to enforce secure password standards.
2. Enter the password for the admin user.
3. Enter the password a second time to commit the password.
4. Enter **`yes`** to enter the basic configuration dialog.
5. Create another login account (yes/no) [n]: **Enter**.
6. Configure read-only SNMP community string (yes/no) [n]: **Enter**.
7. Configure read-write SNMP community string (yes/no) [n]: **Enter**.
8. Enter the switch name: <***`Nexus A Switch name`***> **Enter**.
9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: **Enter**.
10. Mgmt0 IPv4 address: <***`Nexus A mgmt0 IP`***> **Enter**.
11. Mgmt0 IPv4 netmask: <***`Nexus A mgmt0 netmask`***> **Enter**.
12. Configure the default gateway? (yes/no) [y]: **Enter**.
13. IPv4 address of the default gateway: <***`Nexus A mgmt0 gateway`***> **Enter**.
14. Enable the telnet service? (yes/no) [n]: **Enter**.
15. Enable the ssh service? (yes/no) [y]: **Enter**.
16. Type of ssh key you would like to generate (dsa/rsa):**`rsa`**.
17. Number of key bits <768–2048>:**`1024`** **Enter**.
18. Configure the ntp server? (yes/no) [y]: **Enter**.

19. NTP server IPv4 address: <***NTP Server IP***> **Enter**.
20. Enter basic FC configurations (yes/no) [n]: **Enter**.
21. Would you like to edit the configuration? (yes/no) [n]: **Enter**.
22. Be sure to review the configuration summary before enabling it.
23. Use this configuration and save it? (yes/no) [y]: **Enter**.
24. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
25. Log in as user admin with the password previously entered.

Cisco Nexus 5548 B

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.

1. Enter **yes** to enforce secure password standards.
2. Enter the password for the admin user.
3. Enter the password a second time to commit the password.
4. Enter **yes** to enter the basic configuration dialog.
5. Create another login account (yes/no) [n]: **Enter**.
6. Configure read-only SNMP community string (yes/no) [n]: **Enter**.
7. Configure read-write SNMP community string (yes/no) [n]: **Enter**.
8. Enter the switch name: <***Nexus B Switch name***> **Enter**.
9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: **Enter**.
10. Mgmt0 IPv4 address: <***Nexus B mgmt0 IP***> **Enter**.
11. Mgmt0 IPv4 netmask: <***Nexus B mgmt0 netmask***> **Enter**.
12. Configure the default gateway? (yes/no) [y]: **Enter**.
13. IPv4 address of the default gateway: <***Nexus B mgmt0 gateway***> **Enter**.
14. Enable the telnet service? (yes/no) [n]: **Enter**.
15. Enable the ssh service? (yes/no) [y]: **Enter**.
16. Type of ssh key you would like to generate (dsa/rsa):**rsa**
17. Number of key bits <768–2048>**:1024 Enter**.
18. Configure the ntp server? (yes/no) [y]: **Enter**.
19. NTP server IPv4 address: <***NTP Server IP***> **Enter**.
20. Enter basic FC configurations (yes/no) [n]: **Enter**.
21. Would you like to edit the configuration? (yes/no) [n]: **Enter**.
22. Be sure to review the configuration summary before enabling it.
23. Use this configuration and save it? (yes/no) [y]: **Enter**.
24. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
25. Log in as user admin with the password previously entered.

Enable Appropriate Cisco Nexus Features

These steps provide details for enabling the appropriate Cisco Nexus features.

For Nexus A and Nexus B

1. Type **config t** to enter the global configuration mode
2. Type **feature lacp**
3. Type **feature fcoe**
4. Type **feature npiv**
5. Type **feature vpc**
6. Type **feature fport-channel-trunk**
7. Type **feature interface-vlan**
8. Type **spanning-tree port type network default** to ensure that, by default, the ports are considered as network ports in regards to spanning-tree.
9. Type **spanning-tree port type edge bpduguard default** to enable bpduguard on all edge ports by default.
10. Type **spanning-tree port type edge bpdufilter default** to enable bpdufilter on all edge ports by default.
11. Type **copy run start**.

Configure Fibre Channel Ports

These steps provide details for configuring the necessary FC ports on the Nexus switches.

Nexus A and Nexus B

1. Type **slot 1**.
2. Type **port 29-32 type fc**.
3. Type **copy run start**.
4. Type **reload**.

The Nexus switch will reboot. This will take several minutes.

Create Necessary VLANs

These steps provide details for creating the necessary VLANs. Note that the SMB (or iSCSI) VLANs are not created on the Nexus switches. The SMB (or iSCSI) connections are made directly from the Fabric Interconnects to the EMC VNX array. The Nexus switches do not see this SMB (or iSCSI)-related traffic.

Nexus A and Nexus B

Following the switch reloads, log in with user admin and the password previously entered.

5. Type **config**.
6. Type **vlan** <***MGMT VLAN ID***>.
7. Type **name Mgmt**.
8. Type **exit**.
9. Type **vlan** <***CSV VLAN ID***>.
10. Type **name CSV**.
11. Type **exit**.
12. Type **vlan** <***Live Migration VLAN ID***>.
13. Type **name LiveMigration**.
14. Type **exit.**
15. Type **vlan** <***ClusComm VLAN ID***>.

16. Type **name ClusComm**.
17. Type **exit**.
18. Type **vlan** <***VMaccess VLAN ID***>.
19. Type **name VMaccess**.
20. Type **exit.**
21. Type **vlan** <***VEM VLAN ID***>.
22. Type **name VEM**.
23. Type **exit.**
24. Type **vlan** <***SMB-A VLAN ID***>.
25. Type **name SMB-A**.
26. Type **exit.**
27. Type **vlan** <***SMB-B VLAN ID***>.
28. Type **name SMB-B**.
29. Type **exit.**
30. Type **vlan** <***iSCSI-A VLAN ID***>.
31. Type **name iSCSI-A**.
32. Type **exit.**
33. Type **vlan** <***iSCSI-B VLAN ID***>.
34. Type **name iSCSI-B**.
35. Type **exit.**
36. Type **copy run start**.

Add Individual Port Descriptions for Troubleshooting

These steps provide details for adding individual port descriptions for troubleshooting activity and verification.

Cisco Nexus 5548 A

1. From the global configuration mode, type **interface Eth1/1**.
2. Type **description** <***Nexus B:Eth1/1***>.
3. Type **exit**.
4. Type **interface Eth1/2**.
5. Type **description** <***Nexus B:Eth1/2***>.
6. Type **exit**.
7. Type **interface Eth1/17**.
8. Type **description** <***UCSM A:Eth1/17***>.
9. Type **exit**.
10. Type **interface Eth1/18**.
11. Type **description** <***UCSM B:Eth1/17***>.
12. Type **exit**.
13. Type **copy run start**.

Cisco Nexus 5548 B

1. From the global configuration mode, type **interface Eth1/1**.
2. Type **description** <***Nexus A:Eth1/1***>.
3. Type **exit**.
4. Type **interface Eth1/2**.
5. Type **description** <***Nexus A:Eth1/2***>.
6. Type **exit**.
7. Type **interface Eth1/17**.
8. Type **description** <***UCSM B:Eth1/18***>.
9. Type **exit**.
10. Type **interface Eth1/18**.
11. Type **description** <***UCSM A:Eth1/18***>.
12. Type **exit**.
13. Type **copy run start**.

Create Necessary Port Channels

These steps provide details for creating the necessary Port Channels between devices.

Cisco Nexus 5548 A

1. From the global configuration mode, type **interface Po10**.
2. Type **description vPC Peer-Link**.
3. Type **exit**.
4. Type **interface Eth1/1-2**.
5. Type **channel-group 10 mode active**.
6. Type **no shutdown**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **description** <***PvtCld-UCS-A***>.
10. Type **exit**.
11. Type **interface Eth1/17**.
12. Type **channel-group 201 mode active**.
13. Type **no shutdown**.
14. Type **exit**.
15. Type **interface Po202**.
16. Type **description** <***PvtCld-UCS-B***>.
17. Type **exit**.
18. Type **interface Eth1/18**.
19. Type **channel-group 202 mode active**.
20. Type **no shutdown**.
21. Type **exit**.
22. Type **copy run start**.

Cisco Nexus 5548 B

1. From the global configuration mode, type **interface Po10**.
2. Type **description vPC Peer-Link**.
3. Type **exit**.
4. Type **interface Eth1/1-2**.
5. Type **channel-group 10 mode active**.
6. Type **no shutdown**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **description** <***PvtCld-UCS-B***>.
10. Type **exit**.
11. Type **interface Eth1/17**.
12. Type **channel-group 201 mode active**.
13. Type **no shutdown**.
14. Type **exit**.
15. Type **interface Po202**.
16. Type **description** <***PvtCld-UCS-A***>.
17. Type **exit**.
18. Type **interface Eth1/18**.
19. Type **channel-group 202 mode active**.
20. Type **no shutdown**.
21. Type **exit**.
22. Type **copy run start**.

Add Port Channel Configurations

These steps provide details for adding PortChannel configurations.

Cisco Nexus 5548 A

1. From the global configuration mode, type **interface Po10**.
2. Type **switchport mode trunk**.
3. Type **switchport trunk native vlan** <***Native VLAN ID***>.
4. Type **switchport trunk allowed vlan** <***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID***>.
5. Type **spanning-tree port type network**.
6. Type **no shutdown**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **switchport mode trunk**.
10. Type **switchport trunk native vlan** <***MGMT VLAN ID***>.

11. Type **switchport trunk allowed vlan** < ***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID*** >.
12. Type **spanning-tree port type edge trunk**.
13. Type **no shut**.
14. Type **exit**.
15. Type **interface Po202**.
16. Type **switchport mode trunk**.
17. Type **switchport trunk native vlan** <***MGMT VLAN ID***>.
18. Type **switchport trunk allowed vlan** < ***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID*** >.
19. Type **spanning-tree port type edge trunk**.
20. Type **no shut**.
21. Type **exit**.
22. Type **copy run start**.

Cisco Nexus 5548 B

1. From the global configuration mode, type **interface Po10**.
2. Type **switchport mode trunk**.
3. Type **switchport trunk native vlan** <***Native VLAN ID***>.
4. Type **switchport trunk allowed vlan** < ***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID*** >.
5. Type **spanning-tree port type network**.
6. Type **no shutdown**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **switchport mode trunk**.
10. Type **switchport trunk native vlan** <***MGMT VLAN ID***>.
11. Type **switchport trunk allowed vlan** <***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID*** >.
12. Type **spanning-tree port type edge trunk**.
13. Type **no shut**.
14. Type **exit**.
15. Type **interface Po202**.
16. Type **switchport mode trunk**.
17. Type **switchport trunk native vlan** <***MGMT VLAN ID***>.
18. Type **switchport trunk allowed vlan** <***MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN ID, VMaccess VLAN ID, VEM VLAN ID, SMB-A VLAN ID, SMB-B VLAN ID, iSCSI-A VLAN ID, iSCSI-B VLAN ID*** >.

19. Type **spanning-tree port type edge trunk**.
20. Type **no shut**.
21. Type **exit**.
22. Type **copy run start**.

Configure Virtual Port Channels

These steps provide details for configuring virtual PortChannels (vPCs)

Cisco Nexus 5548 A

1. From the global configuration mode, type **vpc domain** <***Nexus vPC domain ID***>.
2. Type **role priority 10**.
3. Type **peer-keepalive destination** <***Nexus B mgmt0 IP***> **source** <***Nexus A mgmt0 IP***>.
4. Type **exit**.
5. Type **interface Po10**.
6. Type **vpc peer-link**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **vpc 201**.
10. Type **exit**.
11. Type **interface Po202**.
12. Type **vpc 202**.
13. Type **exit**.
14. Type **copy run start**.

Cisco Nexus 5548 B

1. From the global configuration mode, type **vpc domain** <***Nexus vPC domain ID***>.
2. Type **role priority 20**.
3. Type **peer-keepalive destination** <***Nexus A mgmt0 IP***> **source** <***Nexus B mgmt0 IP***>.
4. Type **exit**.
5. Type **interface Po10**.
6. Type **vpc peer-link**.
7. Type **exit**.
8. Type **interface Po201**.
9. Type **vpc 201**.
10. Type **exit**.
11. Type **interface Po202**.
12. Type **vpc 202**.
13. Type **exit**.
14. Type **copy run start**.

Configure Fibre Channel Ports

Nexus A and Nexus B

1. Type **interface fc1/29**
2. Type **switchport trunk mode off**
3. Type **no shutdown**
4. Type **exit**
5. Type **interface fc1/30**
6. Type **switchport trunk mode off**
7. Type **no shutdown**
8. Type **exit**
9. Type **interface fc1/31**
10. Type **switchport trunk mode off**
11. Type **no shutdown**
12. Type **exit**
13. Type **interface fc1/32**
14. Type **switchport trunk mode off**
15. Type **no shutdown**
16. Type **exit**
17. Type **copy run start**

Link into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the private cloud environment. If an existing Cisco Nexus environment is present, Cisco recommends using vPCs to uplink the Cisco Nexus 5548 switches included in the private cloud environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment.

4.2 Configure Cisco Unified Computing System Fabric Interconnects

The following section provides a detailed procedure for configuring the Cisco Unified Computing System for use in a private cloud environment. These steps should be followed precisely because a failure to do so could result in an improper configuration.

Note: You will need to have the following information identified before you begin.

Table 14 Cisco UCS Manager Configuration Information

Item	Value
Node A IPv4 mgmt0 address / netmask	
Node B IPv4 mgmt0 address	
Default gateway address	
Cluster IPv4 address	
DNS address	
Domain name	

Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects

These steps provide details for initial setup of the Cisco UCS 6248 fabric Interconnects

Cisco UCS 6248 A

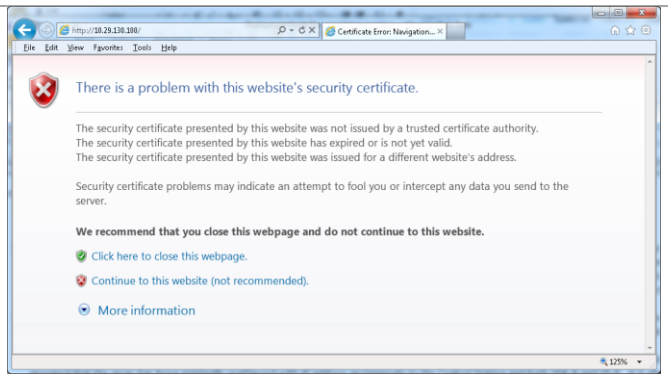
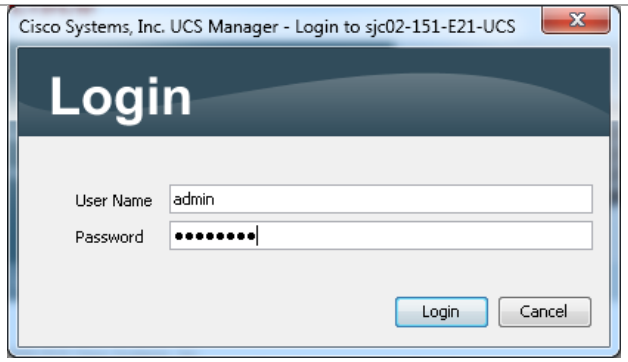
1. Connect to the console port on the first Cisco UCS 6248 fabric interconnect.
2. At the prompt to enter the configuration method, enter **`console`** to continue.
3. If asked to either do a new setup or restore from backup, enter **`setup`** to continue.
4. Enter **`y`** to continue to set up a new fabric interconnect.
5. Enter **`y`** to enforce strong passwords.
6. Enter the password for the admin user.
7. Enter the same password again to confirm the password for the admin user.
8. When asked if this fabric interconnect is part of a cluster, answer **`y`** to continue.
9. Enter **`A`** for the switch fabric.
10. Enter the <***cluster name***> for the system name.
11. Enter the <***Mgmt0 IPv4 address***>.
12. Enter the <***Mgmt0 IPv4 netmask***>.
13. Enter the <***IPv4 address of the default gateway***>.
14. Enter the <***cluster IPv4 address***>.
15. To configure DNS, answer **`y`**.
16. Enter the <***DNS IPv4 address***>.
17. Answer **`y`** to set up the default domain name.
18. Enter the default <***domain name***>.
19. Review the settings that were printed to the console, and if they are correct, answer **`yes`** to save the configuration.
20. Wait for the login prompt to ensure the configuration has been saved.

Cisco UCS 6248 B

1. Connect to the console port on the second Cisco UCS 6248 fabric interconnect.
2. When prompted to enter the configuration method, enter **`console`** to continue.
3. The installer detects the presence of the partner fabric interconnect and adds this fabric interconnect to the cluster. Enter **`y`** to continue the installation.
4. Enter the admin password for the first fabric interconnect.
5. Enter the <***Mgmt0 IPv4 address***>.
6. Answer **`yes`** to save the configuration.
7. Wait for the login prompt to confirm that the configuration has been saved.

Log into Cisco UCS Manager

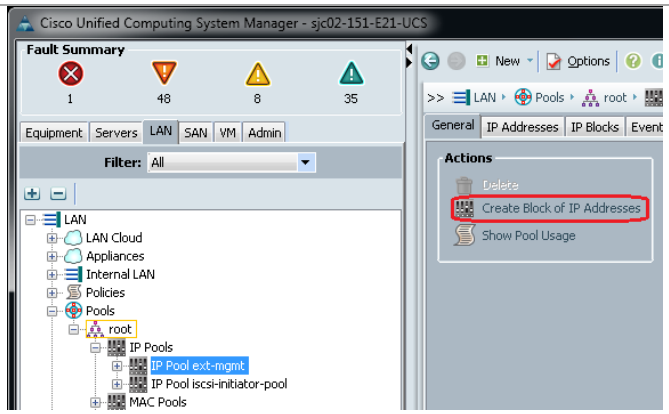
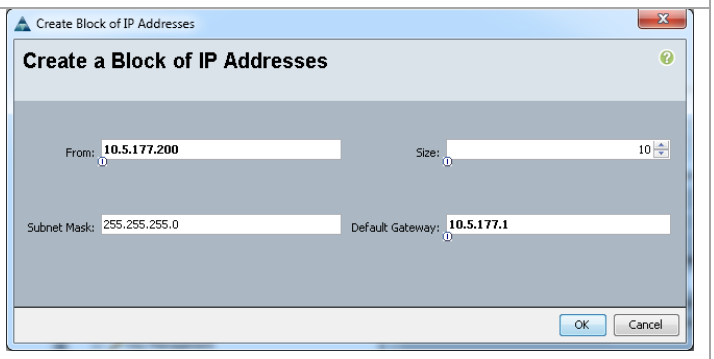
These steps provide details for logging into the Cisco UCS environment.

Open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address. You will see a web page complaining about the website's security certificate. Click **Continue to this website (not recommended)**.	
Select the **Launch** link to download the Cisco UCS Manager software. If prompted to accept security certificates, accept as necessary.	
When prompted, enter admin for the username and enter the administrative password and click Login to log in to the Cisco UCS Manager software.	

Add a Block of IP Addresses for KVM Access

These steps provide details for creating a block of KVM IP addresses for server access in the Cisco UCS environment.

Cisco UCS Manager

Select the **LAN** tab at the top of the left window. Select **Pools > root > IP Pools > IP Pool ext-mgmt**. Select **Create Block of IP Addresses**.	
Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information. Click **OK** to create the IP block. Click **OK** in the message box	

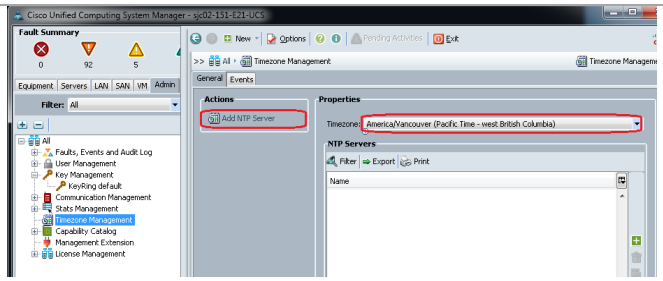
Cisco UCS PowerTool

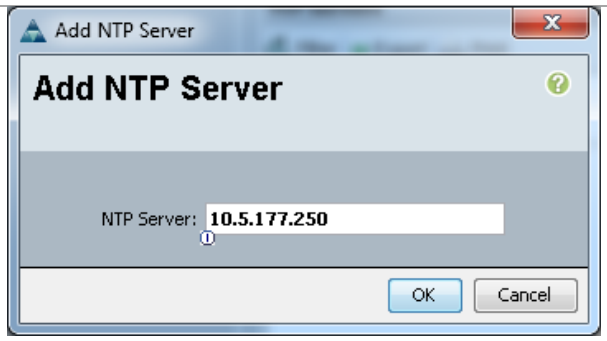
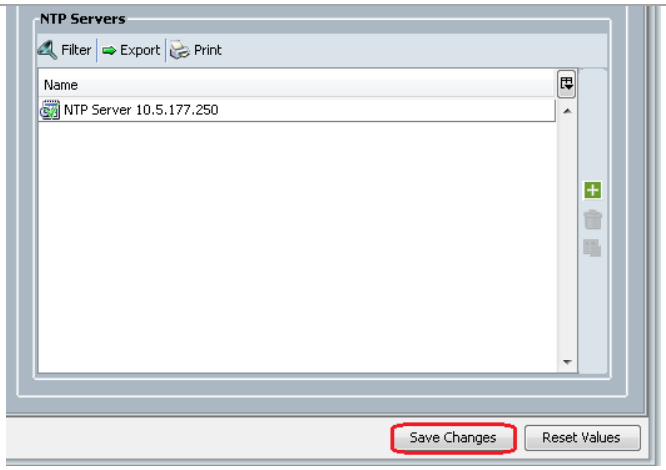
Get-UcsOrg -Level root | Get-UcsIpPool -Name "ext-mgmt" -LimitScope | Add-UcsIpPoolBlock -DefGw “10.5.177.1” -From “10.5.177.200” -To “10.5.177.209”

Synchronize Cisco Unified Computing System to NTP

These steps provide details for synchronizing the Cisco UCS environment to the NTP server.

Cisco UCS Manager

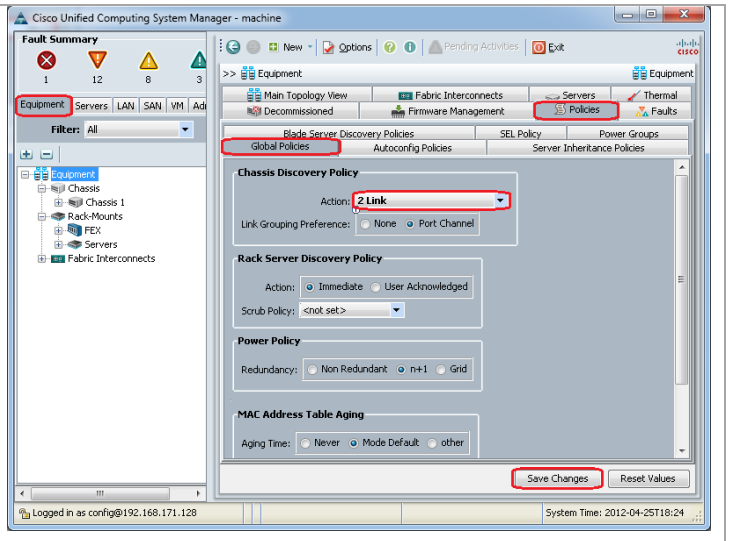
Select the **Admin** tab at the top of the left window. Select **All > Timezone Management**. In the right pane, select the appropriate timezone in the **Timezone** drop-down menu. Click **Add NTP Server**.	

Input the NTP server IP and click **OK**.	
Click **Save Changes** and then **OK**.	

Edit the Chassis Discovery Policy

These steps provide details for modifying the chassis discovery policy as the base architecture includes two uplinks from each fabric extender installed in the Cisco UCS chassis.

Cisco UCS Manager

Navigate to the **Equipment** tab in the left pane. In the right pane, click the **Policies** tab. Under Global Policies, change the Chassis Discovery Policy to **2-link**. Select the **Port Channel** radio button for the Link Grouping Preference. Click **Save Changes** in the bottom right corner.	

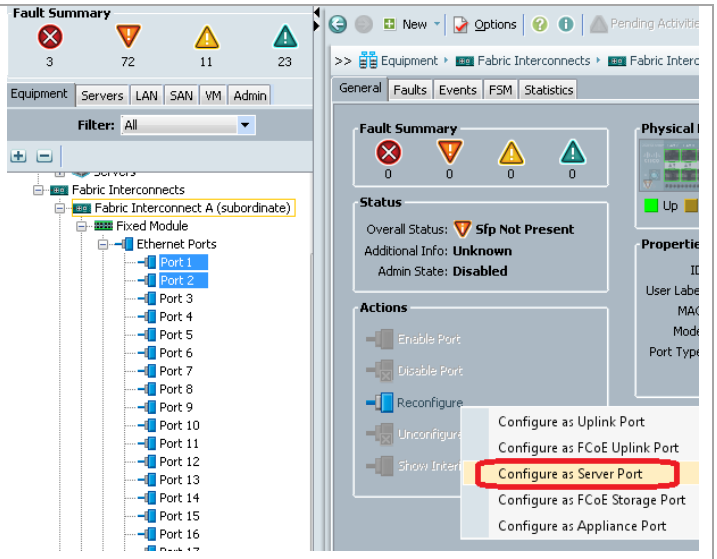
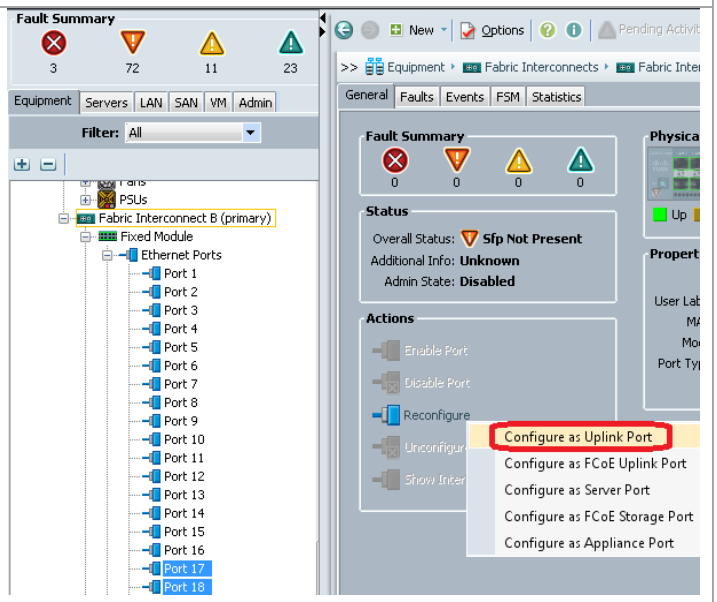
Cisco UCS PowerTool

```
Get-UcsOrg -Level root | Get-UcsChassisDiscoveryPolicy | Set-UcsChassisDiscoveryPolicy -Action "2-Link" -Force
```

Enable Server and Uplink Ports

These steps provide details for enabling Fibre Channel, server and uplinks ports.

Cisco UCS Manager

Select the **Equipment** tab on the top left of the window. Select **Equipment** > **Fabric Interconnects** > **Fabric Interconnect A (primary)** > **Fixed Module**. Expand the **Unconfigured Ethernet Ports** section. Select the ports that are connected to the Cisco UCS chassis (2 per chassis). Click **Reconfigure**, then select **Configure as Server Port** from the drop-down menu. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue. Repeat for Fabric Interconnect B. **Note:**	
Continue working on Fabric Interconnect B. Select ports 17 and 18 that are connected to the Cisco Nexus 5548 switches. Click **Reconfigure**, then select **Configure as Uplink Port** from the drop-down menu. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue. Switch back to working on Fabric Interconnect A. Repeat for Fabric Interconnect A. **Note:** After a port is configured, you can select the port and select the option to Show Interface. This allows you to add a description, if you so desire.	

Cisco UCS PowerTool

Cisco UCS PowerTool can work on both fabrics when setting up server and uplink ports.

```
$var = Get-UcsFabricServerCloud -Id "A"
```

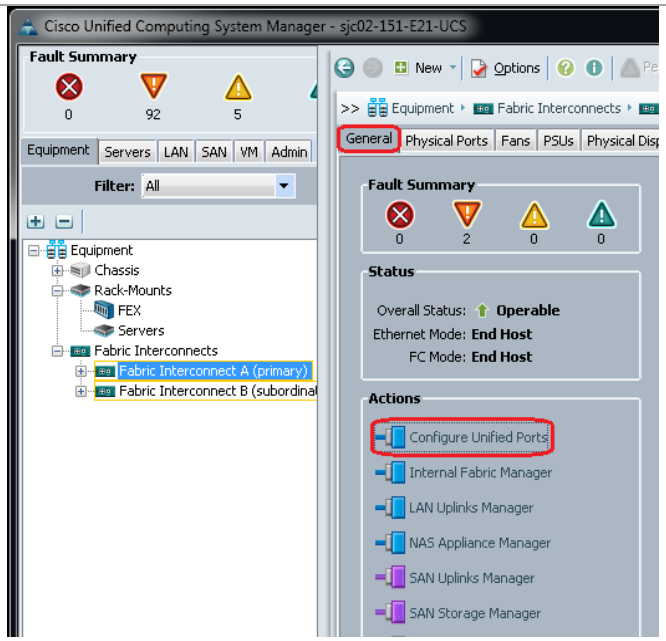
```
$var | Add-UcsServerPort -PortId 1 -SlotId 1 –UsrLbl “Blade Server Port”
$var | Add-UcsServerPort -PortId 2 -SlotId 1 –UsrLbl “Blade Server Port”
$var = Get-UcsFabricLanCloud –Id “A”
$var | Add-UcsUplinkPort -PortId 17 -SlotId 1 –UsrLbl “Uplink Port”
$var | Add-UcsUplinkPort -PortId 18 -SlotId 1 –UsrLbl “Uplink Port”
```

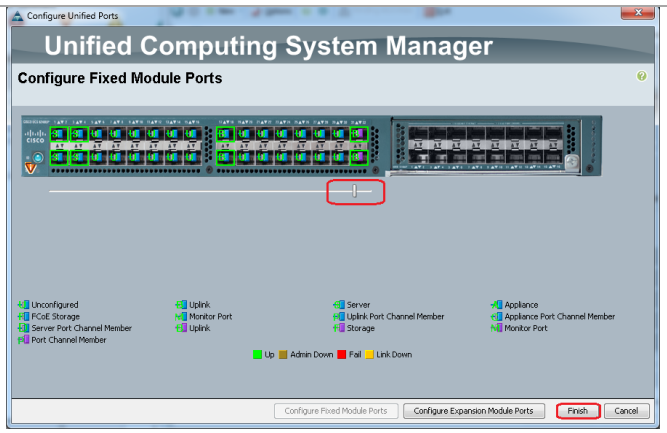
Configure Unified Ports for Fibre Channel

These steps provide details for modifying an unconfigured Ethernet port into a FC uplink port ports in the Cisco UCS environment.

Note: Modifications of the unified ports leads to a reboot of the fabric interconnect being modified. This reboot can take up to 10 minutes.

Cisco UCS Manager

Navigate to the **Equipment** tab in the left pane. Select **Fabric Interconnect A**. In the right pane, click the **General** tab. Select **Configure Unified Ports**. Select **Yes** to launch the wizard.	

Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports. Ports 31 and 32 now have the "B" indicator indicating their reconfiguration as FC uplink ports. Click **Finish**, then click **OK**. The Cisco UCSM GUI will close as the primary fabric interconnect reboots. Upon successful reboot, open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address. When prompted, enter `admin` for the username and enter the administrative password and click **Login** to log in to the Cisco UCS Manager software. Repeat the above steps for Fabric B. Navigate to the **Equipment** tab in the left pane. Select **Fabric Interconnect B**. In the right pane, click the **General** tab. Select **Configure Unified Ports**. Select **Yes** to launch the wizard. Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports. Ports 31 and 32 now have the "B" indicator indicating their reconfiguration as FC uplink ports. Click **Finish**, then click **OK**.	

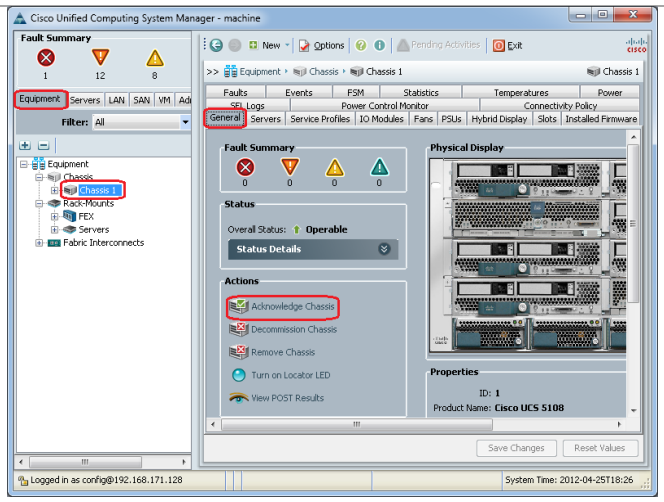
Cisco UCS PowerTool

1. Connect to Fabric Interconnect A, `Connect-UCS <FQDN or IP>`
2. `$var = Get-UcsFabricSanCloud -Id A`
3. `Add-UcsFcUplinkPort ($var) -PortId 1 -SlotId 31 -AdminState enabled`
4. This causes the Fabric Interconnect A to reboot
5. Upon successful reboot, `Connect-Ucs <FQDN or IP>`.
6. `$var = Get-UcsFabricSanCloud -Id B`
7. `Add-UcsFcUplinkPort ($var) -PortId 1 -SlotId 31 -AdminState enabled`
8. This causes Fabric Interconnect B to reboot
9. Upon successful reboot, `Connect-Ucs <FQDN or IP>`

Acknowledge the Cisco UCS Chassis

The connected chassis needs to be acknowledged before it can be managed by Cisco UCS Manager.

Cisco UCS Manager

On the **Equipment** tab, select **Chassis 1** in the left pane. Click **Acknowledge Chassis**.	

Cisco UCS Manager acknowledges the chassis and the blades servers in it. Do this for each chassis in your configuration.

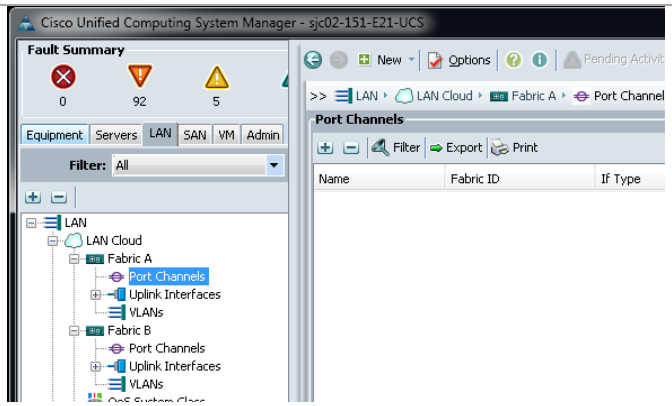
Cisco UCS PowerTool

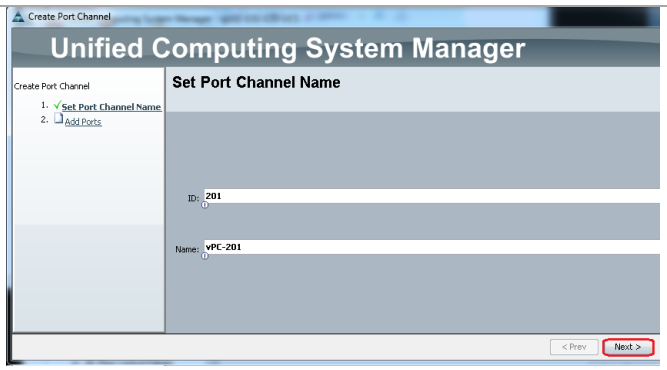
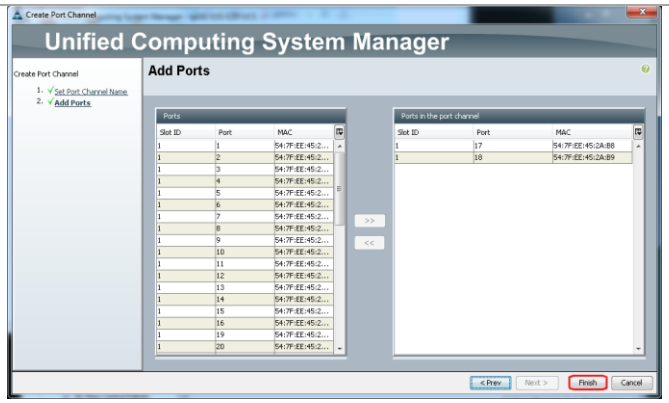
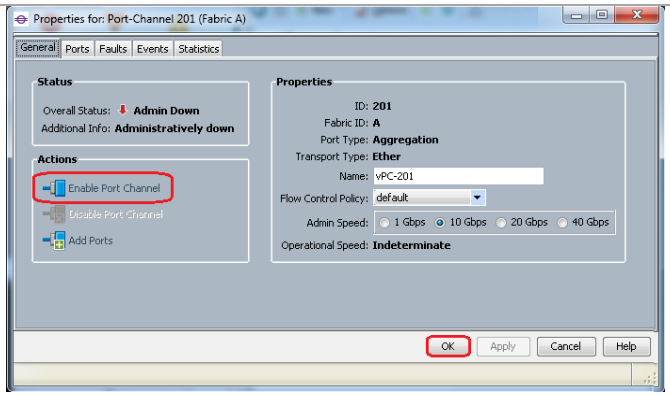
Get-UcsChassis –Id 1 | Set-UcsChassis –AdminState “re-acknowledge”

Create Uplink PortChannels to the Cisco Nexus 5548 Switches

These steps provide details for configuring the necessary PortChannels out of the Cisco UCS environment.

Cisco UCS Manager

Select the **LAN** tab on the left of the window. **Note:** Two PortChannels are created, one from fabric A to both Cisco Nexus 5548 switches and one from fabric B to both Cisco Nexus 5548 switches. Under **LAN Cloud**, expand the **Fabric A** tree. Right-click **Port Channels**. Select **Create Port Channel**.	

Enter `201` as the unique **ID** of the PortChannel. Enter `vPC-201` as the **Name** of the PortChannel. Click **Next**.	
Select the port with slot ID 1 and port 17 and also the port with slot ID 1 and port 18 to be added to the PortChannel. Click **>>** to add the ports to the PortChannel. Click **Finish** to create the PortChannel. Right-click the newly created port channel and select **Show navigator**	
Under Actions, select **Enable Port Channel**. In the pop-up box, click **Yes**, then **OK** to enable. Wait until the overall status of the Port Channel is up. Click **OK** to close the Navigator. Repeat for Fabric B using `202` as the unique ID of the Port Channel and `vpc-202` as the name.	

Cisco UCS PowerTool

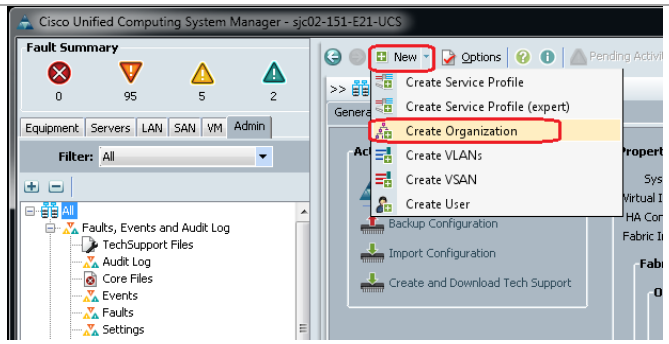
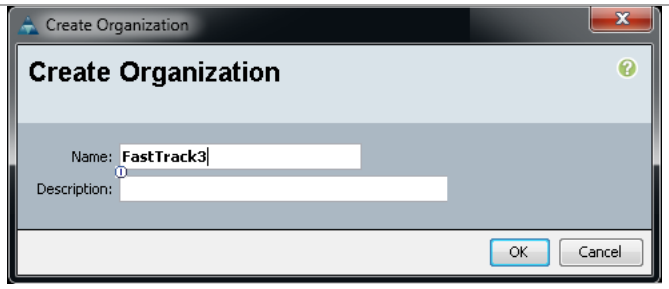
```
$var = Get-UcsFabricLanCloud -Id A | Add-UcsUplinkPortChannel -PortId
201 -AdminState enabled -Name <vPC-201>
$var | Add-UcsUplinkPortChannelMember -PortId 17 -SlotId 1 -AdminState
enabled
$var | Add-UcsUplinkPortChannelMember -PortId 18 -SlotId 1 -AdminState
enabled
$var = Get-UcsFabricLanCloud -Id B | Add-UcsUplinkPortChannel -PortId
202 -AdminState enabled -Name <vPC-202>
$var | Add-UcsUplinkPortChannelMember -PortId 17 -SlotId 1 -AdminState
enabled
$var | Add-UcsUplinkPortChannelMember -PortId 18 -SlotId 1 -AdminState
enabled
```

4.3 Configure Service Profiles

Create an Organization

These steps provide details for configuring an organization in the Cisco UCS environment. Organizations are used as a means to organize and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources. This document assumes the use of an Organization for FastTrack3, and the necessary steps are included below.

Cisco UCS Manager

From the **New...** menu at the top of the window, select **Create Organization**	
Enter a name for the organization. Enter a description for the organization (optional). Click **OK**. In the message box that displays, click **OK**.	

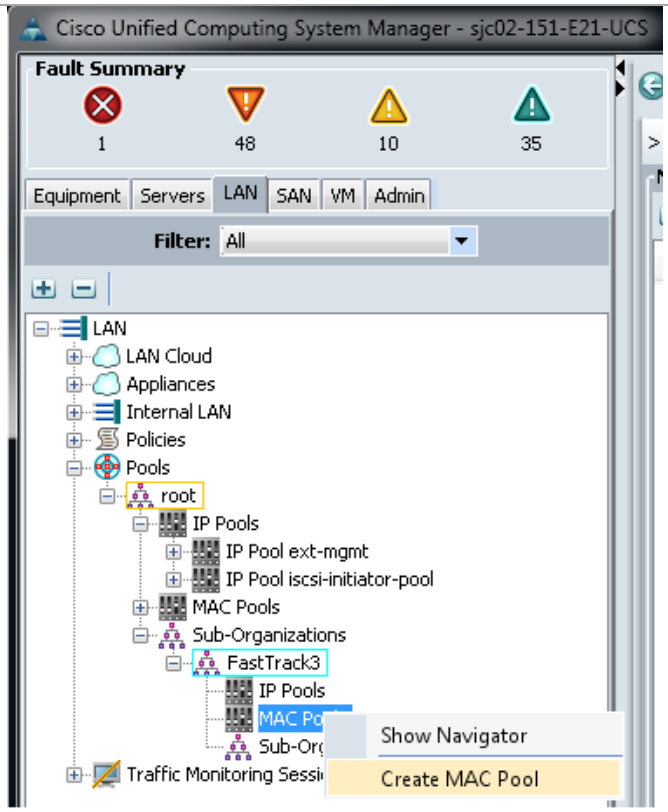
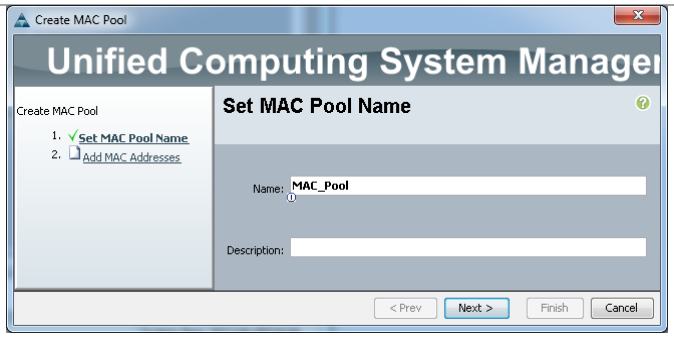
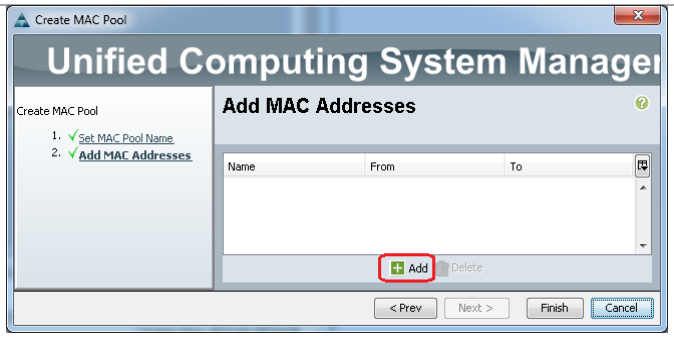
Cisco UCS PowerTool

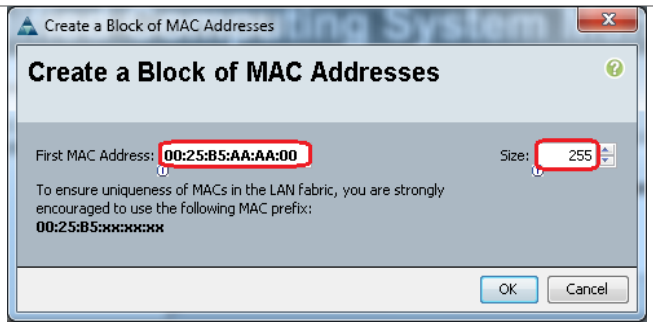
```
Add-UcsOrg -Org root -Name <sub-organization name> -Descr "<description>"
```

Create a MAC Address Pool

These steps provide details for configuring the necessary MAC address pool for the Cisco UCS environment.

Cisco UCS Manager

Select the **LAN** tab on the left of the window. Select **Pools > root > Sub-Organizations > FastTrack3**. Right-click **MAC Pools** under the FastTrack3 organization. Select **Create MAC Pool** to create the MAC address pool. **Note:** Depending on the desired configuration of MAC addresses, you can create multiple pools.	
Enter <***MAC_Pool***> for the name of the MAC pool. (Optional) Enter a description of the MAC pool.	
Click **Next**. Click **Add**.	

Specify a starting MAC address. Specify a size of the MAC address pool sufficient to support the available blade resources. Click **OK**, then click **Finish**. In the message box that displays, click **OK**.	

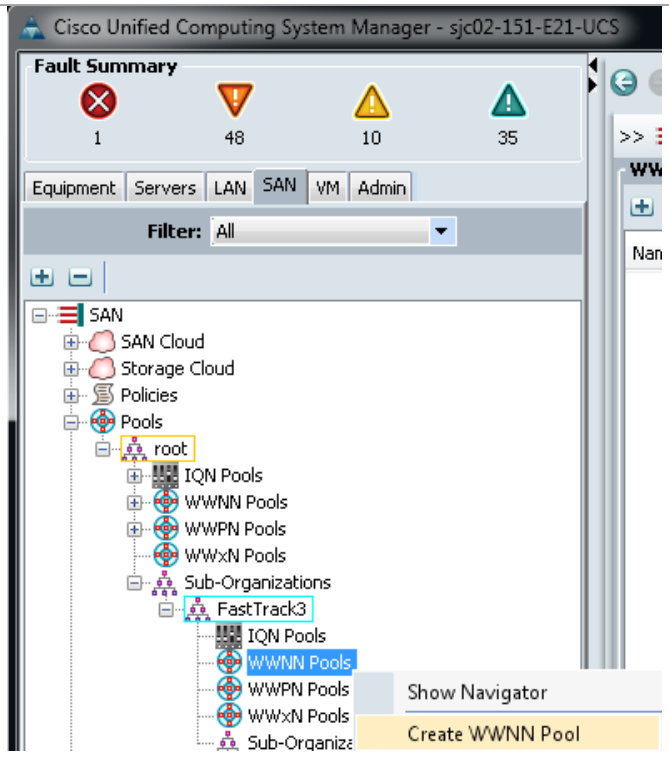
Cisco UCS PowerTool

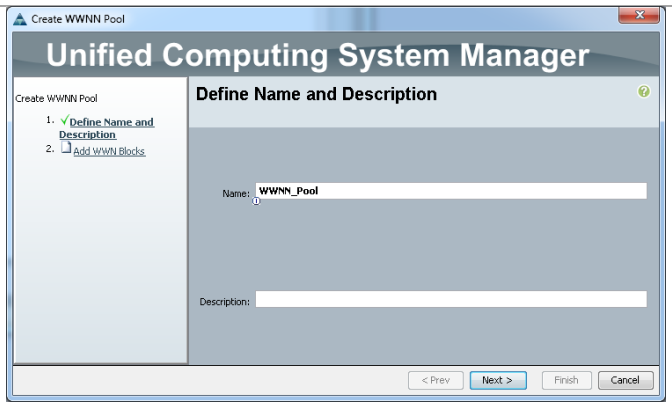
```
Add-UcsMacPool -Name <MAC_Pool> | Add-UcsMacMemberBlock -From <00:25:B5:AA:AA:00> -To <00:25:B5:AA:AA:FE>
```

Create WWNN Pools

These steps provide details for configuring the necessary WWNN pools for the Cisco UCS environment.

Cisco UCS Manager

Select the **SAN** tab at the top left of the window. Select **Pools > root > Sub-Organizations > FastTrack3**. Right-click **WWNN Pools** Select **Create WWNN Pool**.	

Enter <*WWNN_Pool*> as the Name of the WWNN pool. (Optional) Add a description for the WWNN pool. Click **Next** to continue.	
Click **Add** to add a block of WWNN's. The default is fine, modify if necessary. Specify a Size of the WWNN block sufficient to support the available blade resources. Click **OK,** the click **Finish** to proceed. Click **OK** to finish.	

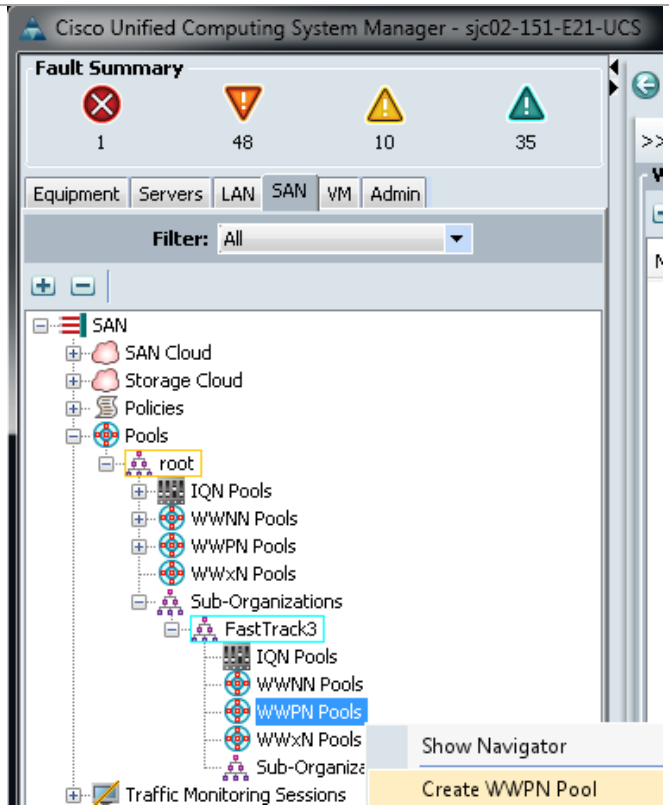
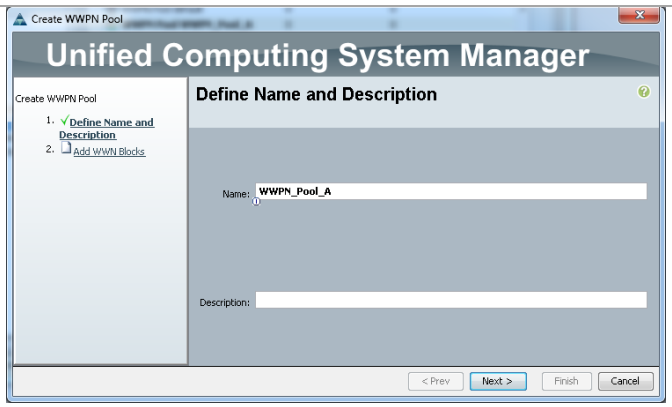
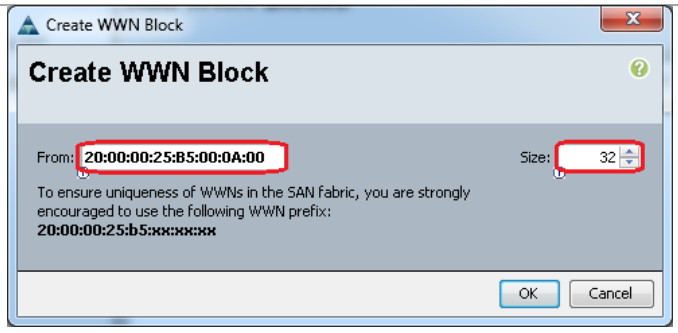
Cisco UCS PowerTool

```
$var = Add-UcsWwnPool -Name <WWNN_Pool> -Purpose node-wwn-assignment
$var | Add-UcsWwnMemberBlock -From <20:00:00:25:B5:AA:AA:00> -To
<20:00:00:25:B5:AA:AA:3F>
```

Create WWPN Pools

These steps provide details for configuring the necessary WWPN pools for the Cisco UCS environment. Two WWPN pools are created, one for fabric A and one for Fabric B.

Cisco UCS Manager

Select the **SAN** tab at the top left of the window. Select **Pools > root > Sub-Organizations > FastTrack3**. Right-click **WWPN Pools** Select **Create WWPN Pool**.	
Enter <WWPN_Pool_A> as the Name for the WWPN pool for fabric A. (Optional). Give the WWPN pool a description. Click **Next**.	
Click **Add** to add a block of WWPNs. Enter the starting WWPN in the From block for fabric A. Specify a Size of the WWPN block sufficient to support the available blade resources. Click **OK**. Click **Finish** to create the WWPN pool. Click **OK**. (Optional, but recommended) Repeat the above steps to create a pool for the B fabric.	

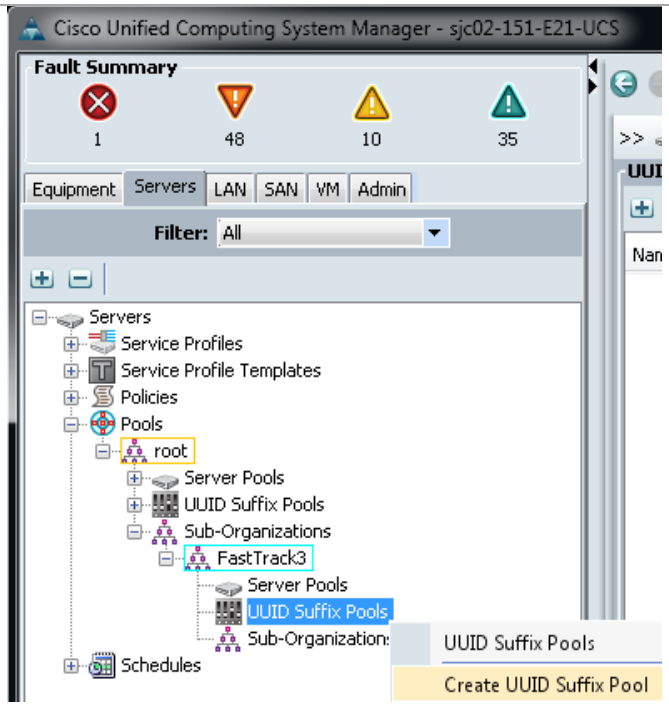
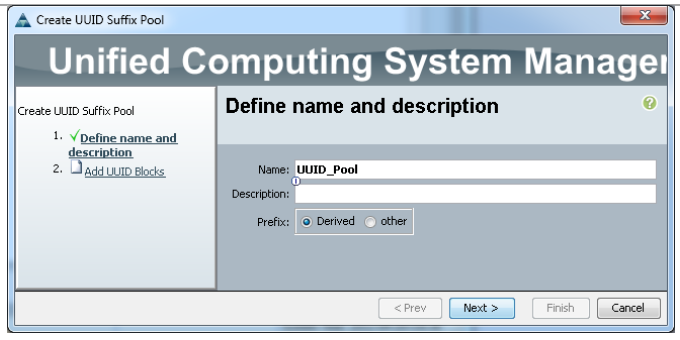
Cisco UCS PowerTool

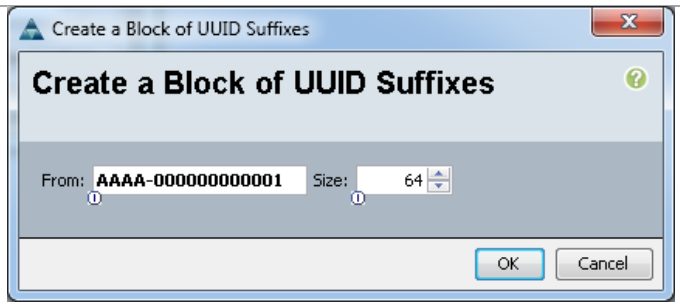
```
$var = Add-UcsWwnPool -Name <WWPN_Pool_A> -Purpose port-wwn-assignment
$var | Add-UcsWwnMemberBlock -From <20:00:00:25:B5:00:0A:00> -To
<20:00:00:25:B5:B8:0A:1F>
$var = Add-UcsWwnPool -Name <WWPN_Pool_B> -Purpose port-wwn-assignment
$var | Add-UcsWwnMemberBlock -From <20:00:00:25:B5:00:0B:00> -To
<20:00:00:25:B5:B8:0B:1F>
```

Create UUID Suffix Pools

These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

Cisco UCS Manager

Select the **Servers** tab on the top left of the window. Select **Pools > root > Sub-Organizations > FastTrack3**. Right-click **UUID Suffix Pools** Select **Create UUID Suffix Pool**.	
Name the UUID suffix pool <UUID_Pool>. (Optional) Give the UUID suffix pool a description. Leave the prefix at the derived option. Click **Next** to continue.	

Click **Add** to add a block of UUID's The **From** field is fine at the default setting, or you can create a hexadecimal string that is unique for your environment. Specify a **Size** of the UUID block sufficient to support the available blade resources. Click **OK**, then click **Finish** to proceed. Click **OK** to finish.	

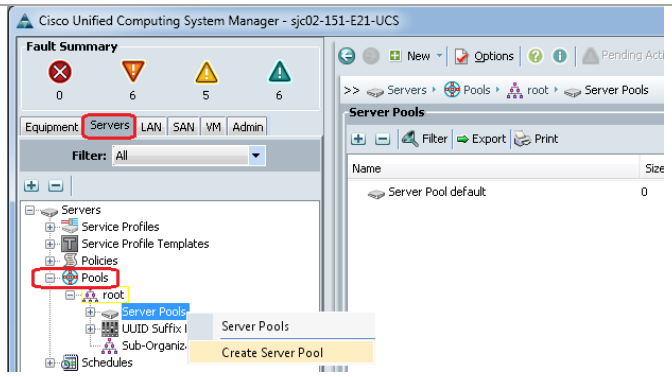
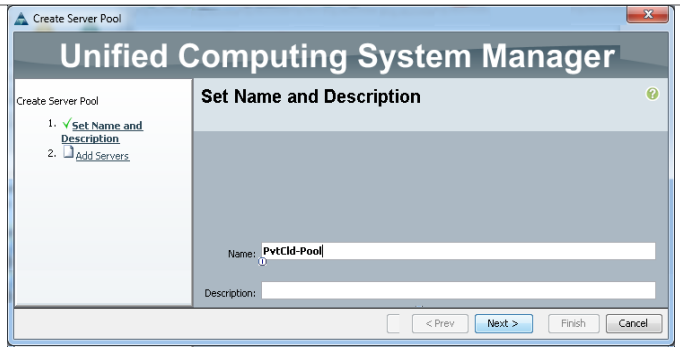
Cisco UCS PowerTool

```
$var = Add-UcsUuidSuffixPool -Name <UUID_Pool>
$var | Add-UcsUuidSuffixBlock -From <AAAA-000000000001> -To <AAAA-000000000040>
```

Create Server Pools

These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

Cisco UCS Manager

Select the **Servers** tab at the top left of the window. Select **Pools > root**. Right-click **Server Pools**. Select **Create Server Pool**.	
Name the server pool <PvtCld-Pool>. (Optional) Give the server pool a description. Click **Next** to continue to add servers. Select the **B200 servers** to be added to the PvtCld-Pool server pool. Click **>>** to add them to the pool. Click **Finish**, then select **OK** to finish.	

Cisco UCS PowerTool

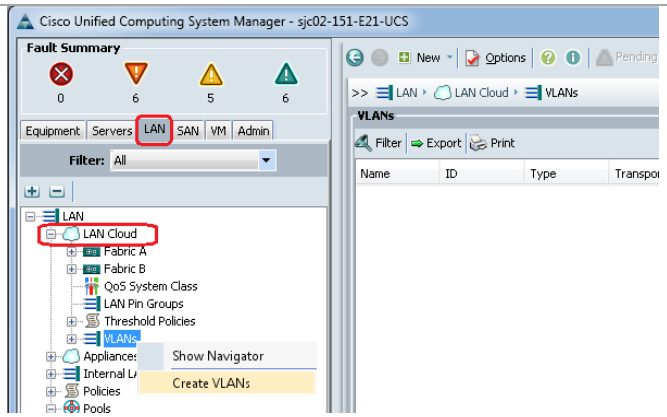
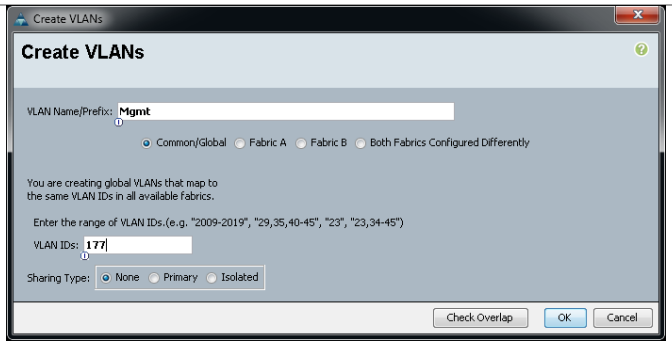
```
$var = Add-UcsServerPoolPool -Name <PvtCld-Pool>
$var | Add-UcsComputePooledSlot -ChassisId 1 -SlotId 1
$var | Add-UcsComputePooledSlot -ChassisId 1 -SlotId 2
```

Create VLANs

These steps provide details for configuring the necessary VLANs for the Cisco UCS environment.

Note: Six VLANs are created as Common/Global and four or six are created on specific fabrics.

Cisco UCS Manager

Select the **LAN** tab on the left of the window. Select **LAN Cloud**. Right-click **VLANs**. Select **Create VLANs**.	
Enter <Mgmt> as the **name** of the VLAN to be used for management traffic. Keep the **Common/Global** option selected for the scope of the VLAN. Enter the <Mgmt VLAN ID> for the management VLAN. Keep the sharing type as **none**. Click **OK**.	
Repeat above steps to create the CSV, ClusComm, VEM, and VMaccess VLANs.	
Creating the VLANs for iSCSI-A, iSCSI-B, LiveMigration-A, LiveMigration-B, SMB-A, and SMB-B are similar, except instead of specifying the **Common/Global** option for the scope of the VLAN, select either **Fabric A** or **Fabric B**, depending on which fabric is indicated by the suffix name.	

Cisco UCS PowerTool

```
$var = Get-UcsLanCloud
$var | Add-UcsVlan -Name <Mgmt> -Id <Mgmt VLAN ID>
$var | Add-UcsVlan -Name <CSV> -Id <CSV VLAN ID>
$var | Add-UcsVlan -Name <ClusComm> -Id <ClusComm VLAN ID>
$var | Add-UcsVlan -Name <VEM> -Id <VEM VLAN ID>
$var | Add-UcsVlan -Name <VMaccess> -Id <VMaccess VLAN ID>

$varA = Get-UcsLanCloud -Id "A"
$varA | Add-UcsVlan -Name <iSCSI-A> -Id <iSCSI VLAN ID>
$varA | Add-UcsVlan -Name <LiveMigration-A> -Id <LiveMigration VLAN ID>
$varA | Add-UcsVlan -Name <SMB-A> -Id <SMB VLAN ID>
```

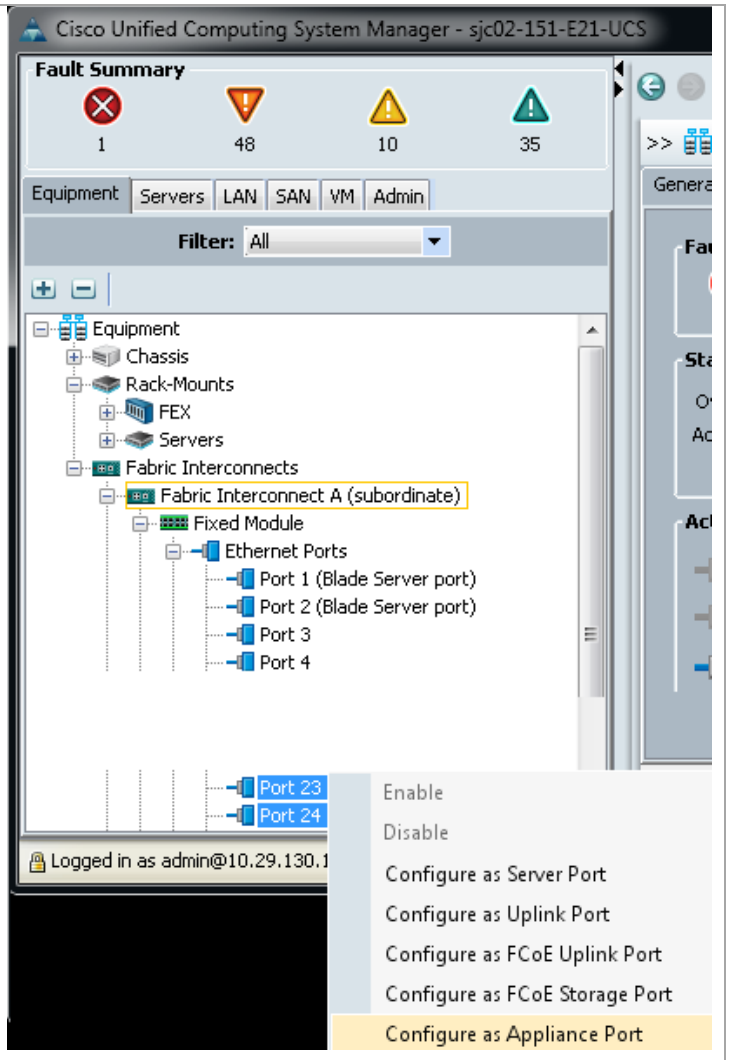
```
$varB = Get-UcsLanCloud -Id "B"
$varB | Add-UcsVlan -Name <iSCSI-B> -Id <iSCSI VLAN ID>
$varB | Add-UcsVlan -Name <LiveMigration-B> -Id <LiveMigration VLAN ID>
$varB | Add-UcsVlan -Name <SMB-B> -Id <SMB VLAN ID>
```

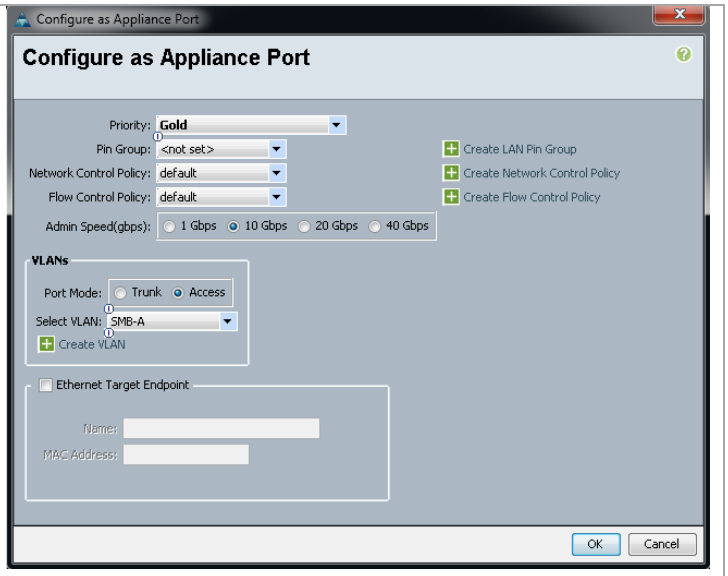
Configure Appliance Ports for iSCSI (optional SMB)

These steps provide details for modifying unconfigured Ethernet ports into appliance ports in the Cisco UCS environment. This enables connecting directly to iSCSI (or SMB) storage without connecting through the Nexus switches.

Cisco UCS Manager

Navigate to the **Equipment** tab in the left pane.
Select **Fabric Interconnects > Fabric Interconnect A > Fixed Module**.
Expand **Unconfigured Ethernet Ports**.
Select ports 23 and 24, right-click and select **Configure Appliance Port**.
Click **Yes**.

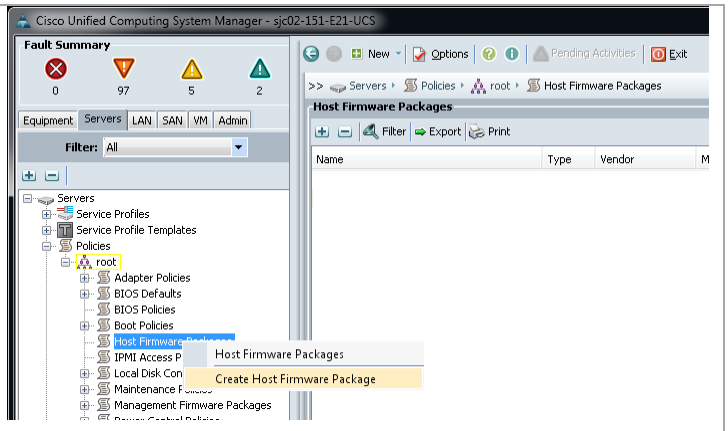


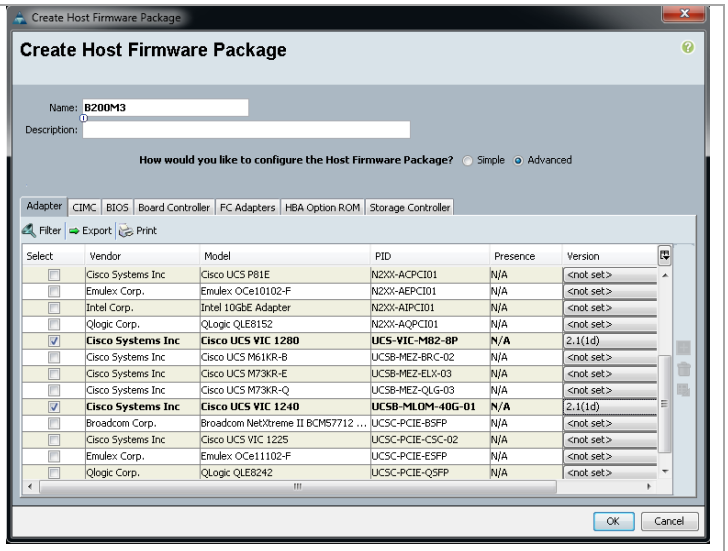
In the **Configure as Appliance Port** window, select **Gold** as the Priority to assign a QoS to this traffic. Ensure **Access** is selected, then select iSCSI-A (SMB-A) as the VLAN. Click **OK**. Repeat on Fabric Interconnect B for iSCSI-B (SMB-B).	

Create Host Firmware Package Policy

These steps provide details for creating a firmware management policy for a given server configuration in the Cisco UCS environment. Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These often include adapter, BIOS, board controller, FC adapters, HBA option ROM, and storage controller properties.

Cisco UCS Manager

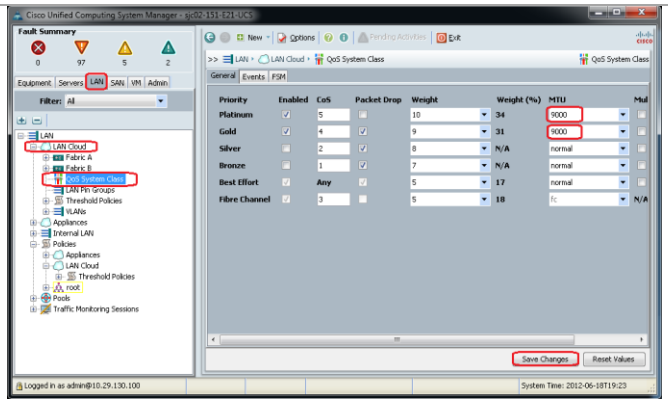
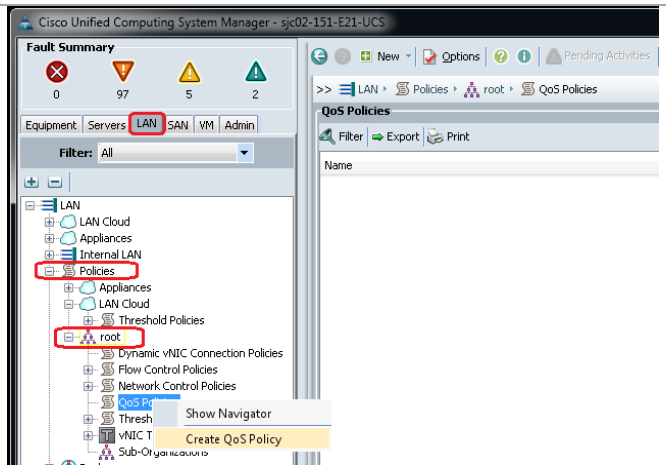
Select the **Servers** tab at the top left of the window. Select **Policies > root**. Right-click **Host Firmware Packages**. Select **Create Host Firmware Package**.	

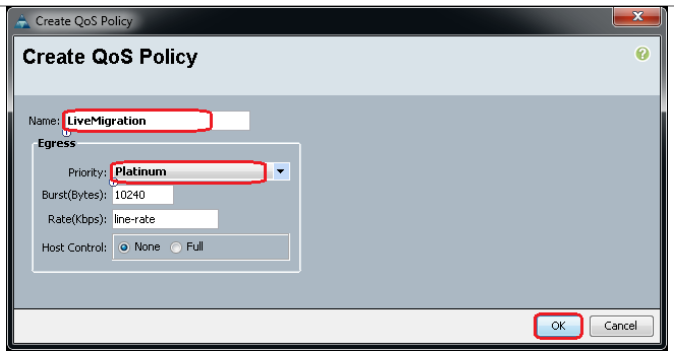
Enter the name of the host firmware package for the corresponding server configuration. Select the radio button for **Advanced** configuration. Navigate the tabs of the Create Host Firmware Package Navigator and select the appropriate packages and versions for the server configuration. Click **OK** to complete creating the host firmware package. Click **OK**.	

Enable Quality of Service in Cisco UCS Fabric

These steps provide details for enabling the quality of service in the Cisco UCS Fabric and setting Jumbo frames.

Cisco UCS Manager

Select the **LAN** tab at the top left of the window. Go **to LAN Cloud > QoS System Class**. In the right pane, click the **General** tab On the Platinum, Gold, and Best Effort rows, type **9000** in the MTU boxes. Click **Save Changes** in the bottom right corner. Click **OK** to continue.	
Select the **LAN** tab on the left of the window. Go to **LAN > Policies > Root >** Right-click **QoS Policies**. Select **Create QoS Policy**.	

Enter <LiveMigration> as the QoS Policy name. Change the Priority to Platinum. Leave Burst (Bytes) set to **10240**. Leave Rate (Kbps) set to **line-rate**. Leave Host Control set to **None**. Click **OK** in the bottom right corner.	
Repeat to create a QoS policy for SMB (or iSCSI). Right-click **QoS Policies**. Select **Create QoS Policy**. Enter <SMB> as the QoS Policy **name**. Change the Priority to Gold. Leave Burst (Bytes) set to **10240**. Leave Rate (Kbps) set to **line-rate**. Leave Host Control set to **None**. Click **OK** in the bottom right corner.	

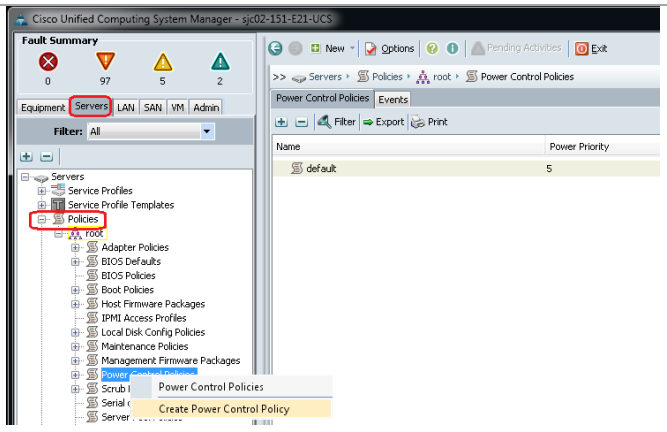
Cisco UCS PowerTool

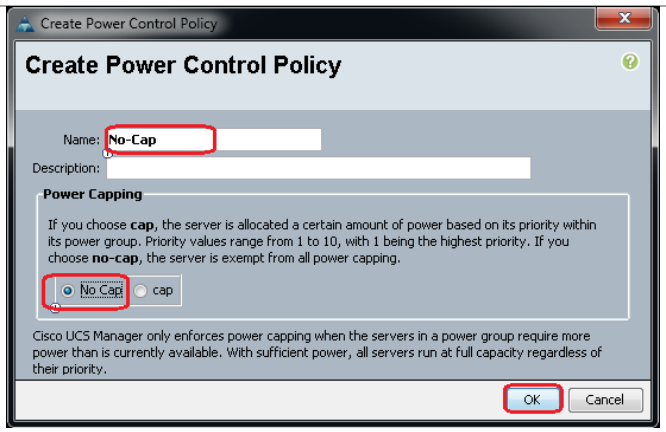
Set-UcsQosClass –QosClass (Get-UcsQosClass –Priority gold) –AdminState enabled –Mtu 9000 -Force
Set-UcsQosClass –QosClass (Get-UcsQosClass –Priority platinum) –AdminState enabled –Mtu 9000 –Force
$*var* = Add-UcsQosPolicy –Name “LiveMigration”
$*var* | Get-UcsVnicEgressPolicy | Set-UcsVnicEgressPolicy -Prio platinum -Force
$*var* = Add-UcsQosPolicy –Name “SMB”
$*var* | Get-UcsVnicEgressPolicy | Set-UcsVnicEgressPolicy -Prio gold -Force

Create a Power Control Policy

These steps provide details for creating a Power Control Policy for the Cisco UCS environment.

Cisco UCS Manager

Select the **Servers** tab at the top left of the window. Go to **Policies > root**. Right-click **Power Controller Policies**. Select **Create Power Control Policy**	

Enter <No-Cap> as the power control policy **Name**. Change the **Power Capping** to **No Cap**. Click **OK** to complete creating the host firmware package. Click **OK**.	

Cisco UCS PowerTool

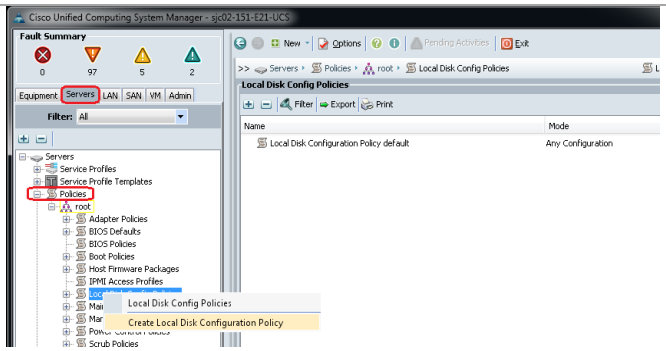
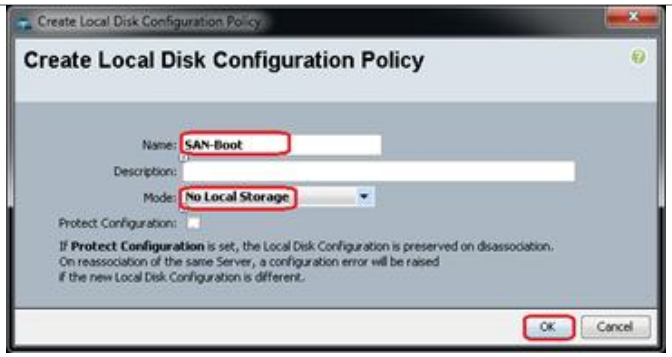
Add-UcsPowerPolicy -Name <No-Cap> -Prio “no-cap”

Create a Local Disk Configuration Policy

These steps provide details for creating a local disk configuration for the Cisco UCS environment, which is necessary if the servers in question do not have a local disk.

Note: This policy is recommended for cloud servers even if they do have local disks. Flexibility is a key component of clouds, so it is best to have configurations as loosely tied to physical hardware as possible. By not making provision for local disks and SAN booting, you ensure that moving the profile to another system will not create an environment that will lose something as it moves.

Cisco UCS Manager

Select the **Servers** tab on the left of the window. Go to **Policies > root**. Right-click **Local Disk Config Policies**. Select **Create Local Disk Configuration Policy**.	
Enter <SAN-Boot> as the local disk configuration policy **Name**. Change the **Mode** to **No Local Storage**. Uncheck the **Protect Configuration** box. Click **OK** to complete creating the host firmware package. Click **OK**.	

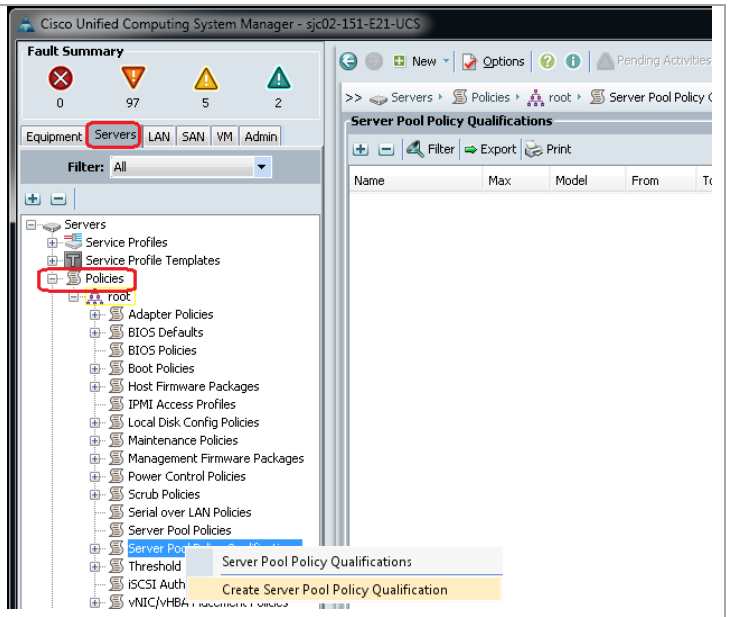
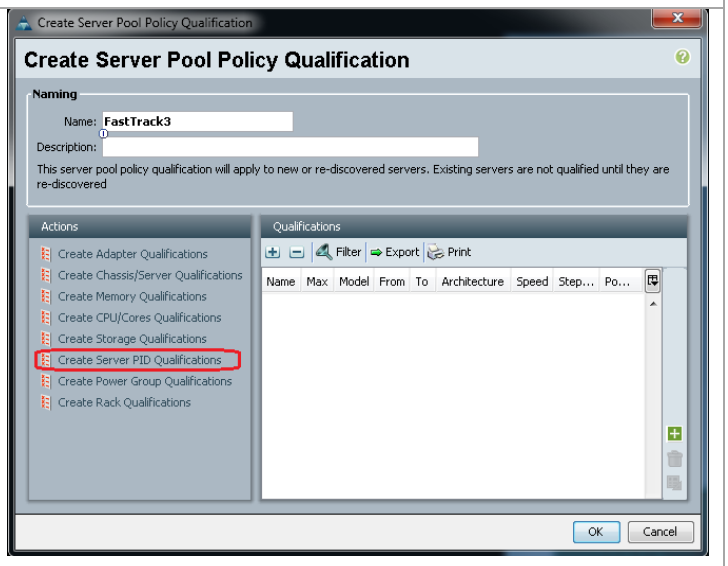
Cisco UCS PowerTool

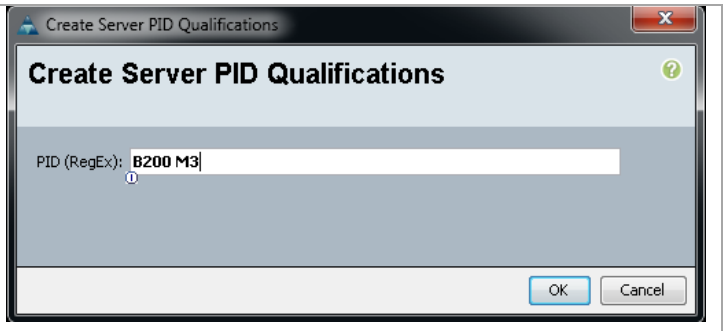
Add-UcsLocalDiskConfigPolicy -Name <SAN-Boot> -Mode no-local-storage

Create a Server Pool Qualification Policy

These steps provide details for creating a server pool qualification policy for the Cisco UCS environment.

Cisco UCS Manager

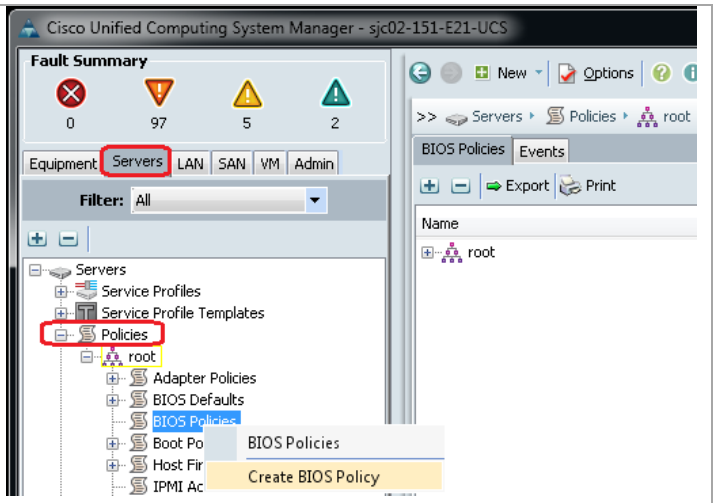
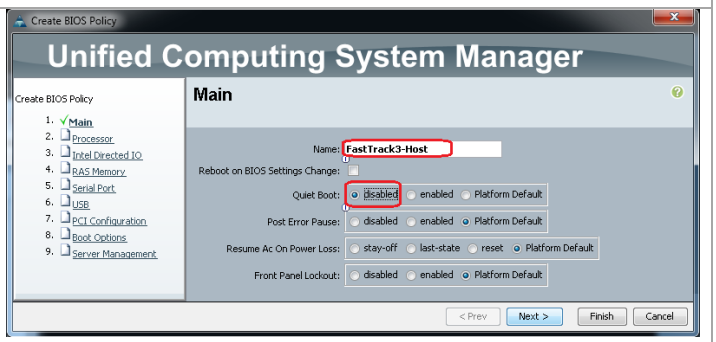
Select the **Servers** tab on the left of the window. Go to **Policies > root**. Right-click **Server Pool Policy Qualification**. Select **Create Server Pool Policy Qualification**.	
Enter <*FastTrack3*> as the **name**. Select **Create Server PID Qualifications**.	

Enter **B200 M3** as the **Model (RegEx)**. Click **OK** to complete creating the host firmware package. Click **OK**.	

Create a Server BIOS Policy

These steps provide details for creating a server BIOS policy for the Cisco UCS environment.

Cisco UCS Manager

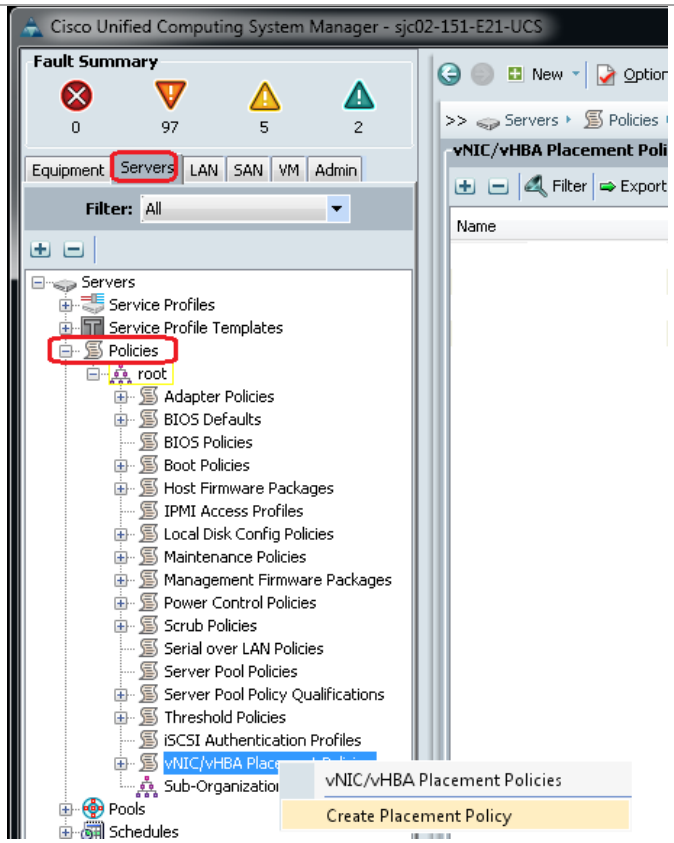
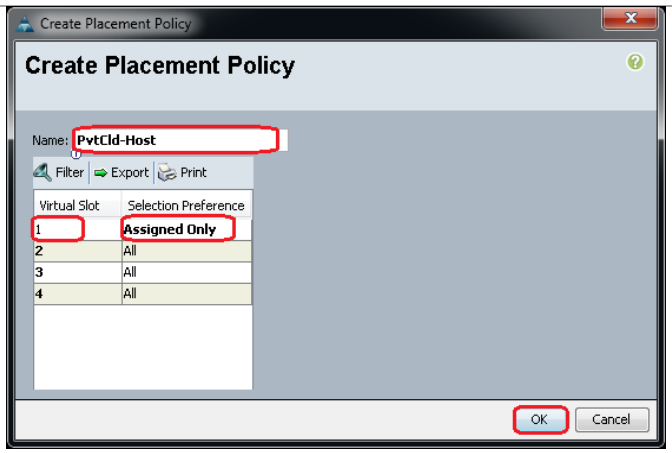
Select the **Servers** tab on the left of the window. Go to **Policies > root**. Right-click **BIOS Policies**. Select **Create BIOS Policy**.	
Enter <*FastTrack3-Host*> as the BIOS policy **Name**. Change the **Quiet Boot** property to **Disabled**. Click **Finish** to complete creating the BIOS policy. Click **OK**.	

Cisco UCS PowerTool

Add-UcsBiosPolicy -Name <FastTrack3-Host> | Set-UcsBiosVfQuietBoot -VpQuietBoot disabled -Force

Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts

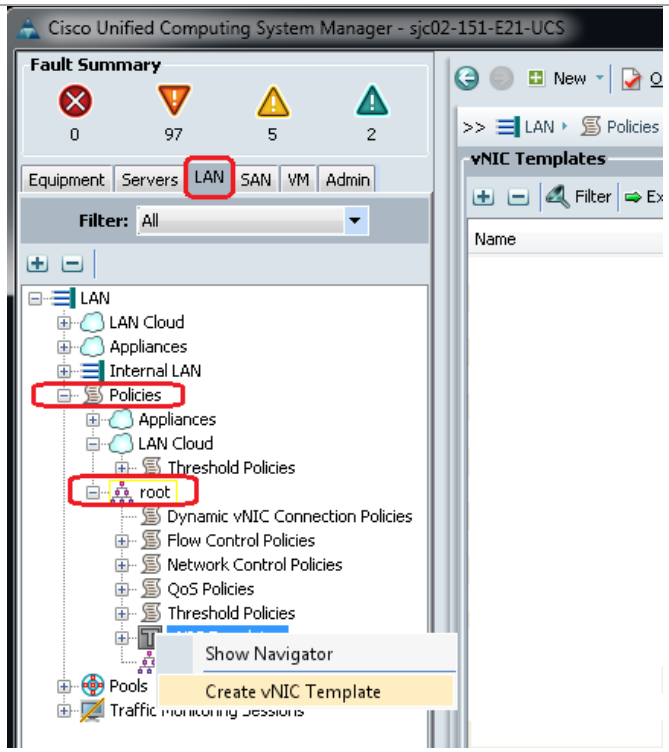
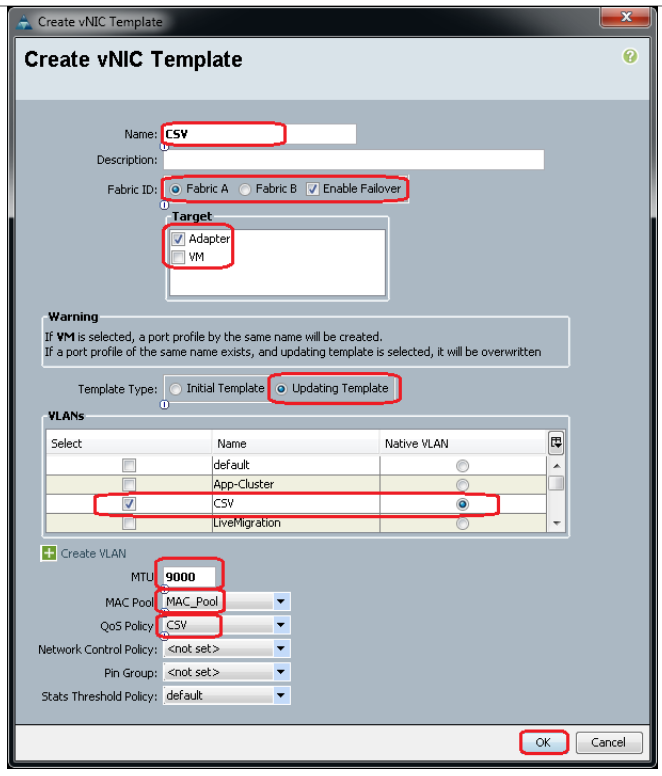
Cisco UCS Manager

Select the **Servers** tab on the left of the window. Go to **Policies > root**. Right-click **vNIC/HBA Placement Policies** and select **Create Placement Policy**.	
Enter the **Name** <FastTrack3-Host>. Click **1** and select **Assigned Only**. Click **OK**.	

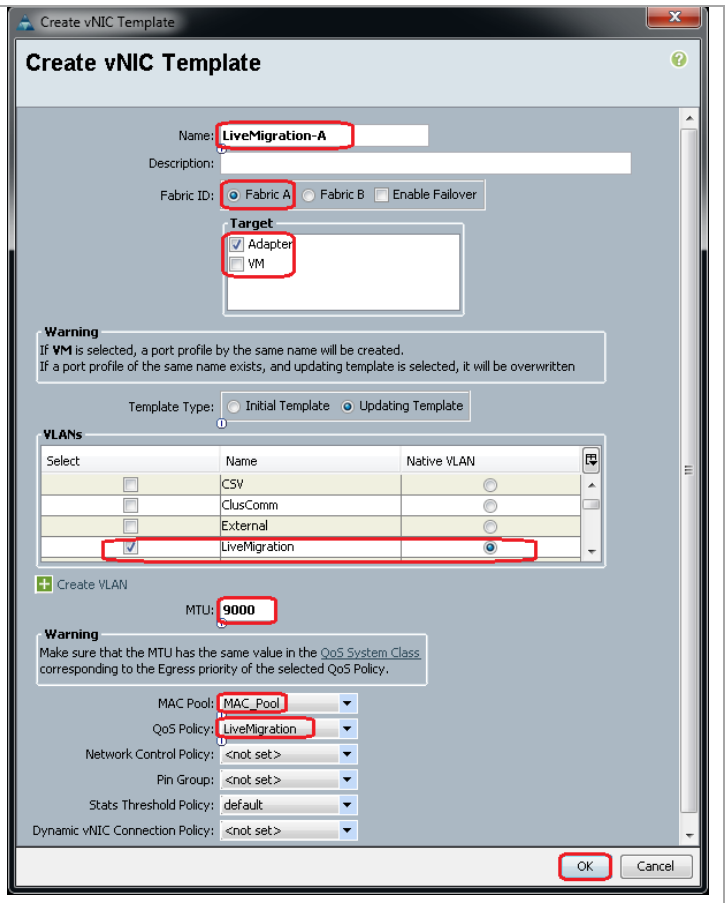
Create vNIC Templates

These steps provide details for creating multiple vNIC templates for the Cisco UCS environment.

Cisco UCS Manager

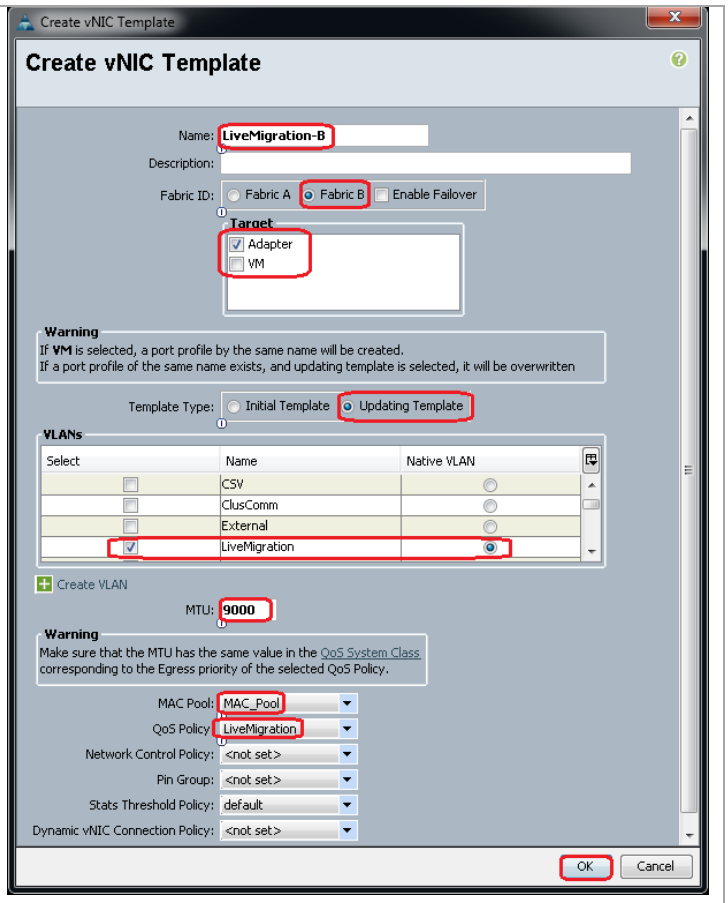
Select the **LAN** tab on the left of the window. Go to **Policies > root**. Right-click **vNIC Templates**. Select **Create vNIC Template**.	
Enter <*CSV*> as the vNIC template **Name**. Check **Fabric A**. Check the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under VLANs, select <*CSV*>. Set **Native VLAN**. Under MTU, set to **9000**. Under MAC Pool, select <*MAC-Pool*>. For QoS Policy, select <*CSV*> Click **OK** to complete creating the vNIC template	

Right-click **vNIC Templates**.
Select **Create vNIC Template**.
Enter <*LiveMigration-A*> as the vNIC template **Name**.
Check **Fabric A**.
Ensure the **Enable Failover** box is cleared.
Under target, unselect the **VM** box.
Select **Updating Template** as the Template Type.
Under VLANs, select <LiveMigration>. Set **Native VLAN**.
Under MTU, set to **9000**.
Under MAC Pool, select <*MAC-Pool*>.
For QoS Policy, select <*LiveMigration*>.
Click **OK** to complete creating the vNIC template

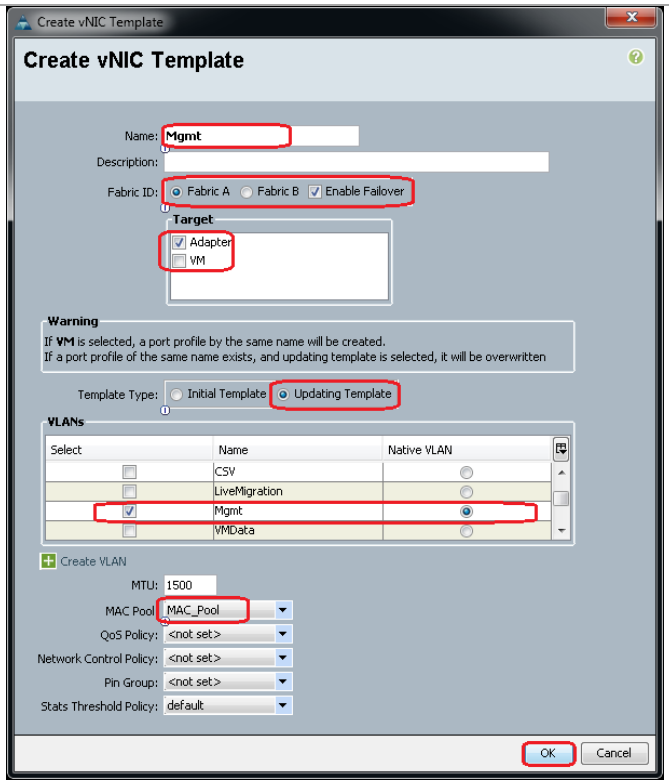


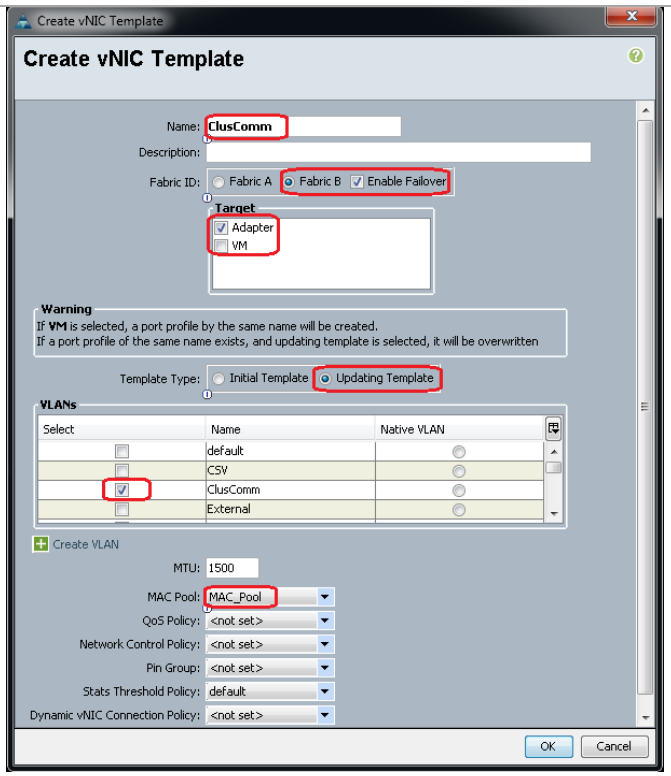
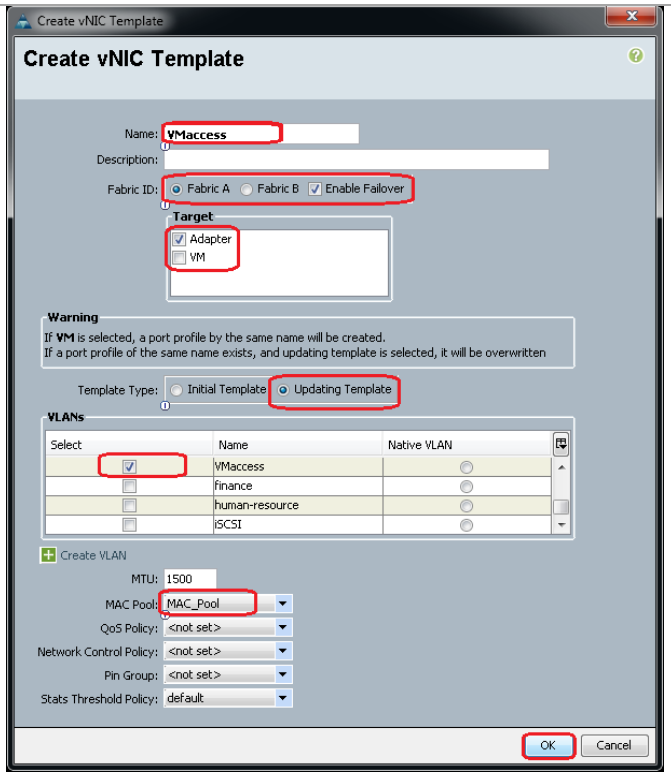
Right-click **vNIC Templates**.
Select **Create vNIC Template**.
Enter <*LiveMigration-B*> as the vNIC template **Name**.
Check **Fabric B**.
Ensure the **Enable Failover** box is cleared.
Under target, unselect the **VM** box.
Select **Updating Template** as the Template Type.
Under VLANs, select <LiveMigration>. Set **Native VLAN**.
Under MTU, set to **9000**.
Under MAC Pool, select <*MAC-Pool*>.
For QoS Policy, select <*LiveMigration*>.
Click **OK** to complete creating the vNIC template

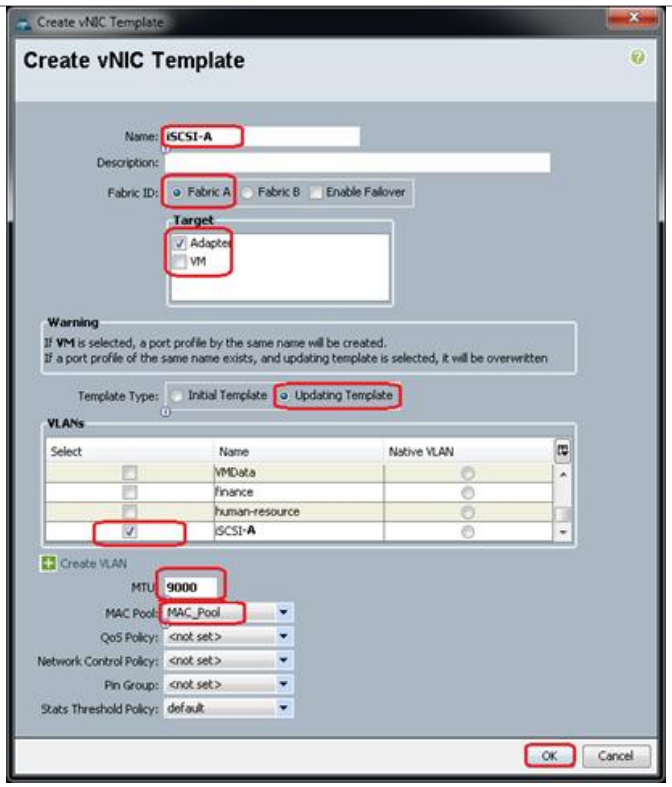
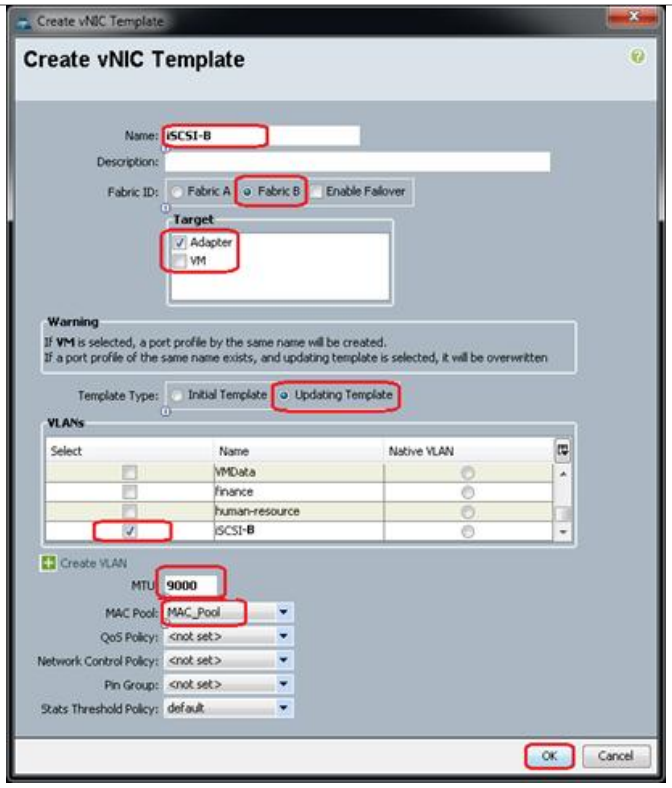
Note: This example creates two NICs that will be teamed within Windows Server 2012. You could also use a single VNIC, configured for failover, if you wish to use VPCs. Either method works



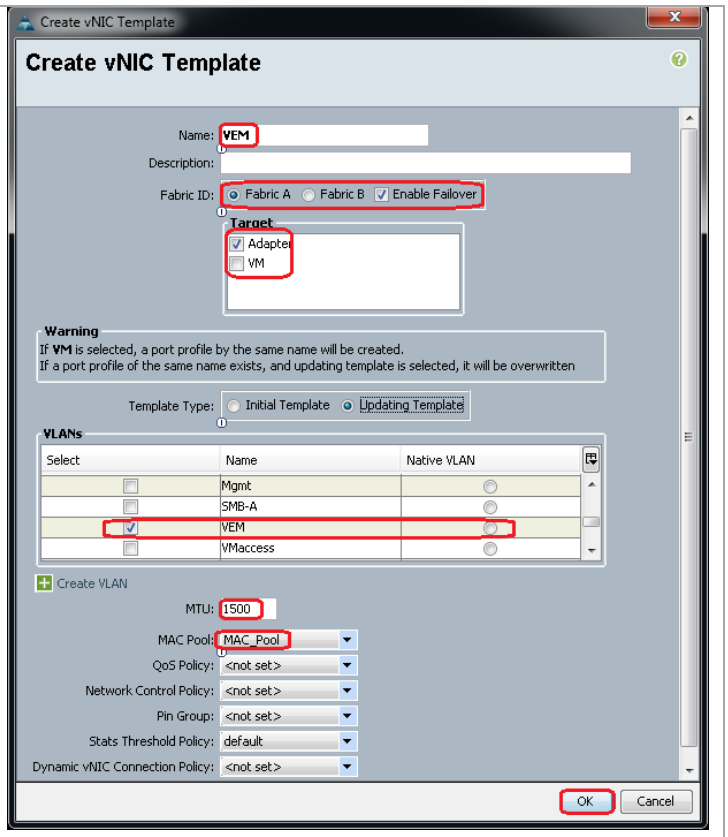
Right-click **vNIC Templates**.
Select **Create vNIC Template**.
Enter <*Mgmt*> as the vNIC template **Name**.
Check **Fabric A**.
Check the **Enable Failover** box.
Under target, unselect the **VM** box.
Select **Updating Template** as the Template Type.
Under VLANs, select <*Mgmt*>. Set **Native VLAN**.
Under MTU, leave **1500**.
Under MAC Pool, select <*MAC-Pool*>.
Click **OK** to complete creating the vNIC template



Right-click **vNIC Templates**. Select **Create vNIC Template**. Enter <*ClusComm*> as the vNIC template **Name**. Check **Fabric B**. Check the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under VLANs, select <*ClusComm*>. Do not set a **Native VLAN**. Under MTU, leave **1500**. Under MAC Pool, select <*MAC-Pool*>. Click **OK** to complete creating the vNIC template	
Right-click **vNIC Templates**. Select **Create vNIC Template**. Enter <*VMaccess*> as the vNIC template **Name**. Check **Fabric A.** Check the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under VLANs, select <*VMaccess*>. Do not set a **Native VLAN**. Under MTU, leave **1500**. Under MAC Pool, select <*MAC-Pool*>. Click **OK** to complete creating the vNIC template.	

Right-click **vNIC Templates**. Select **Create vNIC Template**. Enter <*iSCSI-A*> (and/or SMB-A) as the vNIC template **Name**. Check **Fabric A**. Uncheck the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under VLANs, select <*iSCSI-A*> (and/or SMB-A). Do not set a **Native VLAN**. Under MTU, enter **9000**. Under MAC Pool, select <*MAC-Pool*>. Click **OK** to complete creating the vNIC template.	
Right-click **vNIC Templates**. Select **Create vNIC Template**. Enter <*iSCSI-B*> (and/or SMB-B) as the vNIC template **Name**. Check **Fabric B**. Uncheck the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under VLANs, select <*iSCSI-B*> (and/or SMB-B). Do not set a **Native VLAN**. Under MTU, enter **9000**. Under MAC Pool, select <*MAC-Pool*>. Click **OK** to complete creating the vNIC template.	

Right-click **vNIC Templates**.
Select **Create vNIC Template**.
Enter <*VEM*> as the vNIC template **Name**.
Check **Fabric** A.
Check the **Enable Failover** box.
Under target, unselect the **VM** box.
Select **Updating Template** as the Template Type.
Under VLANs, select <*VEM*>. Do not set a **Native VLAN**.
Under MTU, enter **1500**.
Under MAC Pool, select <*MAC-Pool*>.
Click **OK** to complete creating the vNIC template.



Cisco UCS PowerTool

```
$Template = Add-UcsVnicTemplate -Name <CSV> -IdentPoolName <MAC_Pool> -SwitchId A-B –Target adaptor -TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <CSV-VLAN>
$Template | Get-UcsVnicInterface -Name <CSV> | Set-UcsVnicInterface -DefaultNet true -Force
$Template = Add-UcsVnicTemplate -Name <LiveMigration> -IdentPoolName <MAC_Pool> -Mtu 9000 -QosPolicyName <LiveMigration> -SwitchId B-A -Target adaptor -TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <LiveMigration-VLAN>
$Template | Get-UcsVnicInterface -Name <LiveMigration> | Set-UcsVnicInterface -DefaultNet true -Force
$Template = Add-UcsVnicTemplate -Name <Mgmt> -IdentPoolName <MAC_Pool> -SwitchId A-B –Target adaptor -TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <Mgmt-VLAN>
$Template | Get-UcsVnicInterface -Name <Mgmt> | Set-UcsVnicInterface -DefaultNet true -Force
$Template = Add-UcsVnicTemplate -Name <ClusComm> -IdentPoolName <MAC_Pool> -SwitchId B-A –Target adaptor -TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <ClusComm-VLAN>
$Template | Get-UcsVnicInterface -Name <ClusComm> | Set-UcsVnicInterface -DefaultNet true -Force
$Template = Add-UcsVnicTemplate -Name <VMaccess> -IdentPoolName <MAC_Pool> -SwitchId A-B –Target adaptor -TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <VMaccess-VLAN>
$Template | Get-UcsVnicInterface -Name <VMaccess> | Set-UcsVnicInterface -DefaultNet true -Force
```

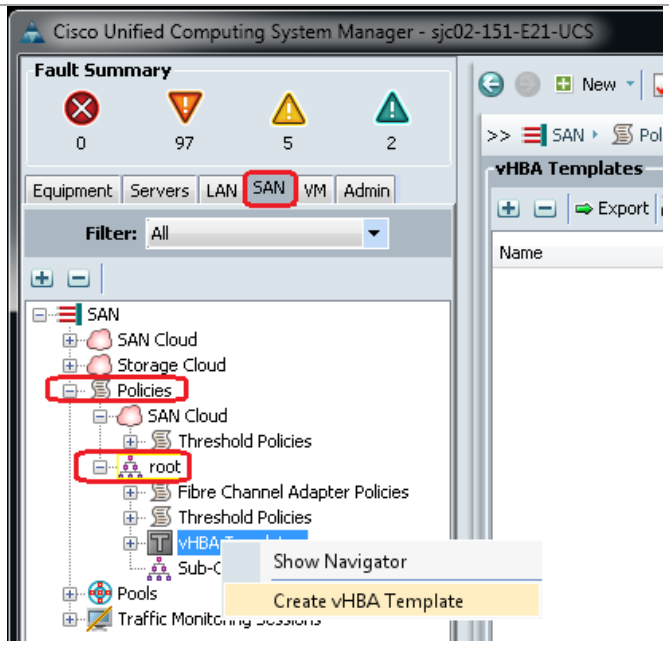
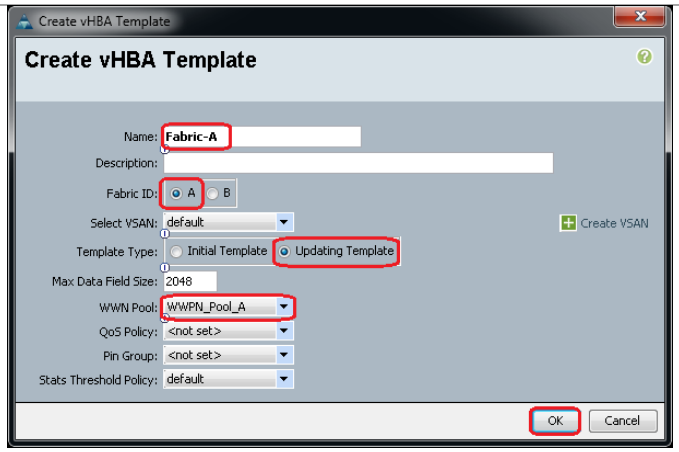
```
$Template = Add-UcsVnicTemplate -Name <iSCSI-A> -IdentPoolName
<MAC_Pool> -Mtu 9000 -QosPolicyName <iSCSI> -SwitchId A -Target adaptor
-TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <iSCSI-VLAN-A>
$Template | Get-UcsVnicInterface -Name <iSCSI-A> | Set-UcsVnicInterface
-DefaultNet true -Force
$Template = Add-UcsVnicTemplate -Name <iSCSI-B> -IdentPoolName
<MAC_Pool> -Mtu 9000 -QosPolicyName <iSCSI> -SwitchId B -Target adaptor
-TemplType updating-template
Add-UcsVnicInterface -VnicTemplate ($Template) -Name <iSCSI-VLAN-B>
```

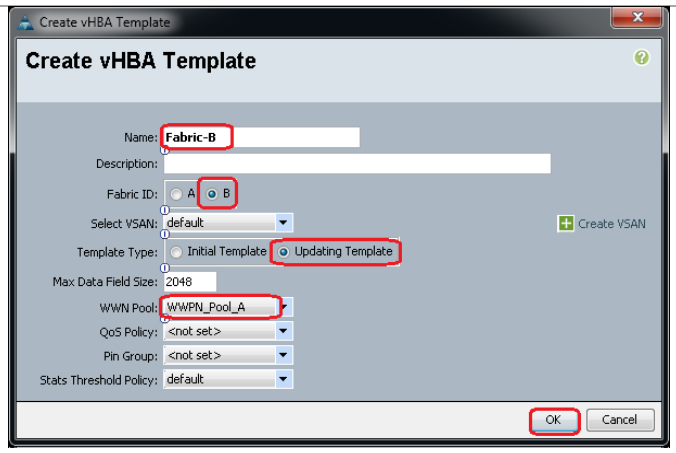
$*Template* | Get-UcsVnicInterface -Name <*iSCSI-B*> | Set-UcsVnicInterface -DefaultNet true -Force

Create vHBA Templates for Fabric A and B

These steps provide details for creating a vHBA template each for fabric A and fabric B for the Cisco UCS environment.

Cisco UCS Manager

Select the **SAN** tab on the left of the window. Go to **Policies > root**. Right-click **vHBA Templates**. Select **Create vHBA Template**.	
Enter <*Fabric-A*> as the vHBA template **Name**. Select **Fabric A**. Under Template Type select **Updating Template**. Under WWN Pool, select <*WWPN_Pool*>. Click **OK** to complete creating the vHBA template. Click **OK**.	

Right-click **vHBA Templates**. Select **Create vHBA Template**. Enter <*Fabric-B*> as the vHBA template **Name**. Select **Fabric B**. Under Template Type select **Updating Template**. Under WWN Pool, select <*WWPN_Pool*>. Click **OK** to complete creating the vHBA template. Click **OK**.	

Cisco UCS PowerTool

```
$mo = Get-UcsOrg -Level root | Get-UcsOrg -Name "<FastTrack3>" -
LimitScope | Add-UcsVhbaTemplate -Descr "" -IdentPoolName
"<wwpnFastTrack3>" -MaxDataFieldSize 2048 -Name "<F3-Fabric-B>" -
PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -
SwitchId "B" -TemplType "updating-template"
$mo_1 = $mo | Add-UcsVhbaInterface -ModifyPresent -Name "default"
```

Create Boot Policies

These steps provide details for creating boot policies for the Cisco UCS environment. In these steps, 2 boot policies will be configured. The first policy will configure the primary target to be SPA Slot A0 Port 0 and the second boot policy will configure the primary target will be SPB Slot B0 Port 1.

Table 15 WWPN Values from Customer Environment

Port	WWPN
SPA-A2	
SPA-A3	
SPB-B2	
SPB-B3	

First, obtain the WWPN information from the EMC VNX5500 by using the NaviSecCli that is installed on your Windows management system and record it in the above table. Following is an example for obtaining the WWPNs from the connections to the VNX5500. It may be necessary to provide additional parameters, for login, password and scope options. The example below returns configuration information for all ports configured within the array. This includes both Fiber Channel ports, and iSCSI targets. The WWPN for any given Fiber Channel port is derived from the last half of the SP UID entry. The first half of the SP UID is the WWNN entry. As an example, the WWPN of Port 0 on SP-A Port ID 4 is 50:06:01:64:3D:E0:25:10.

```
C:\> naviseccli -address <<IP Address of SP-A or SP-B>> -User <<Admin
user>> -Password <<Admin user password>> -Scope 0 port -list -sp

SP Name:             SP                                          A
SP Port ID:          4
```

```
SP UID:              50:06:01:60:BD:E0:25:10:50:06:01:64:3D:E0:25:10
Link Status:         Up
Port Status:         Online
Switch Present:      YES
Switch UID:          20:02:00:05:73:A1:DA:C1:20:02:00:05:73:A1:DA:C1
SP Source ID:        0

...
```

(report truncated)

Alternatively EMC Storage Integrator (ESI) PowerShell Toolkit can be used to obtain WWPN and IQN information like the following examples.

```
$targetports = Get-EmcTargetPort
$targetports | Where {$_.PortLocation -like "*Module 0*"} | fl
PortLocation,
@{Expression={$_.Wwn.tostring().substring(0,23)};Label="WWNN"},
@{Expression={$_.Wwn.tostring().substring(24)};Label="WWPN"}
```

```
PortLocation    :SPA    I/O     Module 0        Port    0
WWNN            :50:06:01:60:BD:E0:25:10
WWPN            :50:06:01:60:3D:E0:0A:63

PortLocation    :SPA    I/O     Module 0        Port    1
WWNN            :50:06:01:60:BD:E0:25:10
WWPN            :50:06:01:61:3D:E0:0A:63

PortLocation    :SPB    I/O     Module 0        Port    0
WWNN            :50:06:01:60:BD:E0:25:10
WWPN            :50:06:01:68:3D:E0:0A:63

PortLocation    :SPB    I/O     Module 0        Port    1
WWNN            :50:06:01:60:BD:E0:25:10
WWPN            :50:06:01:69:3D:E0:0A:63
```

```
$targetports = Get-EmcTargetPort
$targetports | Where {$_.PortLocation -like "*Module 1*"} | fl PortLocation,
Iqn, Ipaddress
```

```
PortLocation    :SPA    I/O     Module 1        Port    0
Iqn             :iqn.1992-04.com.emc:cx.apm00122900053.a6
IpAddress       :192.168.18.200

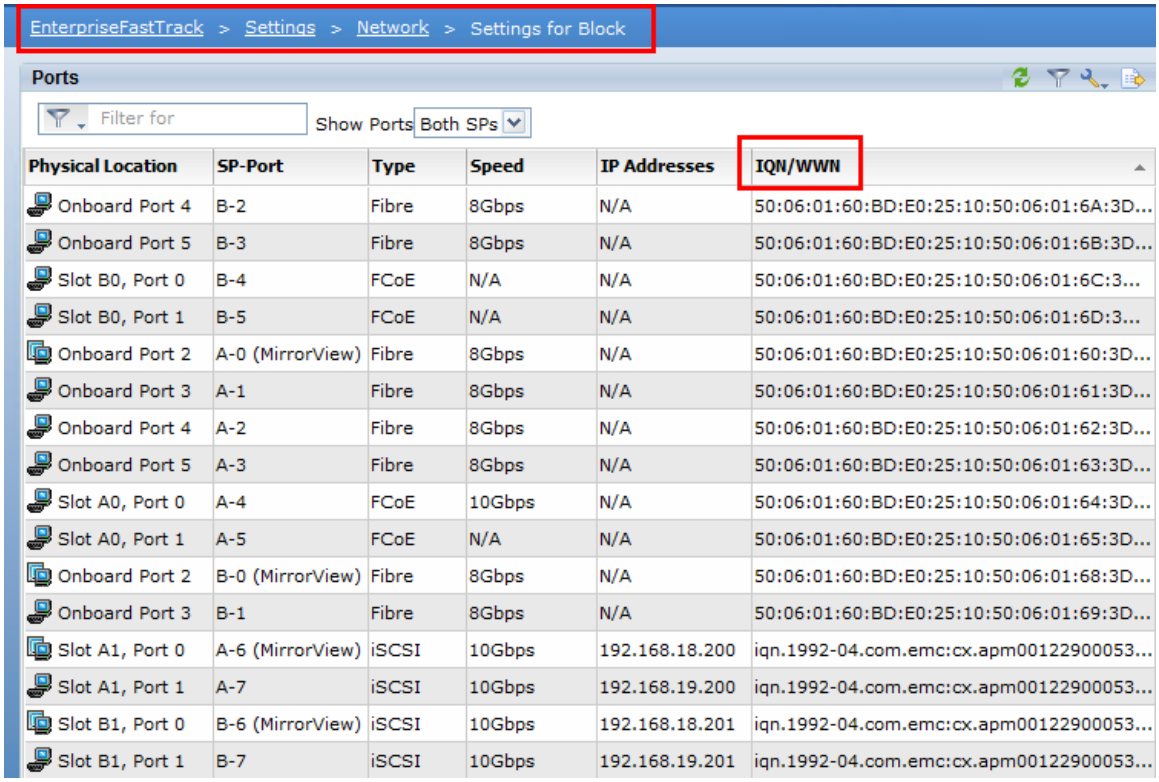
PortLocation    :SPA    I/O     Module 1        Port    1
Iqn             :iqn.1992-04.com.emc:cx.apm00122900053.a7
IpAddress       :192.168.19.200

PortLocation    :SPB    I/O     Module 1        Port    0
Iqn             :iqn.1992-04.com.emc:cx.apm00122900053.b6
IpAddress       :192.168.18.201

PortLocation    :SPB    I/O     Module 1        Port    1
Iqn             :iqn.1992-04.com.emc:cx.apm00122900053.b7
IpAddress       :192.168.19.201
```

Alternatively, the WWPN and IQN information can be obtained from Unisphere via the Settings > Network > Settings for Block menu as shown in the following figure.

Figure 4 Finding WWN from Unisphere

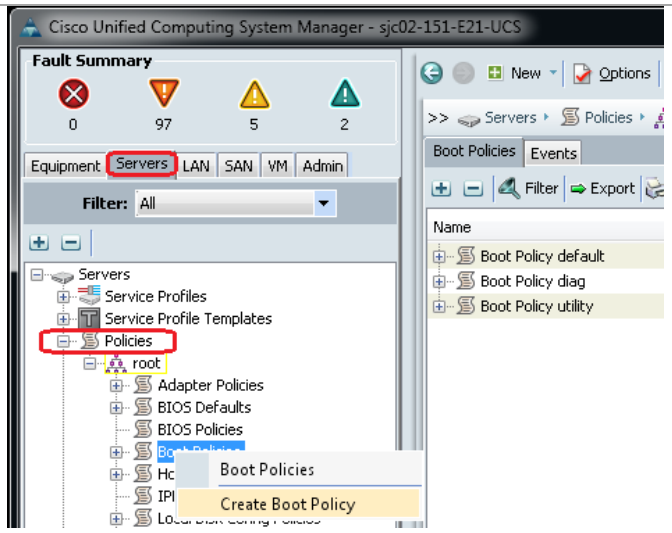


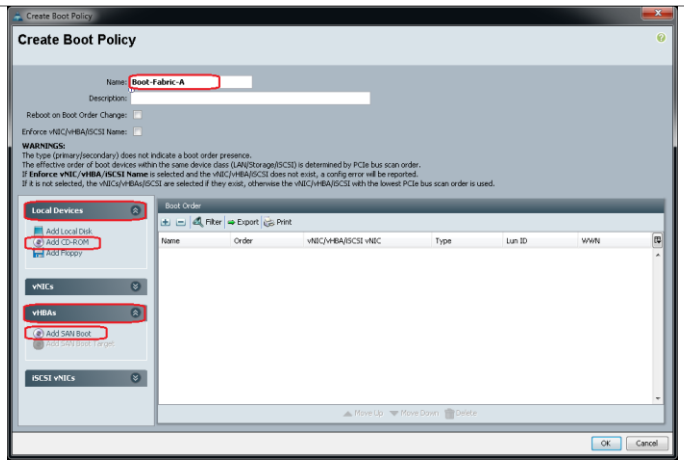
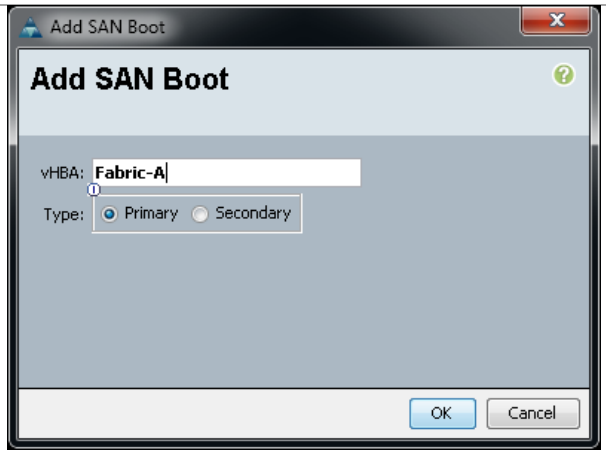
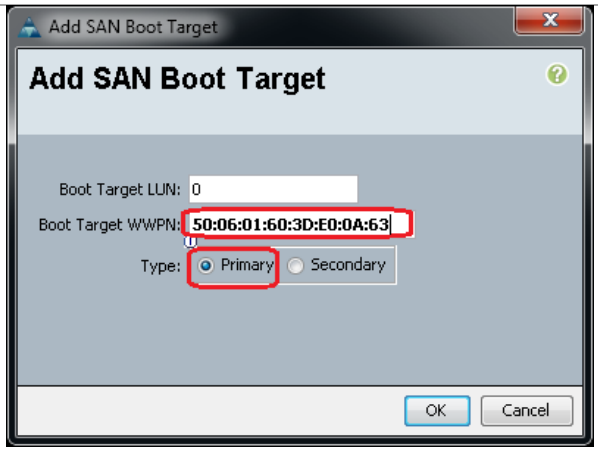
Physical Location	SP-Port	Type	Speed	IP Addresses	IQN/WWN
Onboard Port 4	B-2	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:6A:3D...
Onboard Port 5	B-3	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:6B:3D...
Slot B0, Port 0	B-4	FCoE	N/A	N/A	50:06:01:60:BD:E0:25:10:50:06:01:6C:3...
Slot B0, Port 1	B-5	FCoE	N/A	N/A	50:06:01:60:BD:E0:25:10:50:06:01:6D:3...
Onboard Port 2	A-0 (MirrorView)	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:60:3D...
Onboard Port 3	A-1	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:61:3D...
Onboard Port 4	A-2	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:62:3D...
Onboard Port 5	A-3	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:63:3D...
Slot A0, Port 0	A-4	FCoE	10Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:64:3D...
Slot A0, Port 1	A-5	FCoE	N/A	N/A	50:06:01:60:BD:E0:25:10:50:06:01:65:3D...
Onboard Port 2	B-0 (MirrorView)	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:68:3D...
Onboard Port 3	B-1	Fibre	8Gbps	N/A	50:06:01:60:BD:E0:25:10:50:06:01:69:3D...
Slot A1, Port 0	A-6 (MirrorView)	iSCSI	10Gbps	192.168.18.200	iqn.1992-04.com.emc:cx.apm00122900053...
Slot A1, Port 1	A-7	iSCSI	10Gbps	192.168.19.200	iqn.1992-04.com.emc:cx.apm00122900053...
Slot B1, Port 0	B-6 (MirrorView)	iSCSI	10Gbps	192.168.18.201	iqn.1992-04.com.emc:cx.apm00122900053...
Slot B1, Port 1	B-7	iSCSI	10Gbps	192.168.19.201	iqn.1992-04.com.emc:cx.apm00122900053...

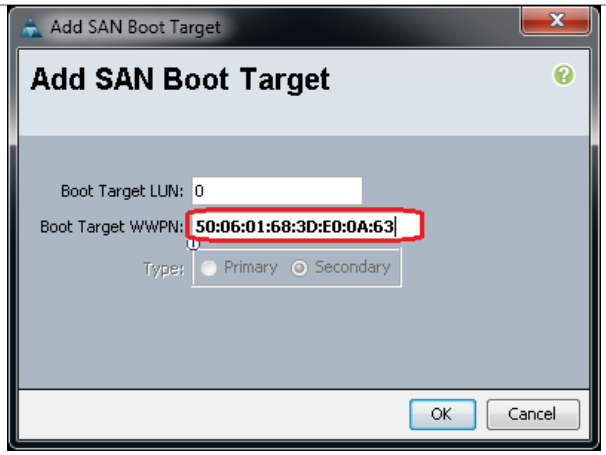
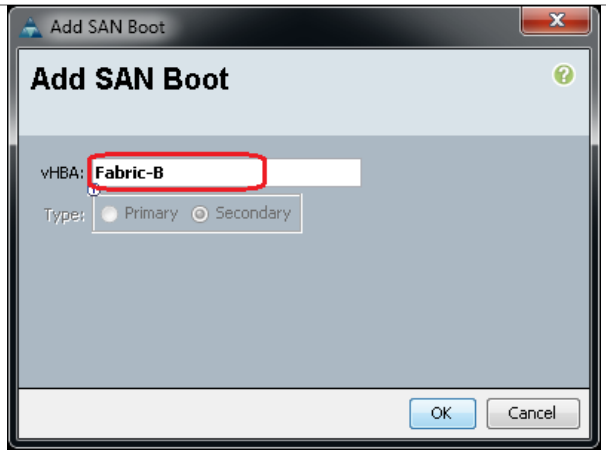
When you have recorded the WWPNs from the VNX5500 for the correct ports, proceed to configuring Cisco UCS Manager.

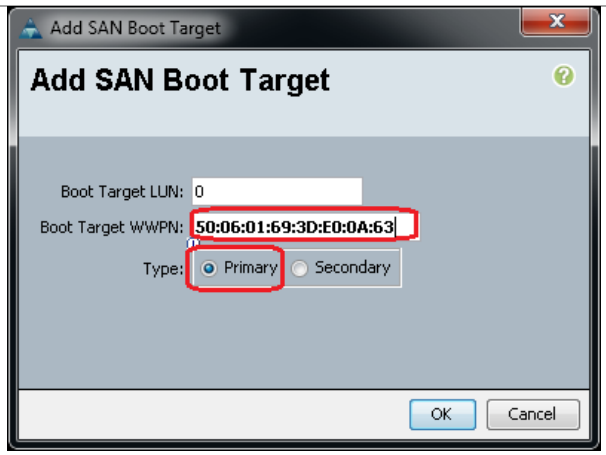
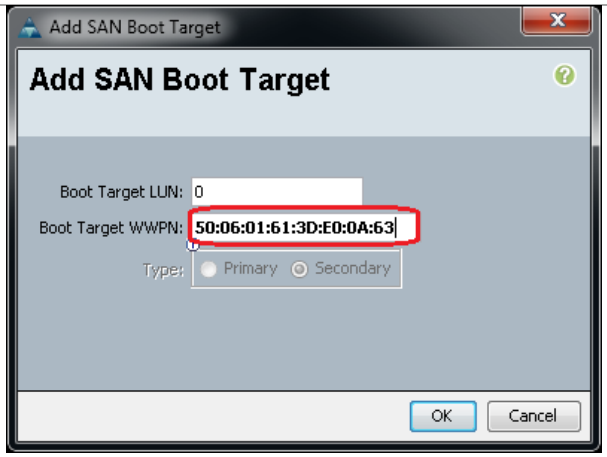
Cisco UCS Manager for Fabric A

Select the **Servers** tab at the top left of the window.
Go to **Policies > root**.
Right-click **Boot Policies**.
Select **Create Boot Policy**.



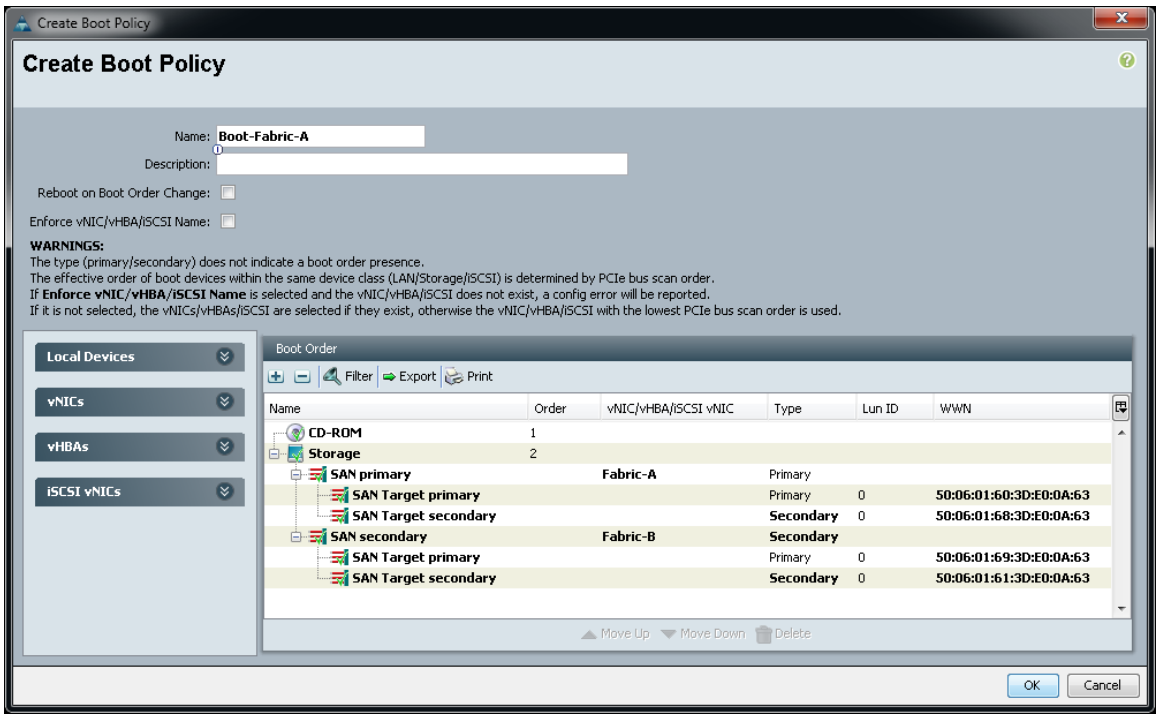
Name the boot policy <Boot-Fabric-A>. (Optional) Give the boot policy a description. Leave **Reboot on Boot Order Change** and **Enforce vNIC/vHBA Name** unchecked. Expand the **Local Devices** drop-down menu and select **Add CD-ROM**. Expand the **vHBAs** drop-down menu and select **Add SAN Boot**.	
Enter <*Fabric-A*> in the **vHBA** field in the **Add SAN Boot** window that displays. Ensure that **Primary** is selected as the **Type**. Click **OK** to add the SAN boot initiator	
Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0.	
Enter the WWPN for the primary FC adapter interface SPA-A2 as the Boot Target WWPN. Keep the **Type** as **Primary**. Click **OK** to add the SAN boot target.	

Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0.	
Enter the WWPN for the primary FC adapter interface SPB-B2 as the Boot Target WWPN. Select the **Type** as **Secondary**; it is the default and cannot be changed on the second entry. Click **OK** to add the SAN boot target.	
Select **Add SAN Boot** under the **vHBA** drop-down menu.	
Enter <*Fabric-B*> in the **vHBA** field in the Add SAN Boot window that displays. The type should automatically be set to **Secondary** and it should be grayed out. This is fine. Click **OK** to add the SAN boot target.	
Select **Add SAN Boot Target** under the **vHBA** drop-down menu.	

The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0. Enter the WWPN for the secondary FC adapter interface SPA-B3 as the Boot Target WWPN. Keep the **Type** as **Primary**. Click **OK** to add the SAN boot target.	
Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0. Enter the WWPN for the secondary FC adapter interface SPB-A3 as the Boot Target WWPN. Select the **Type** as **Secondary**. Click **OK** to add the SAN boot target.	

Verify your configuration looks something like the following:

Figure 5 Boot Policy Example



Cisco UCS Manager for Fabric B

Creating a Boot Policy for Fabric B is similar to creating for Fabric A. You simply change the order of primary and secondary WWNs.

1. Select the **Servers** tab at the top left of the window.
2. Go to **Policies > root**.
3. Right-click **Boot Policies**.
4. Select **Create Boot Policy**.
5. Name the boot policy <***Boot-Fabric-B***>.
6. (Optional) Give the boot policy a description.
7. Leave **Reboot on Boot Order Change and Enforce vNIC/vHBA Name** unchecked.
8. Expand the **Local Devices** drop-down menu and select **Add CD-ROM**.
9. Expand the **vHBAs** drop-down menu and select **Add SAN Boot**.
10. Enter <***Fabric-B***> in the vHBA field in the **Add SAN Boot** window that displays.
11. Ensure that **Primary** is selected as the Type.
12. Click **OK** to add the SAN boot initiator.
13. Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as **0**.
14. Enter the <***WWPN***> for the primary FC adapter interface SPB-B3 as the Boot Target WWPN. Keep the Type as **Primary**.
15. Click **OK** to add the SAN boot target.
16. Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as **0**.

17. Enter the <***WWPN***> for the primary FC adapter interface SPA-A3 as the Boot Target WWPN. Select the Type as **Secondary**.
18. Click **OK** to add the SAN boot target.
19. Select **Add SAN Boot** under the **vHBA** drop-down menu.
20. Enter <***Fabric-A***> in the **vHBA** field in the **Add SAN Boot** window that displays.
21. The type should automatically be set to **Secondary** and it should be grayed out. This is fine.
22. Click **OK** to add the SAN boot target.
23. Select **Add SAN Boot Target** under the **vHBA** drop-down menu.
24. The **Add SAN Boot Target** window displays. Keep the value for Boot Target LUN as **0**.
25. Enter the <***WWPN***> for the secondary FC adapter interface SPA-A2 as the Boot Target WWPN. Keep the Type as **Primary**.
26. Click **OK** to add the SAN boot target.
27. Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as **0**.
28. Enter the <***WWPN***> for the secondary FC adapter interface SPB-B2 as the Boot Target WWPN. Select the Type as **Secondary**.
29. Click **OK** to add the SAN boot target.

Cisco UCS PowerTool

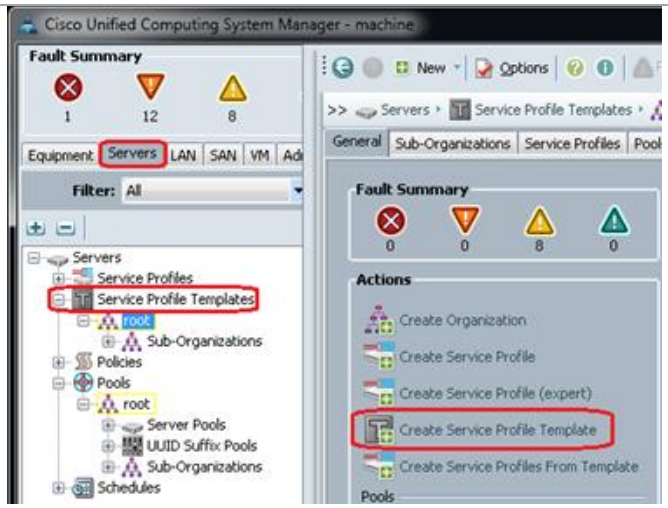
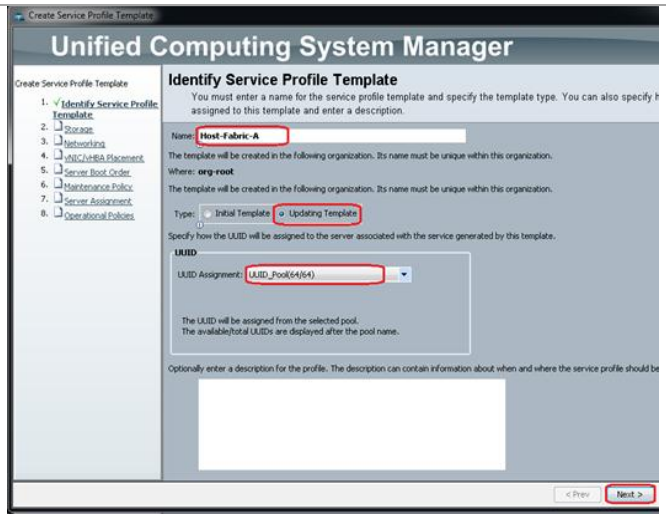
```
$var = Add-UcsBootPolicy –Name <Boot-Fabric-A>
$var | Add-UcsLsbootVirtualMedia –Access read-only –Order 1
$var | Add-UcsLsbootStorage –Order 2
$var | Get-UcsLsbootStorage | Add-UcsLsbootSanImage –Type primary –
VnicName <Fabric-A>
$var | Get-UcsLsbootStorage | Add-UcsLsbootSanImage –Type secondary –
VnicName <Fabric-B>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage –Type primary |
Add-UcsLsbootSanImagePath -Lun 0 -Type primary –Wwn
<50:06:01:60:3D:E0:0A:63>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage –Type primary |
Add-UcsLsbootSanImagePath -Lun 0 -Type secondary –Wwn
<50:06:01:68:3D:E0:0A:63>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage –Type secondary |
Add-UcsLsbootSanImagePath -Lun 0 -Type primary –Wwn
<50:06:01:69:3D:E0:0A:63>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage –Type secondary |
Add-UcsLsbootSanImagePath -Lun 0 -Type secondary –Wwn
<50:06:01:61:3D:E0:0A:63>
$var = Add-UcsBootPolicy –Name <Boot-Fabric-B>
$var | Add-UcsLsbootVirtualMedia –Access read-only –Order 1
$var | Add-UcsLsbootStorage –Order 2
$var | Get-UcsLsbootStorage | Add-UcsLsbootSanImage –Type primary –
VnicName <Fabric-B>
$var | Get-UcsLsbootStorage | Add-UcsLsbootSanImage –Type secondary –
VnicName <Fabric-A>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage –Type primary |
Add-UcsLsbootSanImagePath -Lun 0 -Type primary –Wwn
<50:06:01:69:3D:E0:0A:63>
```

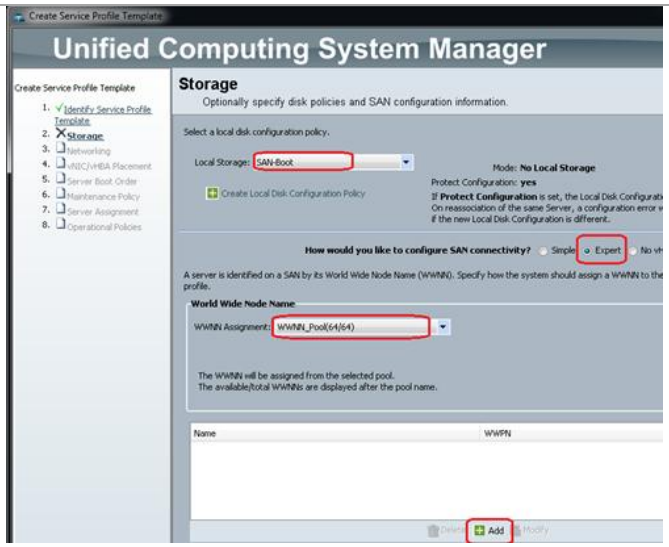
```
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage -Type primary |
Add-UcsLsbootSanImagePath -Lun 0 -Type secondary -Wwn
<50:06:01:61:3D:E0:0A:63>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage -Type secondary |
Add-UcsLsbootSanImagePath -Lun 0 -Type primary -Wwn
<50:06:01:60:3D:E0:0A:63>
$var | Get-UcsLsbootStorage | Get-UcsLsbootSanImage -Type secondary |
Add-UcsLsbootSanImagePath -Lun 0 -Type secondary -Wwn
<50:06:01:68:3D:E0:0A:63>
```

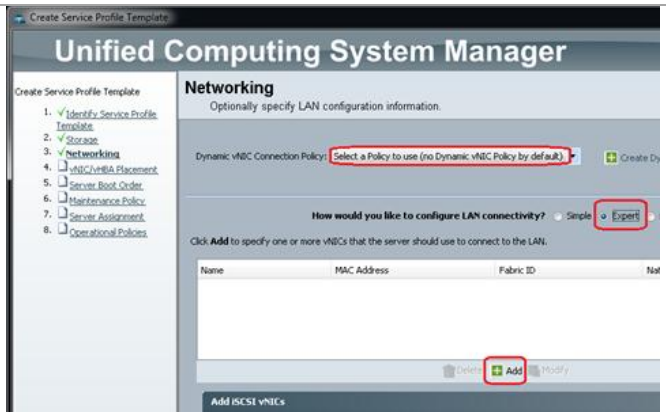
Create Service Profile Templates

This section details the creation of two service profile templates: one for fabric A and one for fabric B.

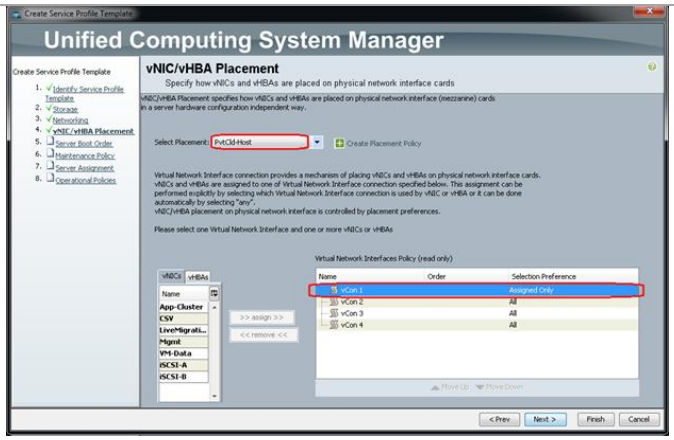
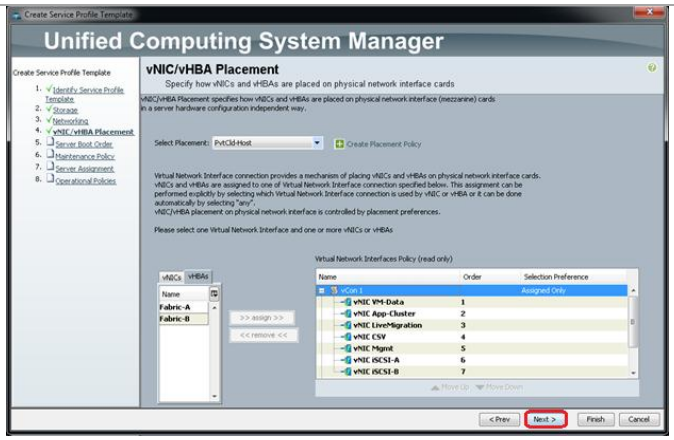
Cisco UCS Manager

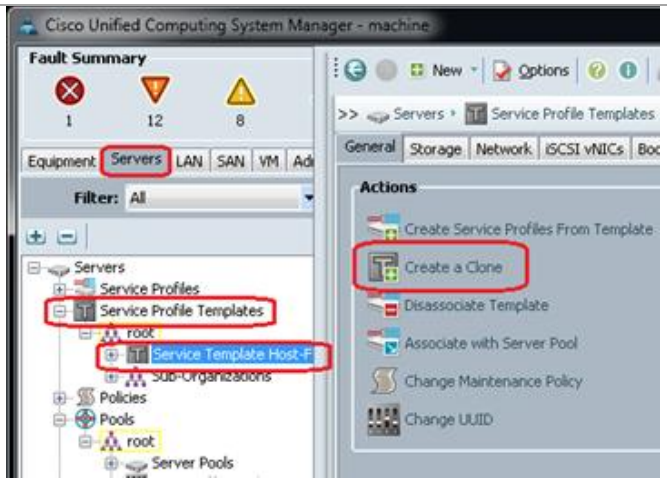
Select the **Servers** tab at the top left of the window. Go to **Service Profile Templates > root**. Right-click **root**. Select **Create Service Profile Template**.	
The **Create Service Profile Template** window displays. **Identify the Service Profile Template** Section. Name the service profile template <Host-Fabric-A>. This service profile template is configured to boot from SPA-A2. Select **Updating Template**. In the UUID section, select <UUID_Pool> as the UUID pool. Click **Next** to continue to the next section.	

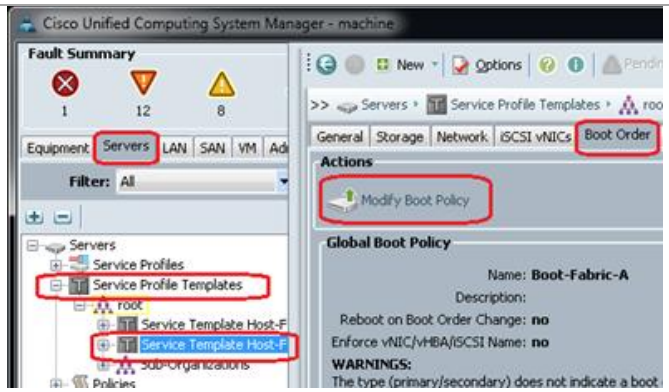
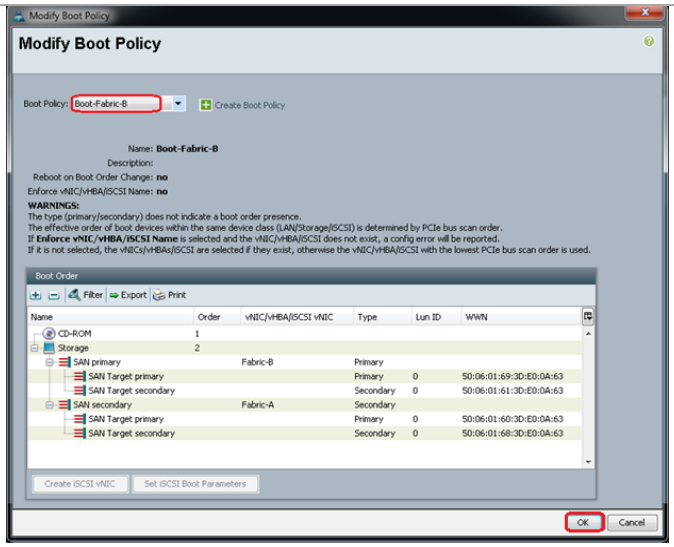
Storage section Select <*SAN-Boot*> for the Local Storage field. Select the **Expert** option for the How would you like to configure SAN connectivity field. In the WWNN Assignment field, select <*WWNN_Pool*>. Click the **Add** button at the bottom of the window to add vHBAs to the template.	
The **Create vHBA** window displays. Name the vHBA <*Fabric-A*>. Check the box for **Use SAN Connectivity Template**. Select <*Fabric-A*> in the **vHBA Template** field. Select Windows in the **Adapter Policy** field. Click **OK** to add the vHBA to the template. This returns you to the **Storage** window.	
Click the **Add** button at the bottom of the window to add vHBAs to the template. The **Create vHBA** window displays. Name the vHBA <*Fabric-B*>. Check the box for **Use SAN Connectivity Template**. Select <Fabric-B> in the **vHBA Template** field. Select **Windows** in the **Adapter Policy** field. Click **OK** to add the vHBA to the template. This returns you to the **Storage** window.	
Verify – Review the table to Ensure that both of the vHBAs were created. Click **Next** to continue to the next section.	

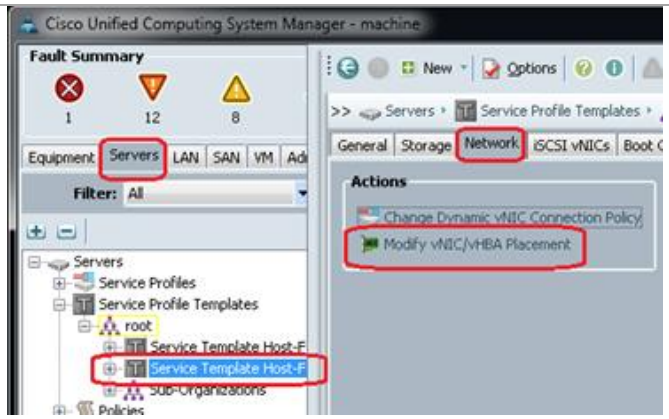
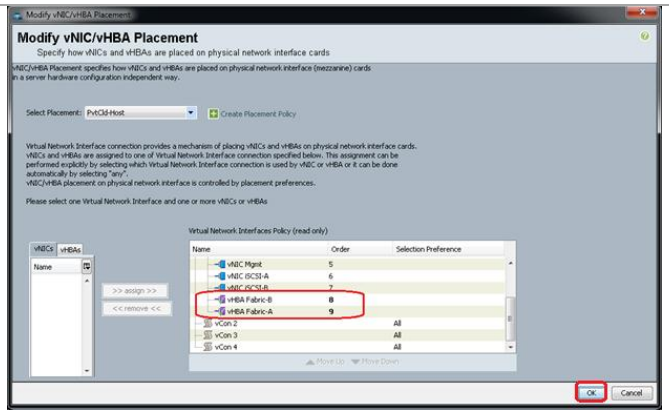
Networking Section Leave the **Dynamic vNIC Connection Policy** field at the default. Select **Expert** for the **How would you like to configure LAN connectivity?** option. Click **Add** to add a vNIC to the template.	
The **Create vNIC** window displays. Name the vNIC <*CSV*>. Check the **Use LAN Connectivity Template** checkbox. Select <*CSV*> for the **vNIC Template** field. Select **Windows** in the **Adapter Policy** field. Click **OK** to add the vNIC to the template. This returns you to the **Networking** window.	
Repeat the above steps for all the desired vNICs. Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*LiveMigration-A*>. Check the **Use LAN Connectivity Template** checkbox. Select <*LiveMigration-A*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*LiveMigration-B*>. Check the **Use LAN Connectivity Template** checkbox. Select <*LiveMigration-B*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	

Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*Mgmt*>. Check the **Use LAN Connectivity Template** checkbox. Select <*Mgmt*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*ClusComm*>. Check the **Use LAN Connectivity Template** checkbox. Select <*ClusComm*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*VMaccess*>. Check the **Use LAN Connectivity Template** checkbox. Select <*VMaccess*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*iSCSI-A*> (and/or SMB-A). Check the **Use LAN Connectivity Template** checkbox. Select <*iSCSI-A*> (and/or SMB-A) for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*iSCSI-B*> (and/or SMB-B). Check the **Use LAN Connectivity Template** checkbox. Select <*iSCSI-B*> (and/or SMB-B) for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Click **Add** to add a vNIC to the template. The **Create vNIC** window displays. Name the vNIC <*VEM*>. Check the **Use LAN Connectivity Template** checkbox. Select <*VEM*> for the **vNIC Template** field. Select **Windows** in the Adapter Policy field. Click **OK** to add the vNIC to the template.	
Verify: Review the table to ensure that all of the vNICs were created. Click **Next** to continue to the next section.	

vNIC/vHBA Placement Section Select the <PvtCld-Host> placement policy in the **Select Placement** field. Select vCon1 and assign the vNICs in the following order: VMaccess ClusComm LiveMigration CSV Mgmt iSCSI-A iSCSI-B	
Click the **vHBA** tab and add the vHBAs in the following order: Fabric-A Fabric-B **Verify**: Review the table to ensure all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not important. Click **Next** to move to the next section.	
Server Boot Order Section Select <*Boot-Fabric-A*> in the **Boot Policy** field. **Verify**: Review the table to ensure all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence. Click **Next** to continue to the next section.	

Maintenance Policy Section • Keep the default of no policy used by default. • Click **Next** to continue to the next section. **Server Assignment** Section • Select <*Server-Pool*> in the **Pool Assignment** field. • Select <*PvtCld-Host*> for the **Server Pool Qualification** field. • Select **Up** for the power state. • Select <*PvtCld-Host*> in the **Host Firmware** field. • Select <*PvtCld-Host*> in the **Management Firmware** field. • Click **Next** to continue to the next section. **Operational Policies** Section • Select <*PvtCld-Host*> in the **BIOS Policy** field. • Expand **Power Control Policy Configuration**. • Select <*No-Cap*> in the **Power Control Policy** field. • Expand **Scrub Policy**. • Select <*No-Scrub*> in the **Scrub Policy** field. Click **Finish** to create the Service Profile template. Click **OK** in the pop-up window to proceed.	
Select the **Servers** tab at the top left of the window. Go to **Service Profile Templates > root**. Select the previously created <Host-Fabric-A> template Click **Create a Clone**.	

Enter <*Host-Fabric-B*> in the **Clone Name** field and click **OK**.	
Select the newly created service profile template and select the **Boot Order** tab. Click **Modify Boot Policy**.	
Select <*Boot-Fabric-B*> as the **Boot Policy** and click **OK**.	

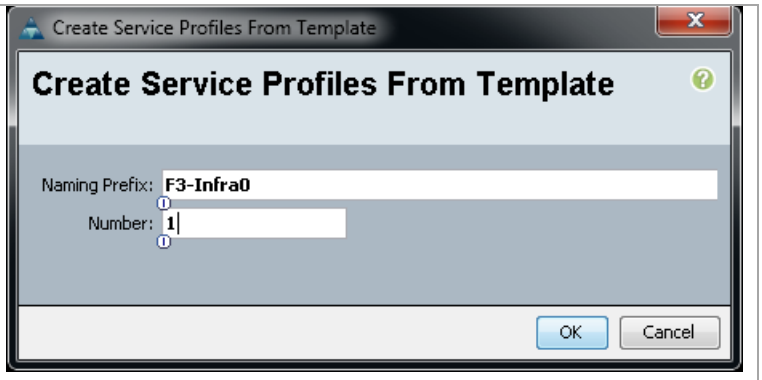
Select the **Network** tab and click **Modify vNIC/HBA Placement Policy**.	
Move <*vHBA Fabric-B*> ahead of <*vHBA Fabric-A*> in the placement order and click **OK**.	

Create Service Profiles

These steps provide details for creating two service profiles from a template. One service profile will boot from fabric A and the other will boot from fabric B.

Cisco UCS Manager

Select the **Servers** tab at the top left of the window. Select **Service Profile Templates** <*Host-Fabric-A*> Right-click and select C**reate Service Profile From Template**.	

Enter <F3-Infra0> for the **Naming Prefix**. Enter **1** for the **Number** of service profiles to create. Click **OK** to create the service profile. Click **OK** in the message box.	
Select **Service Profile Templates** <*Host-Fabric-B*> Right-click and select **Create Service Profile From Template**. Enter <*F3-Infra0*> for the **Naming Prefix**. Enter **1** for the **Number** of service profiles to create. Click **OK** to create the service profile. Click **OK** in the message box. Verify that Service Profiles <*F3-Infra01*> and <*F3-Infra02*> are created. The service profiles will automatically be associated with the servers in their assigned server pools. This procedure can be followed to create as many Service Profiles as you have blades installed.	

5 EMC VNX5500 Deployment: Part 2

5.1 Create VNX LUNs for Private Cloud Environment

The Private cloud environment implements a boot from SAN environment, using the concept of a Master Boot LUN. The Master Boot LUN is a storage area that will be used to maintain an image of a Windows Server 2012 image to be used as a Clone source. This image should be configured as a base image to be used for subsequent installations, so all patching and custom configuration steps should be taken. For example, maybe a desired configuration setting is to ensure that all physical servers are able to be remotely managed. Once the image is configured according to customer policy, the Microsoft sysprep utility can be run against this image to prepare it for use as a Clone. Ensure the Microsoft hotfixes listed in the software revision table have been applied before running sysprep.

Clones created from the Master Boot LUN will be presented to the physical servers defined by Service Profiles in the UCS environment. This style of deployment allows Service Profiles to be fully transportable between different physical blades as the boot device is external to the chassis, and also allows for multiple Master Boot images to be implemented providing support for different operating system versions or configurations which may need to be implemented over time.

Management of the boot LUN requires special consideration, and needs to ensure that the LUN ID provided to the LUN, as seen from the host is set to 0 (zero). The ESI (EMC Storage Integrator) PowerShell commands do not allow the manipulation of the LUN ID for devices presented to servers, and simply default to the sequential allocation of LUN IDs as implemented by the VNX array. As a result of this behavior, the boot LUN must be the first device that is mapped to the server (UCS

service profile). If this is incorrectly implemented, then the wrong target will be selected for Windows boot operations on server power-up.

As described, the ESI PowerShell commands are utilized for provisioning of the LUNs required within the environment, and assume that the storage pool creation outlined in the previous section have been completed. For this procedure, a single LUN is created, and is used to install a Windows Server 2012 instance. This server instance subsequently will be processed with Windows sysprep, and be removed from the server. All compute nodes will then use a Clone of the sysprep image, and will be customized as individual server instances.

Creation of all necessary LUNs within the Private Cloud environment can be executed with the PowerShell script ProcessStorageRequests.ps1 provided Appendix B. The defined XML configuration file is read by the PowerShell script. This XML configuration file contains five parameter. There are two classes that can be repeated multiple times. The XML class <luns> can be repeated multiple times to define multiple LUNs for a server. The <Server> class can be repeated to create multiple server records.

For the purpose of defining and creating the Master Boot LUN, it is recommended to create a unique XML configuration file that defines only this specific device. Later the format of the XML configuration file can be followed for creating multiple LUNs.

- <label> - the name that will be assigned to the LUN that is created
- <pool> - the storage pool from which the LUN will be created
- <size> - the size of the LUN (in GB) to be created
- <ServerName> - the name of the server that will be assigned the LUN that must match the Service Profile name in UCS Manager, including case. This name is also used for management purposes on the VNX array
- <IPAddress> - the management IP address of the server

In addition to the five parameters listed above that can be repeated, there are two other parameters that are defined only once. The <Array> parameter is the name of the VNX array. The <UCSAddress> parameter is the IP address for accessing the UCS management console. An example of the contents of a configuration are shown below for a configuration file called "CFG_STORAGE_LUNS.xml".

```
<StorageParams>
<Servers>
  <Server>
    <ServerName>F3-Infra01</ServerName>
    <IPAddress>10.29.130.21</IPAddress>
      <luns>
        <label>MASTER-BOOT-2012</label>
         <pool>PVTCLD_DATA1_R5</pool>
         <size>60GB</size>
      </luns>
  </Server>
</Servers>
<Array>EnterpriseFastTrack</Array>
<UCSAddress>10.5.177.10</UCSAddress>
</StorageParams>
```

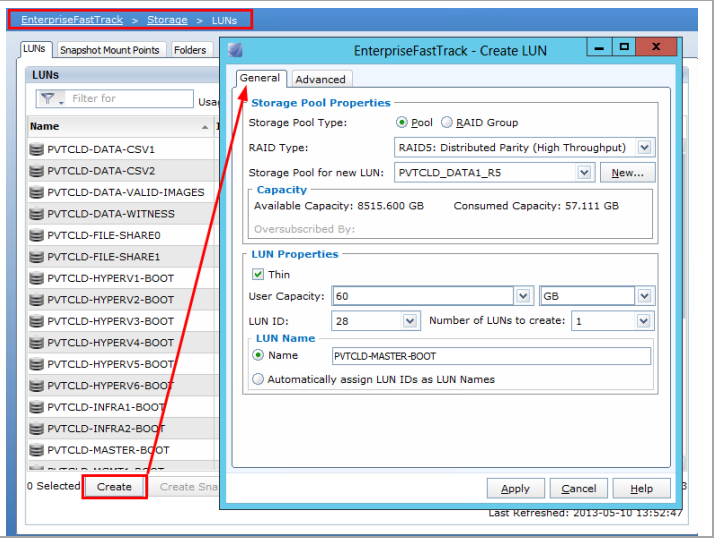
This configuration file is read by the ProcessStorageRequests.ps1 PowerShell script to result in a LUN named Master-Boot-2012 of size 60 GB being created in the storage pool called PVTCLD_DATA. The execution of such a process is shown in the following figure.

Figure 6 Example Execution of Master Boot LUN Creation

```
PS C:\> C:\Users\fulladmin\Desktop\ProcessStorageRequests.ps1
System '[Name = EnterpriseFastTrack. UserFriendlyName = VNXFT]' has been updated successfully.
Creating LUN MASTER-BOOT-2012
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed

PS C:\>
```

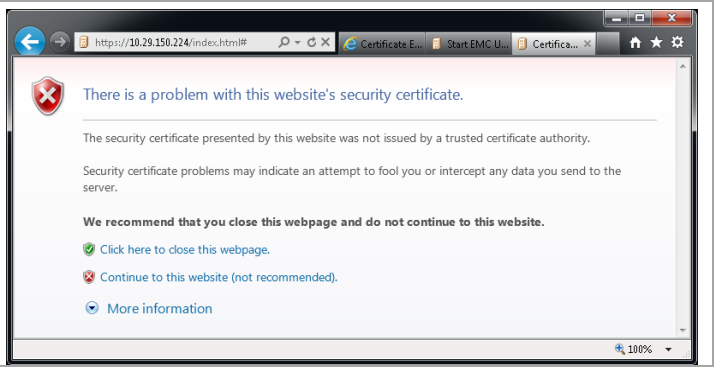
Unisphere can also be used for the purposes of creating LUNs for the boot from SAN deployment.

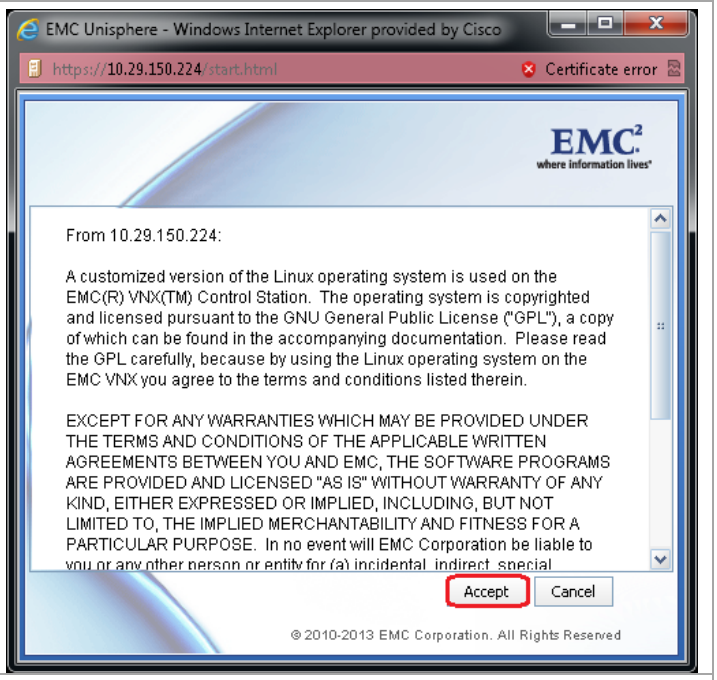
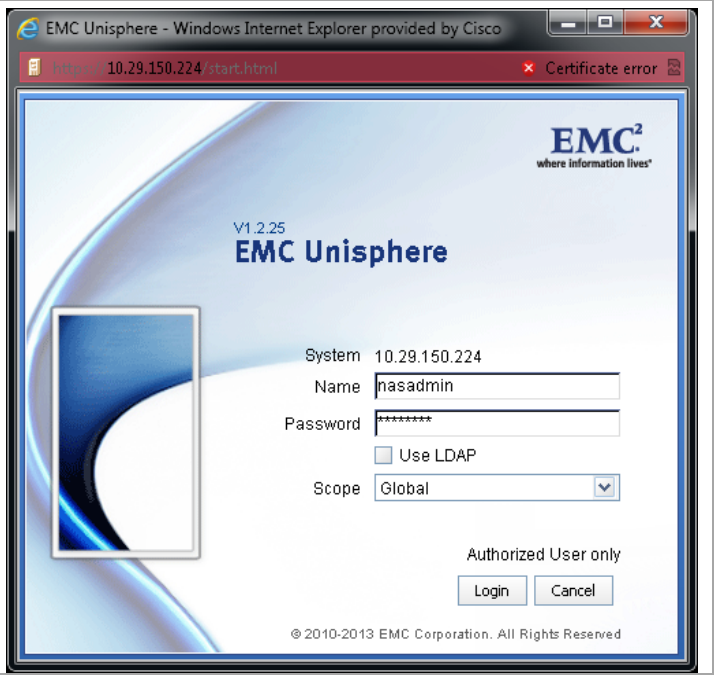
From the Storage > LUNs menu, select **Create** and create the LUN.	

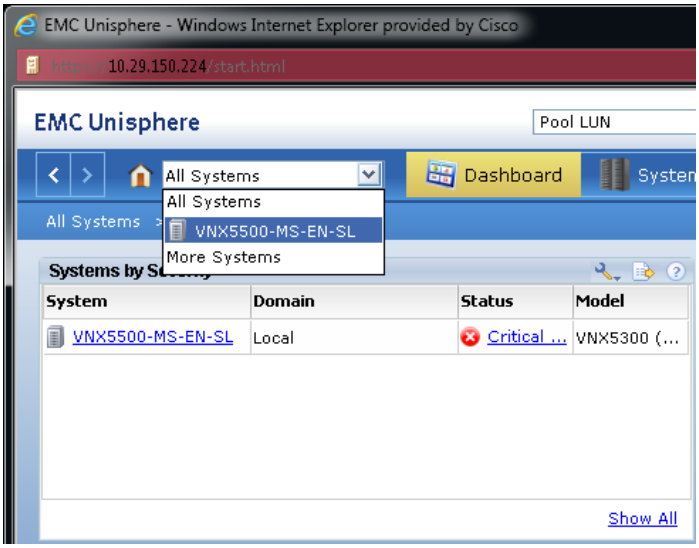
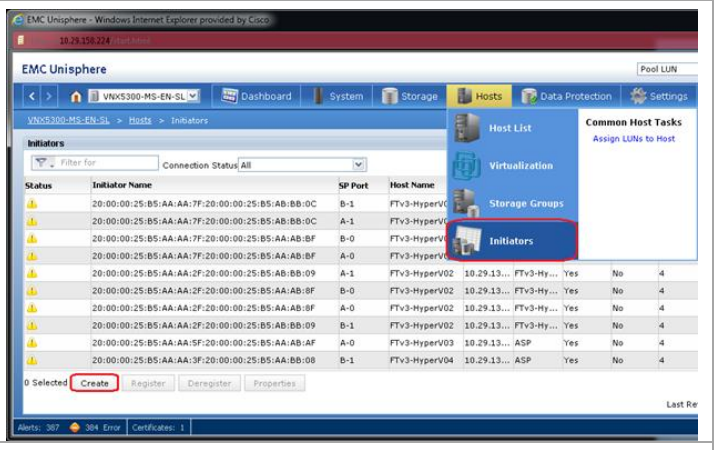
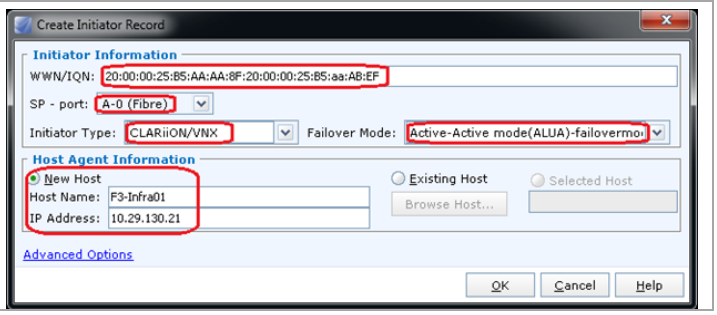
After creation of the required LUN, it is necessary to present the LUN to the Service Profile. The example PowerShell script found in Appendix B, PrepMasterBoot_AddViaWWPN.ps1, utilizes both EMC Storage Integrator and the UCS PowerTool, and expects that both have been successfully installed. After presentation of the LUN to the WWPNs defined within the Service Profile, it will be possible to proceed with Windows Server installation.

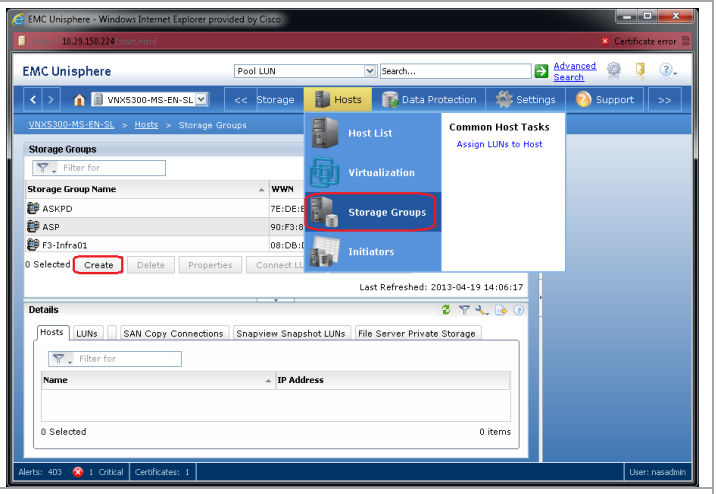
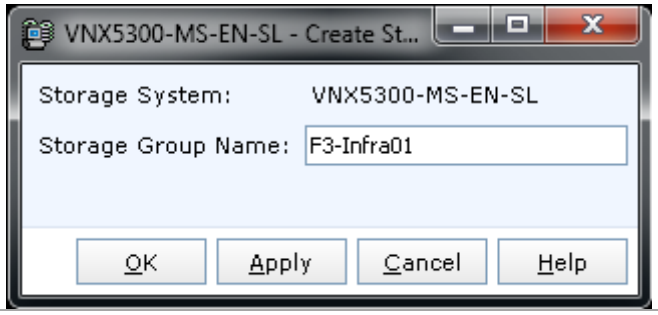
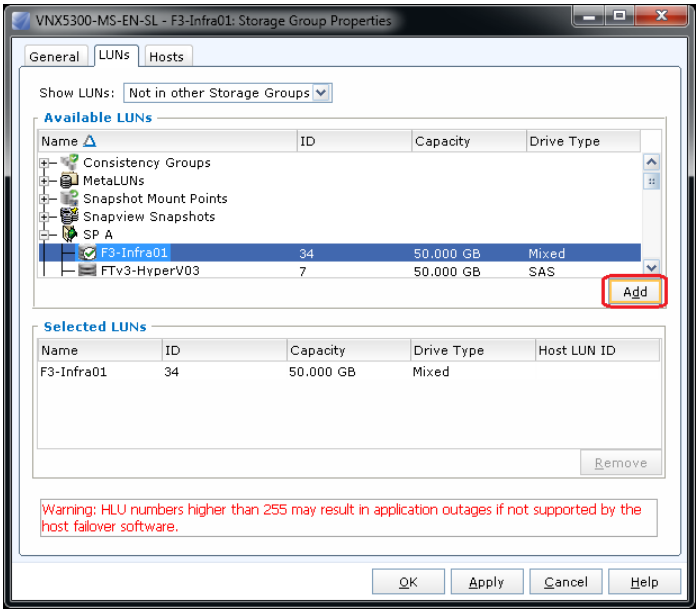
An alternative to using ESI PowerShell would be to manually present storage using Unisphere as in the following example.

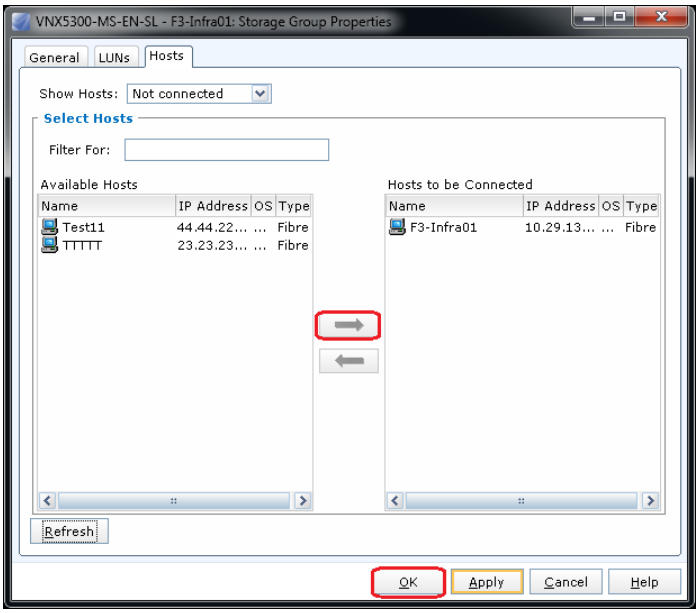
Mask Boot LUN with EMC Unisphere

Open your browser. Enter the IP address of your EMC VNX5500 SAN with an **https://** prefix. Click on Continue to this website (not recommended).	

Click on **Accept** to accept EMC's licensing agreement.	
Enter the **Name** and **Password** for your installation.	

From the drop-down, select your EMC VNX5500 SAN.	
Select **Initiators** from the **Hosts** tab. Select **Create** to create a host initiator for accessing the boot LUN.	
Enter the host's WWNN and WWPN in the **WWN/IQN** field. Select the A0 port in the **SP-port** drop-down list. Select CLARiiON/VNX from the **Initiator Type** drop-down list. Ensure that **Failover Mode** is ALUA. Select the radio button for **New Host**. Enter your **Host Name** and its **IP Address**. Click **OK**.	

Select **Storage Groups** from the Hosts tab. Click on **Create**.	
Enter a name for a storage group to be assigned to this server in the **Storage Group Name** field.	
On the LUNs tab, select the boot LUN that was created for this server. Click **Add** and an entry will appear in the Selected LUNs section of the screen.	

Select the **Hosts** tab. Select the initiator record you created earlier for this server. Click on the right-pointing arrow to move it to the **Hosts to be Connected** column. Click **OK**.	

5.2 Cisco Nexus 5548 Switch: Configure for SAN Boot

These steps detail the procedure for configuring the UCS environment to boot the blade servers from the EMC VNX5500 SAN.

Gather Necessary Information

After the Cisco UCS service profiles have been created (earlier section), each infrastructure management blade has a unique configuration. To proceed with the deployment, specific inforzmation must be gathered from each Cisco UCS blade to enable SAN booting. Insert the required information in the following table. WWPNs from the EMC VNX5500 needed for this configuration were obtained in the Create Boot Policies step. Both WWNN and WWPN from the UCS service profiles are needed for masking the LUNs on the VNX5500 SAN.

Table 16 WWPN for Hyper-V Host Servers

Device	Port	WWPN	WWNN
F3-Infra01	Fabric A		
F3-Infra01	Fabric B		
F3-Infra02	Fabric A		
F3-Infra02	Fabric B		
Repeat for all profiles	…		

Create Device Aliases and Create Zone for First Server

These steps provide details for configuring device aliases for all devices on both Nexus A and Nexus B. It also creates a zone for the primary boot path for the first server that will be installed and used for creating a 'gold image'. The initial zoning provides a single path to the SAN. If more than one path is defined to the boot volume, and there is no multipath software available, as is the case for an initial installation of Windows Server 2012, data corruption can occur on the disk. After the

operating system is installed and configured for MPIO, the secondary boot path can be defined. This configuration assumes the use of the default VSAN 1.

Cisco Nexus 5548 A

1. From the global configuration mode, type **device-alias database**
2. Type **device-alias name** <***F3-Infra01-A***> **pwwn** <***F3-Infra01 Fabric-A WWPN***>
3. Type **device-alias name** <***VNX5500-SPA-A0***> **pwwn** <***SPA-A0 WWPN***>
4. Type **device-alias name** <***VNX5500-SPB-B0***> **pwwn** <***SPB-B0 WWPN***>
5. Type **device-alias commit**
6. Type **zone name** <***F3-Infra01***> **vsan 1**
7. Type **member device-alias** <***F3-Infra01-A***>
8. Type **member device-alias** <***VNX5500-SPA-A0***>
9. Type **exit**
10. Type **zoneset name** <***PvtCld***> **vsan 1**
11. Type **member** <***F3-Infra01***>
12. Type **exit.**
13. Type **zoneset activate name** <***PvtCld***> **vsan 1**
14. The Nexus should respond with "Zoneset activation initiated. Check zone status."
15. Type **copy run start**

Cisco Nexus 5548 B

1. Create the device-alias database on Nexus B at this time. Later in the process the zones and zoneset for Nexus B will be created will be created
2. From the global configuration mode, type **device-alias database**
3. Type **device-alias name** <***F3-Infra01-B***> **pwwn** <***F3-Infra01 Fabric-B WWPN***>
4. Type **device-alias name** <***VNX5500-SPA-A1***> **pwwn** <***SPA-A1 WWPN***>
5. Type **device-alias name** <***VNX5500-SPB-B1***> **pwwn** <***SPB-B1 WWPN***>
6. Type **device-alias commit**
7. Type **zoneset name** <***PvtCld***> **vsan 1**
8. Type **exit**
9. Type **copy run start**

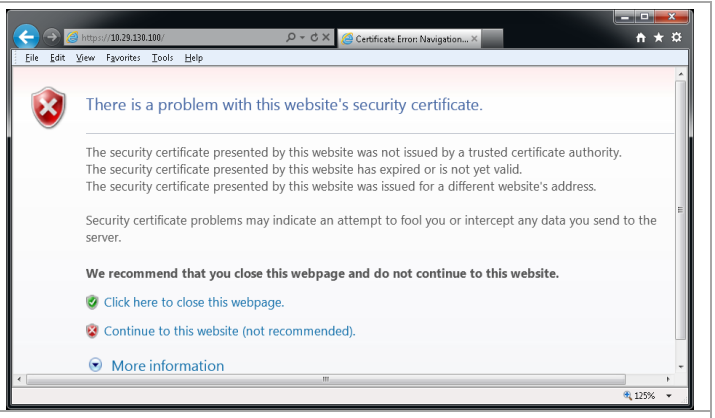
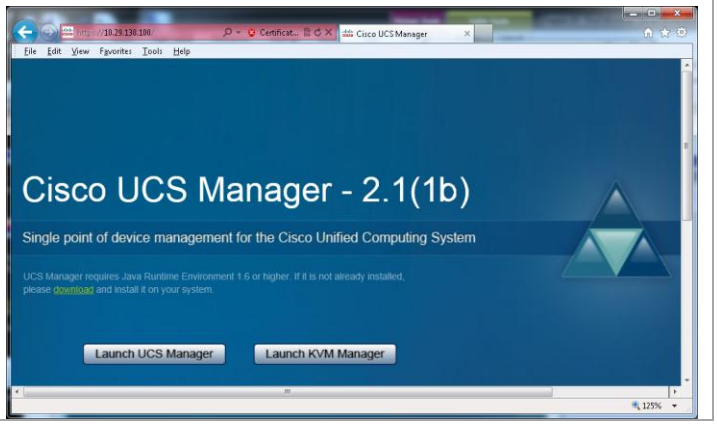
6 First Installation Windows Server 2012 Datacenter Edition

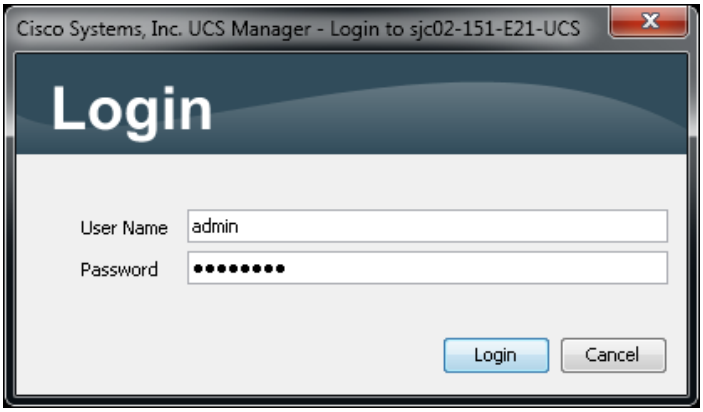
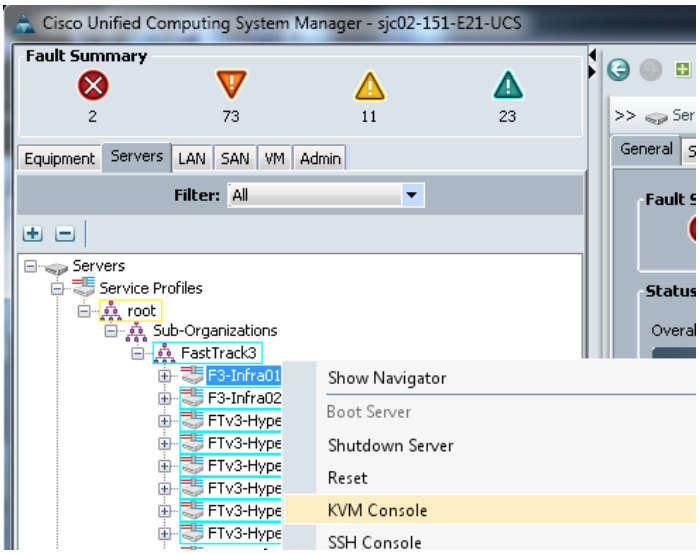
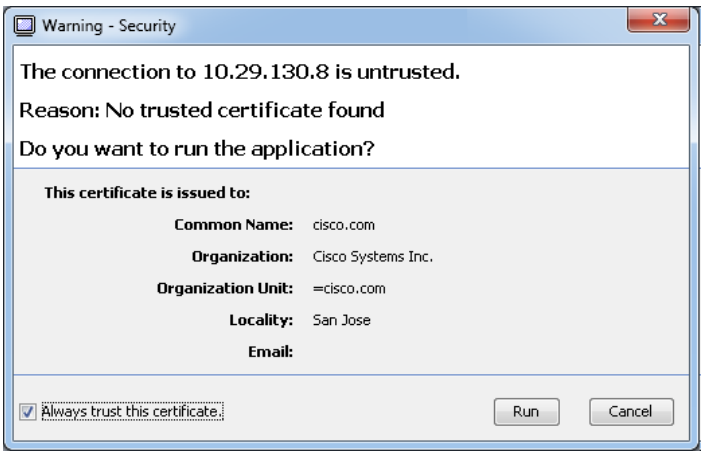
These steps provide the details necessary to prepare the host for the installation of Windows Server 2012 Datacenter Edition. It assumes that the SAN has been zoned and the VNX5500 has masked the LUN so that only a single path to server is available.

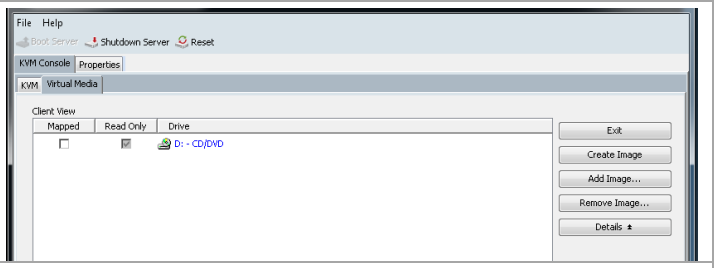
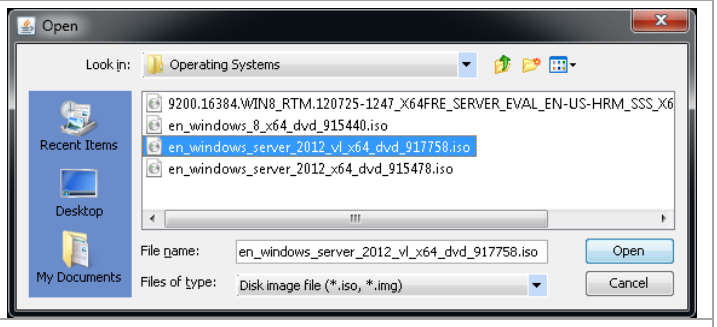
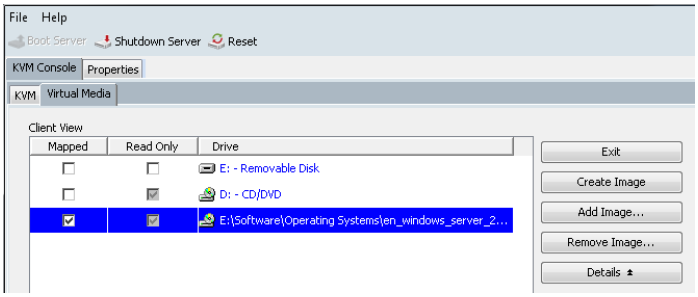
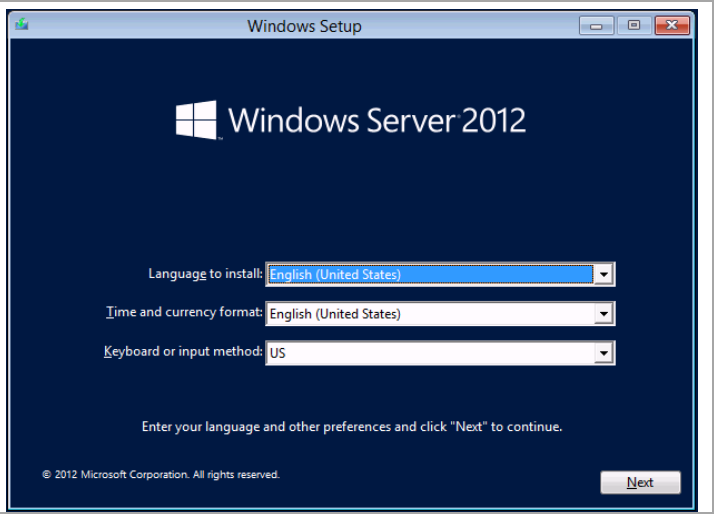
To speed the process of installing Windows Server 2012 across all the physical hosts, a multiple step process is employed.

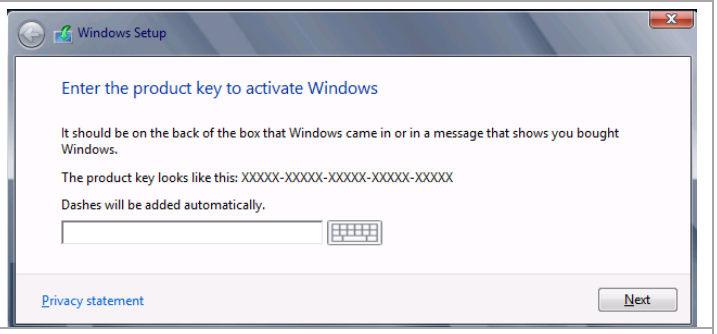
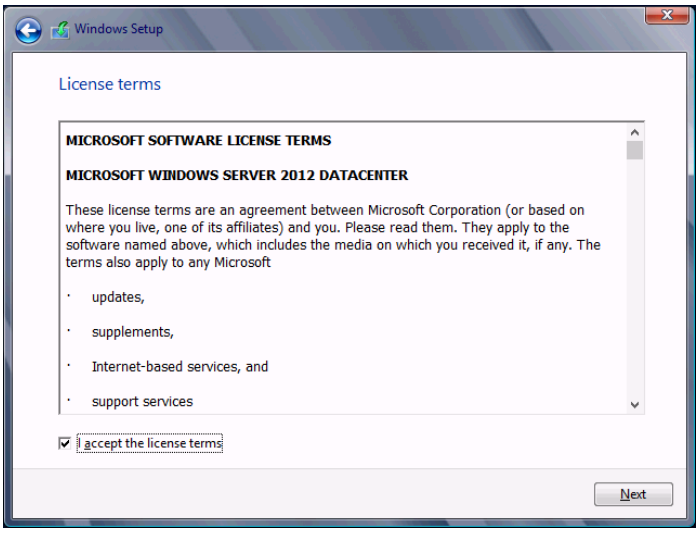
- Install Windows Server 2012 on a single physical server with the boot volume on the EMC VNX5500.
- Perform some initial configuration tasks that are common for all servers used in the private cloud.
- Update the installation with the latest patches from Microsoft Update.
- Install specific hotfixes from Microsoft for some issues that are not fixed by Microsoft Update.
- Present the boot LUN to both vHBAs and configure MPIO.
- Sysprep the image.
- Remove the boot volume from the server on which it was installed.
- Make clones of the sysprepped volume within the EMC VNX5500 so each physical server will have its own clone to boot from.
- Configure zoning and masking for other servers.
- Start each host and complete the mini-setup to tailor each node with things like name, IP addressing (if fixed IP addresses are used), and join to the domain. (It is possible to configure this sort of information with unattend command files. That is beyond the scope of this document, and many shops already have such procedures in place.)

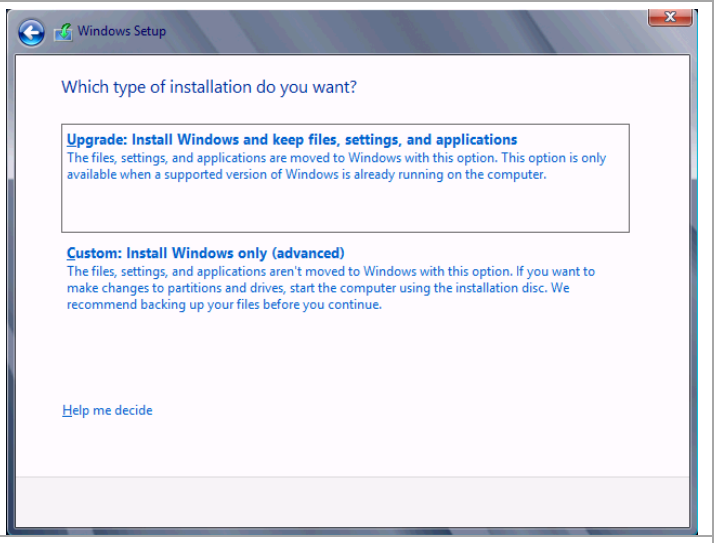
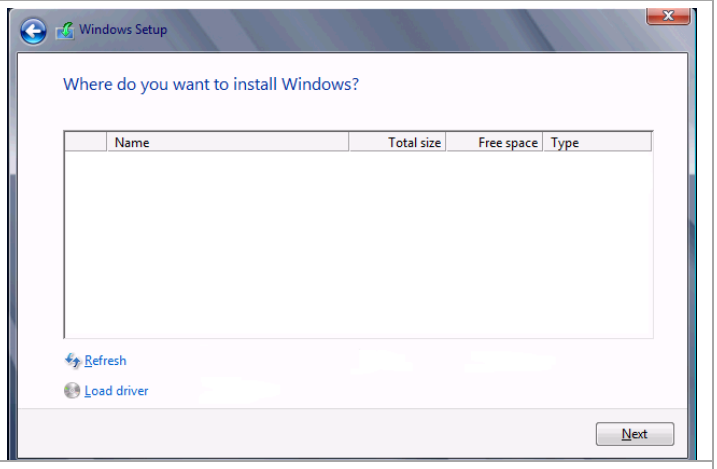
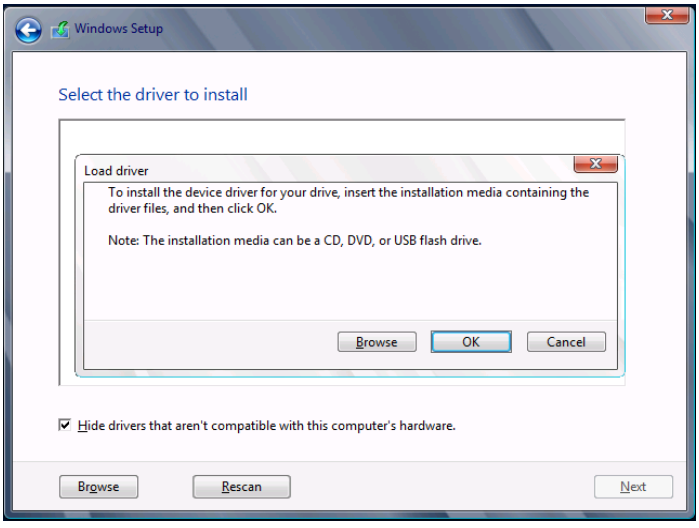
Note: In order for the Windows Installer to recognize the Fibre Channel SAN boot disk for the initial server, the Cisco UCS fnic (storage) driver must be loaded into the Windows installer during installation. Download the latest Unified Computing System (UCS) drivers from www.cisco.com under Cisco UCS B-Series Blade Server Software and place the ISO on the same machine with the Windows Server 2012 DVD ISO.

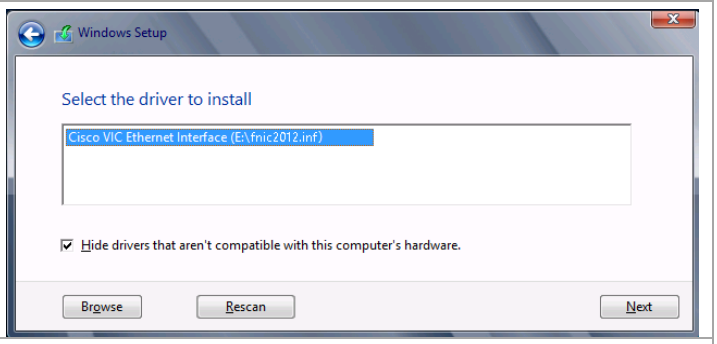
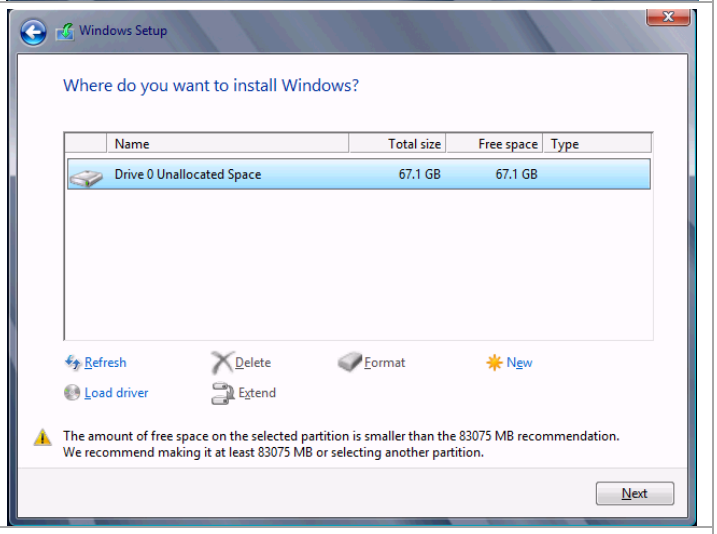
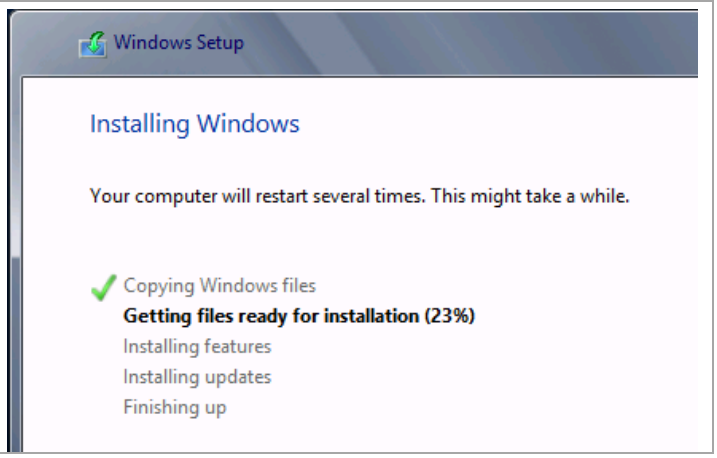
Open your browser. Enter the IP address of your fabric interconnect cluster with an **https://** prefix. Click on Continue to this website (not recommended).	
Click Launch UCS Manager.	

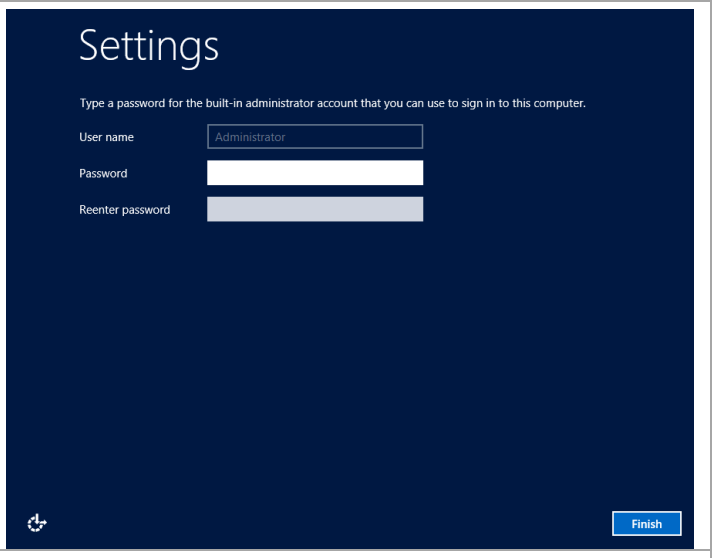
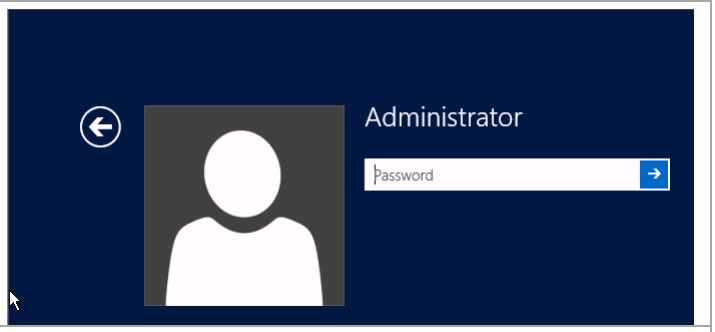
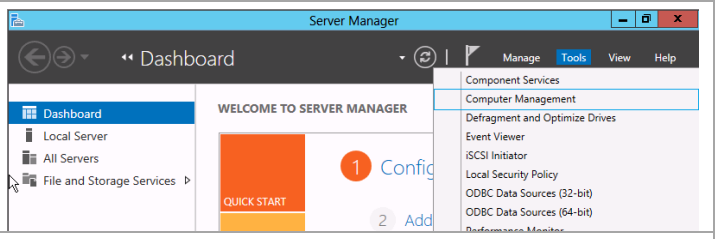
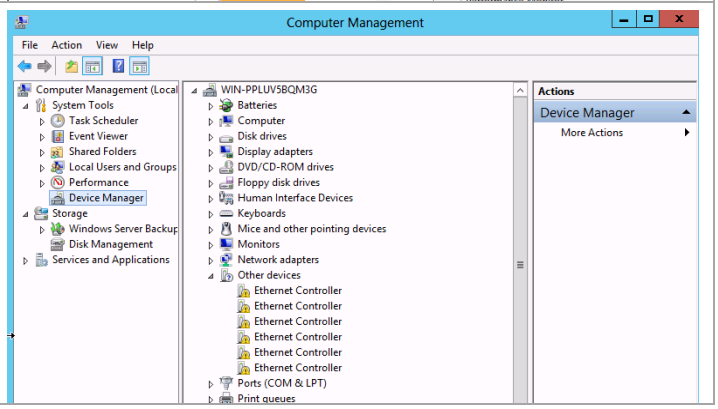
Enter **admin** as the user name. Enter the password specified in the initial setup.	
Select the **Servers** tab. Navigate the tree Servers > Service Profiles > root > F3-Infra01. Right-click **F3-Infra01** and select **KVM Console**.	
You are likely to get a warning due to lack of certificates. Click the Always trust this certificate check box. Click **Run**.	

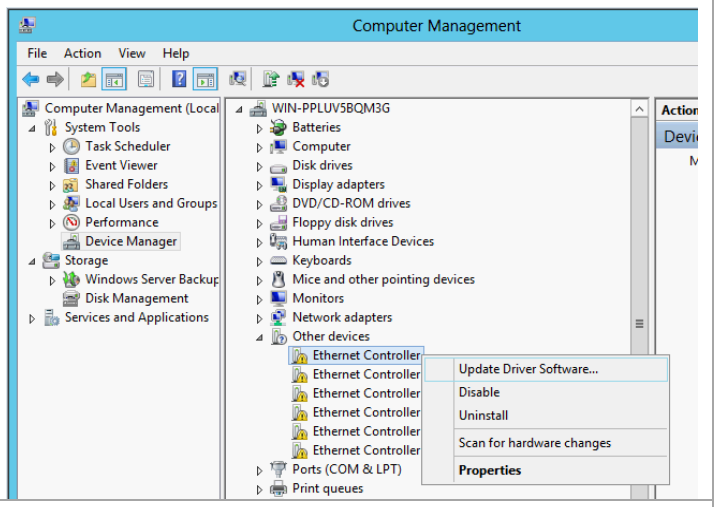
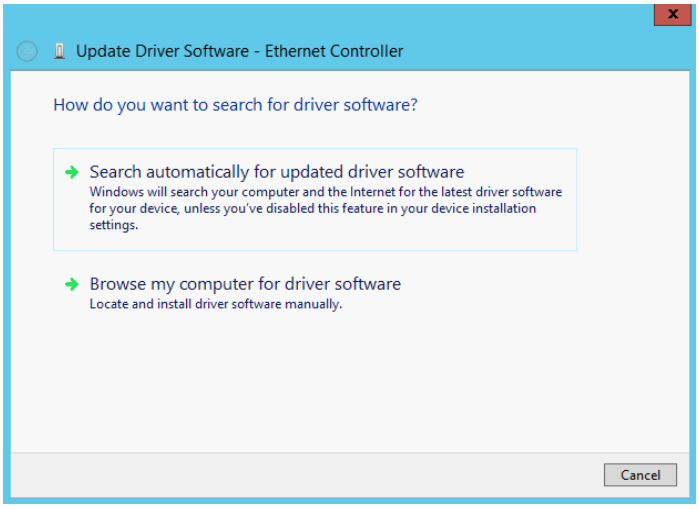
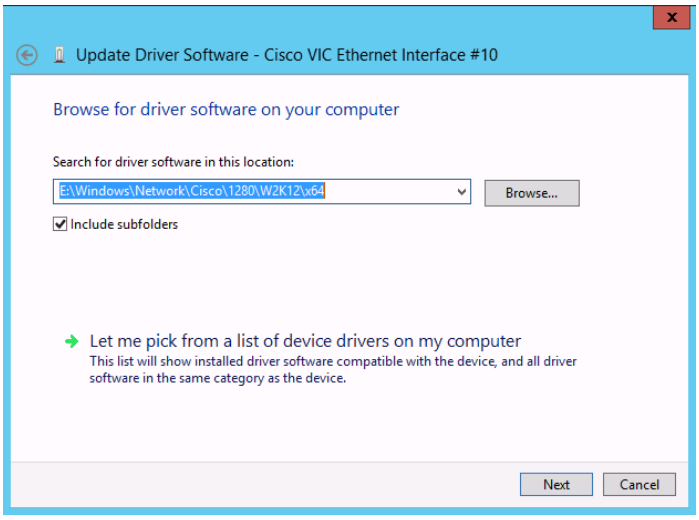
Click on the **Virtual Media** tab of the KVM console. Then click the **Add Image…** button on the right.	
Browse to the location on your configuration workstation where you have stored a copy of the Windows Server 2012 installation media. Click **Open**.	
Click the **Mapped** box in the Virtual Media window. Repeat the process to load an .img or .iso file containing the 1280 VIC drivers, except do not click the Mapped box. Click the KVM tab to return to the KVM window. Click Reset to cause the server to boot to the installation media. The installation will start.	
Select the appropriate localization features. Click **Next**. On next screen, click **Install Now**.	

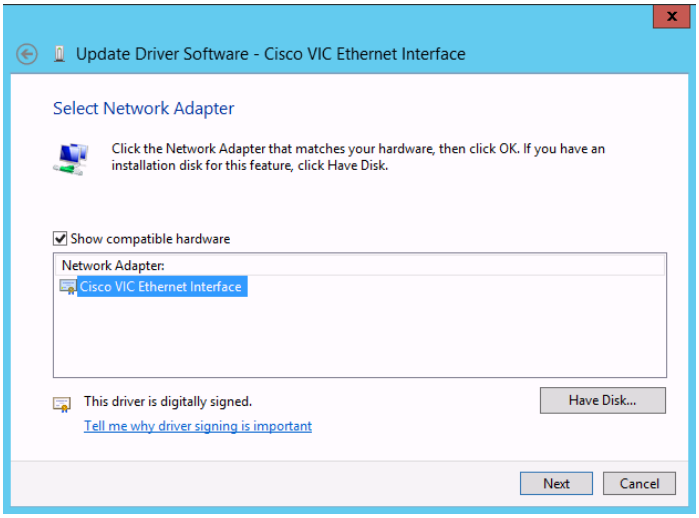
Depending upon the distribution you are using, you may or may not see this window. If you are using a Retail copy, you will see this window. If you are using a volume license copy, you will not see this window. If you are using a Retail copy, enter the 25-character key that came with your software.	
Select the Windows Server 2012 Datacenter (Server with a GUI) option. Click **Next**.	
Click the check box to accept the license terms. Click **Next**.	

Click on **Custom: Install Windows only (advanced)**	
You will not see any disks because the 1280 drivers are not included as part of the Windows Server 2012 installation media. You will have to manually load them. Click **Load driver**.	
Click on the **Virtual Media** tab of the KVM, uncheck the box for the Windows media and check the box for the driver media. You will receive a warning about disconnecting in this manner instead of gracefully dismounting in the operating system. Dismount anyway. Switch back to the **KVM** tab. Click the **Browse** button to browse to the virtual media containing your Cisco UCS 1280 drivers and install the storage driver for the 1280.	

Click **Next** to install the driver. Repeat these steps for loading the NIC drivers. If you do not load the NIC drivers at this time, you will need to do it after the system has been installed.	
When the driver installation is complete, you will be returned to this window. You may have to click **Refresh** to get the storage to show. Return to the **Virtual Media** tab and swap the media back to the Windows distribution. Ignore the size warning at the bottom of the window. Click **Next**.	
Windows will now proceed through its initial setup. As noted, Windows will reboot during this process. You may see a message to **Press any key to boot from CD or DVD ....** Do not enter any key as it will start the installation process from the beginning again. (You can ensure this message does not appear by removing the Windows Server 2012 virtual media.)	

Enter password for local administrator account. Re-enter password to validate.	
Login to the new machine.	
If you did not load the NIC drivers during the installation process, follow these steps to load them now. Start the Computer Management tool by clicking the **Tools** menu and selecting **Computer Management**.	
Click on **Device Manager**. Expand **Other** Devices. You now have to update the driver for each of the other networks defined on the host. Ensure that you have selected the Cisco UCS driver image in the Virtual Media tab of the KVM.	

Right-click on the first Ethernet Controller that shows in the Other Devices section. Select **Update Driver Software…**.	
Select **Browse my computer for driver software**.	
Browse to your virtual media that contains the Cisco drivers. Click **Next**.	

Click on the Cisco VIC Ethernet Interface. Click **Next** to continue. Click **Close** in the next window. Repeat process for all Ethernet Controller entries within Other devices.	

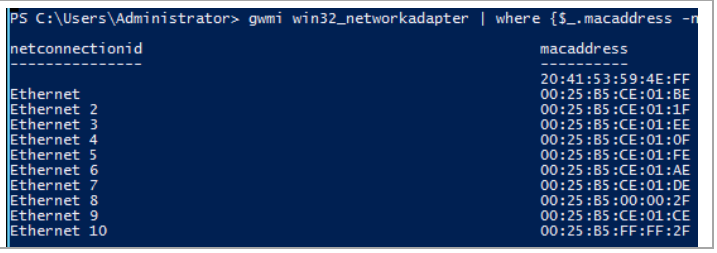
6.1 Local Configuration Tasks

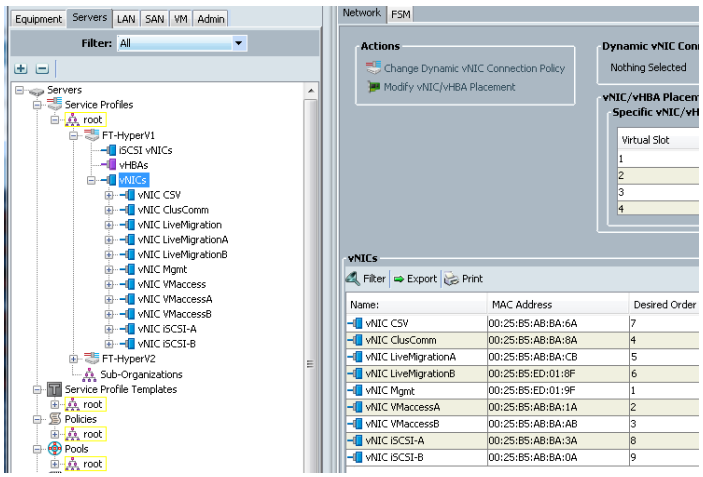
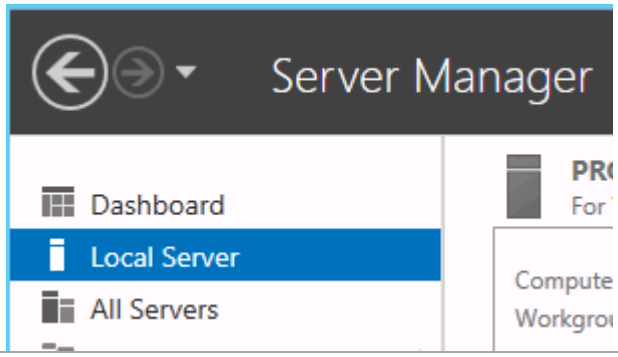
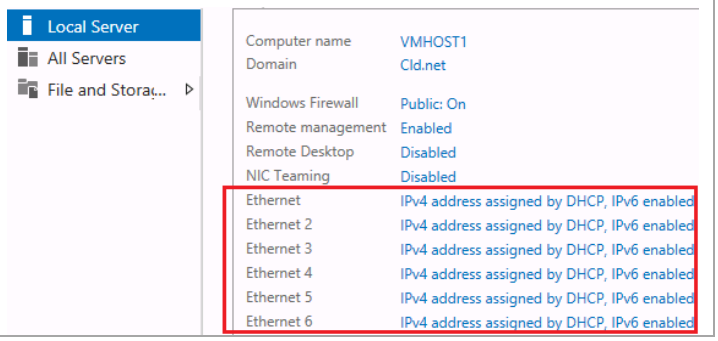
At this point, if you have a DHCP server installed on your Management Network, the Management Network Interface should come up with an IP address. If you do not have DHCP, use the following steps to determine which Network Interface is on the Management VLAN and configure it with a static IP with connection to the outside world.

Initial Network Configuration

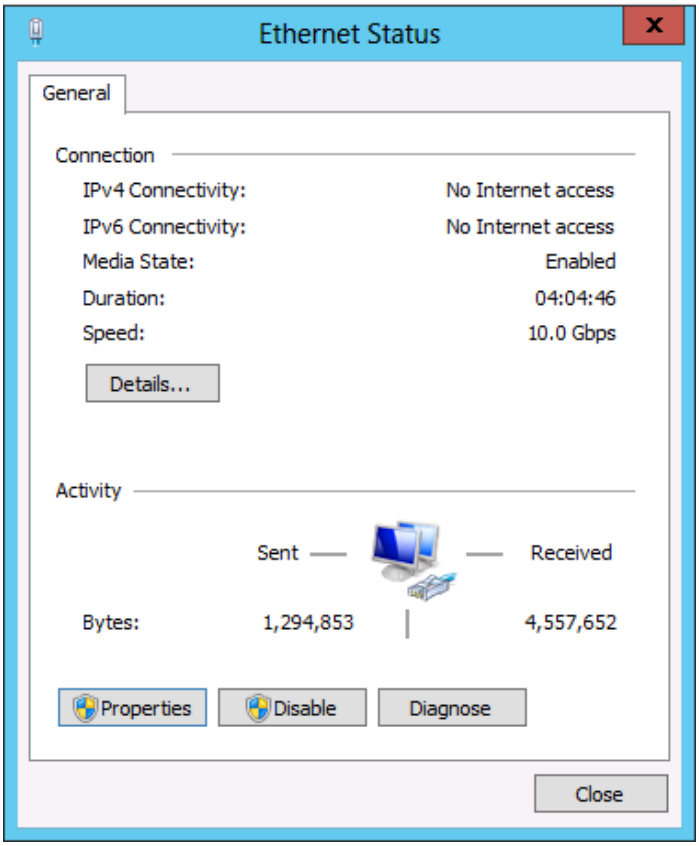
What is seen in the following sample screen shots may vary significantly from the actual customer environment. This is due to the fact that there are many variables in the potential customer network, and all variations are not covered in these samples. These samples assume that there is no DHCP server (which would make this a little easier, but is beyond the scope of this document). By assuming there is no DHCP server, all NICs will initially be configured with 169.254/16 APIPA addresses. These steps will assign fixed IP addresses to all the NICs.

It is necessary to find the NIC through which host management is performed. This is not the out-of-band NIC used by Cisco UCS Manager, but the NIC dedicated to host management.

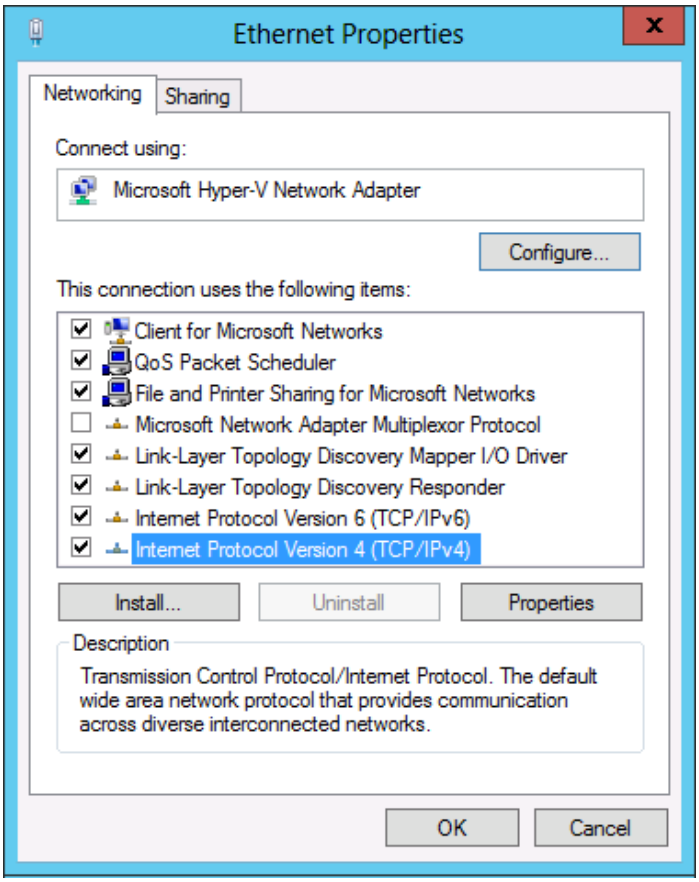
Log into the server. Enter the following PowerShell command. **`Gwmi Win32_NetworkAdapter | Where {$_.MACaddress -ne $Null} | FT NetConnectionID, MACaddress`** This returns a table of the network names and their associated MAC addresses.	

Go to the **Servers** tab in UCSM. Select **Servers > Service Profiles > root** and the service profile for the machine you are working on. Expand the Service Profile. Click on **vNICs**. This enables you to see the MAC addresses for the Mgmt vNIC (in this example, Mgmt is the NIC used for host management). Find the MAC address in the table displayed in the previous step, and take note of the assigned name. For example purposes, assume it is "Ethernet"	
In Server Manager click on **Local Server**.	
Click on any one of the networks. This will bring up the **Network Manager** window.	

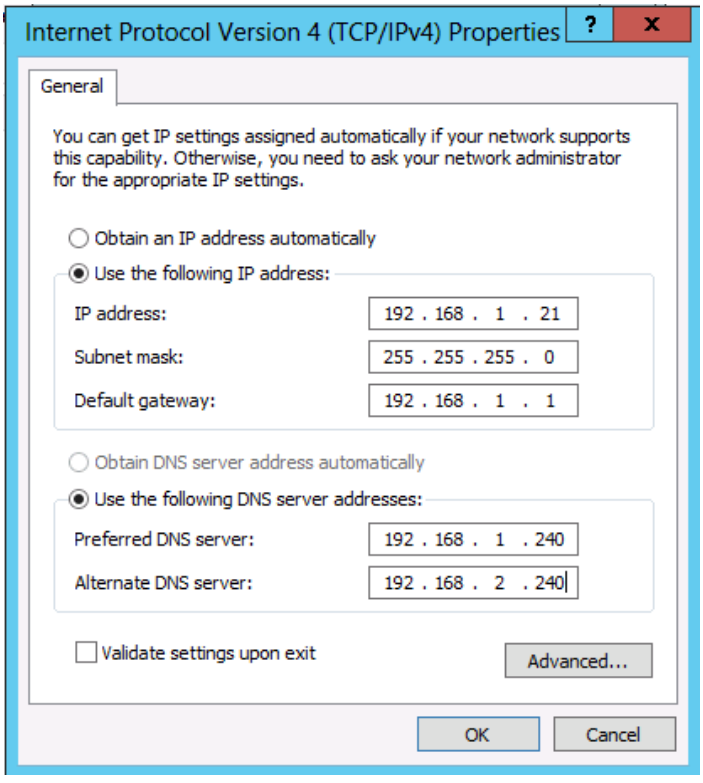
Double-click the entry for “Ethernet”.
This brings up the Status window for the Ethernet NIC.
Click **Details…** to ensure you have the right MAC address.
Click **Properties**.



Click on the **Internet Protocol Version 4 (TCP/IPv4)** line. (Leave the check box checked.)
Click **Properties**.



Configure the IP settings appropriately for the customer environment.
Click **OK**.
Click **Close**.
Click **Close**.
Back in the Windows PowerShell window, ping the Domain Controller by its name to ensure you have properly configured the network settings.



Common Configuration Tasks

There are some tasks that are performed to ensure the ability for the hosts to be remotely managed for the rest of these instructions. In an existing customer environment, the customer may handle some of these tasks via Active Directory group policy objects. Setting up these tasks to be handled by group policies is beyond the scope of this document, so they should be reviewed with the customer. Appendix B contains a sample PowerShell script, Set-UcsHyperVRemoteMgmt.ps1, that sets a number of firewall rules to enable remote management, enables some services to automatically start, and enable remote desktop. Run this script from a PowerShell command window.

While the KVM still has the Windows Server installation media still mounted (if it is not still mounted, re-mount it for this command), it is necessary to add the .NET Framework 3.5 feature. Assuming the Windows Server installation media is mounted on drive E:, issue the following PowerShell command to add the feature.

```
Install-WindowsFeature –Name NET-Framework-Core –Source E:\sources\sxs
```

Run Windows Update

It is highly recommended to fully patch the server at this time from Windows Update. Depending on the patches, it might be necessary to reboot and check for updates multiple times before the server is completely patched.

Install Microsoft Hotfixes

Install the following Windows Server 2012 hot fixes. These are not available through Windows Update. You have to make specific requests for each one.

1. KB2796995 – http://support.microsoft.com/kb/2796995; fix for an ODX issue
2. KB2785638 – http://support.microsoft.com/kb/2785638; fix for SR-IOV issue
3. Check http://social.technet.microsoft.com/wiki/contents/articles/15576.hyper-v-update-list-for-windows-server-2012.aspx for any other hotfixes that your particular environment might need.

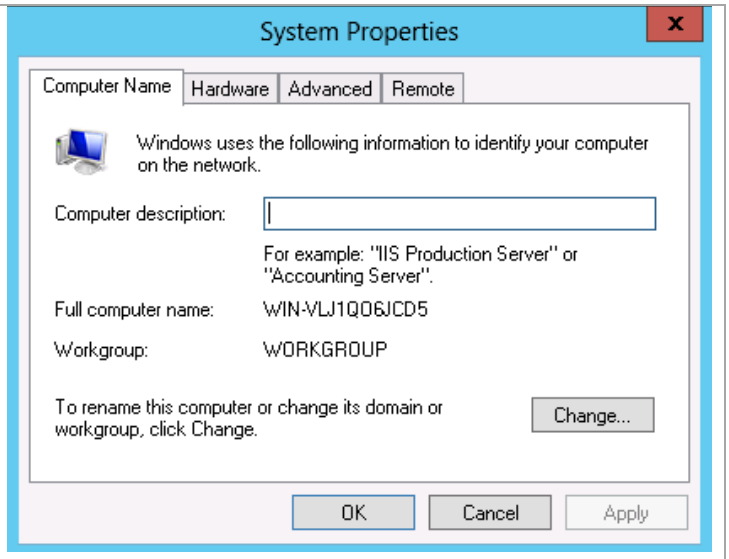
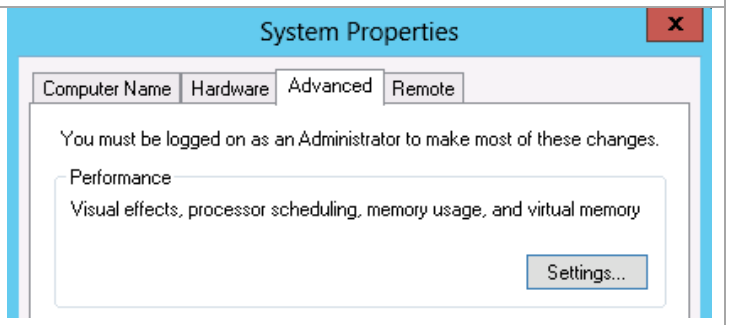
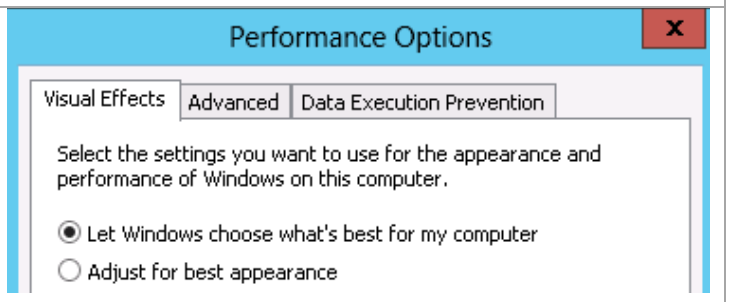
Note: This may require multiple reboots.

Install Windows Roles and Features

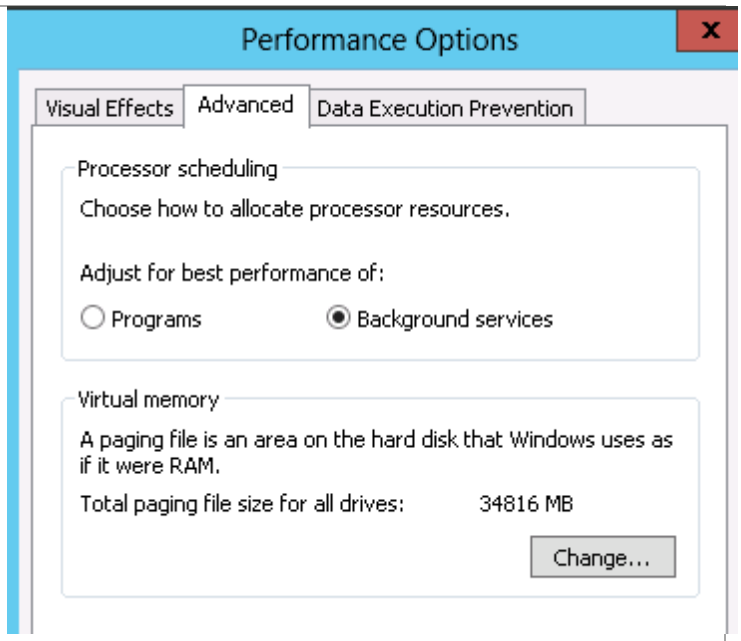
Appendix B contains a sample PowerShell script, Add-UcsHyperVFeatures.ps1, installs the MPIO and Failover Cluster features, and the Hyper-V role. Run this script from a PowerShell command window. Installation of the Hyper-V role causes a reboot.

Configure Paging File

By default, Windows allocates and manages a portion of the system disk to be used as a paging file based on the amount of physical memory on a server. Since the workload running on Hyper-V servers really runs in the VMs, the majority of paging occurs within the VMs, minimizing the need for a large page file on the physical server. Therefore, it makes sense to minimize the size of the paging file of the Hyper-V host to minimize the amount of storage on the boot volume that is reserved for the paging file.

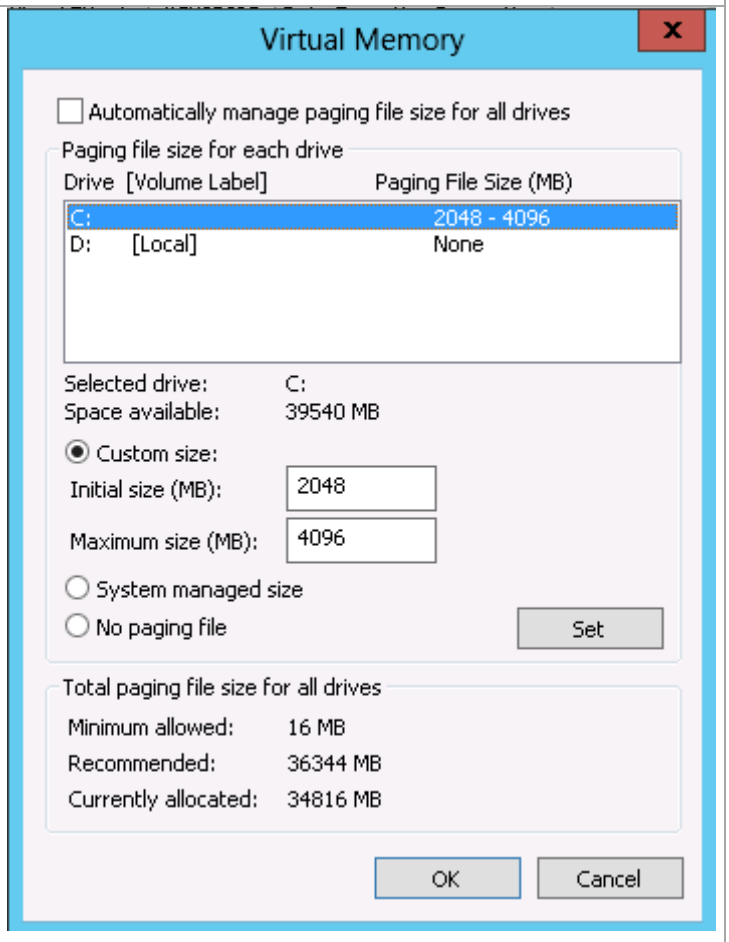
In **Server Manager**, click on the **Computer Name** to bring up the **System Properties** window. Click on the **Advanced** tab.	
Click the **Settings...** button in the **Performance** section of the window.	
Click the **Advanced** tab.	

Click on the **Change...** button.



Uncheck the **Automatically manage paging file size for all drives box**.
Click the **Custom size**: radio button.
Enter **2048** into the Initial size (MB): field.
Enter **4096** into the Maximum size (MB): field.
Click the **Set** button to set the new values.
Click **OK** button four times to accept the change. System must be rebooted to implement the change.

Note: The server will be powered down in the next step, so there is no need to reboot it at this point.



Configure MPIO

After the server has been configured with the MPIO feature, it is necessary to present the additional paths to the boot LUN and configure MPIO. Since the goal is to sysprep this operating system image, and then clone the LUN for use by all other physical servers, this means MPIO only has to be configured once. Then, since the operating system image that will be used for booting the additional blades will already have MPIO configured, it is possible to configure paths through both Nexus switches for initial boot of the sysprepped image.

The first thing to do is to prepare the Cisco Nexus 5548 switches with zones that reflect all paths to the boot LUN.

Cisco Nexus 5548 A

We had previously configured only a single path on Cisco Nexus 5548 A for the initial installation. Issue the following commands to create the secondary path.

1. From the global configuration mode, type **zone name** <***F3-Infra01***> **vsan 1**
2. Type **member device-alias** <***VNX5500-SPB-B0***>
3. Type **exit**
4. Type **zoneset activate name** <***PvtCld***> **vsan 1**
5. The Nexus should respond with "Zoneset activation initiated. Check zone status."
6. Type **copy run start**

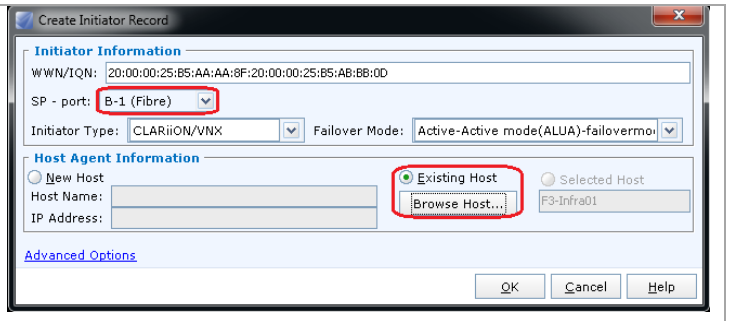
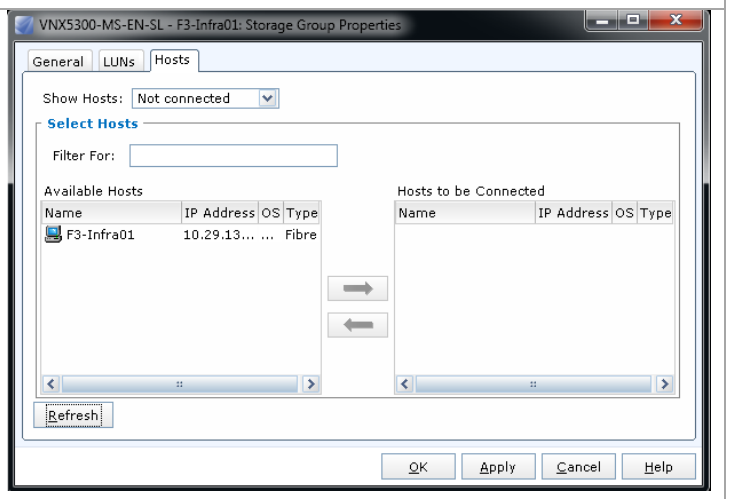
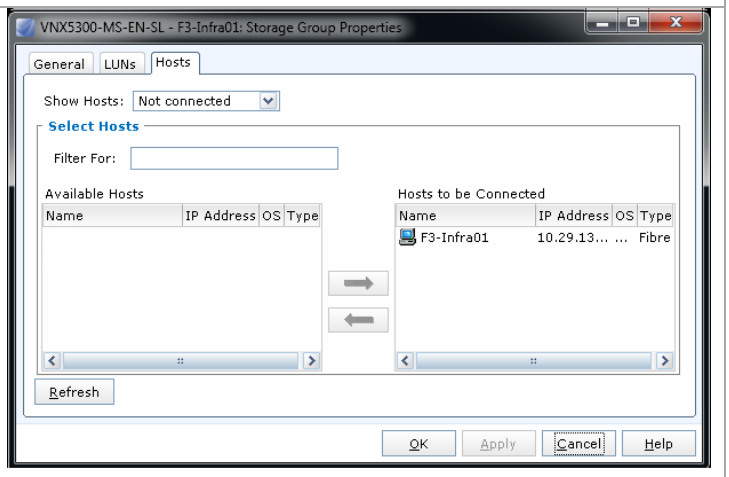
Cisco Nexus 5548 B

1. From the global configuration mode, type **zone name** <***F3-Infra01***> **vsan 1**
2. Type **member device-alias** <***F3-Infra01-B***>
3. Type **member device-alias** <***VNX5500-SPB-B1***>
4. Type **member device-alias** <***VNX5500-SPA-A1***>
5. Type **exit**
6. Type **zoneset name** <***PvtCld***> **vsan 1**
7. Type **member** <***F3-Infra01***>
8. Type **exit.**
9. Type **zoneset activate name** <***PvtCld***> **vsan 1**
10. The Nexus should respond with "Zoneset activation initiated. Check zone status."
11. Type **copy run start**

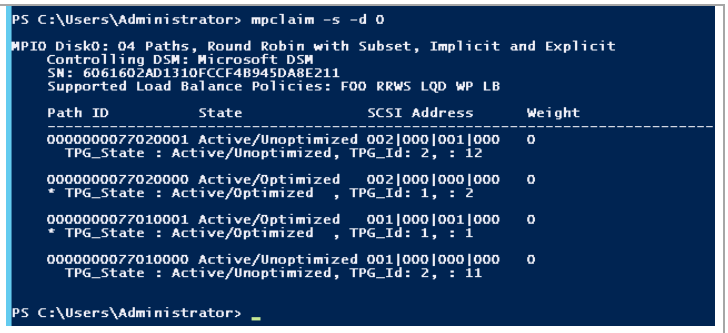
EMC VNX5500

When the zones and zonesets have been updated to reflect the multiple paths to the LUN, it is necessary to configure the EMC VNX5000 SAN to present the boot LUN to the additional paths.

Note: Power off the server before starting.

In Unisphere, go to **Hosts > Initiators** and click the **Create** button to add a new initiator. The goal is to create an initiator to each port on the VNX5500. You will have two initiator records for each WWNN and WWPN combination for the server. Be sure to select the appropriate **SP-Port**. Also select **Existing Host** and select the proper host.	
When all initiators are defined and registered, select **Hosts > Storage Groups**. Select the storage group for this server. Select the server from the **Hosts to be Connected** column and move it to the **Available Hosts** column. Click **OK**,	
Select the server from **Available Hosts** and move it to **Hosts to be Connected**. Click **OK**. Boot the server.	

From an elevated command prompt or PowerShell window issue the command **mpclaim –s –d 0**
You should see four entries, similar to what is shown in this screen shot, validating that you have properly configured MPIO.

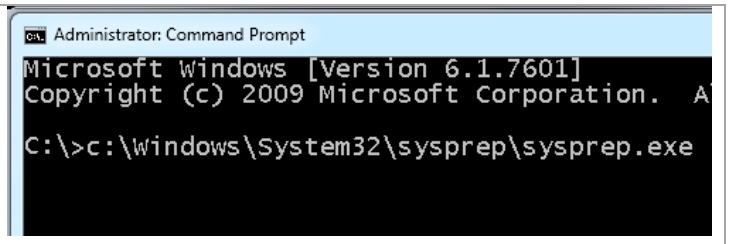


6.2 Sysprep the Image

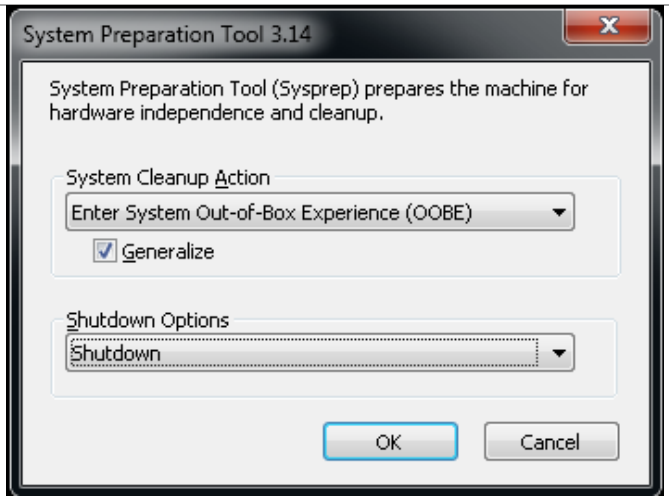
When the image is properly configured for multipath, Microsoft's sysprep utility can be used to create an image that can be used for cloning to quickly provision any additional physical hosts needed in the environment.

From an elevated command window, enter the command
`c:\Windows\System32\sysprep\sysprep.exe`

Note: The sysprep utility is unique for each version of the operating system. Do not try to use one from another installation.



Select **Enter System Out-of-Box Experience (OOBE)** from the System Cleanup Action dropdown menu.
Select the **Generalize** box.
Select **Shutdown** from the Shutdown Options dropdown menu.
Click **OK**.
When the KVM console shows the physical server has shut down, clones can be made of the LUN for use by all the physical hosts.



6.3 Removal of Source Master Image

After installation of the Windows Server instance, and execution of the sysprep process, it is necessary to remove the source LUN from the Service Profile that was used to build the image. To remove the LUN from the Service Profile, the PrepMasterBoot_RemoveViaWWPN.ps1 PowerShell script found in Appendix B can be executed with the same parameters that were provided in the Create VNX LUNs for Private Cloud Environment section, including the configuration file.

After successful execution, the LUN will be removed from Service Profile, and can be used to process SnapShots for the Service Profiles to be placed into operation.

6.4 Create Clones of Sysprep Image

With the base sysprep image created, clones can be taken in order to replicate the contents of the master LUN for other servers in the environment. Prior to copying the data, target devices need to be created to be associated with the planned clone sessions. The clones can be created with ESI or through Unisphere.

Create Clones with ESI

The following XML configuration file format can be used in conjunction with the ProcessStorageRequests.ps1 script to create the appropriate clone target devices.

```
<StorageParams>
  <Servers>
    <Server>
      <ServerName>F3-Infra01</ServerName>
      <IPAddress>10.29.130.21</IPAddress>
      <luns>
        <label>PVTCLD-INFRA1-BOOT</label>
        <pool>PVTCLD_DATA1_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-Infra02</ServerName>
      <IPAddress>10.29.130.22</IPAddress>
      <luns>
        <label>PVTCLD-INFRA2-BOOT</label>
        <pool>PVTCLD_DATA2_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV01</ServerName>
      <IPAddress>10.29.130.31</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV1-BOOT</label>
        <pool>PVTCLD_DATA1_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV02</ServerName>
      <IPAddress>10.29.130.32</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV2-BOOT</label>
        <pool>PVTCLD_DATA2_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV03</ServerName>
      <IPAddress>10.29.130.33</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV3-BOOT</label>
```

```
        <pool>PVTCLD_DATA1_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV04</ServerName>
      <IPAddress>10.29.130.34</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV4-BOOT</label>
        <pool>PVTCLD_DATA2_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV05</ServerName>
      <IPAddress>10.29.130.35</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV5-BOOT</label>
        <pool>PVTCLD_DATA1_R5</pool>
        <size>60GB</size>
      </luns>
    </Server>
    <Server>
      <ServerName>F3-HyperV06</ServerName>
      <IPAddress>10.29.130.36</IPAddress>
      <luns>
        <label>PVTCLD-HYPERV6-BOOT</label>
        <pool>PVTCLD_DATA2_R5</pool>
        <size>60GB</size>
     </luns>
    </Server>
  </Servers>
  <Array>EnterpriseFastTrack</Array>
  <UCSAddress>10.5.177.10</UCSAddress>
</StorageParams>
```

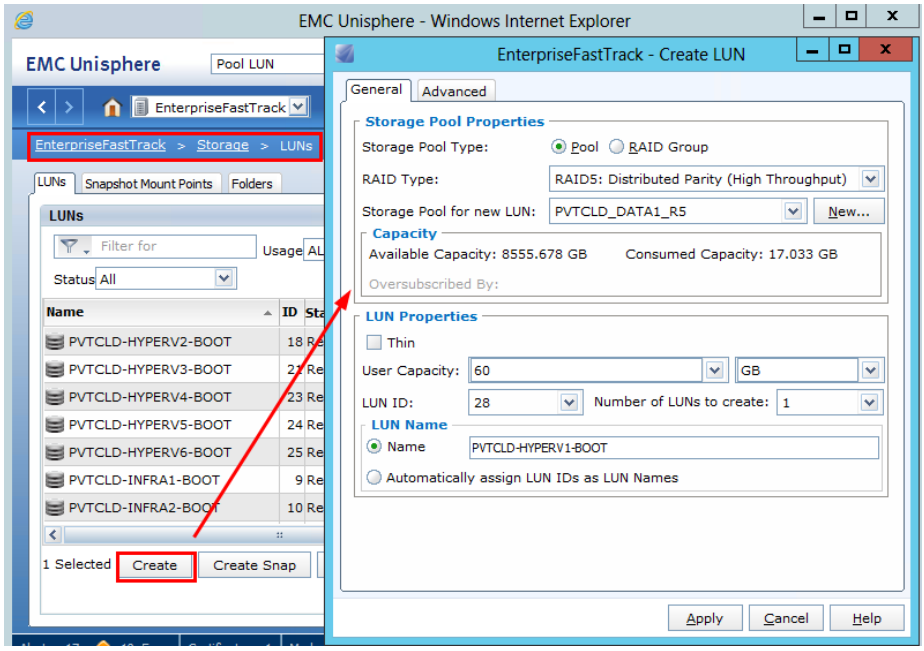
This configuration file passed to the ProcessStorageRequests.ps1 PowerShell script would result in the creation of 8 LUNs of size 60 GB being created in opposite storage pools for each cluster node. The execution of such a process is shown in the following figure.

Figure 7 Example Execution of Clone Target LUN Creation

```
System '[Name = EnterpriseFastTrack. UserFriendlyName = VNXFT]' has been updated successfully.
Creating LUN PVTCLD-INFRA1-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-INFRA2-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV1-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV2-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV3-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV4-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV5-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
Creating LUN PVTCLD-HYPERV6-BOOT
TaskStatus: Started
 10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed
```

Alternatively, the clone target LUNs can be created using Unisphere from the "storage array" > Storage > LUNs page, like the following example.

Figure 8 Creating LUNs



Now that the clone target LUNs are created, the clone process can be run. To automate the clone process, the following XML configuration file contents can be used in conjunction with the 'ProcessClones.ps1' script, found in Appendix B, which leverages ESI and naviseccli.

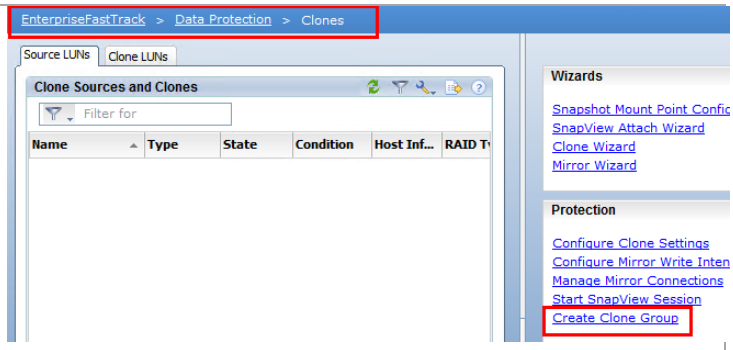
```
<StorageParams>
<SourceLUN>PVTCLD-MASTER-BOOT</SourceLUN>
```

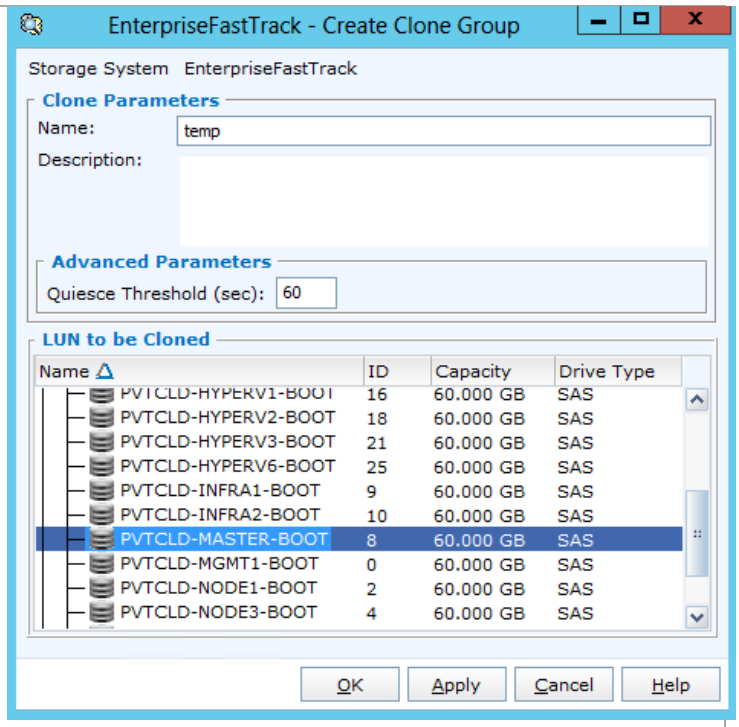
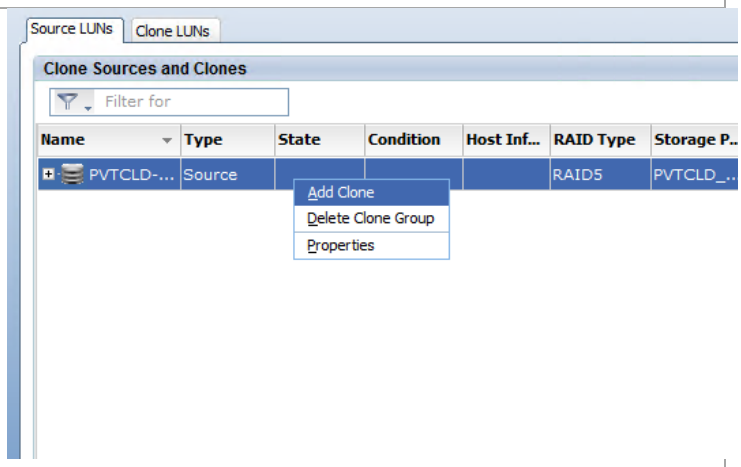
```
<TargetLUNs>
   <lun>PVTCLD-INFRA1-BOOT</lun>
   <lun>PVTCLD-INFRA2-BOOT</lun>
   <lun>PVTCLD-HYPERV1-BOOT</lun>
   <lun>PVTCLD-HYPERV2-BOOT</lun>
   <lun>PVTCLD-HYPERV3-BOOT</lun>
   <lun>PVTCLD-HYPERV4-BOOT</lun>
   <lun>PVTCLD-HYPERV5-BOOT</lun>
   <lun>PVTCLD-HYPERV6-BOOT</lun>
</TargetLUNs>
<CloneGroupName>Temp</CloneGroupName>
<VNXBlockSPAAddress>10.5.223.128</VNXBlockSPAAddress>
</StorageParams>
```

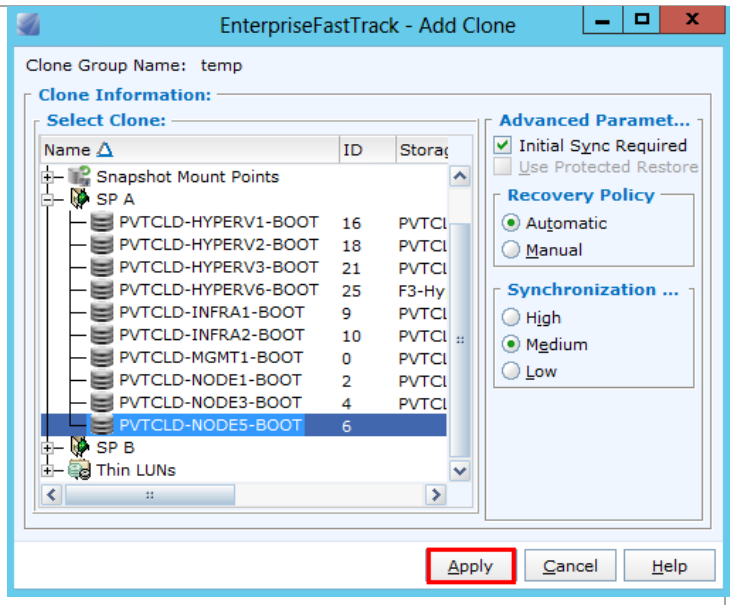
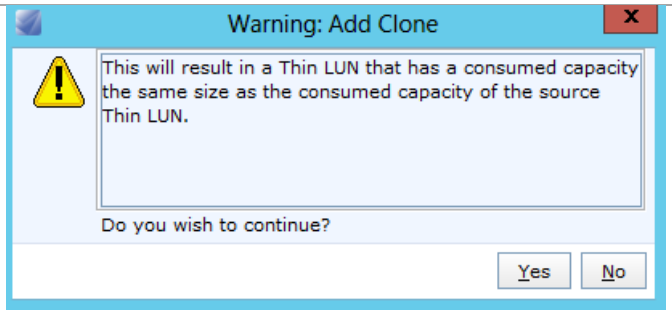
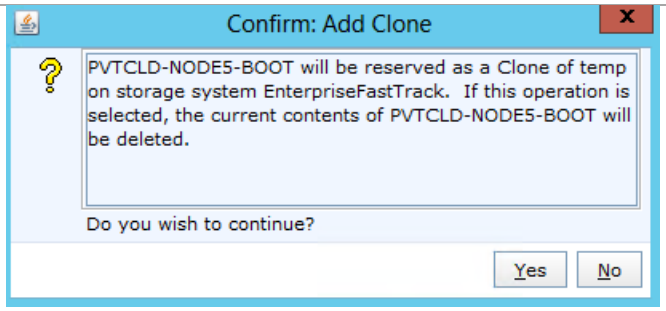
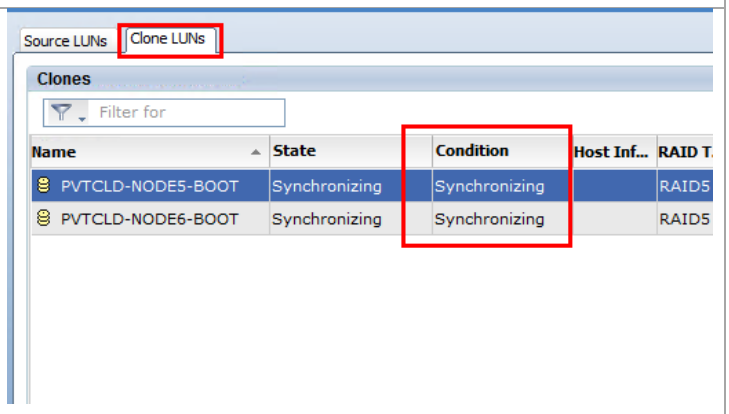
The script will create up to 8 concurrent clone copies and wait for 100% synchronization. Once the copies are complete, the script will delete the clone relationship and the target LUNs can be used for deployment.

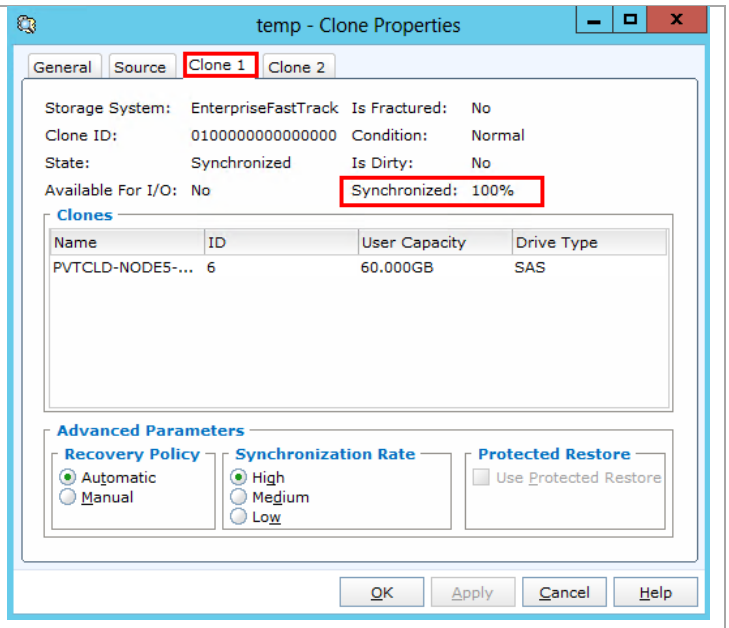
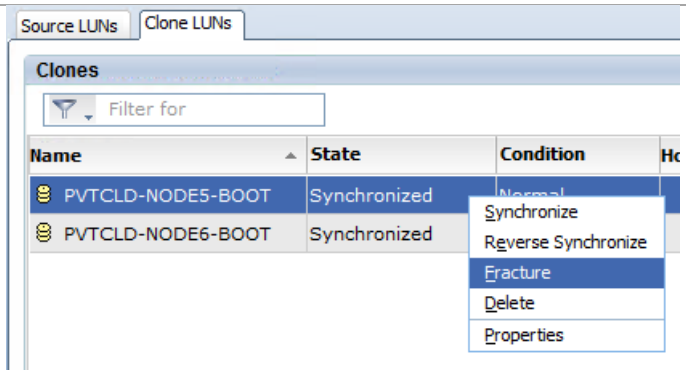
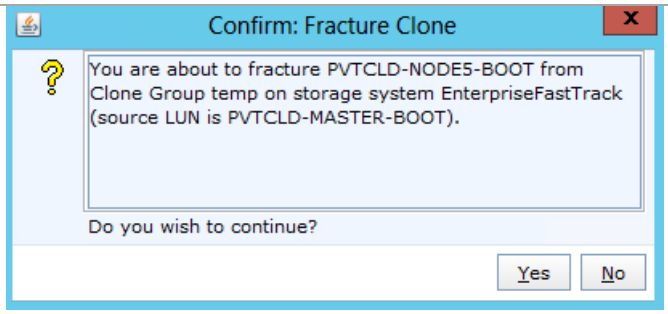
Create Clones through Unisphere

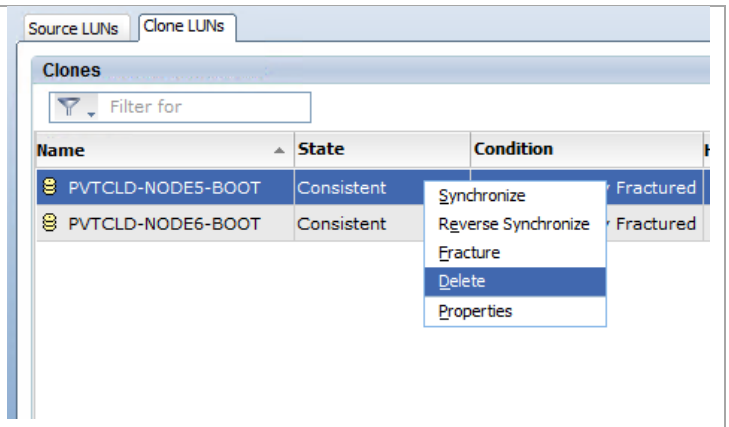
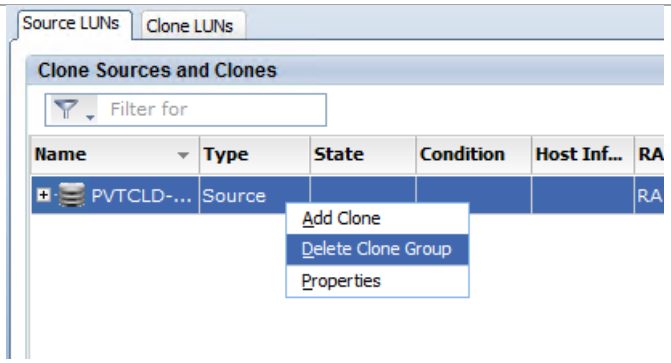
Alternatively, the following process can be executed from Unisphere to create the clone relationships and copy the data from the master LUN to the boot target LUNs.

In Unisphere, go to **Data Protection > Clones** Select the **Create Clone Group** link from the protection side-bar	

Give the Clone Group a name and select the master boot image LUN as the "**LUN to be Cloned.**" Then select **OK** Select **Yes** after reviewing the confirmation screen and **OK** after the group creation returns with success.	
Right click on the newly created **Clone Source** and select **Add Clone**	

Select the appropriate clone target LUN intended for Boot from SAN and select **Apply**.	
When replicating between thin LUNs the following warning will pop up. Select **Yes**.	
Confirm the target LUN will be overwritten by selecting **Yes** Select **OK** after the successful addition of the clone. Repeat the previous steps to add the desired number of clone copies. Up to 8 can be added concurrently.	
Verify the clones are synchronizing from the **Clone LUNs** tab.	

To get more detail on synchronization, right click on a clone LUN and select **Properties.** Each clone will have its own tab. Within each tab will be a **Synchronized** percentage. Wait for all clones to get to a "**Synchronized**" **"State"** before continuing.	
From the **Clone LUNs** tab, select only one clone, right click, and select **Fracture**	
Confirm the fracture operation and select **Yes** Select **OK** following the successful fracture Repeat the fracture process for all synchronized clones.	

Delete each fractured clone. Select one clone at a time, right click, and select **Delete** Select **OK** following the successful delete.	
Optionally delete the clone group. From the **Source LUNs** tab, right click on the group and select **Delete Clone Group.** Confirm the deletion by selecting **Yes** at the following screen. This completes the cloning process.	

6.5 Booting from Sysprepped LUNs

Zone the Network

Presenting the LUNs to the various hosts is a combination of configuring the zones and zonesets on the Cisco Nexus 5548 switches and masking the LUNs through Unisphere or naviseccli. The detailed steps for this were shown previously, so they will be summarized here.

- Create the device alias for each service profile with the value of the fabric A WWPN defined on the A Nexus, and the value of the fabric B WWPN defined on the B Nexus.
- Create a zone for each service profile on each Nexus containing the device alias for appropriate server WWPN and both WWPNs of the associated EMC interfaces.
- Add the created zones to the zoneset and activate it.

The result of this step will provide a listing of the zoneset that looks something like this (WWPN values will differ for each environment).

Figure 9 Example Zoneset for Cisco Nexus 5548 A

```
sjc2-151-E21-5548-A# sho zoneset
zoneset name PvtCld vsan 1
  zone name F3-Infra01 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:ef [F3-Infra01-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name F3-Infra02 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:7f [F3-Infra02-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV01 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:bf [FTv3-HyperV01-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV02 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:8f [FTv3-HyperV02-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV03 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:5f [FTv3-HyperV03-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV04 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:cf [FTv3-HyperV04-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV05 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:3f [FTv3-HyperV05-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]

  zone name FTv3-HyperV06 vsan 1
    pwwn 20:00:00:25:b5:aa:ab:af [FTv3-HyperV06-A]
    pwwn 50:06:01:60:3e:a0:7f:12 [VNX5300-SPA-A0]
    pwwn 50:06:01:68:3e:a0:7f:12 [VNX5300-SPB-B0]
sjc2-151-E21-5548-A#
```

Mask the Boot LUNs to Service Profiles

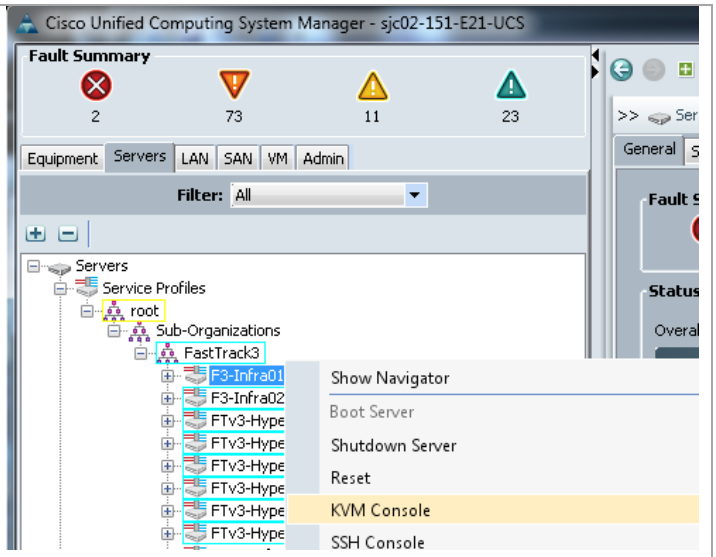
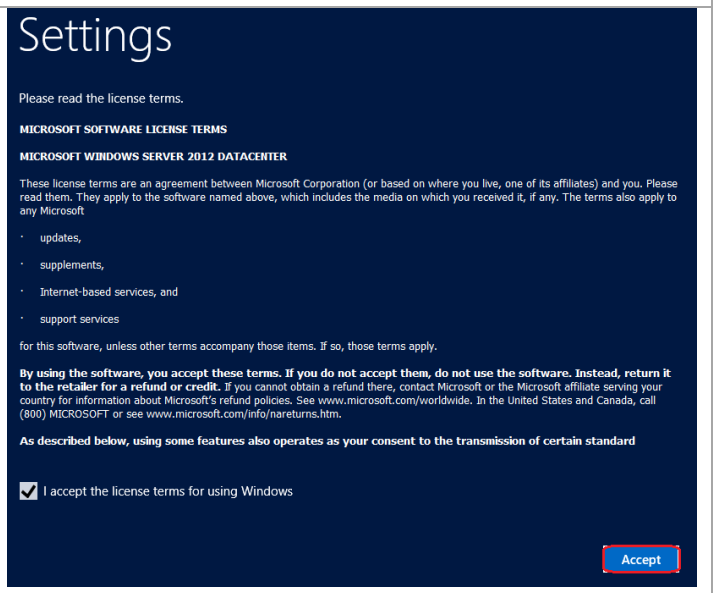
Following the cloning and zoning processes, the boot LUNs can be presented to their respective service profiles. The same XML configuration file used to create the boot LUNs can be used in conjunction with the PostClone_AddViaWWPN.ps1 script to present the boot LUNs to the servers. The script will also register the appropriate initiators with the storage array and create the necessary storage groups along with presenting the LUNs to the appropriate servers.

An alternative to using the script would be to use the Unisphere management GUI as outlined previously in the "Mask Boot LUN with EMC Unisphere" section. Following the masking operations, start each host and complete the mini-setup to tailor each node with things like name, IP addressing (if fixed IP addresses are used), and join to the domain.

6.6 Complete the Image Builds from Sysprepped Images

When the sysprep image has been cloned and the LUNs are properly masked so the boot volumes only appear to the owning host, every server must complete its installation. Booting from a sysprep image runs what is referred to as a 'mini-setup'.

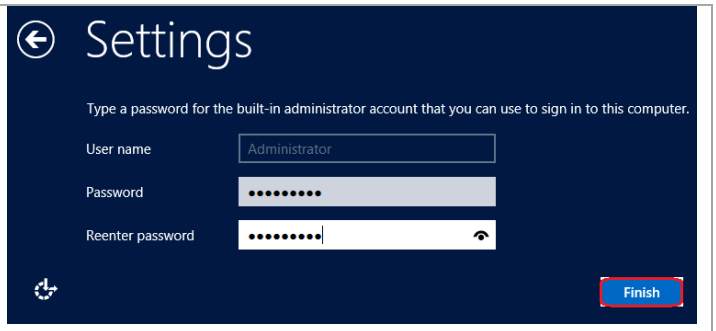
Note: This document does not describe the use of an unattend file. If your organization makes use of unattended installations of sysprep images, that can be used to replace these steps.

Open UCSM. Select the **Servers** tab. Open **Service Profiles**. Select <*F3-Infra01*>. Click on **KVM Console** to open a window from which you can manage the mini-setup. The association between the service profile and the blade should have taken effect when you created the service profile, so you should see the first screen of the Windows Server mini-setup. If it is still booting when you connect to it, you may see a series of progress messages display as the system completes the initial setup.	
Click the box next to **I accept the license terms for using Windows.** Click **Accept**.	
Make any necessary changes to the Region and Language settings. Click **Next**.	

Enter a complex password. The password must contain three of the following and be at least eight characters in length.

- Upper case character
- Lower case character
- Digit
- Special character

Re-enter the same password.
Click **Finish**.



Now you will have a complete base image. This means you will need to activate Windows, change the name of the system, join to the domain, configure your network settings, and complete any other tailoring required to meet your company requirements for Windows Server installation.

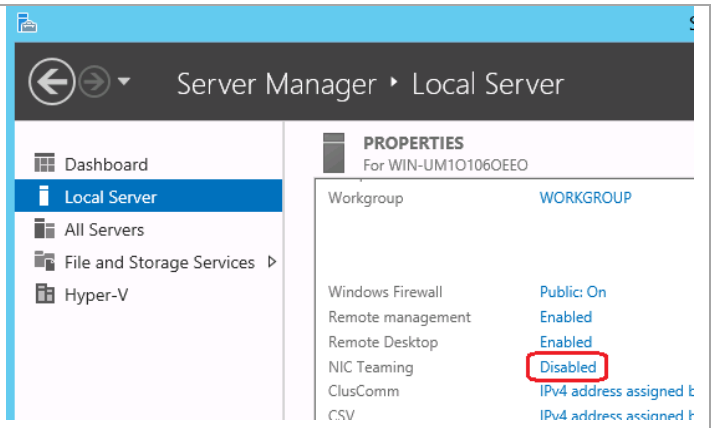
Configure Networks

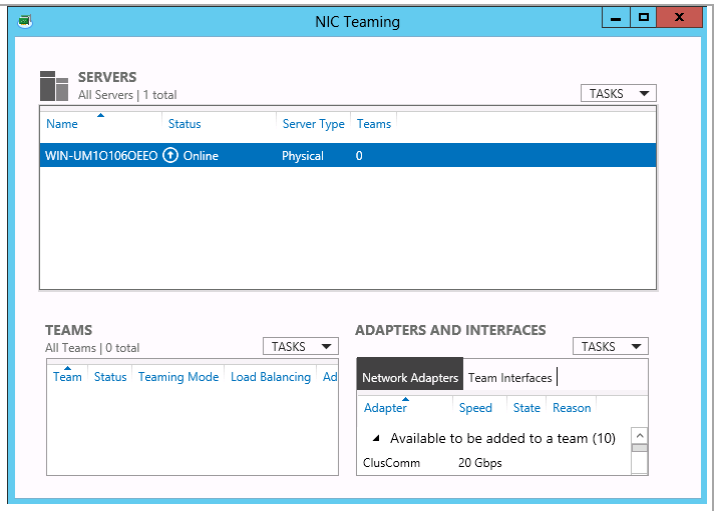
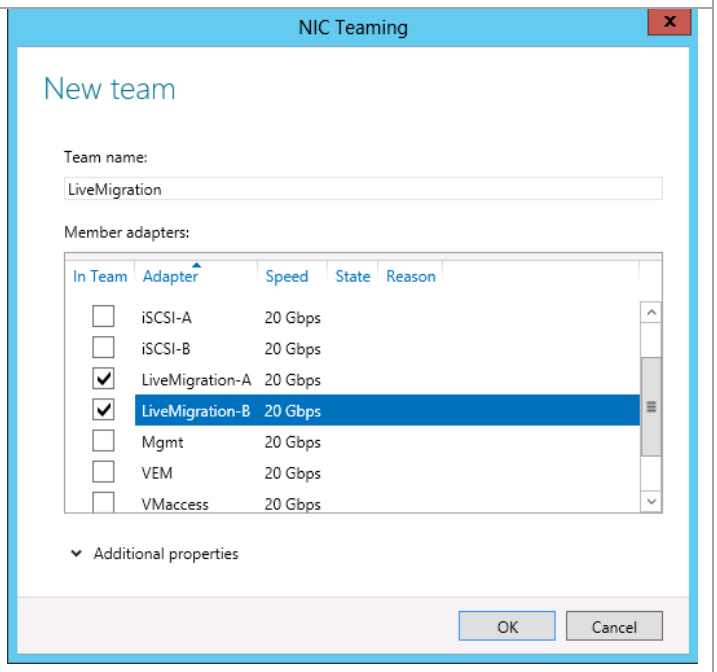
It is highly recommended that you rename the network adapters from the Windows default values of "Local Area Connect #x" to reflect the actual network from the UCS Service Profile. You can use the manual procedure defined earlier in the document, or you can use the sample PowerShell script, Set-UcsHyperVAdapters.ps1, found in Appendix B: Sample Scripts. This script requires that the machine domain-joined and the script is being run from a workstation that has the Cisco UCS PowerTool installed.

Configure NIC Teaming

This configuration uses Microsoft's teaming software to team two NICs to be used for Live Migration. This is an optional step, but it will improve the performance for live migrations if you are performing multiple live migrations simultaneously. If you generally perform only one live migration at a time, you will not notice any performance difference.

From **Server Manager**, select Local Server and click on **Disabled** by NIC Teaming.

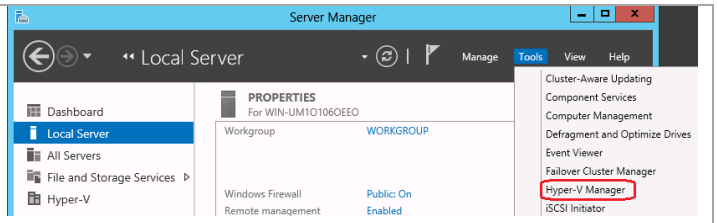
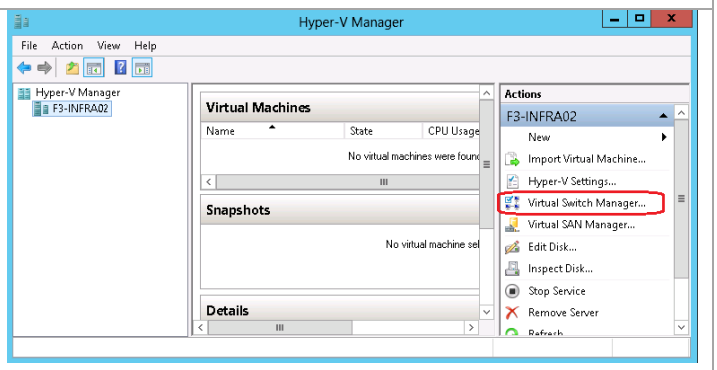
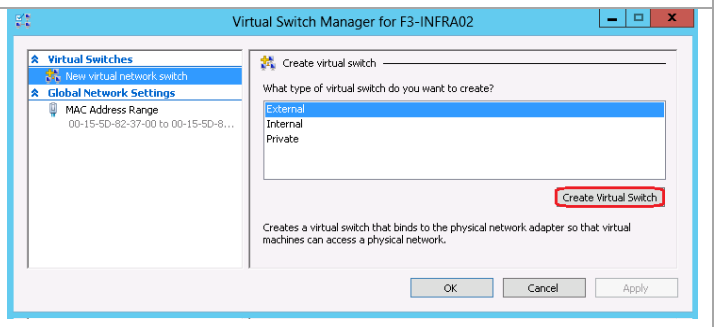
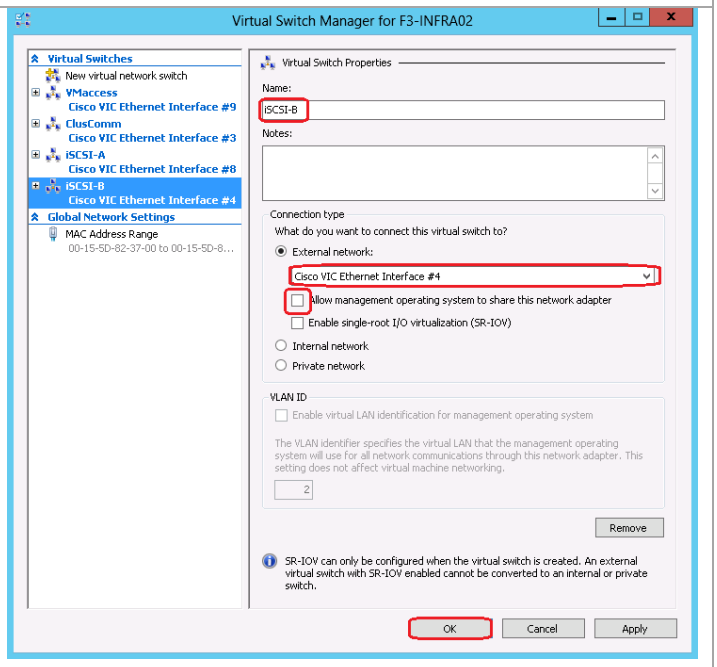


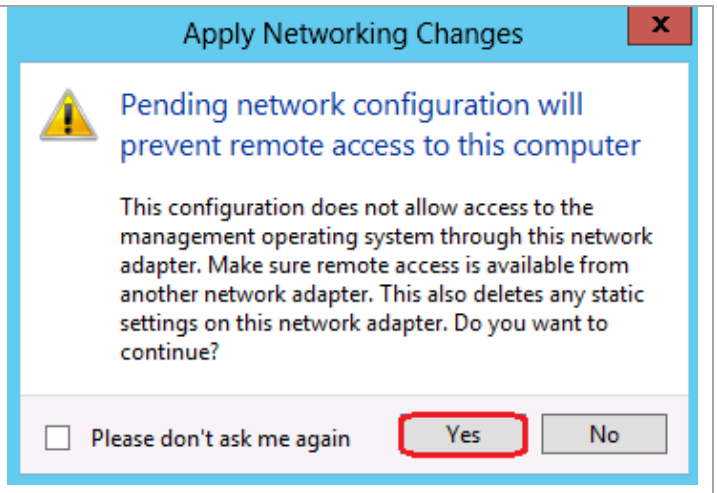
In the **NIC Teaming** window, click **Tasks** on the **TEAMS** portion of the window and select **New Team** from the drop-down list.	
Provide a name in the **Team Name** field and select the LiveMigration-A and LiveMigration-B networks. This will create a switch-independent team that uses address hash for load balancing. If you want some other configuration, select Additional properties to make the changes. Click **OK** to continue. Alternatively, you can issue this PowerShell command: `New-NetLbfoTeam -Name LiveMigration -TeamMembers LiveMigration-A,LiveMigration-B`	

The Set-UcsHyperVAdapters.ps1 script will assign a fixed IP address to each NIC based on the a 192.168.xx.yy notation where xx is the VLAN read in from UCS and yy is a specific value assigned so that the last octet of each address is the same on for each server. It also sets each adapter, except the excluded (generally the management) adapter so that it does not register itself in DNS. It is best to have only the primary (management) addresses register in DNS.

Depending upon your configuration, you might have DHCP set up for every network. In which case, it is not recommended to use this script.

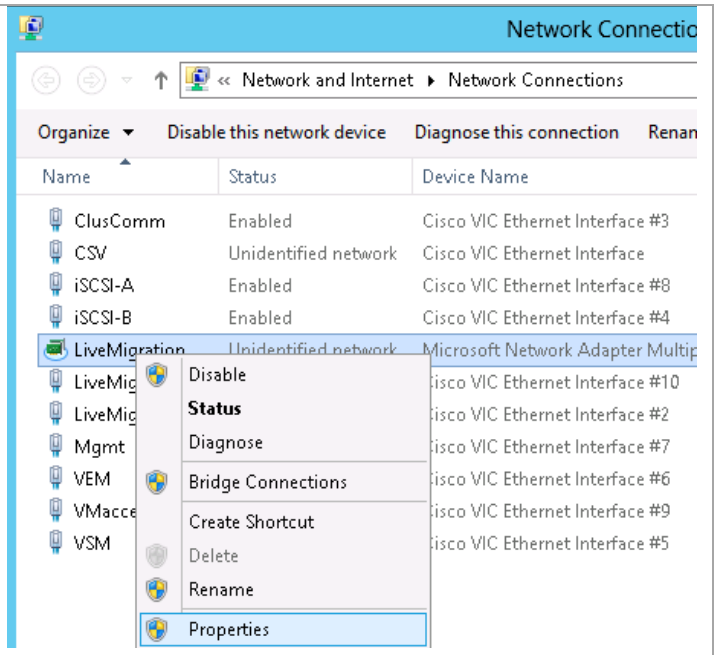
Configure Hyper-V Virtual Switches

From **Server Manager > Tools**, select **Hyper-V Manager**.	
From the Hyper-V management console, select Virtual Switch Manager from the right-hand side.	
Ensure that **New virtual network switch** is highlighted on the left-hand side and **External** is highlighted on the right-hand side. Click **Create Virtual Switch**.	
Enter an appropriate name in the **Name** field. Ensure that you select the correct Cisco VIC Ethernet Interface from the drop-down list for External network. Uncheck the **Allow management operating system to share this network adapter.** Repeat previous step and this step for the VMaccess, ClusComm, iSCSI-A, and iSCSI-B NICs. Click **OK** to complete creating these four virtual network switches.	

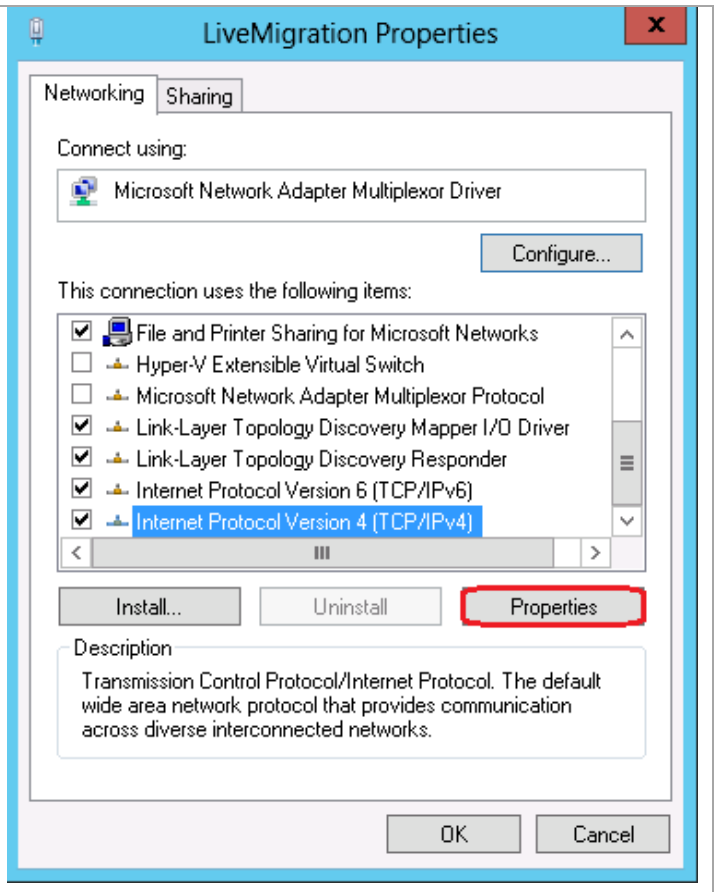
A warning window will display cautioning about possible disconnection from the machine. You are not accessing the physical host through any of the network adapters selected, so you can click **Yes** with no issues.	

Unconfigure DNS Registration

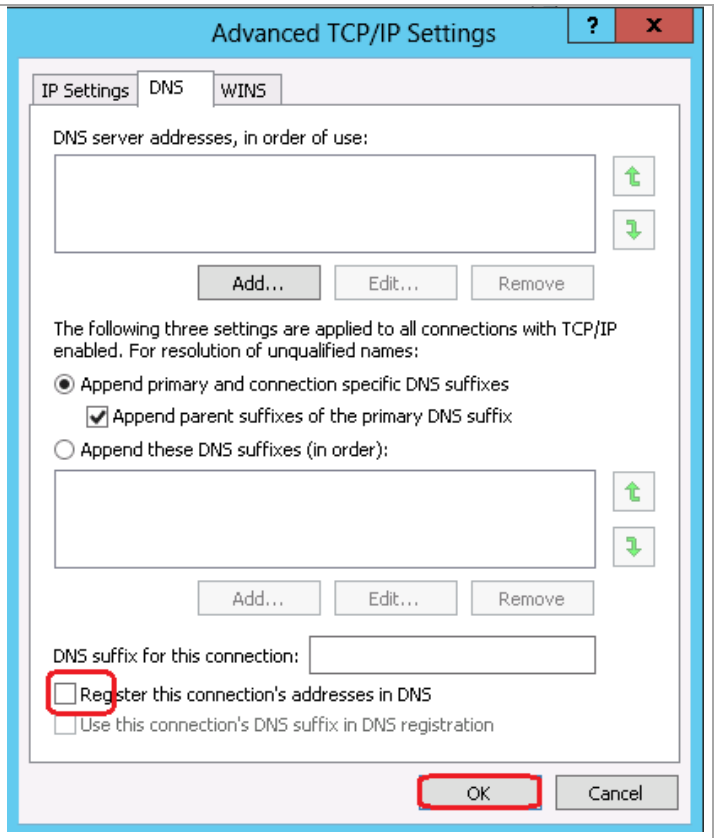
If you do not use the Set-UcsHyperVAdapters.ps1 script to rename and partially configure the NICs, it is a good practice to remove all but the management NIC from DNS registration.

In **Network Connections**, right-click on a network that is still assigned to the host (e.g. CSV or LiveMigration) and select **Properties**.	

In the **Properties** window, scroll down to the Internet Protocol Version 4 (TCP/IPv4) line and select it.
Click on **Properties**.
Click **Advanced…** in the Properties windows that displays.



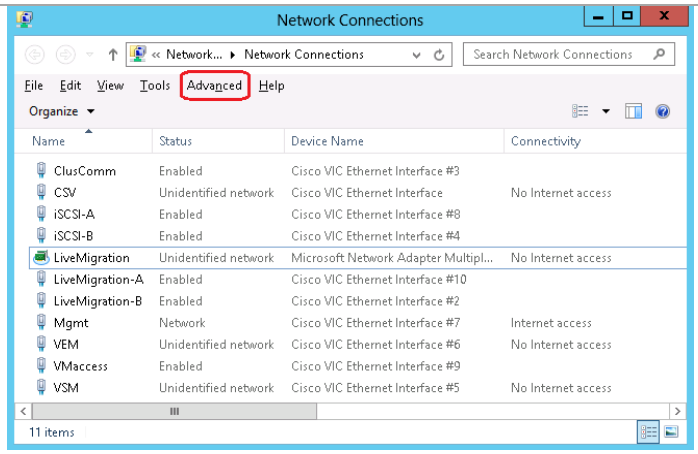
Select the DNS tab and uncheck the **Register this connection's addresses in DNS** box.
Click **OK** twice and then **Close**.

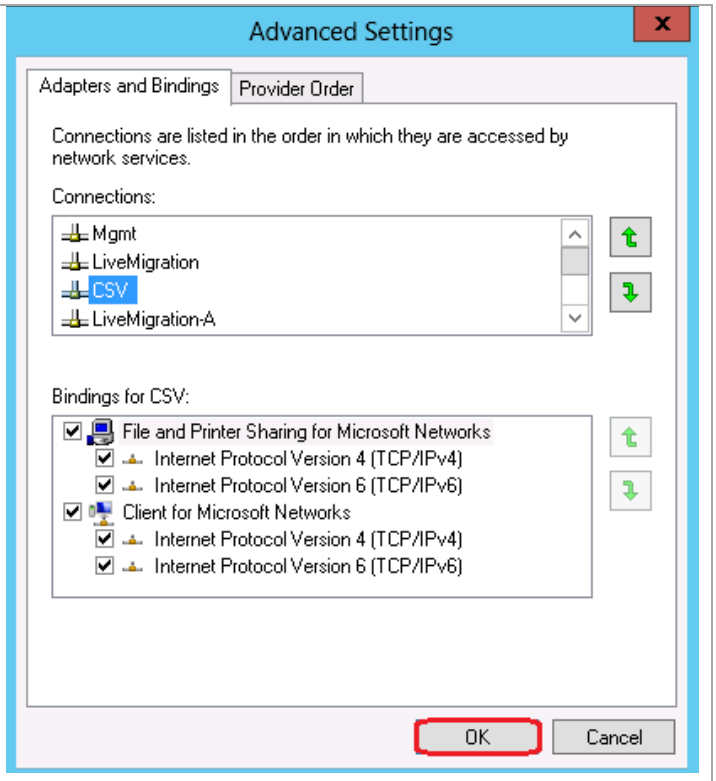


Binding Order

Ensure you have a proper binding order of NICs.

On the Network Connections window, click the **Alt** key on the keyboard to display the toolbar for the window.
Click on **Advanced** and select **Advanced Settings...** from the drop-down menu.

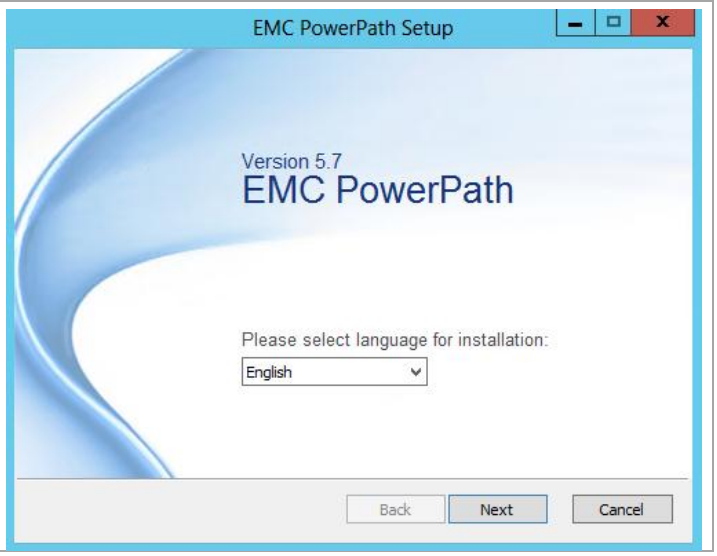


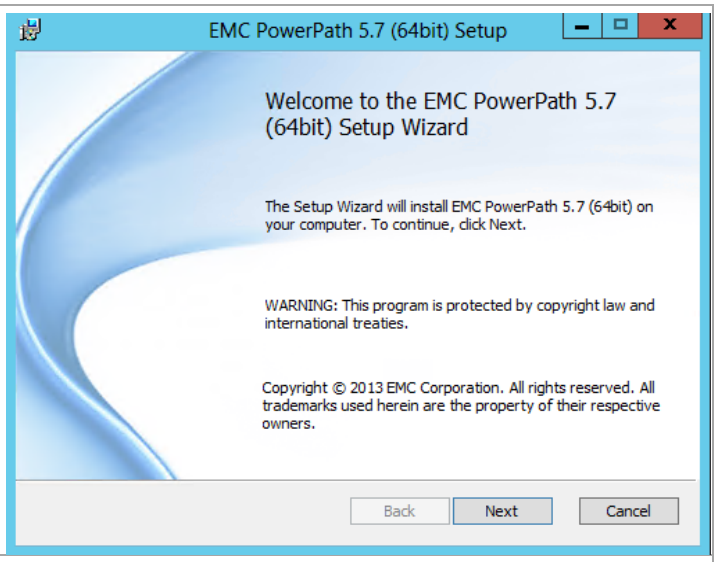
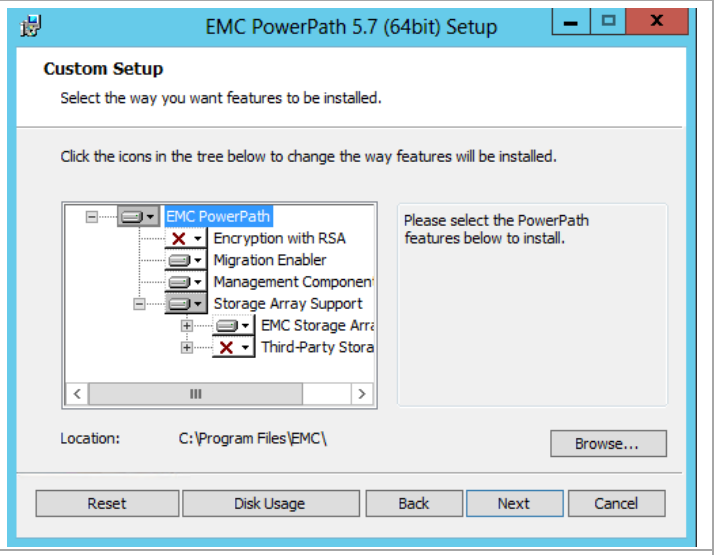
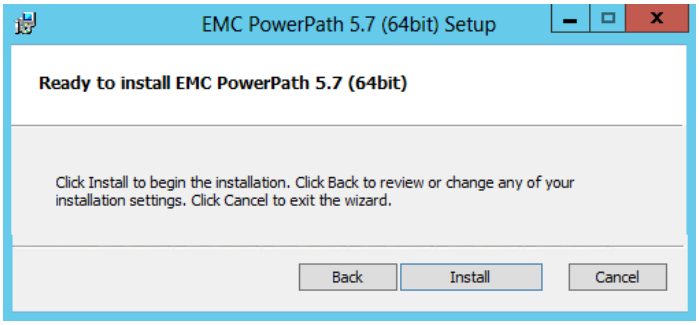
Using the up and down arrows on the right-hand side of the screen, select the various connections and arrange them so Management, LiveMigration, and CSV are ordered as first, second, and third. Click **OK** to continue.	

Repeat this section for each of the Cisco blades in your environment.

Install EMC PowerPath

As a part of tailoring each system, EMC PowerPath can be installed for enhanced mult-pathing functionality. EMC PowerPath for Windows version 5.7 or higher should be used.

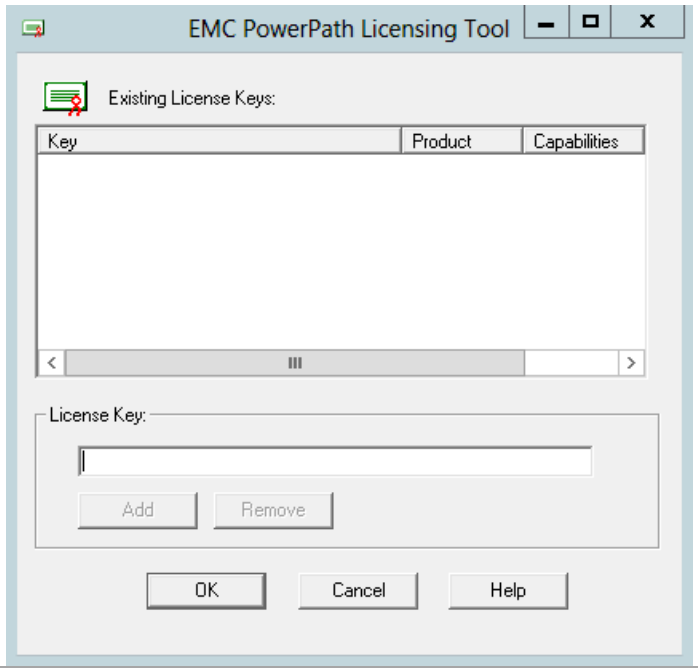
Launch the EMC PowerPath installer, EMCPower.X64.signed.5.7.b223.exe Click **Next**.	

Click **Next** at the copyright information screen	
Accept the default feature installation options and select **Next**	
Select **Install**.	

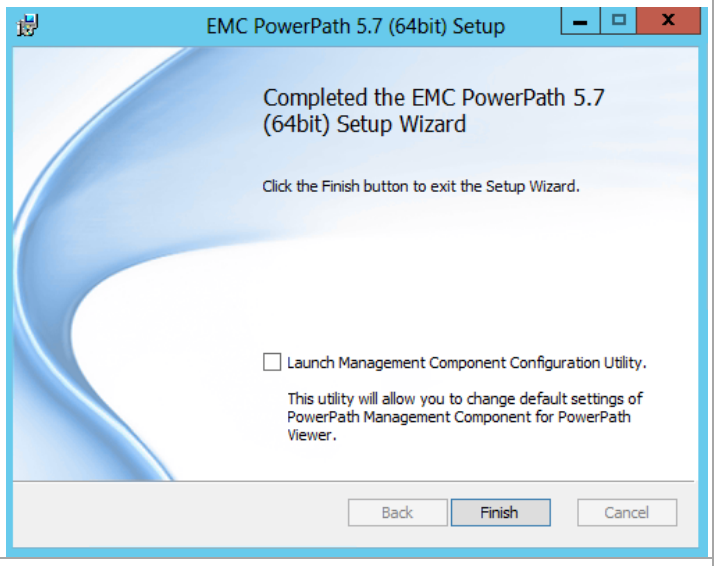
When prompted, enter the appropriate license key for your environment and select **OK**.

Note: If no license key is entered, PowerPath will be unlicensed and will run in a "basic failover" mode, which allows two storage port connections to one HBA. The other HBA will be marked as unlicensed.

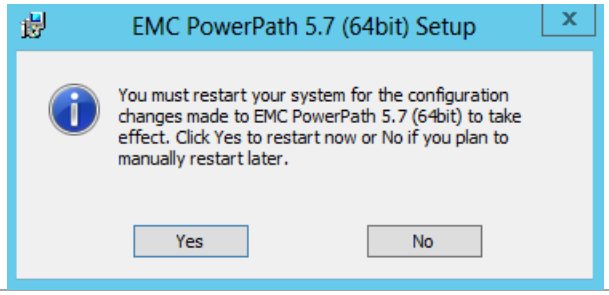
An appropriate license should be obtained, otherwise PowerPath should be uninstalled and native Windows Server 2012 MPIO should be used.



Select **Finish**



Select **Yes** to reboot the server and complete the installation.

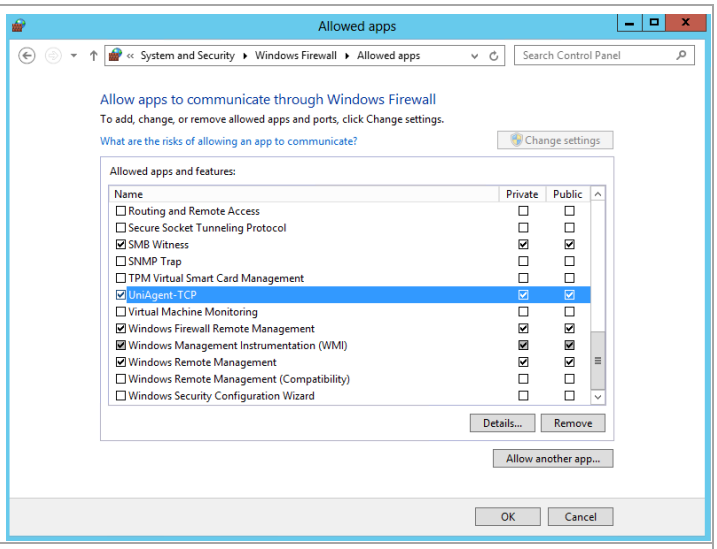
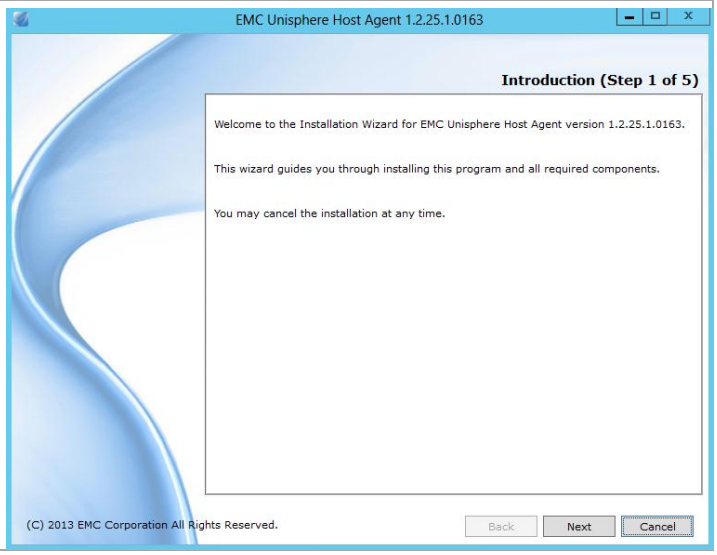


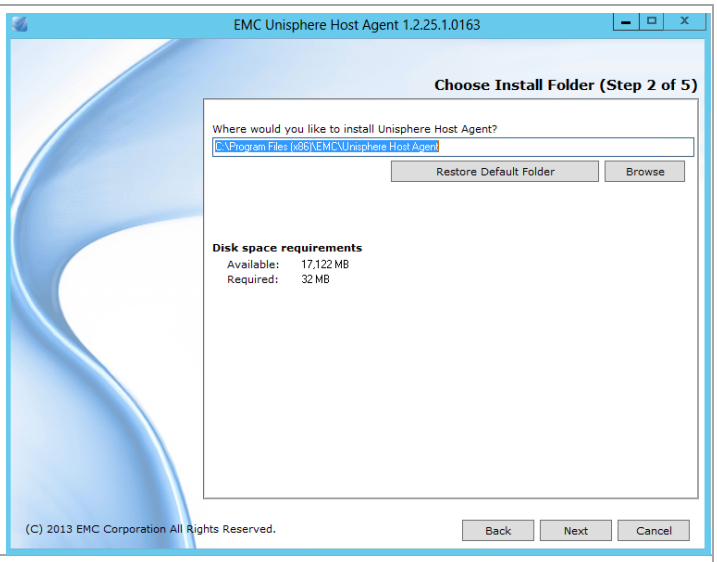
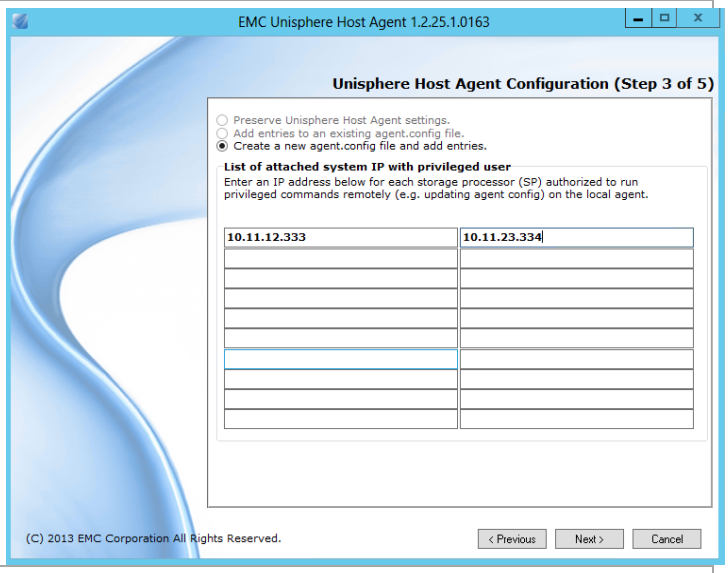
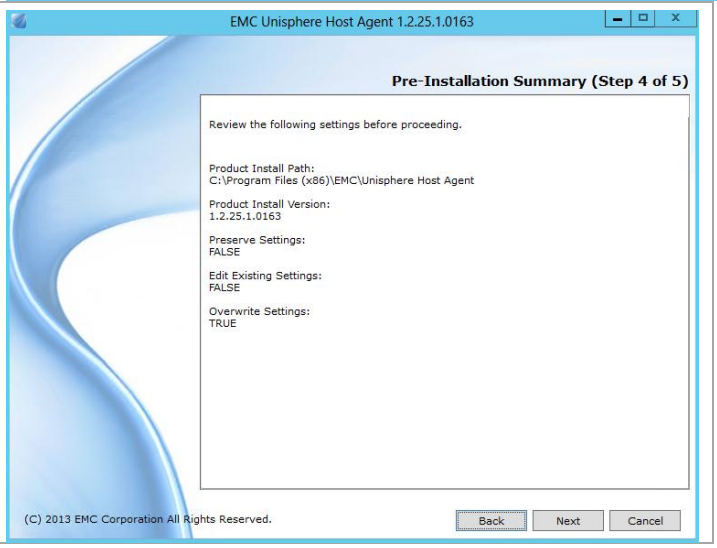
Install Unisphere Host Agent

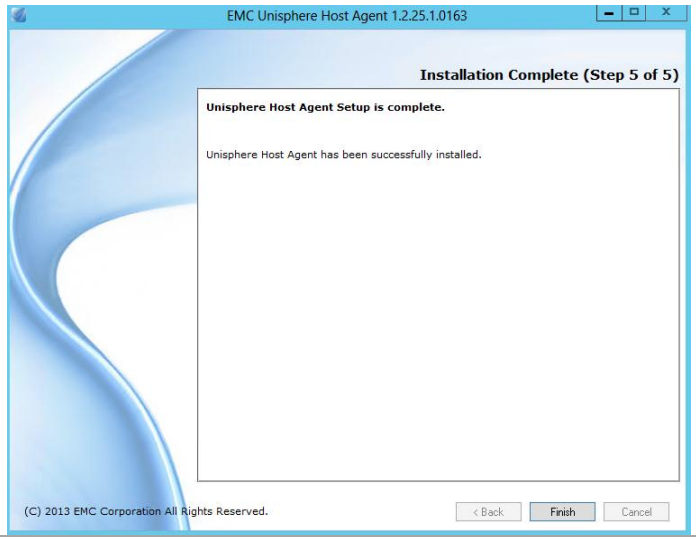
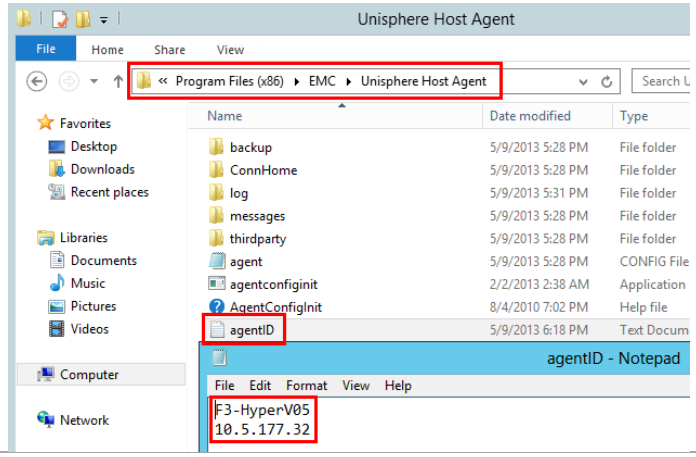
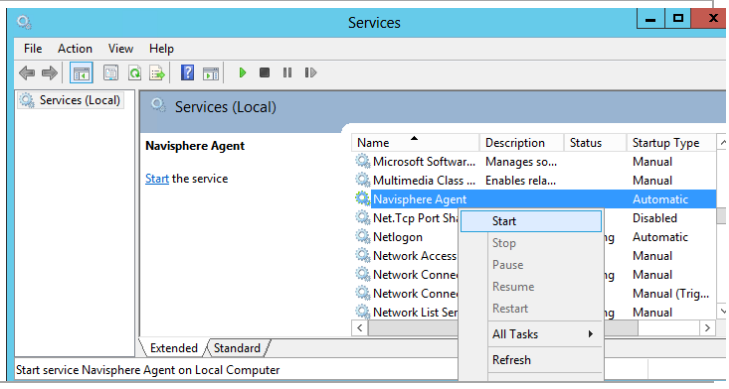
The Unisphere Host Agent allows for host specific information to be sent to management applications, like Unisphere, for ease of administration. LUN mapping and Operating System information as well as initiator information can be forwarded from a server to the VNX via the agent.

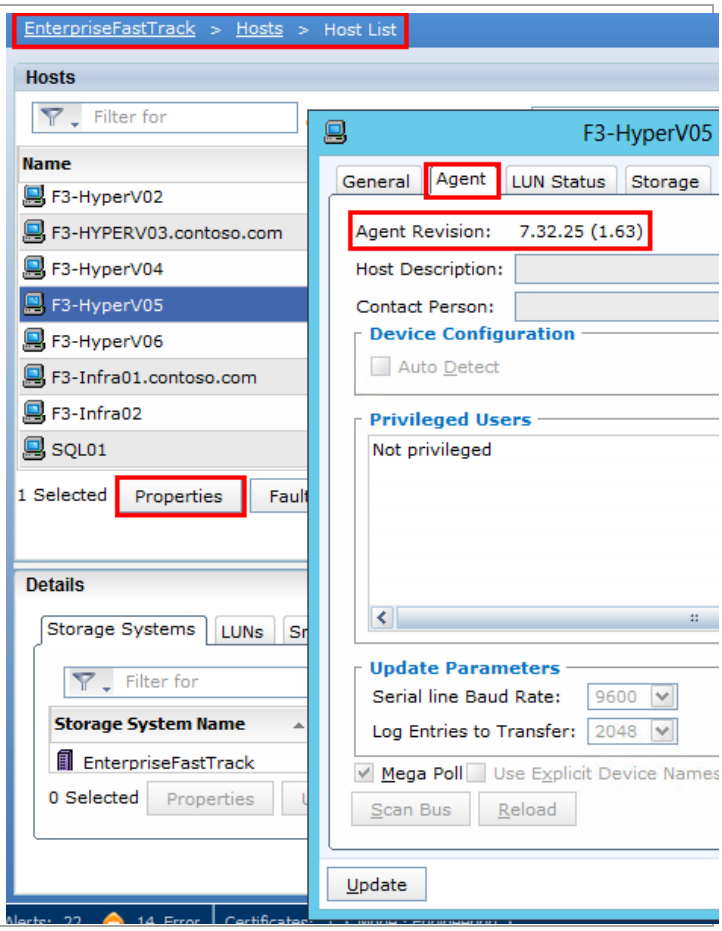
Follow the procedure below to install the Unisphere Host Agent on either a physical Windows Server 2012 server or Virtual Machine.

Note: For virtual machines with iSCSI access to the array, configure the iSCSI connections first prior to installing the agent. This will allow the agent to discover the configured paths and automatically register the iSCSI initiators with the VNX.

Run the following command, from an elevated PowerShell command window, to open the required firewall port for the Unisphere Host Agent: `New-NetFirewallRule -Name UniAgent-TCP -DisplayName UniAgent-TCP -Action Allow -Direction Inbound -Protocol TCP -LocalPort 6389`	
Launch the EMC Unisphere Host Agent installer, UnisphereHostAgent-Win-32-x86-en_US-1.2.25.1.0163-1.exe Click **Next**.	

Choose installation directory and select **Next.**	
Enter the IP Addresses of each block service processor (SPA and SPB) and select **Next**	
Select **Next** after reviewing the Pre-Installation Summary to begin the installation.	

Select **Finish** to complete the install.	
The Unisphere Host Agent will bind to the first NIC within the binding order on the host. This needs to be a NIC which can communicate with the VNX SP IP addresses. If this ends up being the incorrect NIC, use the agentID.txt to set the correct interface. In the installation directory for the Unisphere Host Agent (default = C:\Program Files (x86)\EMC\Unisphere Host Agent) create a file called agentID.txt. Within the file, place the server name on the first line, press enter, and then place the IP address of the desired management interface on the second line.	
From a command window or from the services control panel start the “Navisphere Agent” `net start "Navisphere Agent"`	

Validate the host agent is pushing information to the VNX from the **Hosts > Host List** menu in Unisphere	

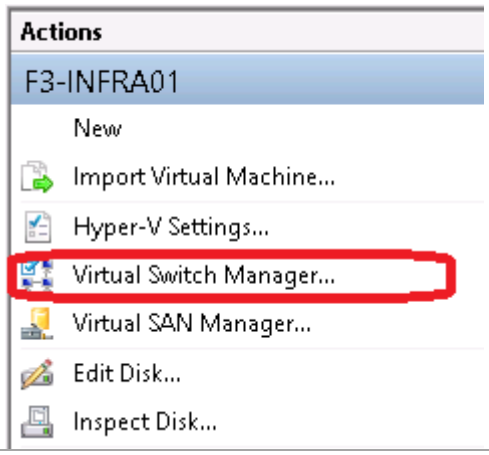
6.7 Create Hyper-V Cluster

When you have completed the build of two servers to SAN boot in a multipath IO environment, have all the network adapters configured the same, and the hosts joined to the Active Directory domain, you will create the cluster on which all the System Center 2012 SP1 virtual machines will be deployed. This cluster can be expanded up to a total of 64 hosts for running VMs within the Microsoft private cloud. It is recommended that the Fabric Management cluster remain a separately managed cluster and that it not be used for tenant VMs, but Windows does provide enough security to isolate different VMs, so it is totally acceptable to use the nodes of the Fabric Management cluster for running VMs, if that is desired.

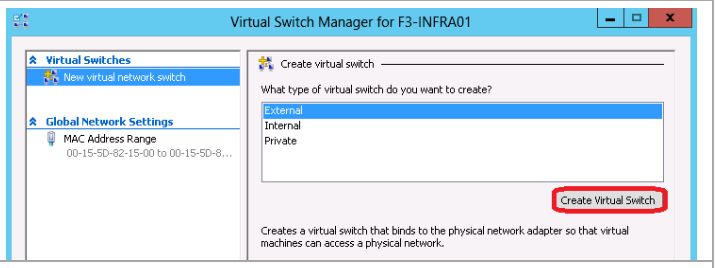
Hyper-V Network Configuration

Before clustering the Hyper-V hosts, configure the various Hyper-V virtual switches that will be used by the virtual machines. This needs to be exactly the same on every Hyper-V host for the infrastructure management cluster.

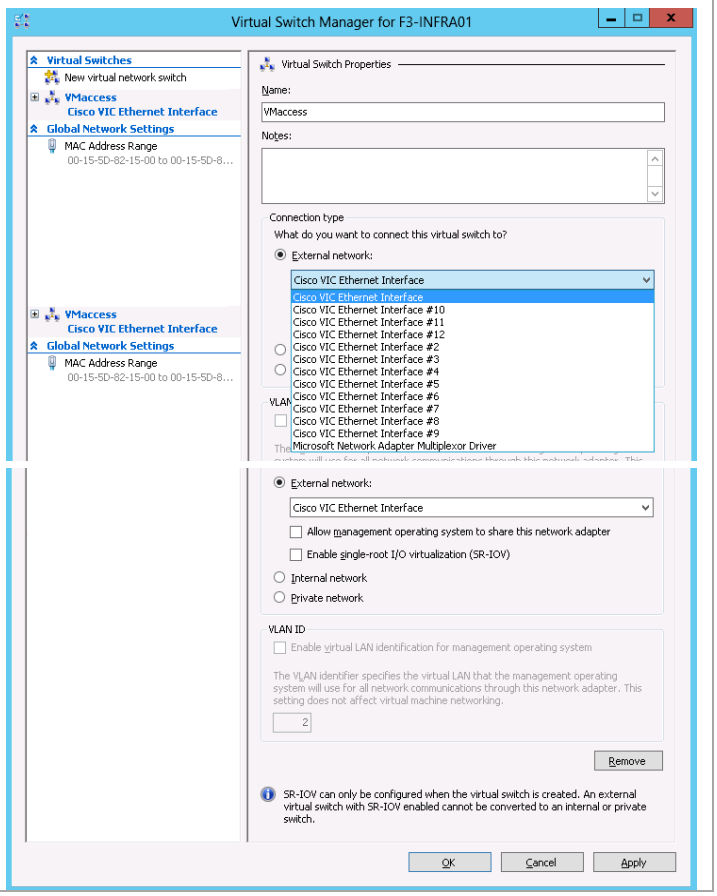
From Server Manager, use the **Tools** menu to launch the Hyper-V Management console.
Alternatively, type **virtmgmt.msc** from a PowerShell window.
From the **Actions** pane, click on **Virtual Switch Manager…**



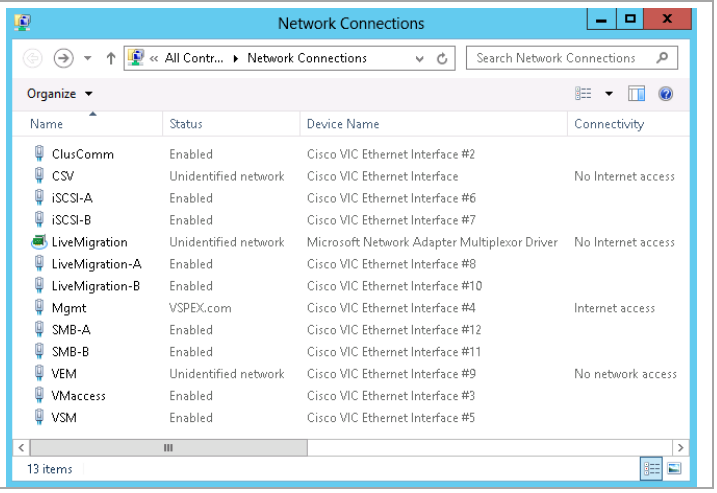
From the Virtual Switch Manager window, ensure **New virtual network switch** is highlighted in the Virtual Switches pane. Ensure **External** is highlighted in the Create virtual switch pane.
Click on the **Create Virtual Switch** button.



In the window that opens, enter the name of one of the virtual switches that will be created into the **Name** field.
Optionally, you can include **Notes** or descriptive information.
Ensure the **External** radio button is selected.
From the dropdown list of NICs, select the NIC that is to be used for creating the virtual switch. You can look at a Network Connections window to see which NIC you need to select.
After selecting the proper interface, ensure no other radio buttons or check boxes are selected.
You can create multiple virtual switches at one time. Simply go back to the top and select **New virtual network switch** and repeat for the other interfaces on which you will be creating virtual switches, i.e. **ClusComm, iSCSI-A, iSCSI-B** and optionally **SMB-A** and **SMB-B.**
Click **OK** to create the virtual switches. You will receive a warning message about possible network disruption, but as you are not changing the network from which you are accessing the Hyper-V host, you will have not issue.



When completed, your Network Connections should look something like this. (Device names will vary)
Network interfaces that have been defined as virtual switches will show **Enabled** in the Status column.
The two interfaces that were teamed for LiveMigration also show as **Enabled**.
The **Unidentified network** entries are networks that are 'private' networks, i.e. not used for accessing the outside network.
For most configurations, you should see only the Mgmt network with internet access.



Create Shared Storage

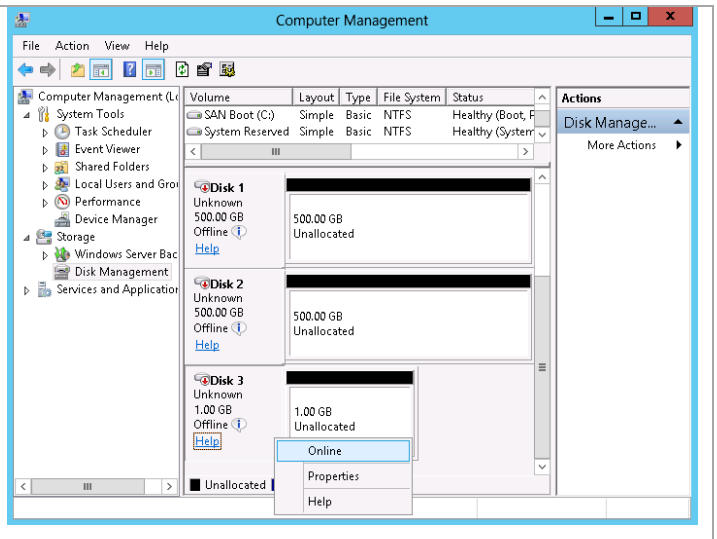
Microsoft Failover Clusters use shared storage for storing the VMs. A minimum of three shared LUNs is recommended for the Fabric Management cluster. If there Fabric Management cluster is also going to be used for other VMs, it would be recommended to create additional LUNs for those VMs.

- Witness Disk – 1 GB
- Cluster Shared Volume 1 – 500 GB (recommended minimum)
- Cluster Shared Volume 2 – 500 GB (recommended minimum)

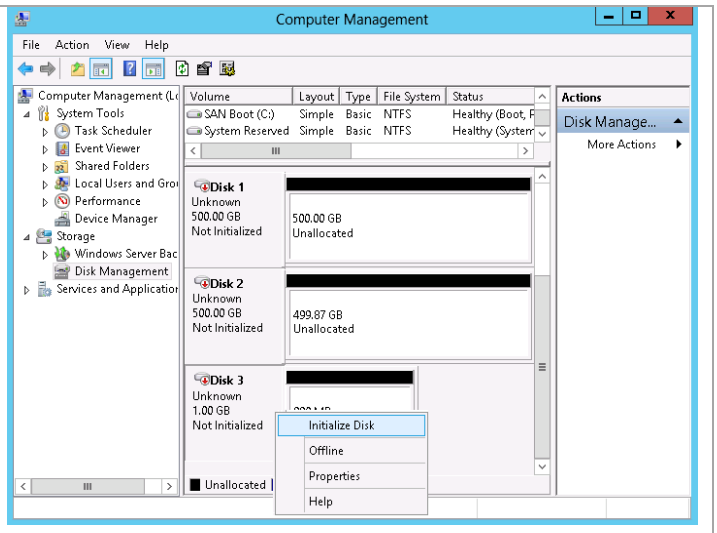
When these LUNs are created, they have to be added to the storage groups assigned to the two hosts that will be used to form the Fabric Management cluster. When the same LUN is added to multiple storage groups, the VNX will display an error message cautioning about the possibility of corrupting data. The clustering software controls access to the LUNs, so that is acceptable.

Note: Before you can test and form the cluster, it is necessary to format the shared LUNs as NTFS volumes. Perform the following steps on only one node of the cluster to format the drives.

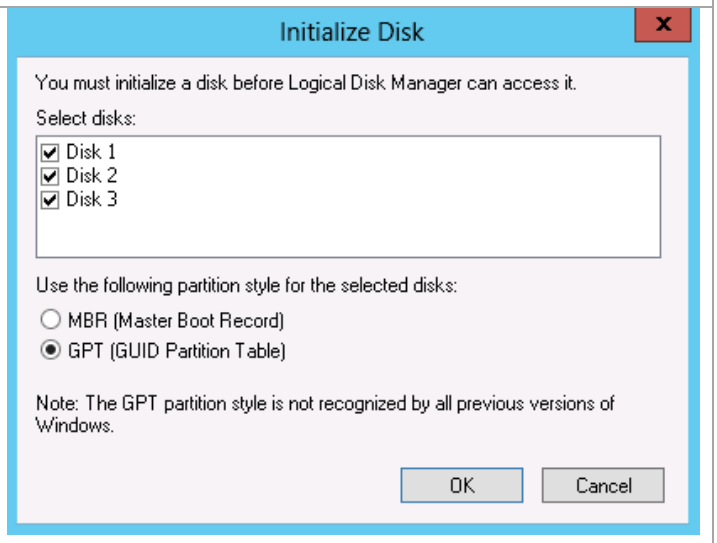
From **Server Manager** on one of the hosts to which the storage has been presented, select **Tools > Computer Management**.
(Alternatively, type `compmgmt.msc` into a command or PowerShell window.)
Right-click on the area under the disk number designation and select **Online** to bring the volume online.
Repeat for each new LUN.



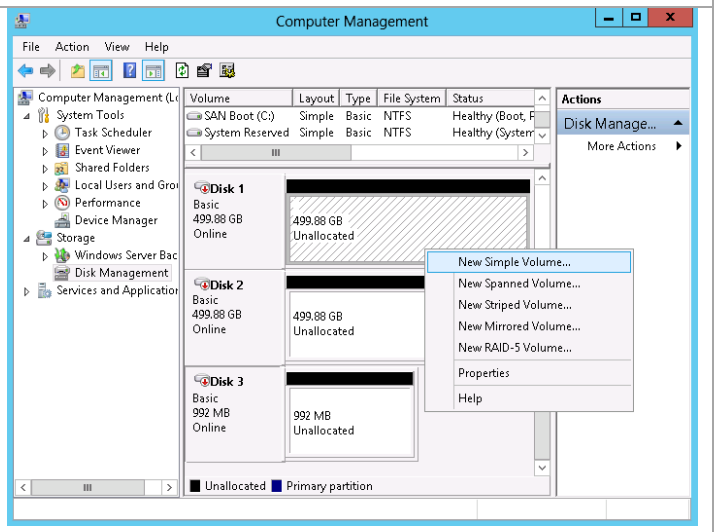
After all disks are online, right-click in the same area on one of the disks and select **Initialize Disk**.

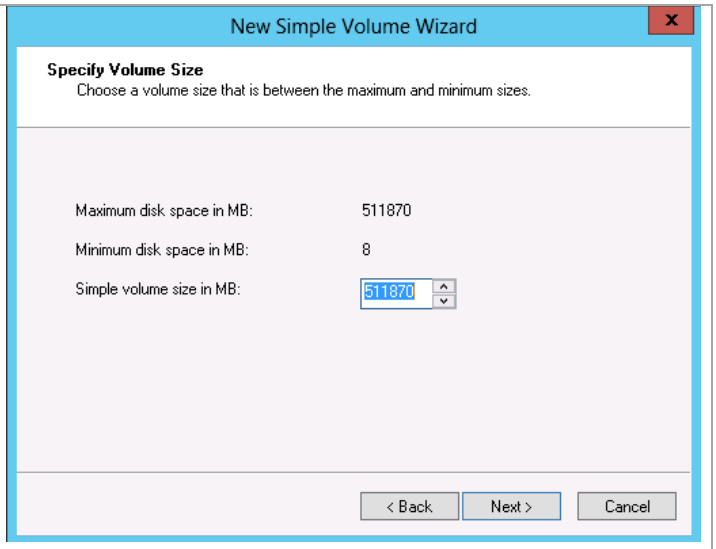
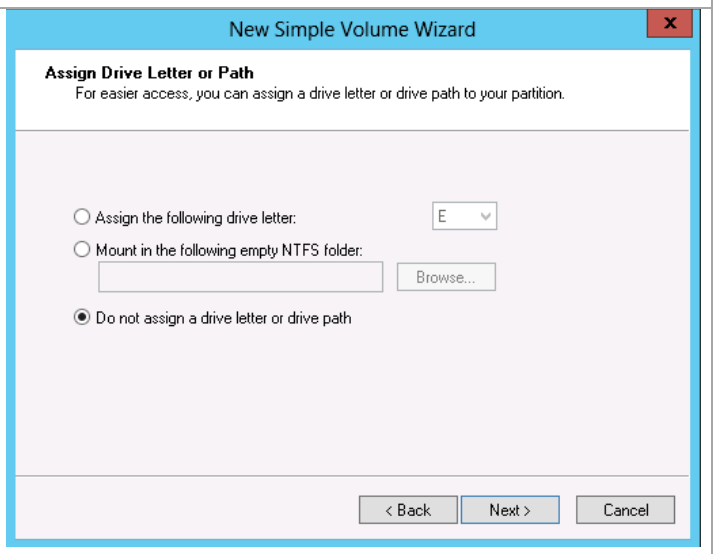


All uninitialized disks will be listed. It is recommended to use GPT disks for clustering, so select the radio button by **GPT (GUID Partition Table)**.
Click **OK** to start the initialization.

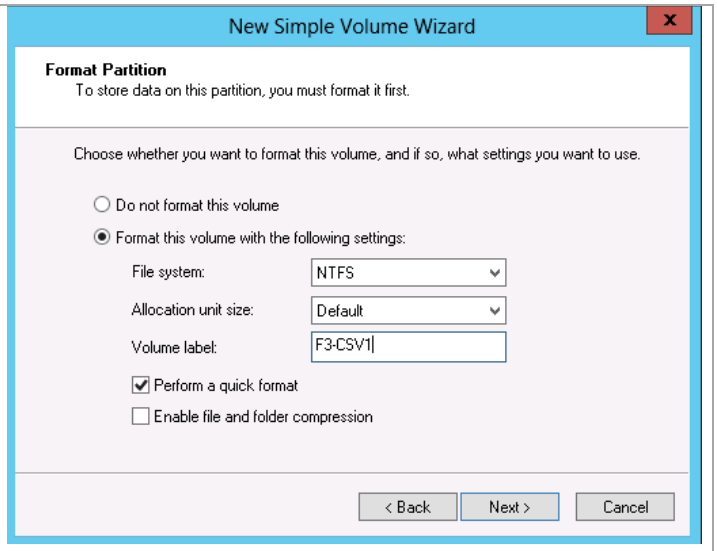


Right-click on one of the disks and select **New Simple Volume…**
This brings up the **New Simple Volume Wizard** window. Click **Next** to continue.

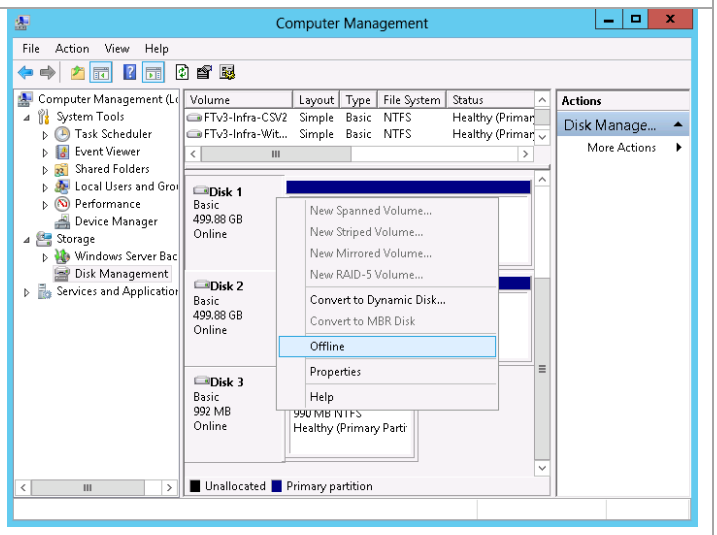


Accept the values in the **Specify Volume Size** window. Click **Next** to continue.	
In the **Assign Drive Letter or Path** window, click the radio button by **Do not assign a drive letter or drive path**. **Note:** Cluster Shared Volumes are accessed from mount points, so no drive letter is needed. Disk Witnesses are not accessed by any user functions, so no drive letter is needed. Click **Next** to continue.	

It is a good practice to enter a useful identifier in the **Volume label** field.
Click **Next** to continue.
A summary window displays. Validate what you selected. If any changes are needed, use the Back button to get to the window to correct it. Otherwise, click **Finish** to complete the formatting process.
Repeat the process to create a new simple volume on each LUN.



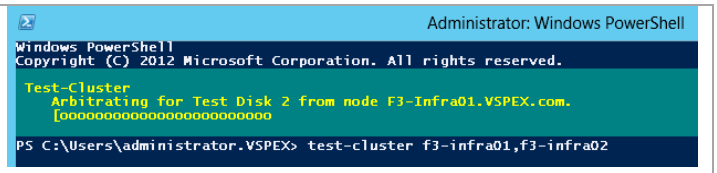
After all disks have been formatted and volumes created, place the disks offline.
Right-click on the disk and select the **Offline** option.



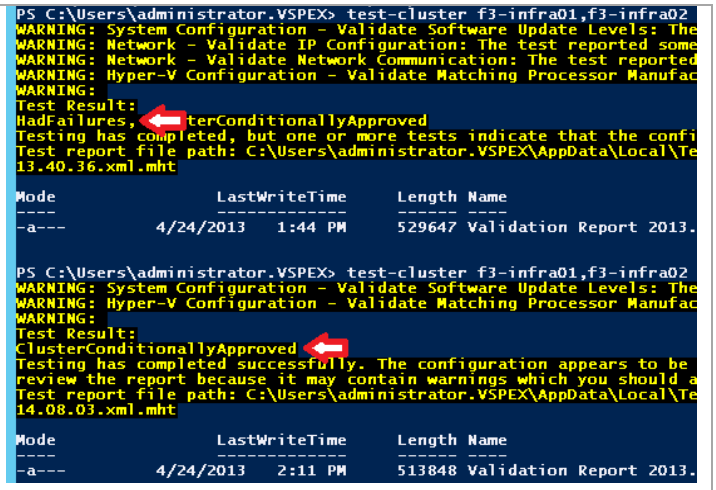
Before running the Cluster Validation Wizard, it is a good practice to bring the disks online and offline on the other node(s) of the cluster. The Cluster Validation Wizard will do this, too, but checking beforehand will save the time it takes to run the wizard if you need to do some troubleshooting.

Run Cluster Validation Wizard

The easiest way to run the Cluster Validation Wizard is to execute from a PowerShell window.
`Test-Cluster F3-Infra01,F3-Infra02`



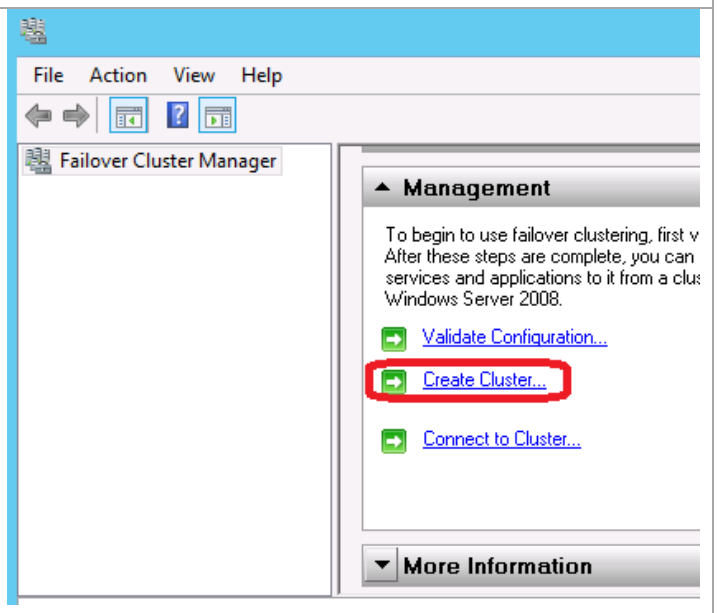
It is not uncommon to have errors or warnings. The first run in the screen shot at the right shows a message of **HadFailures**. Failures must be fixed before creating the cluster.
The second run shows a test run with no failures, but there were some warnings. Upon investigation, it was determined that the warnings were expected and the cluster can be created.
The last line in yellow gives the location of the report file detailing the test results.

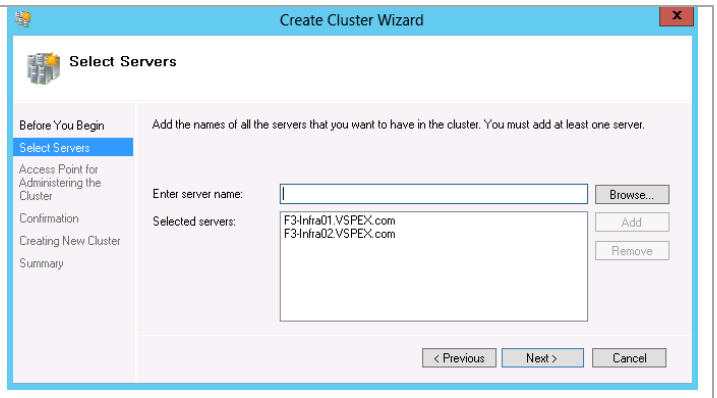
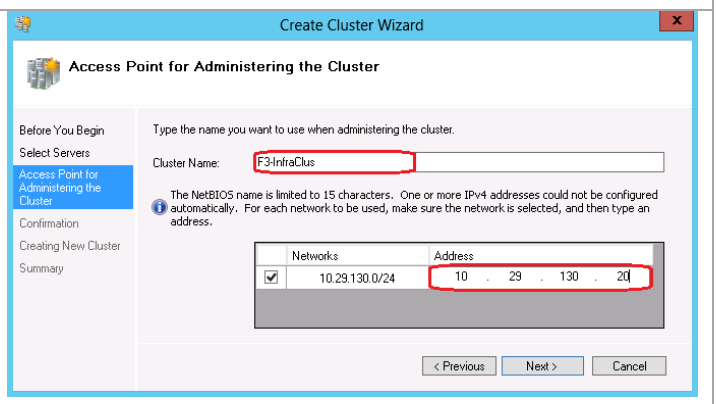
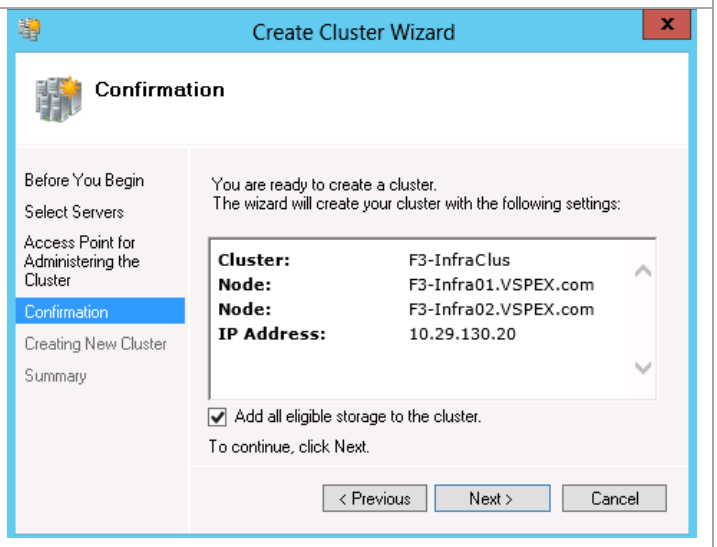


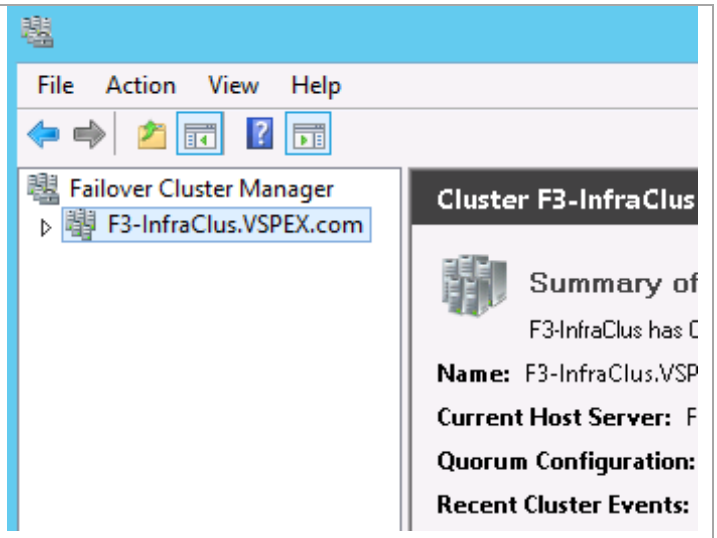
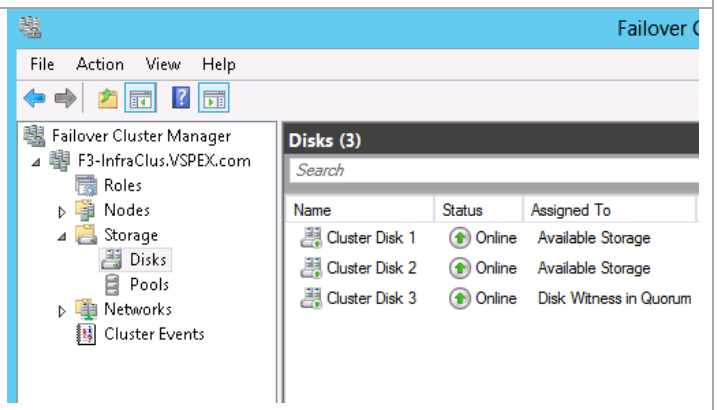
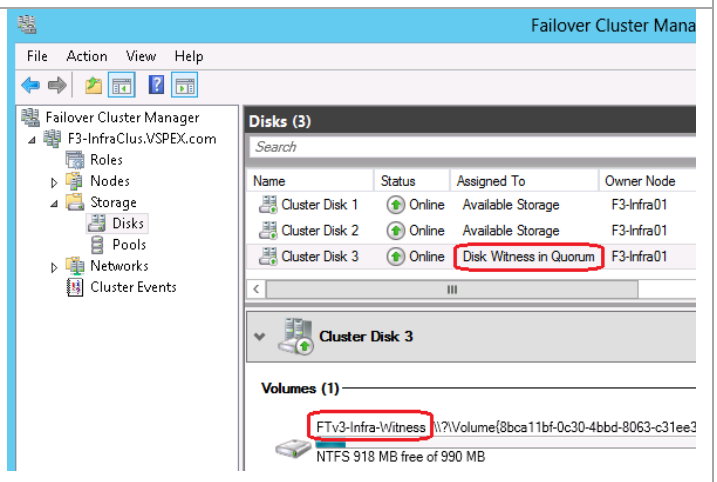
Create Fabric Management Cluster

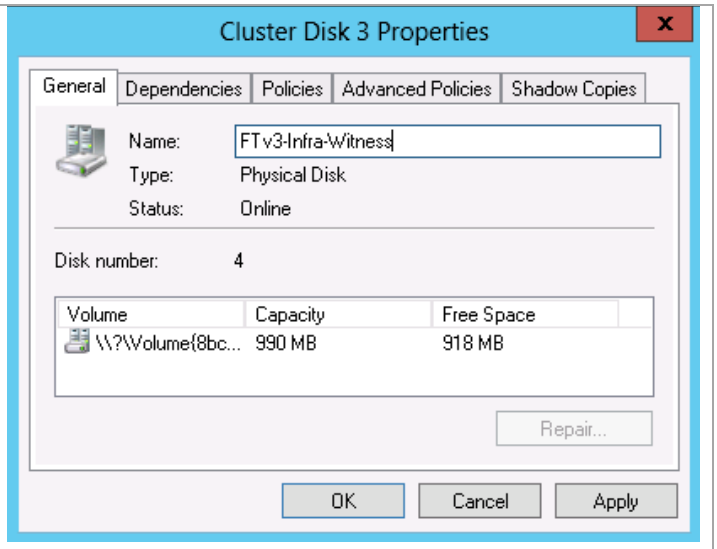
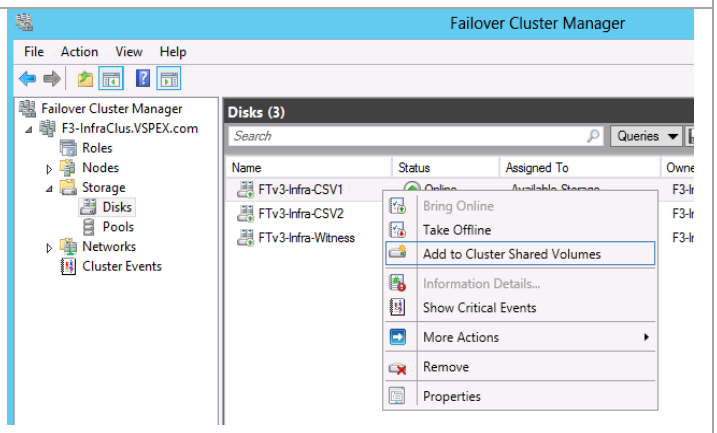
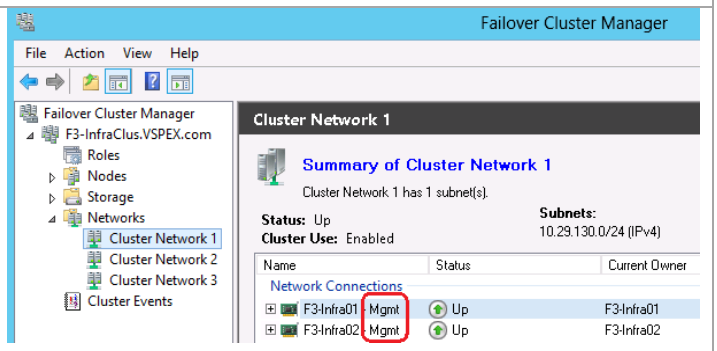
From Server Manager, launch the Failover Cluster Manager from **Tools > Failover Cluster Manager**.

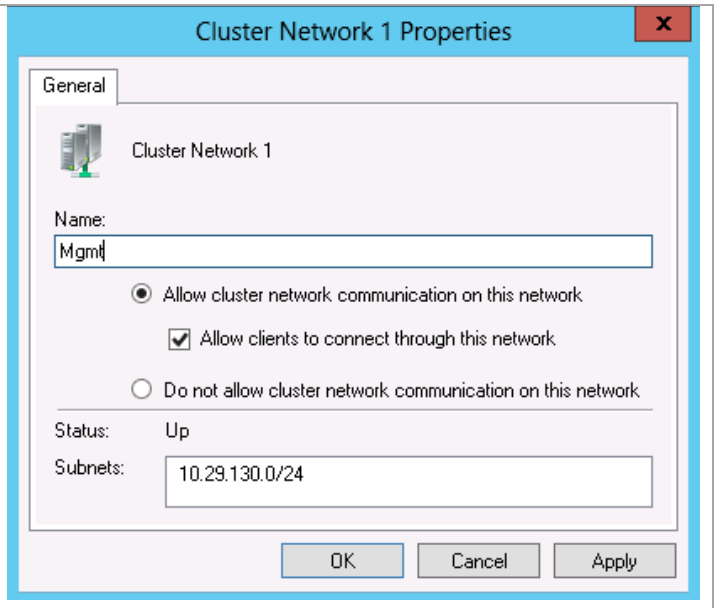
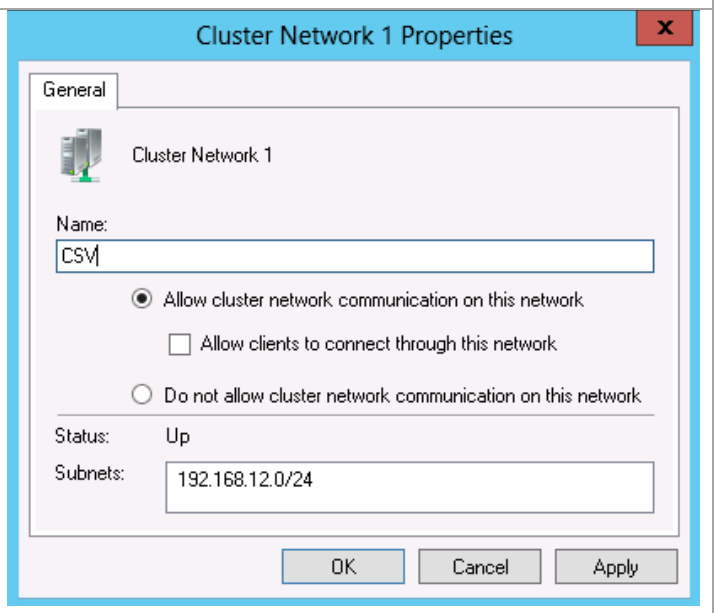
In the **Management** section of the Failover Cluster Manager, select **Create Cluster…**.
This launches the Create Cluster Wizard. On the Before You Begin window, click **Next** to continue.



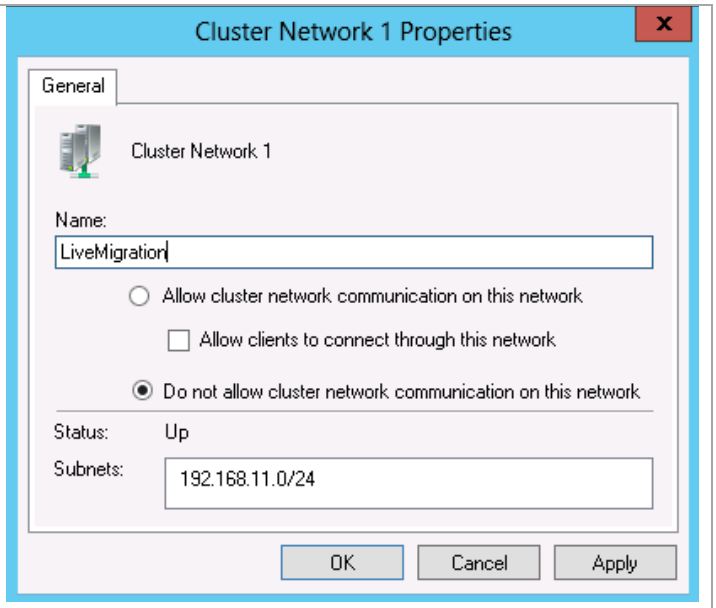
In the **Select Servers** window, browse Active Directory, enter the FQDN or NetBIOS names individually, or enter them in a comma separated list. Click **Next** to continue after the nodes have been selected.	
In the Access Point for Administering the Cluster window, enter a name in the **Cluster Name** field. This name will be added to Active Directory as a Cluster Name Object. If you are not using DHCP for address assignment, you will be prompted to enter an IP address. The Cluster Name and IP address will be registered in DNS.	
Check your answers on the Confirmation window. Click **Next** to create the cluster. Click **Finish** on the Summary window. If any errors occurred, they would be listed on the summary window. They would need to be resolved before continuing. The cluster can also be created with the following PowerShell command: `New-Cluster -Node <Node1>, <Node2> -Name <ClusterName> -StaticAddress <ClusterIPAddress>`	

If you are running from one of the nodes, the Failover Cluster Manager will show the cluster. If you are running from the workstation, you will need to use the option to **Connect to Cluster…** and enter the cluster name.	
Expand the cluster name, expand the Storage, and click on **Disks** to expose the disks. By default, the create cluster process will automatically choose the smallest disk for use as the disk witness.	
It is a good practice to change the name of the disks to be the same as the volume name. Click on any disk and you can see the volume ID of the disk in the disk properties at the bottom of the window. Right-click on the disk at the top of the window and select **Properties**.	

In the properties window, change the **Name** of the disk to be the same as the volume name. Repeat for all disks.	
Right-click on the first disk that you want to be a Cluster Shared Volume. Select the **Add to Cluster Shared Volumes** from the drop-down menu. Repeat for other disks that will be CSVs. **Note:** It is a good practice to ensure the disks are added in a sequence that is meaningful. As disks are added, mount points for referencing the disks are created sequentially.	
Expand the Networks and click on one of the networks. Ensure the networks are named the same on all nodes. **Note:** Same names are not required, but it greatly assists in troubleshooting. Right-click and select **Properties**.	

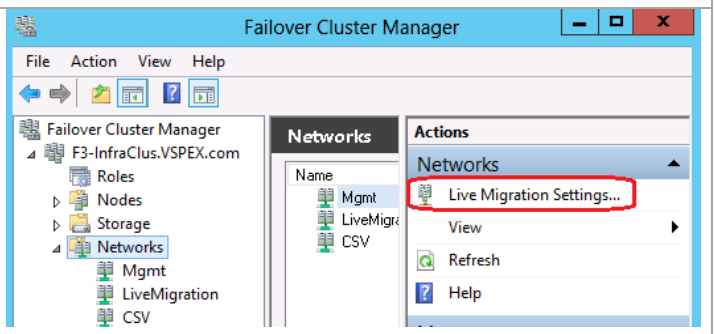
Rename the network names according to the names they are known to by the operating system. Management network should have **Allow cluster network communication on this network** and **Allow clients to connect through this network** selected.	
For the CSV network, ensure just the **Allow cluster communication on this network** is selected.	

On the LiveMigration network, ensure just the **Do not allow cluster network communication on this network** is selected.



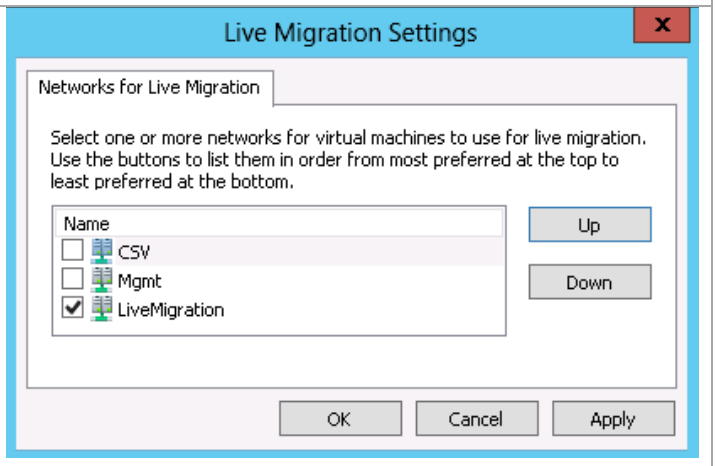
Click on **Networks**.

From the **Actions** menu on the right-hand side of the window, click on **Live Migration Settings…**



In the Live Migrations Settings window, ensure that only the box by the LiveMigration network is checked.

Note: Only this network needs to be checked because we have set this network up as a teamed network. If no team is used, the Management network should be checked to ensure Live Migration capability should the network be lost.



An alternate method to rename the generic network names and assign the proper function to each is to use a PowerShell script with these commands (modified for your environment).

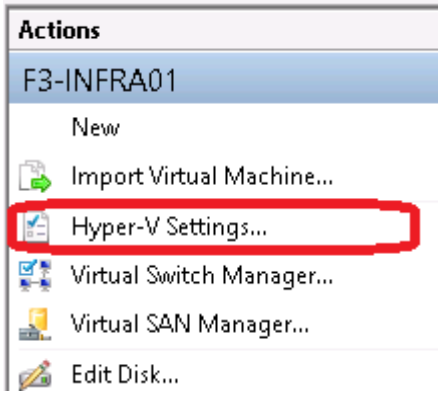
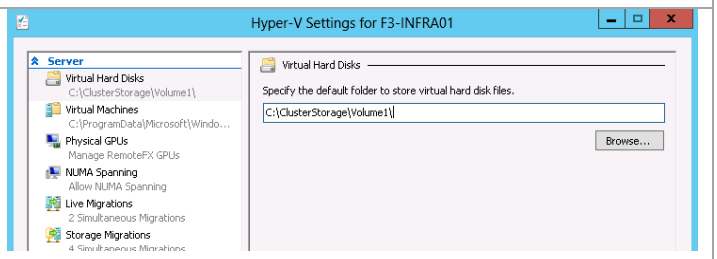
```
(Get-ClusterNetwork -Cluster F3-Infraclus | ? {$_.Address -like "10.29.130.*" }).Name = "Mgmt"
```

```
(Get-ClusterNetwork -Cluster F3-Infraclus | ? {$_.Address -like
"192.168.12.*" }).Name = "CSV"
(Get-ClusterNetwork -Cluster F3-Infraclus | ? {$_.Address -like
"192.168.11.*" }).Name = "LiveMigration"

(Get-ClusterNetwork -Cluster SMB3-Clus -Name Mgmt).Role = 3
(Get-ClusterNetwork -Cluster SMB3-Clus -Name CSV).Role = 1
(Get-ClusterNetwork -Cluster SMB3-Clus -Name LiveMigration).Role = 0
```

The Fabric Management cluster is complete.

By default, Hyper-V will store the virtual hard drives for created virtual machines on the system drive. It is easy to set up Hyper-V to default to the Cluster Shared Volumes for storage. This is not an absolute requirement, but it does make management easier. A good practice is to have the same number of Cluster Shared Volumes as you have nodes in the Hyper-V cluster. Each node in the cluster would have a default storage location of one of the Cluster Shared Volumes.

Within the Hyper-V Management console, select **Hyper-V Settings…** from the Actions pane.	
From the Server column, select **Virtual Hard Disks**. In the right column, browse to the C:\ClusterStorage\Volumex (x is a sequence number) location and select it as the default. Click **OK** to accept the change. Repeat for each node of the cluster.	

7 Fabric Management

7.1 Fabric Management Host and Guest Installation

Provisioning Fabric Management Hosts

In order to properly size Fabric Management host systems, the following table outlines the virtual machines (and their default configurations) that are deployed to compose the fabric management component architecture. These virtual machines are hosted on a dedicated two-to-four node Hyper-V failover cluster. These virtual machines serve as the basis for fabric management operations. The following table summarizes the fabric management virtual machine requirements by the System Center component that supports the product or operating system role.

Note: All VMs except the Service Manager Portal are Windows Server 2012. Service Manager Portal is Windows Server 2008 R2 SP1.

Table 17 Design Pattern 2 Virtual Machine Configurations

Component Roles	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
SQL Server Cluster Node 1	8	16	60 Additional 15 LUNs for DBs[1]
SQL Server Cluster Node 2	8	16	60 Shared LUNs
Virtual Machine Manager	4	8	60
Virtual Machine Manager	4	8	60
App Controller	4	8	60
Operations Manager Management Server	8	16	60
Operations Manager supplemental Management Server	8	16	60
Operations Manager Reporting Server	8	16	60
Orchestrator Runbook Server	4	8	60
Orchestrator supplemental Runbook Server	4	8	60
Service Manager Management Server	4	16	60
Service Manager supplemental Management Server	4	16	60
Service Manager portal (must be Windows Server 2008 R2 SP1)	8	16	60
Service Manager Data Warehouse	8	16	60
Windows Deployment Services/Windows Server Update Services	2	4	60
Totals	86	188 GB	900 GB

[1] This solution uses iSCSI for the guest SQL Server Failover Cluster. These LUNs will be provisioned as iSCSI LUNs.

In addition to the System Center virtual machines listed above, there are two more virtual machines for Cisco's Nexus 1000V.

Table 18 Cisco Nexus 1000V Virtual Machine Configuration

Component Roles	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
Primary Nexus 1000V	2	4	5
Secondary Nexus 1000V	2	4	5

At this stage you are expected to have a supportable Fabric Compute Cluster built to support the VM specifications outlined above. Compute, storage and network functionality should all be verified.

Create Fabric Management Virtual Guests

Windows Failover Cluster Manager is used to create the fabric management virtual machines. The installation of the required Windows operating systems can utilize existing customer automated deployment Solutions or a manual build of each virtual machine.

Appendix C: Sample Scripts contains a sample PowerShell script, Create-UcsFtVms.ps1, that can be modified for your environment. It requires that a single VM be created and sysprepped. Then the virtual hard drive (VHDX) of that sysprepped image is copied to become the base for each of the required System Center infrastructure hosts. The VMs are created with the recommended memory and network configurations.

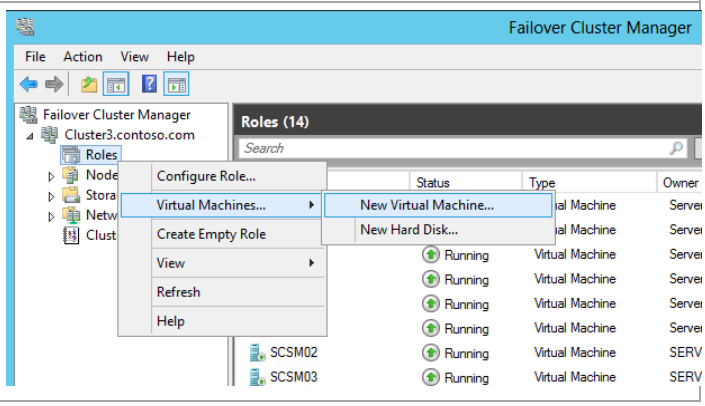
The Create-UcsFtVms.ps1 is a sample script only. It will need to be modified for your particular environment.

If you do not wish to use the Create-UcsFtVms.ps1 PowerShell script, the installation of the required Windows operating systems can leverage existing customer automated deployment solutions or a manual build of each VM. These VMs must be created in the clustered Hyper-V hosts.

The following instructions show how to create the first VM that will be sysprepped for use by the CreateVms.ps1 script. Or these instructions can be used repetitively to individually build each VM with the settings pulled from the table above.

▶ Perform the following steps on the *first fabric management host* computer in the Fabric Management Cluster.

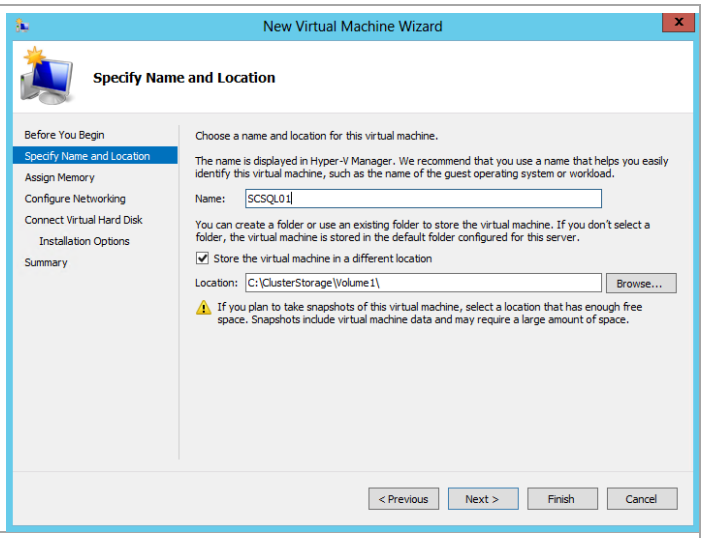
Open the **Failover Cluster Manager** Microsoft Management Console (MMC) snap-in. Navigate to the **Services and applications** node, right-click and select **Virtual Machines…**, and then select **New Virtual Machine…** from the context menu.



The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:

- **Name** – *specify the name of the virtual machine based on the naming conventions of your organization.*

Select the **Store the virtual machine in a different location** check box. In the **Location** text box, specify the location of the cluster shared volumes (CSV) on your fabric management host cluster.
Click **Next** to continue.

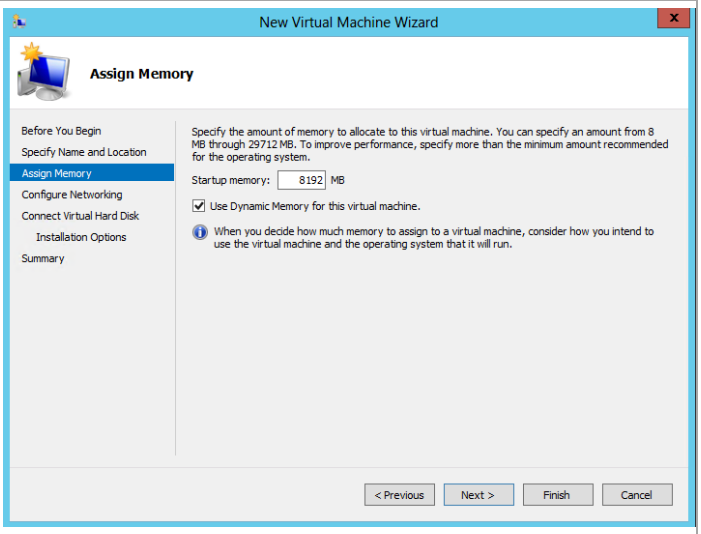


In the **Assign Memory** dialog, provide the following value:

- **Memory** – *specify the amount of memory in megabytes (MB) required for each virtual machine. Identify this value in the configuration table above.*

Click **Next** to continue.

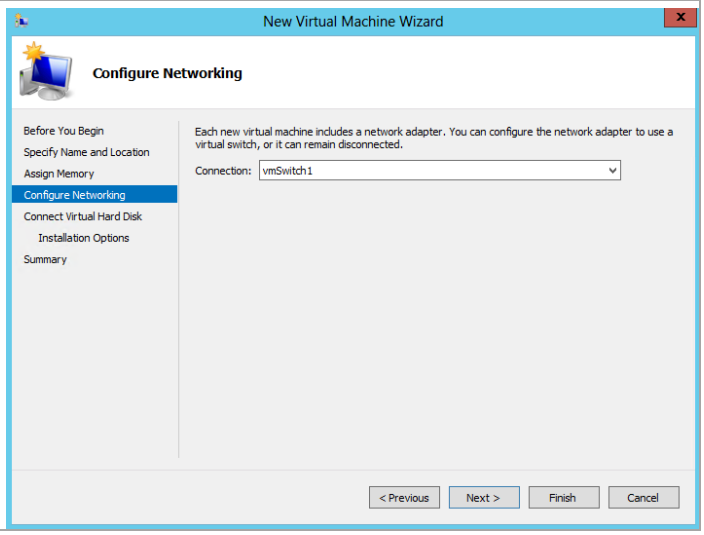
Note: For virtual memory, the products will post a warning if memory is below 8 GB and each virtual machine must have at least 2 GB of startup random access memory (RAM) if dynamic memory is enabled.



In the **Configure Networking** dialog, provide the following value:

- **Connection** – *specify the Virtual Switch network connection this system should participate in from the available connections in the drop-down menu.*

Click **Next** to continue.

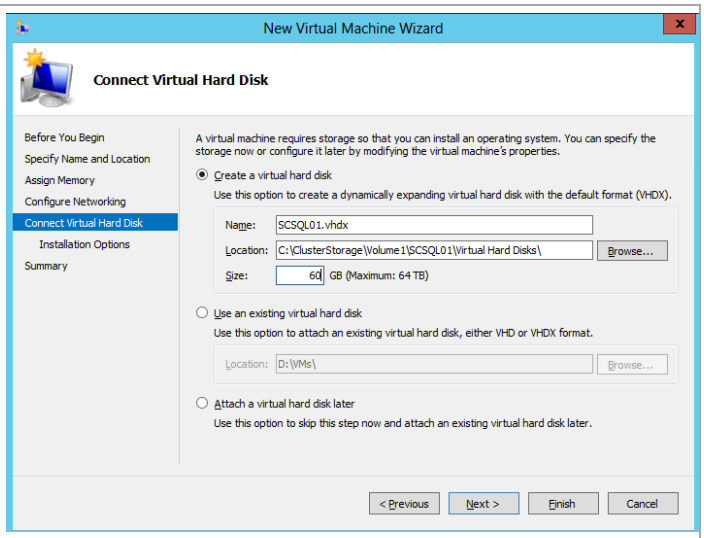


In the **Connect Virtual Hard Disk** dialog, select the **Create a virtual hard disk** option and provide the following values:

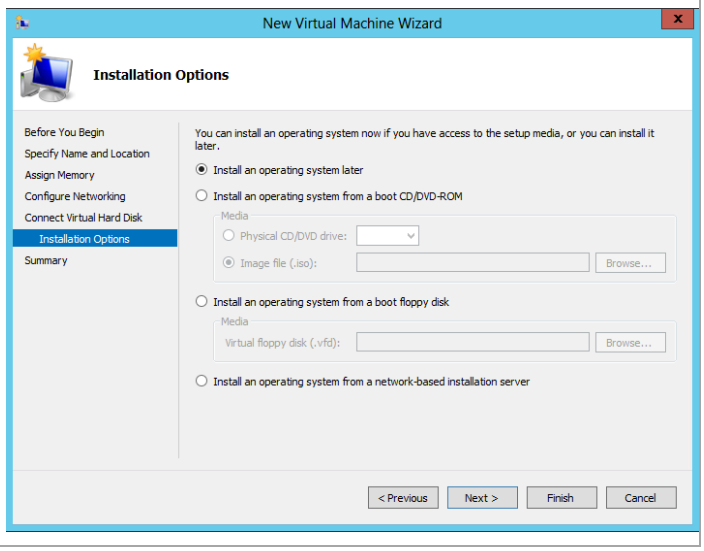
- **Name** – *specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.*
- **Location** – *accept the default location of the CSV on your fabric management host cluster combined with the virtual machine name.*
- **Size** – *specify the size of the VHD (for operating system partitions this should be 60 GB).*

Click **Next** to continue.

Note: Absent any automated imaging process for the new VMs, a VHD (with Windows Server 2012 installed and then sysprepped can be leveraged in place of the new VHD created in this step. This will greatly speed up the provisioning process for the management virtual machines.

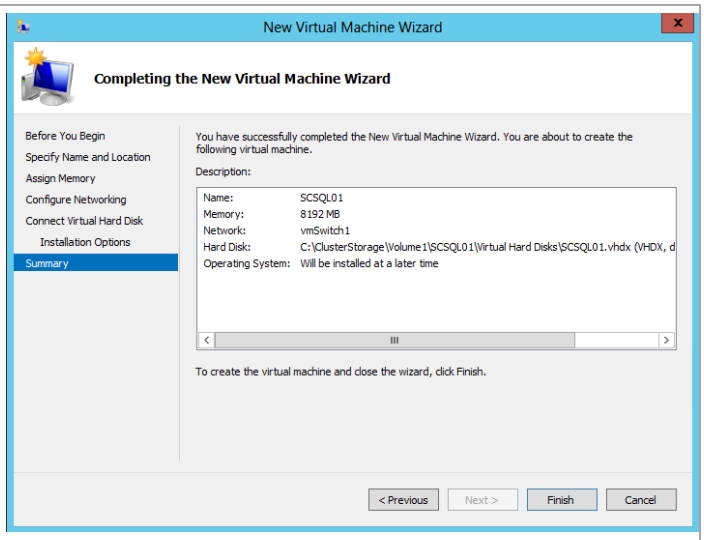


In the **Installation Options** dialog, select the **Install an operating system later** option and click **Next** to continue.

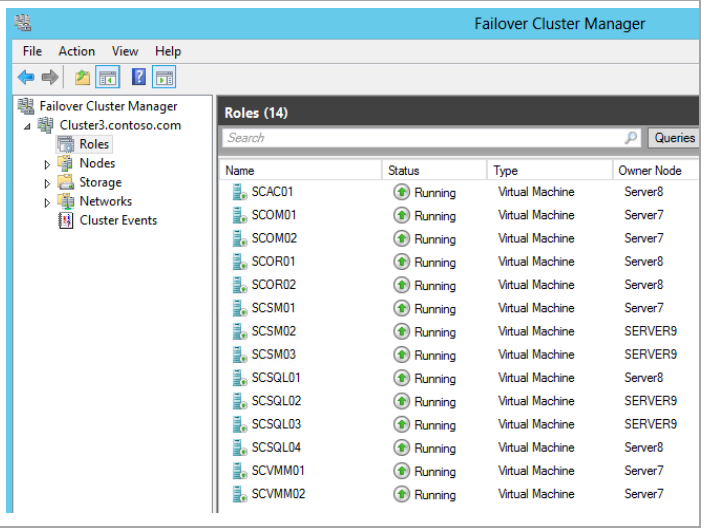


The **Completing the New Virtual Machine Wizard** dialog will display the selections made during the wizard. Click **Finish** to create the virtual machine based on the options selected.

Note: This operation must be completed for each fabric management virtual machine.



After completion, the virtual machines will be available for management in the **Services and applications** node of the **Failover Cluster Manager**.



At this point you can repeat the above steps and manually create all infrastructure VMs. It is much more efficient, though, to sysprep the VM just created and then use it as the basis of all other infrastructure VMs (see the Create-UcsFtVms.ps1 sample script in Appendix B). This is similar to what we did for creating the physical images that were used for creating the host machines. If you manually create all the VMs, remember to install the .Net Framework 3.5.1 Feature within each VM.

Therefore, follow the earlier instructions for running sysprep on this VM by generalizing the image and shutting it down. You can manually make multiple copies of the virtual hard drive (VHD) to multiple directories on the CSVs and manually create the VMs to point to them before running each VM to complete the setup. Or, you can use CreateVms.ps1 script from the appendix to automate that procedure. Remember that the script in the appendix is a sample. It must be modified for each customer environment.

When all the VMs have been created with the sysprepped VHD, you will need to complete the installation of the base operating system environment by booting and running the mini-setup for each VM. Once that is complete, the infrastructure installation can continue with the following instructions.

7.2 Create Required User Accounts and Security Groups

While each System Center 2012 component installation section in this document outlines the individual accounts and groups required for each installation and operation, a short summary is provided in the tables below. Appendix B contains sample scripts for populating users (Add-FTUsers.ps1) and groups (Add-FTGroups.ps1).

Active Directory Domain User Accounts

The following Active Directory user accounts are required for the Fast Track System Center 2012 SP1 installation:

Table 19 Required Active Directory Accounts

Component	User account	Suggested name	Description
System Center	Component installation account	FT-SCInstall	This optional account is used to install all System Center 2012 components.
SQL Server	SQL Server instance service account	FT-SQL-SVC	This account is used as the service account for all instances of SQL Server used in System Center.
Operations Manager	Management server action account	FT-SCOM-Action	This account is used to carry out actions on monitored computers across a network connection.
Operations Manager	System Center Operations Manager configuration service and data access service account	FT-SCOM-SVC	This account is one set of credentials that is used to update and read information in the operational database. Operations Manager verifies that the credentials used for the System Center Operations Manager configuration service and data access service account are assigned to the sdk_user role in the operational database.
Operations Manager	Data Warehouse write account	FT-SCOM-DW	The Data Warehouse write account writes data from the management server to the reporting Data Warehouse and reads data from the operational database.
Operations Manager	Data reader account	FT-SCOM-DR	The data reader account is used to define which account credentials Microsoft SQL Server® Reporting Services uses to run queries against the Operations Manager reporting Data Warehouse.
Virtual Machine Manager	Virtual Machine Manager service account	FT-VMM-SVC	This account is used to run the Virtual Machine Manager service.
Service Manager	Service Manager services account	FT-SCSM-SVC	This account becomes the operational system account. It is assigned to the logon account for all Service Manager services on all Service Manager servers. This account becomes a member of the sdk_users and configsvc_users database roles for the Service Manager database as part of installation. This account also becomes the Data Warehouse system Run As account. If you change the credentials for these two services, ensure that the new account has a SQL Server login in the ServiceManager database and

Component	User account	Suggested name	Description
			that this account is a member of the Builtin\Administrators group.
Service Manager	Service Manager workflow account	FT-SCSM-WF	This account is used for all workflows and is made a member of the Service Manager workflows user role.
Service Manager	Service Manager reporting account	FT-SCSM-SSRS	This account is used by SQL Server Reporting Services (SSRS) to access the DWDataMart database to get data for reporting. The account becomes a member of the db_datareader database role for the DWDataMart database. Becomes a member of the reportuser database role for the DWDatamart database.
Service Manager	Microsoft SQL Server® Analysis Services account for OLAP cubes	FT-SCSM-OLAP	This account is used by SQL Server Analysis Services (SSAS) for Service Manager reports.
Service Manager	Operations Manager alert connector	FT-SCSM-OMAlert	This account is used for Service Manager Operations Manager Alert connector operations.
Service Manager	Operations Manager CI connector	FT-SCSM-OMCI	This account is used for Service Manager Operations Manager continuous integration (CI) connector operations.
Service Manager	Active Directory connector	FT-SCSM-ADCI	This account is used for Service Manager Active Domain connector operations.
Service Manager	Virtual Machine Manager CI connector	FT-SCSM-VMMCI	This account is used for Service Manager Virtual Machine manager connector operations.
Service Manager	Orchestrator CI Connector	FT-SCSM-OCI	This account is used for System Center Orchestrator connector operations.
Orchestrator	Orchestrator services account	FT-SCO-SVC	This account is used to run the Orchestrator Management Service, Orchestrator Runbook Service and Orchestrator Runbook Server monitor service.
App Controller	App Controller services account	FT-SCAC-SVC	This account is used to run all App Controller services.

Active Directory Domain Security Groups

The following Active Directory security groups are required for the Fast Track System Center 2012 installation:

Table 20 Required Active Directory Security Groups

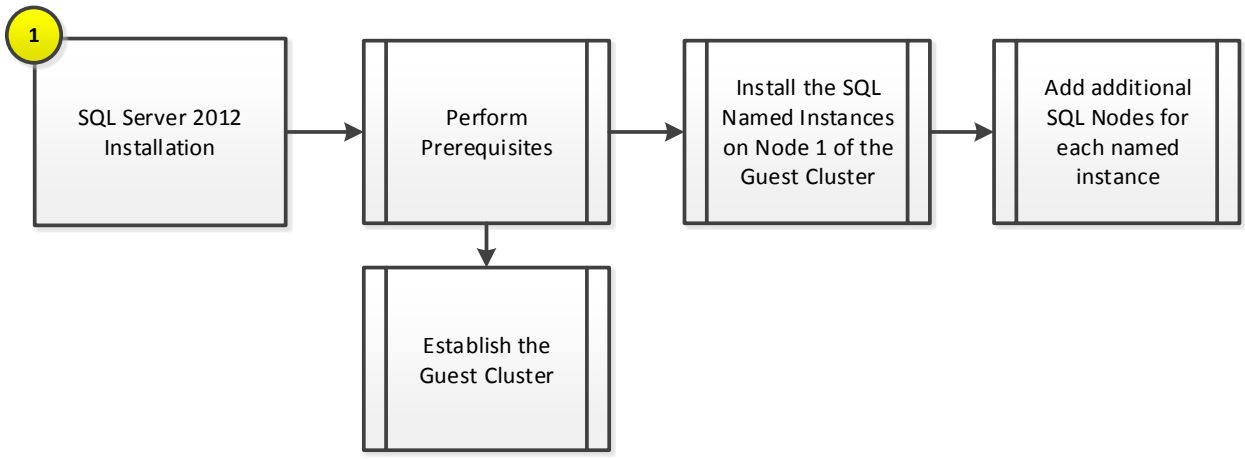
Component	Group	Name	Group notes
System Center 2012	System Center Administrators	FT-SC-Admins	This group's members are full Admins on all System Center components.

Component	Group	Name	Group notes
SQL Server	SQL Server Administrators	FT-SQL-Admins	This group's members are sysadmins on all SQL Server instances and local administrators on all SQL Server nodes.
Operations Manager	Operations Manager Administrators	FT-SCOM-Admins	This group's members are administrators for the Operations Manager installation and hold the Administrators role in Operations Manager.
Virtual Machine Manager	Virtual Machine Manager Administrators	FT-SCVMM-Admins	This group's members are administrators for the Virtual Machine Manager installation and hold the Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Delegated Administrators	FT-SCVMM-FabricAdmins	This group's members are delegated administrators for the Virtual Machine Manager installation and hold the Fabric Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Read Only Admins	FT-SCVMM-ROAdmins	This group's members are read-only administrators for the Virtual Machine Manager installation and hold the Read-Only Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Tenant Administrators	FT-SCVMM-TenantAdmins	This group's members are administrators for Virtual Machine Manager Self-Service users and hold the Tenant Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Self-Service users	FT-VMM-AppAdmins	This group's members are self-service users in the Virtual Machine Manager and hold the Application Administrators role in Virtual Machine Manager.
Orchestrator	Orchestrator Administrators	FT-SCO-Admins	This group's members are administrators for the Orchestrator installation.
Orchestrator	Orchestrator Operators	FT-SCO-Operators	This group's members gain access to Orchestrator through membership in the Orchestrator Operators group. Any user account added to this group is granted permission to use the Runbook Designer and Deployment Manager tools.
Service Manager	Service Manager Admins	FT-SCSM-Admins	This group is added to the Service Manager Administrators user role and the Data Warehouse Administrators user role.

8 Microsoft SQL Server 2012 SP1 Cluster Installation

The SQL Server 2012 installation process is comprised of the following high-level steps:

Figure 10SQL Server 2012 SP1 Installation Process



8.1 Overview

From the choices described above, the standard Fast Track architecture recommends a minimum two-node virtualized SQL Server guest cluster scaled accordingly for your deployment. The subsequent sections of this document contain guidance for deploying a two-node cluster.

This section provides high-level walkthrough on how to install SQL Server 2012 SP1 into the Fast Track fabric management. The following assumptions are made prior to installation:

- Two to four base virtual machines running Windows Server 2012 have been provisioned for SQL Server.
- 15 iSCSI LUNs have been assigned to the virtual machine guests.
  - One LUN – quorum (1 GB)
  - Two LUNs for each fabric management component database (14 LUNs for all components)

As discussed in the Fast Track architecture guide, virtual machines running SQL Server will be deployed as a guest failover cluster to contain all the databases for each System Center product in discrete instances by product and function. In cases that require SQL Server Reporting Services, SQL Server Reporting Services will be installed on the hosting System Center component server (for example, the Operations Manager reporting server). However, this installation will be "Files Only" and the SQL Server Reporting Services configuration will configure remote Reporting Services databases hosted on the component instance on the SQL Server cluster. All instances are required to be configured with Windows Authentication. The table below outlines the options required for each instance.

Table 21 Database Instances and Requirements

Fabric Management Component	Instance Name (Suggested)	Components	Collation[2]	Storage Requirements[3]
Virtual Machine Manager	SCVMMDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Windows Server Update Services (optional)	SCVMMDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	N/A – Shared instance with Virtual Machine Manager
Operations Manager	SCOMDB	Database Engine, Full-Text Search	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Operations Manager Data Warehouse	SCOMDW	Database Engine, Full-Text Search	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Service Manager	SCSMDB	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs
Service Manager Data Warehouse	SCSMDW	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs
	SCSMAS	Analysis Services	Latin1_General_100_CI_AS	2 LUNs
Service Manager Web Parts and Portal	SCDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	N/A – Shared instance with Orchestrator and App Controller
Orchestrator	SCDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
App Controller	SCDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	N/A – Shared instance with Orchestrator and Service Manager Portal

The required SQL instances and associated recommended node placement is outlined in the Assign Preferred Owners for SQL Instances in Failover Cluster Manager section of this document.

8.2 Prerequisites

The following environment prerequisites must be met before proceeding with the installation.

Accounts

Verify that the following accounts have been created:

[2] The default SQL collation settings are not supported for multi-lingual installations of the Service Manager component. Only use the default SQL collation if multiple languages are not required. Note that the same collation must be used for all Service Manager databases (management, DW, and reporting services).

[3] Note that additional LUNs may be required for TempDB management in larger scale configurations

Table 22Prerequisite Accounts

User Name	Purpose	Permissions
<DOMAIN>\FT-SQL-SVC	SQL Service Account	This account will need full admin permissions on all target SQL systems and will serve as the service account for all Instances. It also must be added to the FT-SQL-Admins group and a sysadmin in all instances

Groups

Verify that the following security groups have been created:

Table 23 Prerequisite Security Groups

Security Group Name	Group Scope	Members
<DOMAIN>\FT-SQL-Admins	Universal	All SQL Administrators for the FM solution

Required Networks

VMaccess, ClusComm, iSCSI-A, iSCSI-B

Establish the SQL Server Guest Cluster

The following steps can be followed to create the SQL Guest Cluster using iSCSI shared storage:

The first step in installing SQL is to create the guest cluster. To do this, access to iSCSI LUNs is required to allow each guest VM in the cluster to access shared storage. Prior to the following steps the storage should be provisioned and presented to the nodes, but not yet made online, initialized and formatted. As stated previously, the required storage for the Fast Track solution is as follows:

- 1 LUN – Disk Witness
- 2 LUNs for each Fabric Management component instance (14 LUNs for all components)

The following table provides estimated LUN sizes for the various databases used by the Fabric Management SQL Server cluster. You environment might vary from these sizes. Be sure to reference the appropriate sizing document from Microsoft to ensure you create properly sized LUNs.

Table 24 Fabric Management SQL Server Estimated LUN Sizes

LUN	Component(s)	Instance Name	Purpose	Size
LUN 1/2	Service Manager Management	SCSMDB	Instance Database and Logs	145 GB/70 GB
LUN 3/4	Service Manager Data Warehouse	SCSMDW	Instance Database and Logs	1 TB/ 500 GB
LUN 5/6	Service Manager Analysis Service	SCSMAS	Instance Database and Logs	8 GB/4 GB
LUN 7/8	Service Manager SharePoint Farm Orchestrator App Controller	SCDB	Instance Database and Logs	10 GB/5 GB

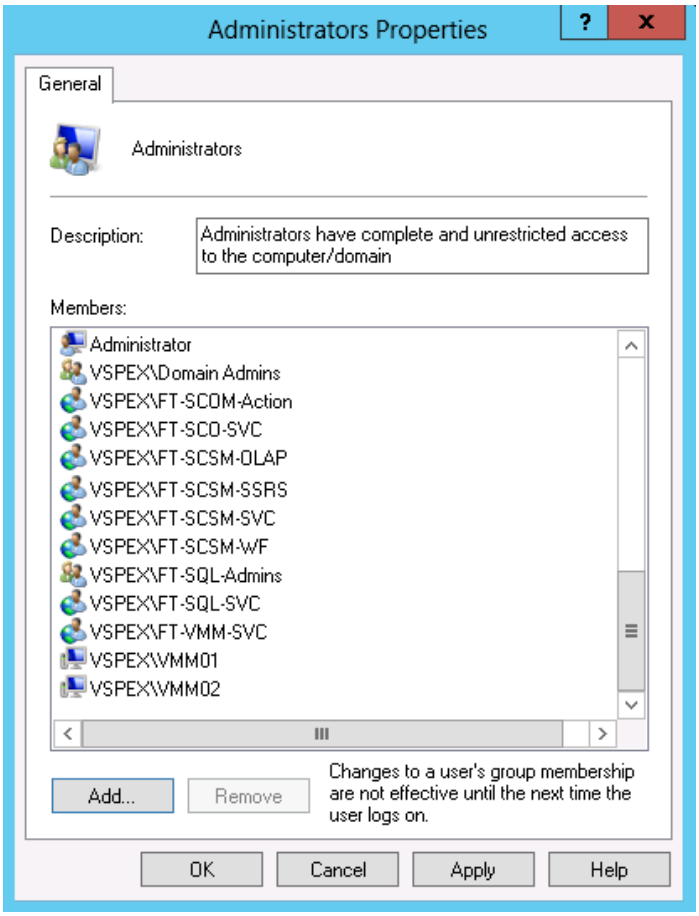
LUN 9/10	Virtual Machine Manager Windows Server Update Services	SCVMMDB	Instance Database and Logs	6 GB/3 GB
LUN 11/12	Operations Manager	SCOMDB	Instance Database and Logs	130 GB/65 GB
LUN 13/14	Operations Manager Data Warehouse	SCOMDW	Instance Database and Logs	1 TB/ 500 GB
LUN 15	N/A	N/A	SQL Server Failover Cluster Disk Witness	1 GB

During the provisioning process, two VMs were built to the specifications outlined in the Fast Track Reference Architecture Guide to support SQL operations for Fabric Management. Once created, the iSCSI targets must be configured within each VM to ensure that they are accessible by each candidate cluster Node.

▶ Perform the following steps on **all fabric management SQL Server** virtual machines.

Log on to the first node in the SQL Server cluster as a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on the first and second SQL Server nodes:

- Fast Track SQL Server service account.
- Fast Track SQL Server Admins group.
- Fast Track Service Manager OLAP account.
- Fast Track Service Manager SSRS account.
- Fast Track Service Manager workflow account.
- Fast Track Service Manager service account.
- Fast Track Operations Manager action account.
- Fast Track Virtual Machine Manager service account.
- Virtual Machine Manager computer accounts.

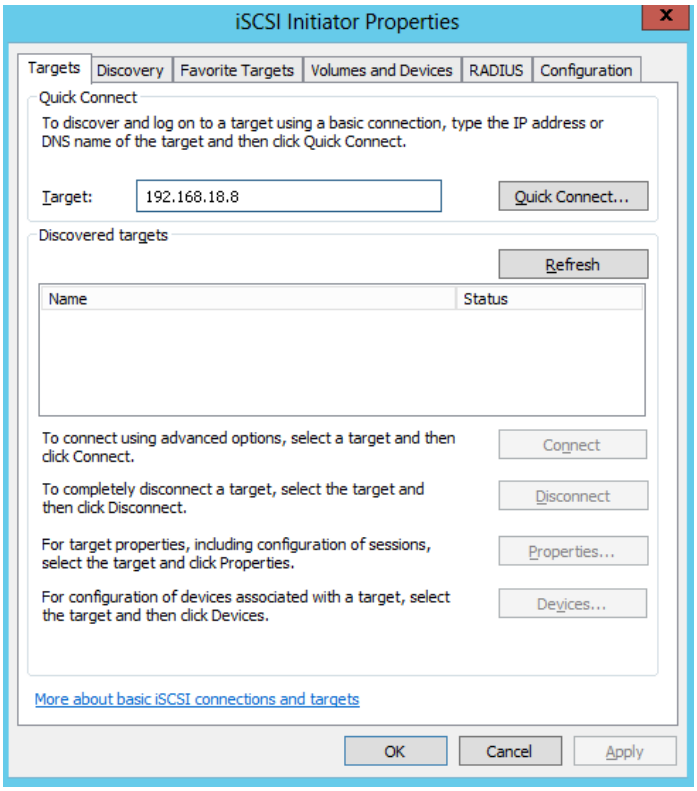


To attach the guest cluster to the iSCSI LUNs, the iSCSI Initiator must be configured on each SQL Server virtual machine. From the **Start** screen click the **iSCSI Initiator** tile.

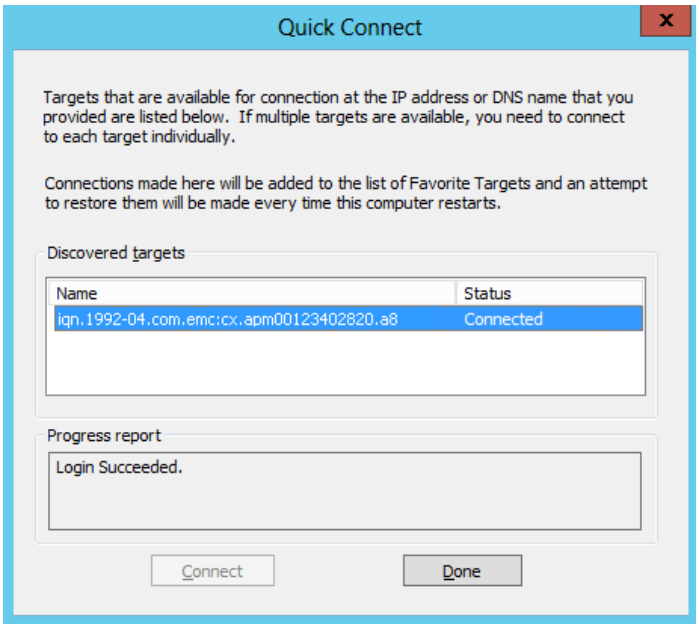
Note: Third-party Storage Area Network (SAN) connectivity software can be used in place of the in-box iSCSI Initiator. If a third-party solution is used, the in-box iSCSI Initiator steps can be skipped.



When the **iSCSI Initiator Properties** dialog appears, click the **Targets** tab. In the **Target** text box, supply the IP address or fully qualified domain name (FQDN) of the iSCSI target and click the **Quick Connect** button to establish connectivity with the desired iSCSI target.

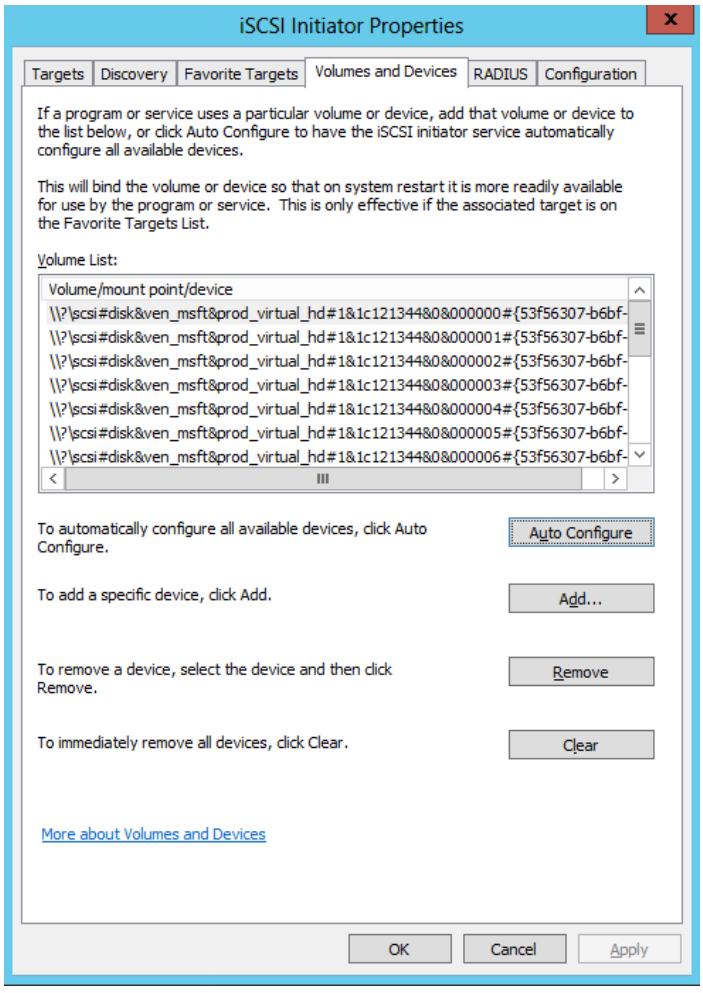


The **Quick Connect** dialog will provide a list of discovered targets. Once the **Progress report** section shows *Login Succeeded*, click **Done** to close the dialog.



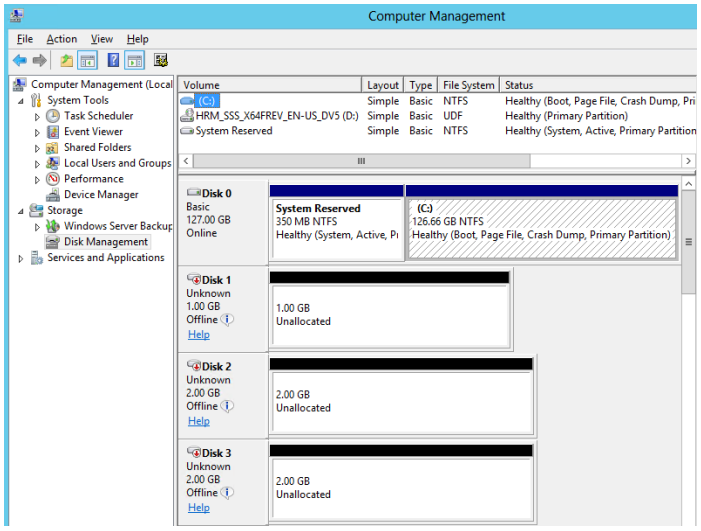
In the **iSCSI Initiator Properties** dialog, click the **Volumes and Devices** tab. In some cases you may need to click the **Auto Configure** button to establish connectivity with the LUNs advertised to this initiator.

Click **OK** to close **the iSCSI Initiator Properties** dialog.

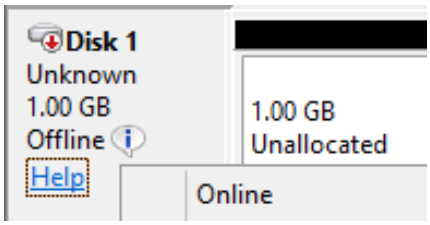


▶ Perform the following steps on the **first fabric management SQL Server** virtual machine. Perform these operations on a single node prior to creating the failover cluster.

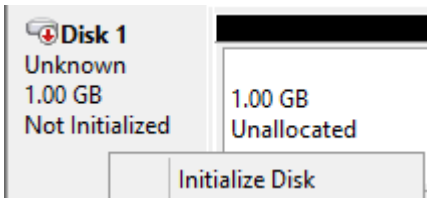
Within **Server Manager**, navigate to the **Storage** node and expand the **Disk Management** snap-in. The iSCSI LUNs should be visible in the snap-in, but should appear offline.



Right-click each disk and select **Online** from the context menu. This step must be completed for each attached iSCSI LUN. As described above, perform this action on the first node of the SQL cluster.

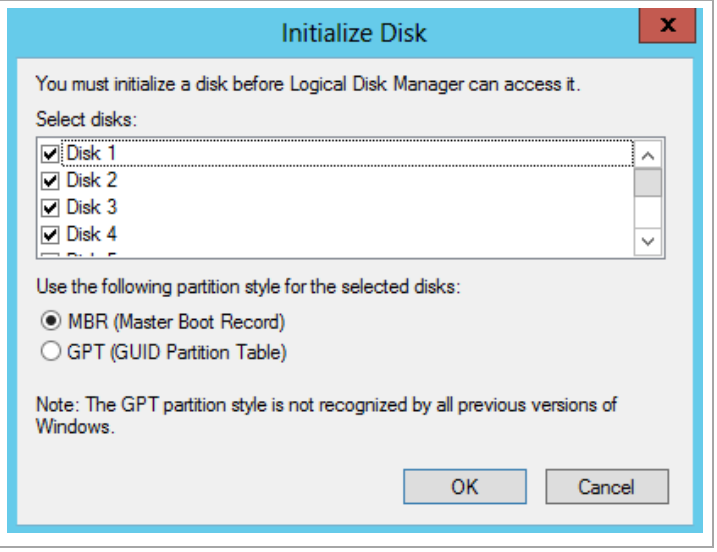


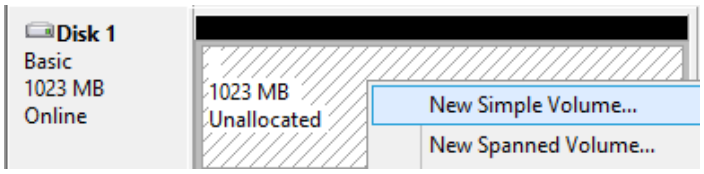
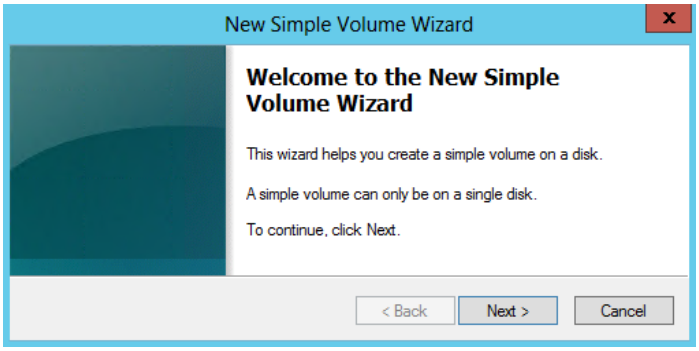
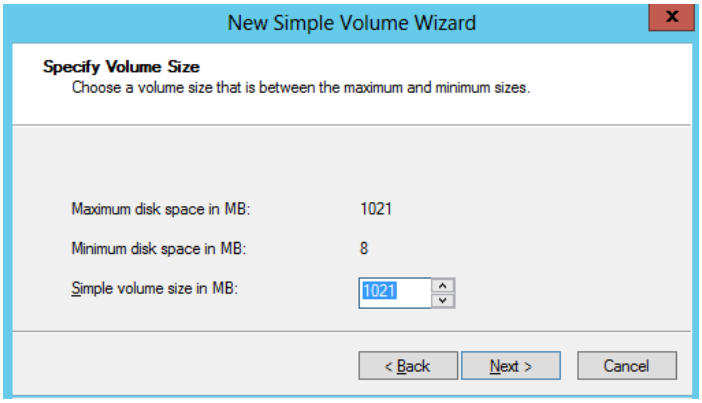
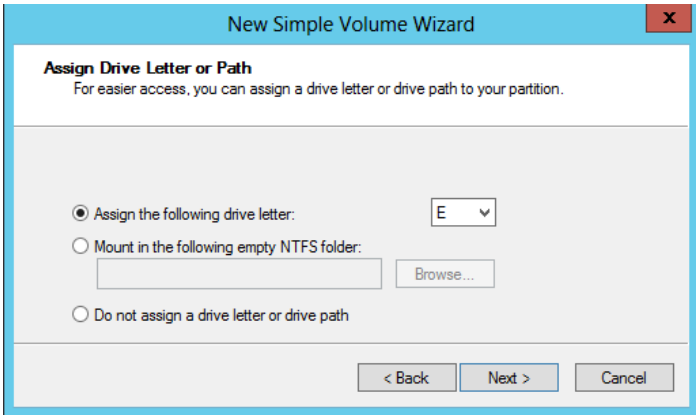
Once each disk is online, right-click the first disk and select **Initialize Disk** from the context menu. As described above, perform this action on the first node of the SQL cluster.

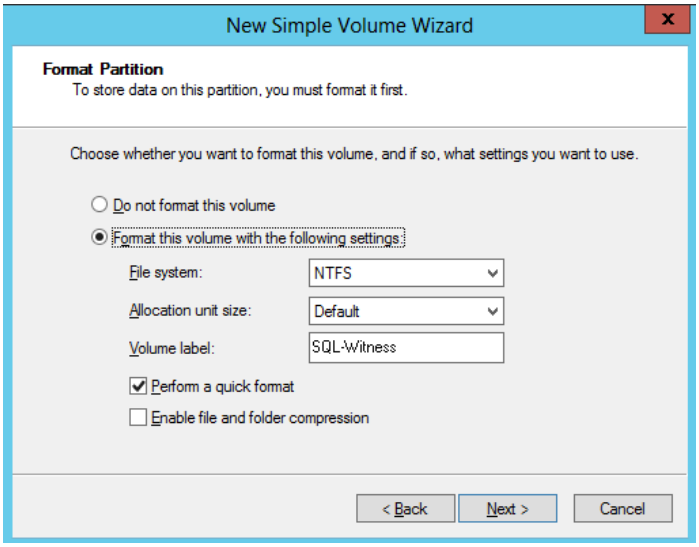
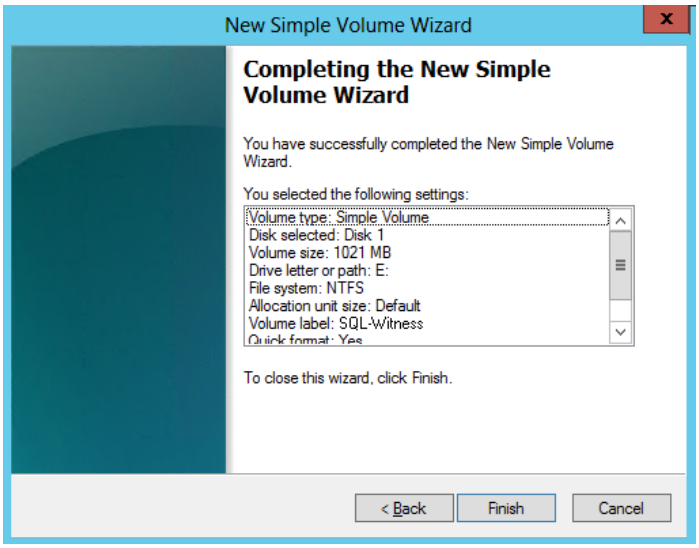


The **Initialize Disk** dialog will appear. Verify that each iSCSI LUN check box is selected in the **Select disks** section. Verify that the **MBR (Master Boot Record)** option is selected and click **OK** to initialize the disks.

Note: You may want to consider GPT partitions for clustered disks. GPT partitioned disks have redundant primary and backup partition tables for improved partition data structure integrity.



Once initialized, on the first node, right-click each disk and select **New Simple Volume…** from the context menu.	
The **New Simple Volume Wizard** will appear. Click **Next** to continue.	
In the **Specify Volume Size** dialog, specify the maximum disk space value in the **Simple volume size in MB** text box. Click **Next** to continue.	
In the **Assign Drive Letter or Path** dialog, select the **Assign the following Drive Letter** option and specify a path in the available text field. Click **Next** to continue. **Note:** If you want to save the use of a single drive letter, it is not needed to assign a driver letter to the disk that will be used as a witness disk.	

In the **Format Partition** dialog, select the **Format this volume with the following settings** option. In the **File system** drop-down menu, select **NTFS**. In the **Allocation unit size** drop-down menu, select **Default**. It is recommended to place a descriptive label in the **Volume Label** text box. Verify that the **Perform a quick format** check box is selected and click **Next** to format the partition.	
Once complete, a confirmation dialog will appear. Click **Finish** to complete the operation and repeat the operation for each disk.	

Organizations should configure the interfaces according to their specific deployment characteristics. If there is a separate physical network(s) used for iSCSI and/or intra-cluster private communications (previously known as 'heartbeat'), you should reconnect the virtual NICs appropriately.

Once complete, the storage should be brought online one at a time, initialized and formatted on the first candidate cluster node. It is also recommended that you specify meaningful volume labels while formatting the disks. This could help in the future if one or more of the disks lose their assignment to the cluster or VMs themselves and need be identified.

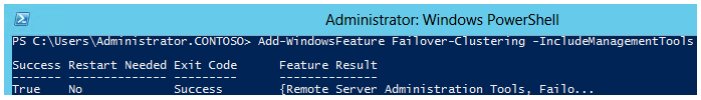
Note: The installation of a SQL Cluster creates computer accounts in Active Directory for each instance in the cluster called cluster name objects (CNO). By default these objects are created in the default Computers container (e.g. cn=Computers) of the target Active Directory domain. The account used to perform the installation of the SQL Cluster requires the rights in Active Directory to create the associated CNOs for each product SQL instance. This occurs as a standard part of the SQL installation process. There are several approaches to mitigate this including using a higher privileged account for installation, delegation of rights in Active Directory for the account used for installation, or pre-creation of the

computer accounts in the target Active Directory domain. Further discussion of this aspect of Windows Server Failover Cluster installation (and mitigation strategies) can be found in the Windows Server 2008 R2 Failover Cluster Step-by-Step Guide[4].

▶ Perform the following steps on the **first fabric management SQL Server node** virtual machine with an account that has both local Administrator rights and permissions in AD DS to create the SQL Server CNOs.

From an elevated Command Prompt within each guest virtual machine (Node 1, Node 2, and additional nodes such as Node 3 and Node 4, if desired). The Failover Clustering feature can be installed from an elevated PowerShell prompt using the following command:

```
Add-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

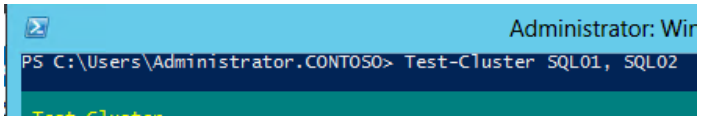


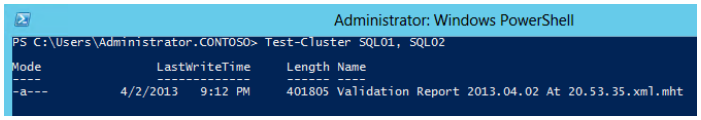
The first step is performing Cluster Validation. From an elevated PowerShell prompt on the first SQL Server node, run the following commands to test the cluster configuration:

```
Test-Cluster <Node1>, <Node2>, <Node3>, <Node4>
```

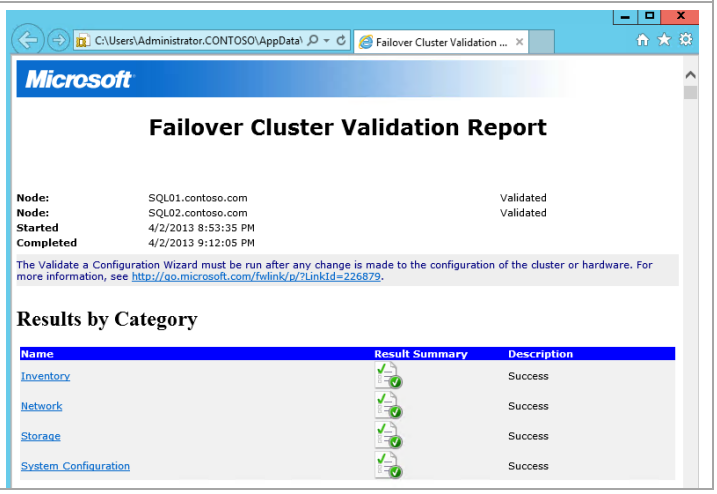
If successful, the Test-Cluster cmdlet provides a validation report that can be opened in a local browser from %TEMP% as outlined below.

Note: The validation stage of the cluster creation may take up to an hour to complete.





Navigate to %TEMP% and review the **Failover Cluster Validation Report** for errors and warnings. Perform any required remediation and re-perform the cluster tests above as required.



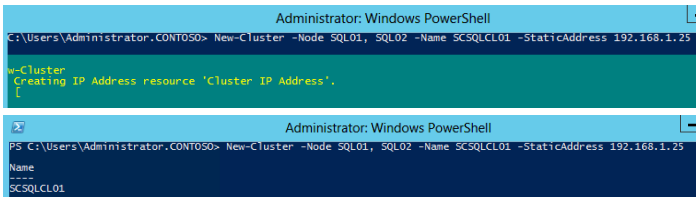
[4] Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory - http://technet.microsoft.com/en-us/library/cc731002(WS.10).aspx

The next step is to create the cluster. From the same elevated PowerShell prompt, run the following commands to create the cluster:

```
New-Cluster -Node <Node1>, <Node2>, <Node3>, <Node4> -Name <ClusterName> -StaticAddress <ClusterIPAddress>
```

If successful, the cluster name will be displayed as output once the process is complete.

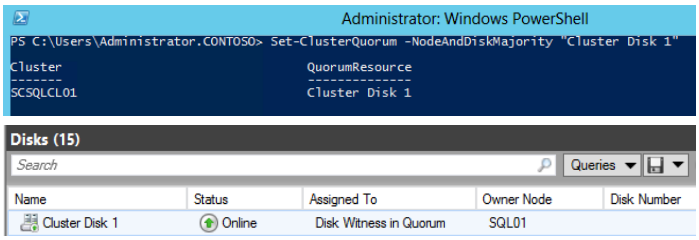
Note: If using Dynamic Host Configuration Protocol (DHCP) for the cluster nodes the **–StaticAddress** parameter should not be used.



Once cluster creation is complete, verify the correct LUN was assigned as the quorum disk. If the incorrect disk was assigned, the correct assignment can be made using the following PowerShell cmdlet:

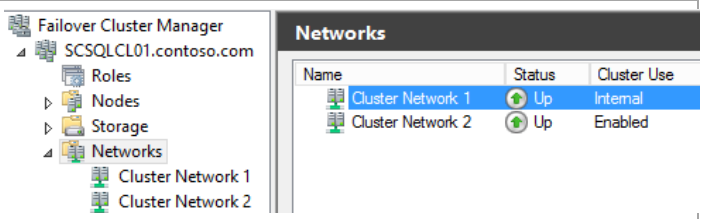
```
Set-ClusterQuorum -NodeAndDiskMajority <ClusterQuorumDisk>
```

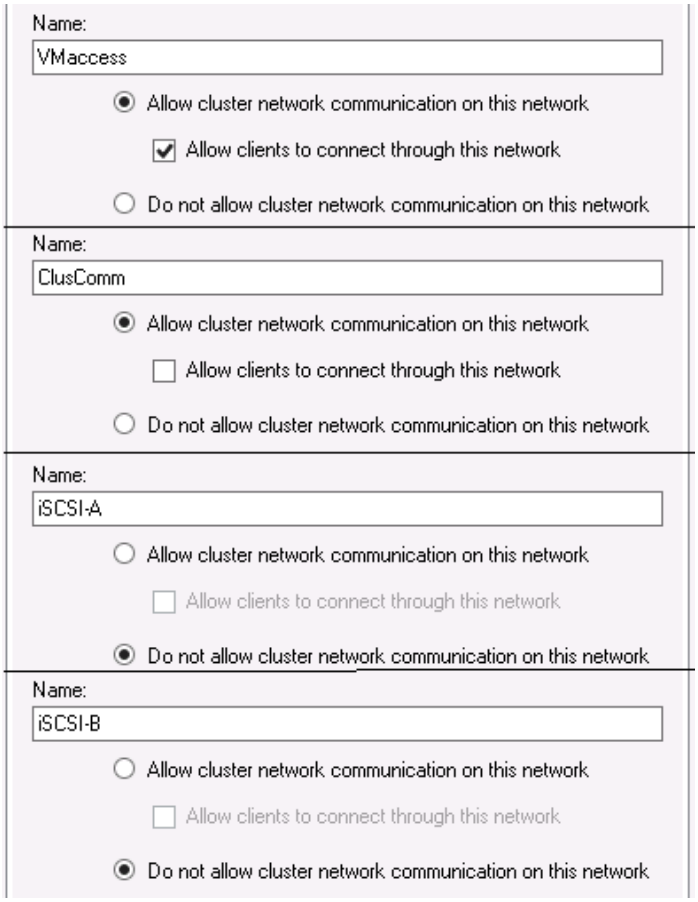
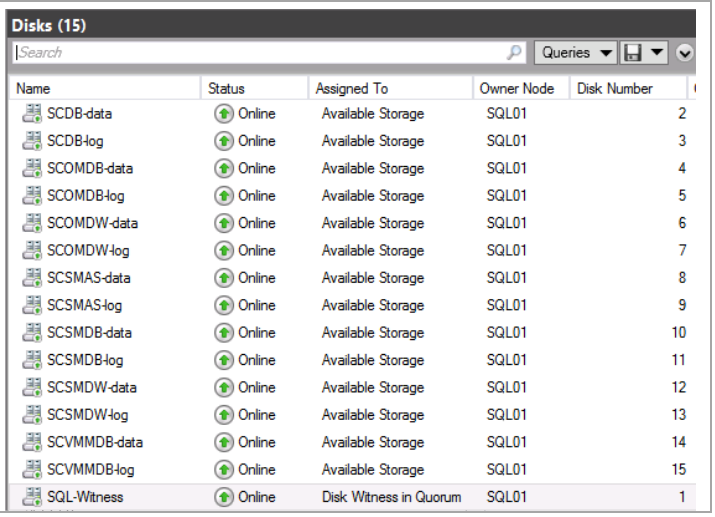
Note: For a three-node initial cluster installation, this command is not applicable.



Verify all cluster networks are assigned properly. Take care to document which cluster network name is assigned to the public and private network interfaces.

Note: It is a good practice to rename the generic names created by the cluster build process to the actual names of the networks as you defined them.



Ensure the property settings for the networks are defined as shown in these screen shots.	
Document all disk assignments in the cluster. Create a mapping table of available storage (by name) to drive letters or mount points. This information will be used during the SQL Server installation. **Note:** It is a good practice to name the disks the same as their initialized names instead of using the default generic names assigned by the cluster build process.	

Name	Status	Assigned To	Owner Node	Disk Number
SCDB-data	Online	Available Storage	SQL01	2
SCDB-log	Online	Available Storage	SQL01	3
SCOMDB-data	Online	Available Storage	SQL01	4
SCOMDB-log	Online	Available Storage	SQL01	5
SCOMDW-data	Online	Available Storage	SQL01	6
SCOMDW-log	Online	Available Storage	SQL01	7
SCSMAS-data	Online	Available Storage	SQL01	8
SCSMAS-log	Online	Available Storage	SQL01	9
SCSMDB-data	Online	Available Storage	SQL01	10
SCSMDB-log	Online	Available Storage	SQL01	11
SCSMDW-data	Online	Available Storage	SQL01	12
SCSMDW-log	Online	Available Storage	SQL01	13
SCVMMDB-data	Online	Available Storage	SQL01	14
SCVMMDB-log	Online	Available Storage	SQL01	15
SQL-Witness	Online	Disk Witness in Quorum	SQL01	1

8.3 Installation

Install the SQL Named Instances on the Guest Cluster (Node 1)

Prior to performing installation of the SQL cluster, the information gathered in previous steps must be compiled to provide a point of reference for the steps required during setup. The following example is provided.

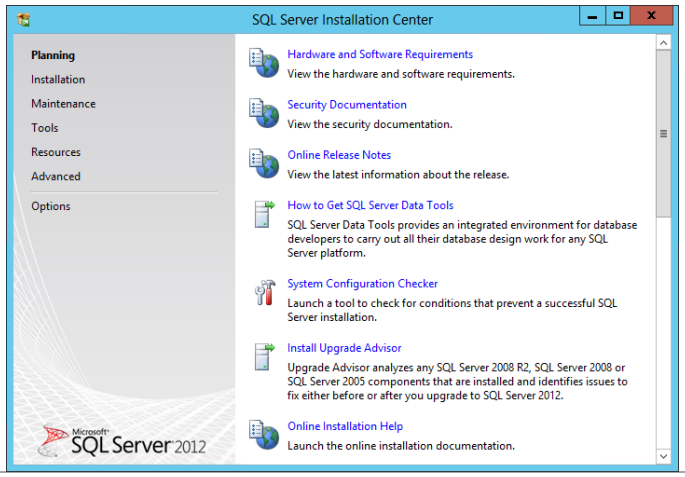
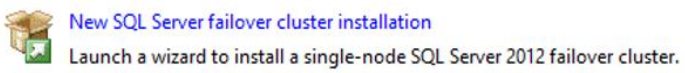
Table 25 Example Database Parameters

Component	Service Manager management server	Service Manager Data Warehouse server	Service Manager analysis server	App Controller, Orchestrator, Microsoft SharePoint® services Farm and WSUS	Virtual Machine Manager	Operations Manager	Operations Manager Data Warehouse
SQL Server Instance Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance Failover Cluster Network Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance DATA Cluster Disk Resource	Cluster Disk 2	Cluster Disk 4	Cluster Disk 6	Cluster Disk 8	Cluster Disk 10	Cluster Disk 12	Cluster Disk 14
SQL Server Instance LOG Cluster Disk Resource	Cluster Disk 3	Cluster Disk 5	Cluster Disk 7	Cluster Disk 9	Cluster Disk 11	Cluster Disk 13	Cluster Disk 15
SQL Server Instance Install Drive	E:	G:	I:	K:	M:	O:	Q:
SQL Server Instance DATA Drive	E:	G:	I:	K:	M:	O:	Q:
SQL Server Instance LOG Drive	F:	H:	J:	L:	N:	P:	R:
SQL Server Instance TEMPDB Drive	F:	H:	J:	L:	N:	P:	R:
Cluster Service Name	SQL Server (SCSMDB)	SQL Server (SCSMDW)	SQL Server (SCSMAS)	SQL Server (SCDB)	SQL Server (SCVMMDB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)
Clustered SQL Server Instance IP Address	10.1.1.22	10.1.1.23	10.1.1.24	10.1.1.25	10.1.1.26	10.1.1.27	10.1.1.28
Host Cluster Public Network Interface Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Host Cluster Public Network Interface Name	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2
SQL Server Instance Listening TCP/IP Port	10437	10438	10439	1433[5]	10434	10435	10436
SQL Server Instance Preferred Owners	Node2, Node4	Node2, Node4	Node2, Node4	Node1, Node4	Node1, Node4	Node3, Node4	Node3, Node4

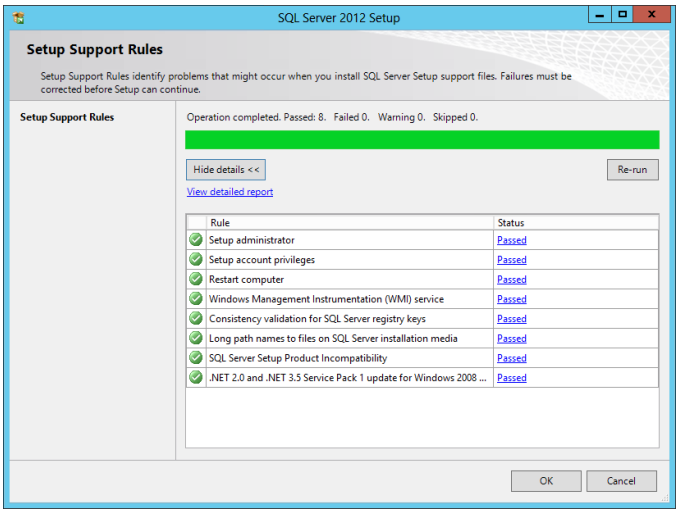
A template is provided in Appendix A of this document to assist with capturing this information for the installation process. Once gathered, the following steps are provided to perform installation. Note that at this point in installation, the first node of the SQL cluster must have ownership of all the LUNs.

- Perform the following steps on the **first fabric management SQL Server node** virtual machine with an account that has both local Administrator rights and permissions in AD DS to create the SQL Server CNOs.

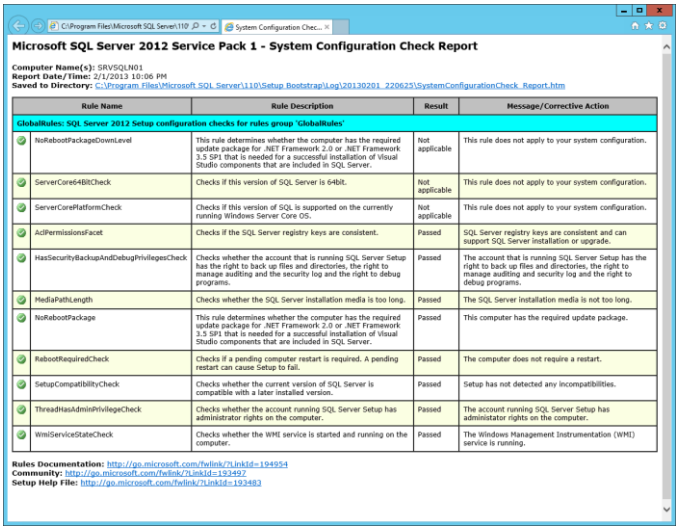
[5] Note that the SCDB instance must be configured to port 1433 if the Cloud Services Process Pack will be used.

As outlined before, Fast Track requires separate instances for each System Center product. The instances associated with these products are: 1. SCSMDB (Service Manager database instance). 2. SCSMDW (Service Manager Data Warehouse instance). 3. SCSMAS (Service Manager SQL Analysis Services instance). 4. SCDB (Shared App Controller, Orchestrator, Service Manager self-service portal Microsoft SharePoint® Foundation 2010 services and WSUS database instance). 5. SCVMMDB (Virtual Machine Manager database instance and optional WSUS database instance). 6. SCOMDB (Operations Manager database instance). 7. SCOMDW (Operations Manager Data Warehouse instance). For multi-instance failover clusters, installation of SQL Server 2012 must be performed once for each instance. As such, these steps must be performed for each instance sequentially.	
From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear. Select the **Installation** menu option.	
From the SQL Server Installation Center, click the New SQL Server failover cluster installation link.	

The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

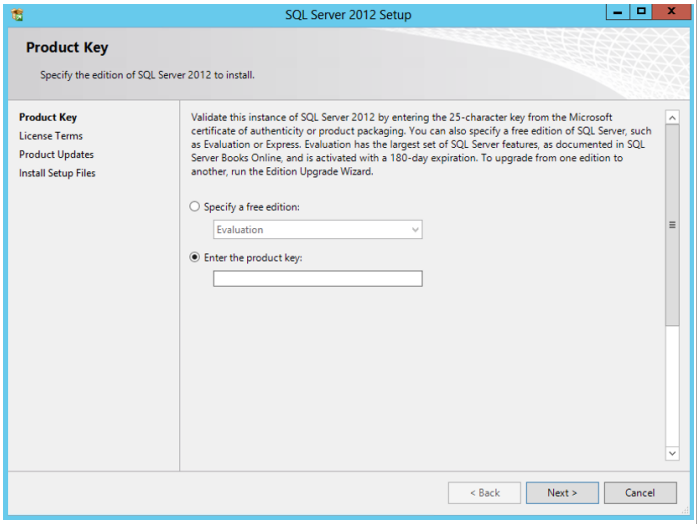


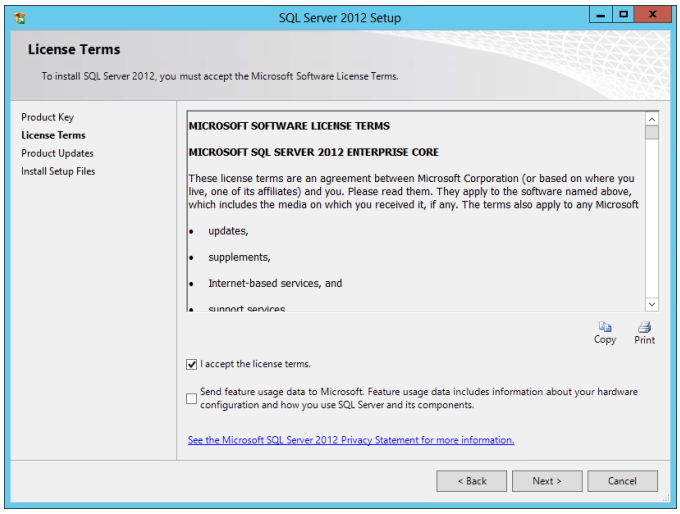
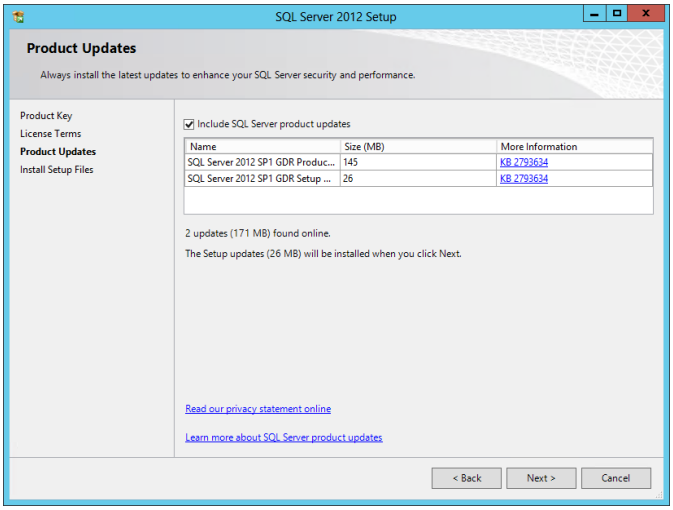
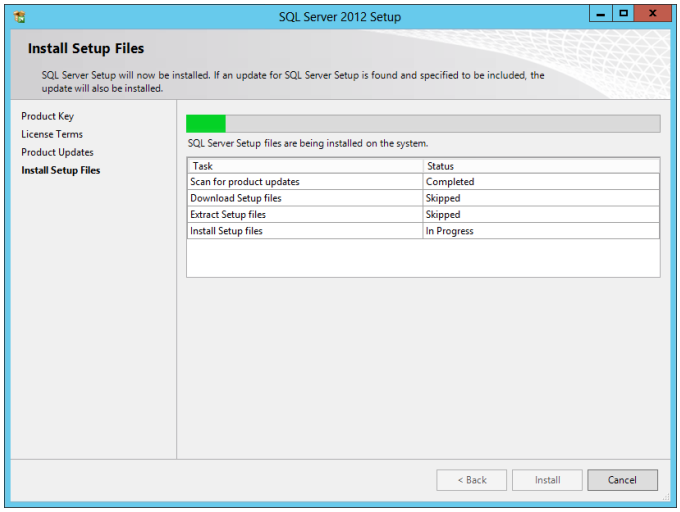
If the **View detailed report** link is selected, the following report is available.

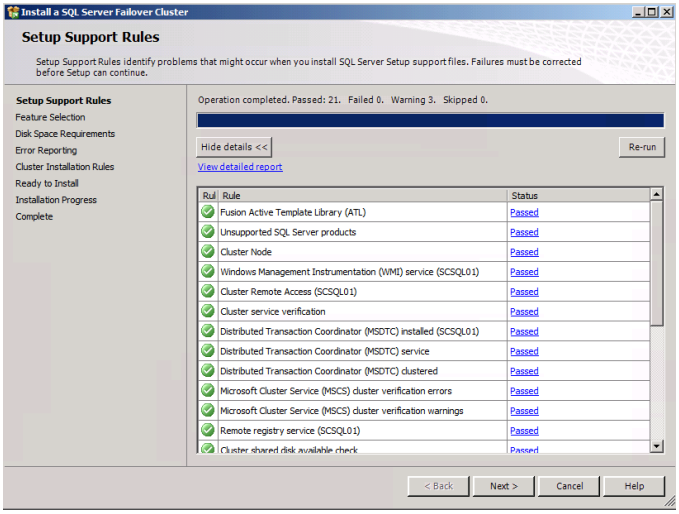
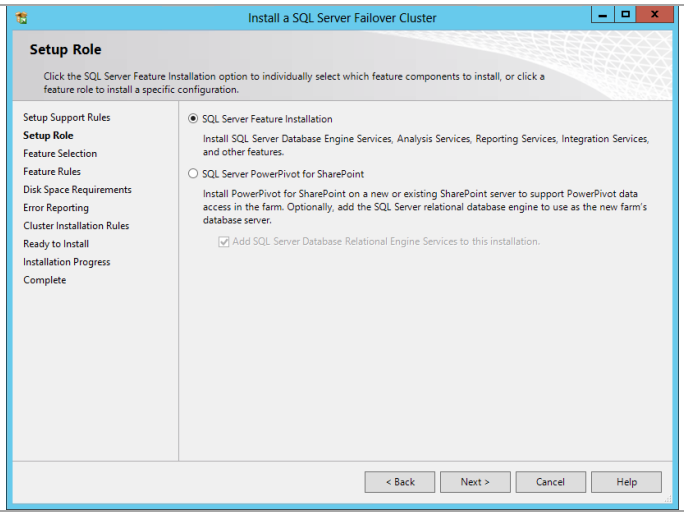


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.	
In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.	
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.	

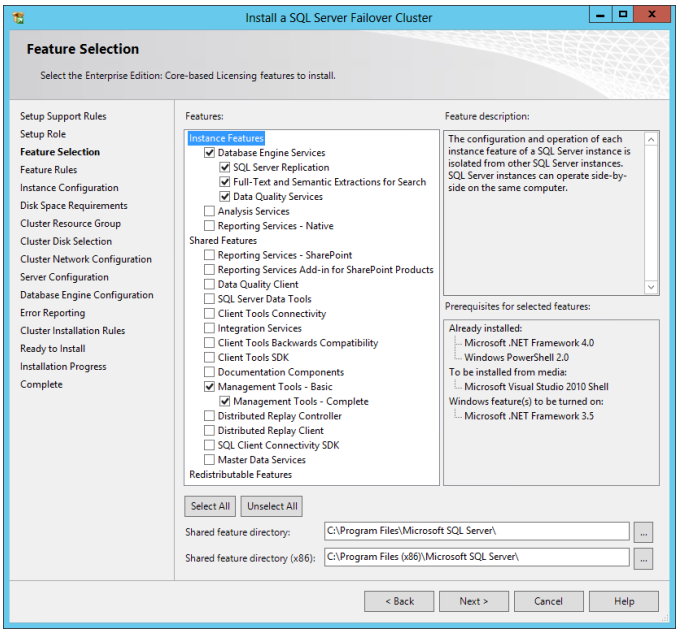
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment. Click **Next** to continue.	
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.	

In the **Feature Selection** dialog, features for the various instances will be selected. Note that not all features are supported for failover cluster installations, so the features for Fast Track are limited to the features as listed below. SQL Server with failover clusters requires the selection of the **SQL Server Replication** check box and **Full-Text Search** check box with every instance. The following additional selections are required for each instance:

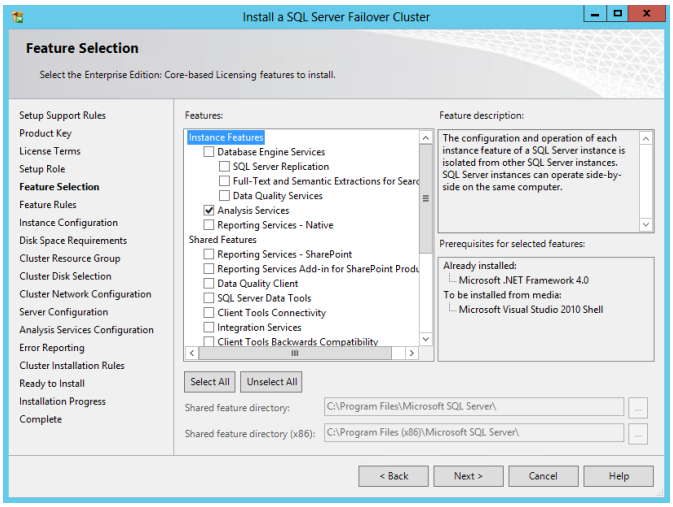
- SCDB
    - Database Engine Services
- SCOMDB
    - Database Engine Services
- SCOMDW
    - Database Engine Services
- SCSMAS
    - Analysis Services
- SCSMDB
    - Database Engine Services
- SCSMDW
    - Database Engine Services
- SCVMMDB
    - Database Engine Services

Select the **Management Tools – Basic** check box and **Management Tools – Complete** check box for at least one instance installation pass. When all selections are made, click **Next** to continue.

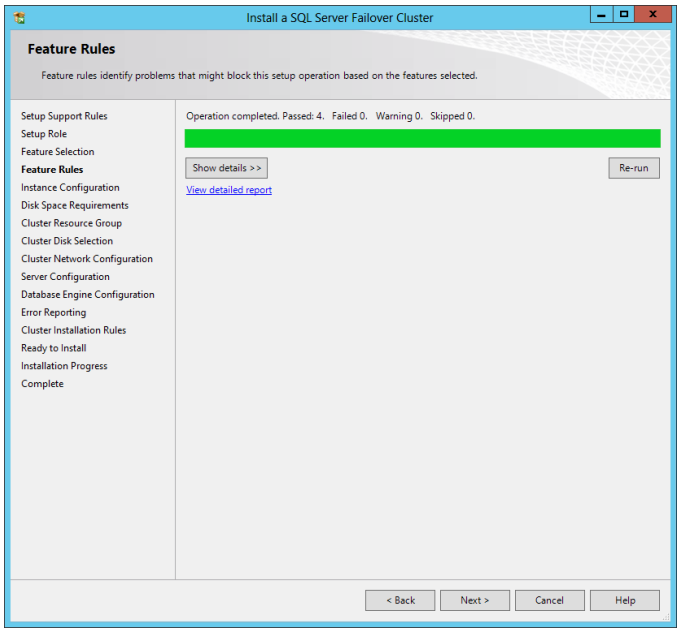
Database Engine Services (all instances except SCSMAS)**:**



Analysis Services (SCSMAS instance only):



In the **Feature Rules** dialog click **Next** to continue. The **Show details** and **View detailed report** can be viewed if required.



In the **Instance Configuration** dialog, make the following selections (refer to the worksheet created earlier):

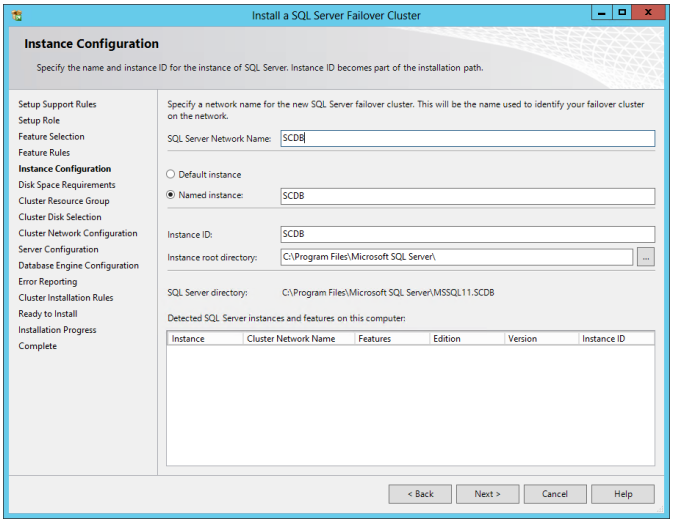
- **SQL Server Network Name** – *specify the cluster network name of the failover cluster instance being installed.*

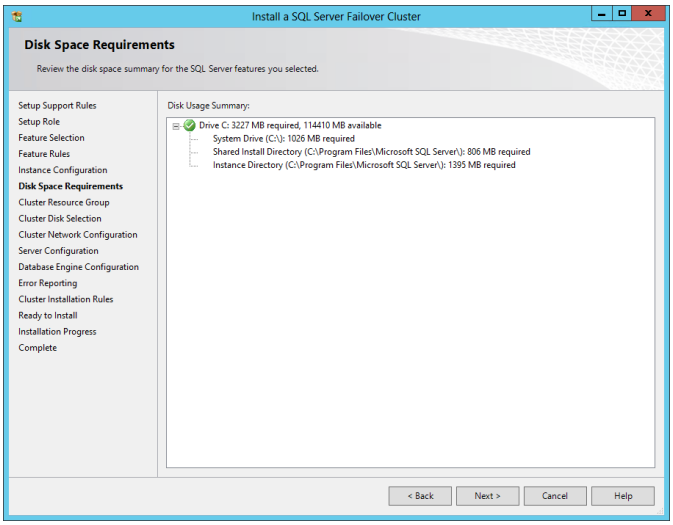
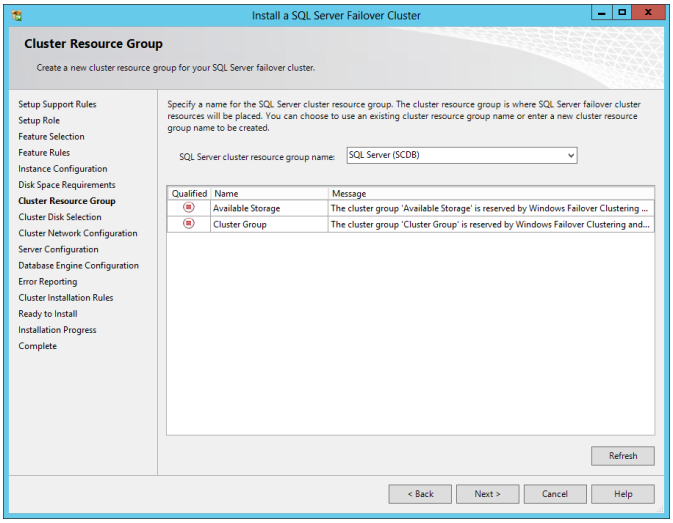
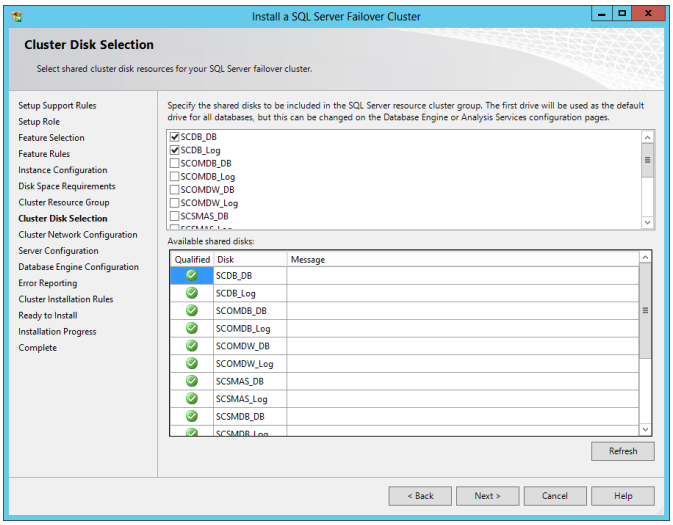
Select the **Named instance** option. In the provided text box, specify the instance name being installed.

- **Instance ID** – *specify the instance name being installed. Verify that it matches the* ***Named instance*** *value.*

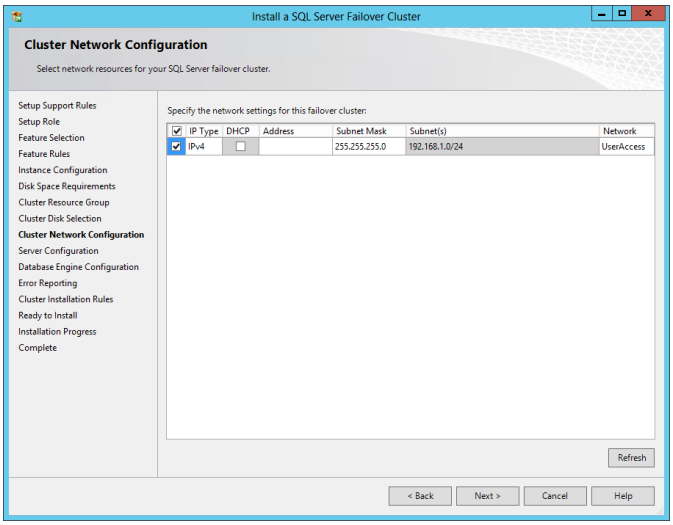
- **Instance root directory** – *accept the default location of %ProgramFiles%\Microsoft SQL Server.*

Click **Next** to continue.



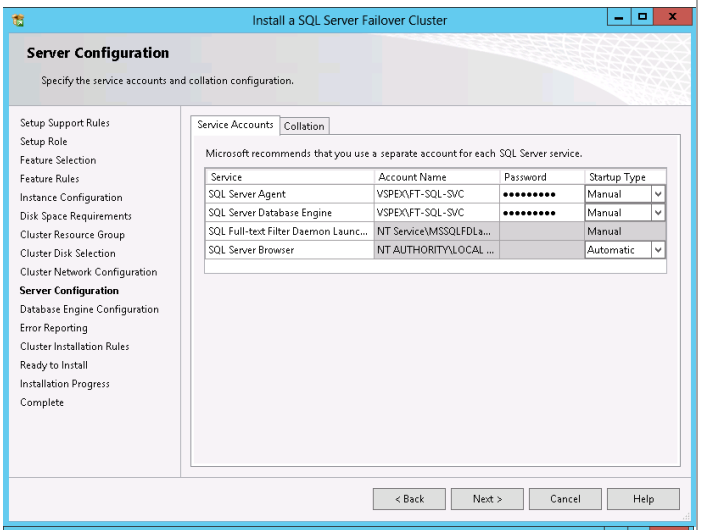
In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.	
In the Cluster Resource Group dialog, in the SQL Server cluster resource group name drop-down menu, accept the default value of SQL Server (*<InstanceName>*). Click **Next** to continue.	
In the **Cluster Disk Selection** dialog, refer to the worksheet created earlier to make the proper disk selections. Two cluster disks will be selected to support separation of databases and logs for each database instance. Make the selections by selecting the appropriate **Cluster Disk** check boxes and click **Next** to continue. **Note:** Cluster disks can be renamed in Failover Cluster Manager to friendly names as illustrated in this dialog.	

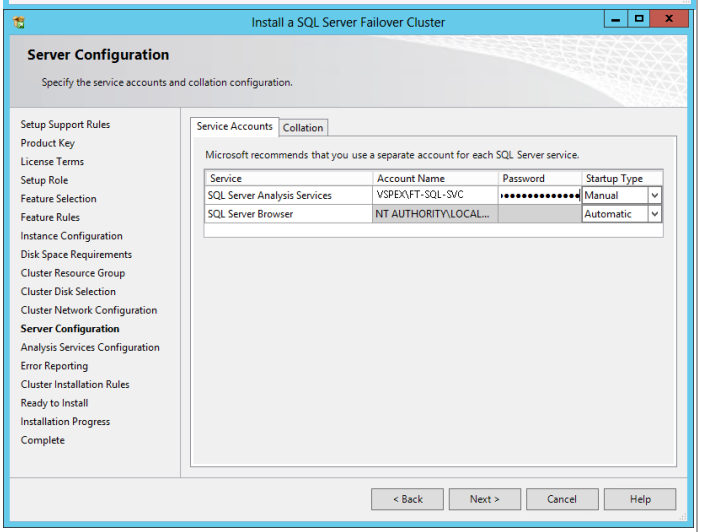
In the **Cluster Network Configuration** dialog, refer to the worksheet created earlier to assign the correct IP for each instance. Clear the **DHCP** check box if you are using static addressing and enter the IP address in the **Address** field text box. Once complete, click **Next** to continue.



In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services.

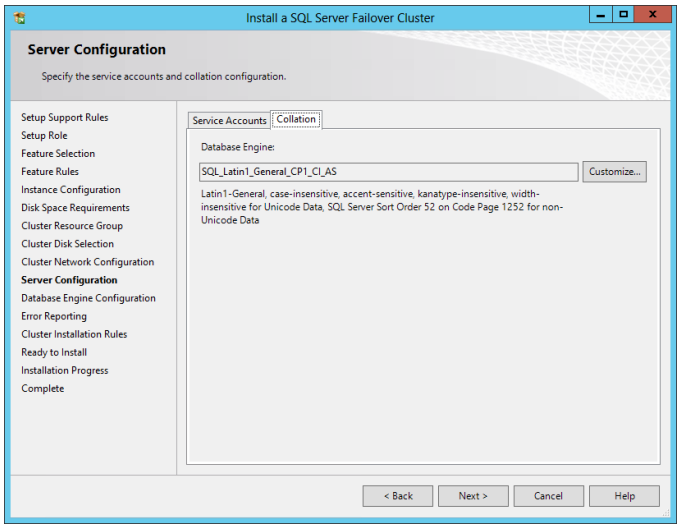
Note: The Fast Track SQL Server Service Account will also be used for the SQL Server Analysis Services service for the instances where these feature are selected.



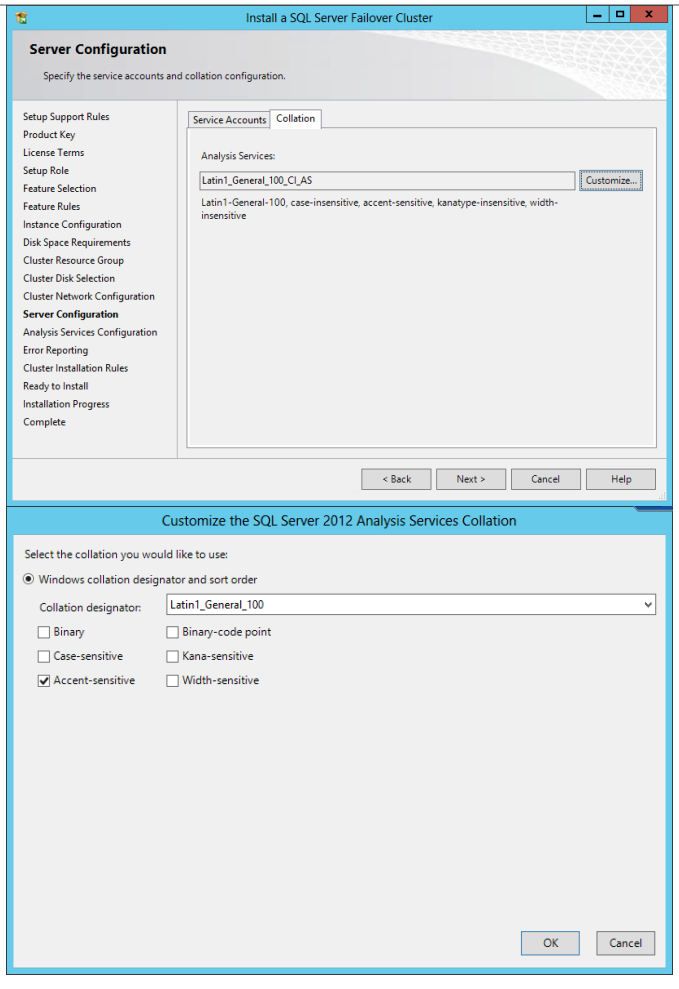


In the same **Server Configuration** dialog, select the **Collation** tab. Accept the default collation in the **Database Engine** field and click **Next** to continue.

Note: It is good practice to use a custom collation for all instances of Service Manager[6]. See next step.

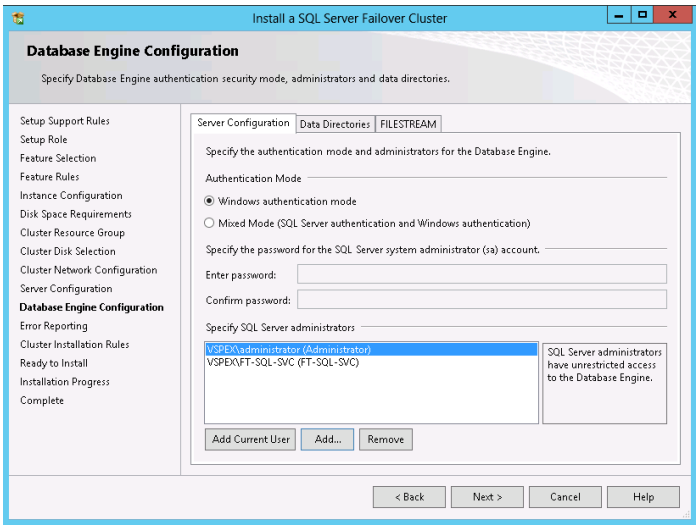


For all Service Manager instances, DB, DW, and AS, the collation should be specified differently. This is done through the **Customize…** button. In these cases you can select accent sensitivity and case insensitivity along with other collation designators. The example is provided.



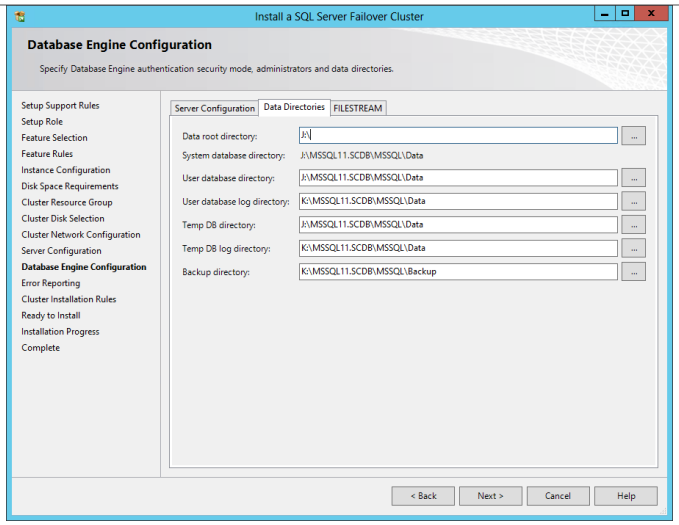
6 http://blogs.technet.com/b/servicemanager/archive/2012/05/24/clarification-on-sql-server-collation-requirements-for-system-center-2012.aspx

In the **Database Engine Configuration** dialog, select the **Server Configuration** tab. In the **Authentication Mode** section, select the **Windows authentication mode** option. In the **Specify SQL Server administrators** section, click the **Add Current User** button to add the current installation user. Click the **Add…** button to select the previously created Fast Track SQL Server Admins group from the object picker.



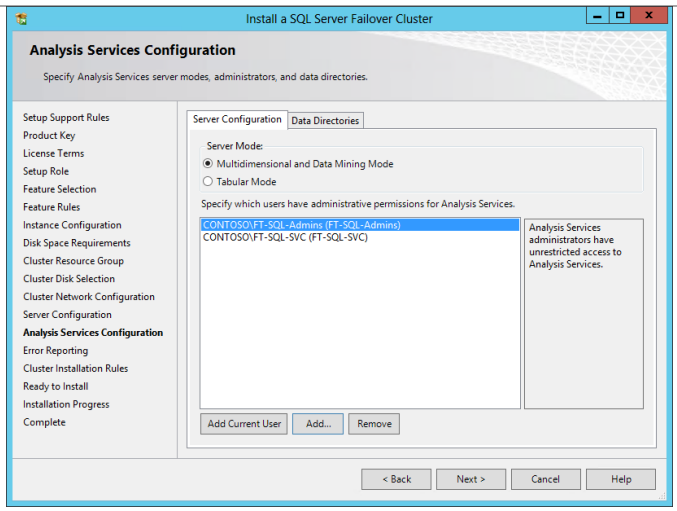
In the same **Database Engine Configuration** dialog, select the **Data Directories** tab. The proper drive letter or mount point associated with the Cluster Disk resource for SQL Server data should be specified. If not, verify that the proper Cluster Disk resource check boxes were selected earlier and enter the proper drive letter in the **Data root directory** text box. To redirect log files by default to the second Cluster Disk resource, change the drive letter in the **User databaselog directory** and **Temp DB log directory** text boxes. It is also recommended to change the Backup Directory to a separate drive such as the log drive. Do not change the folder structure unless your organization has specific standards for this.
Once complete, click **Next** to continue.

Note: It may be necessary to relocate the Temp DB files to a dedicated LUN if performance is not adequate using the two primary SQL LUNs.

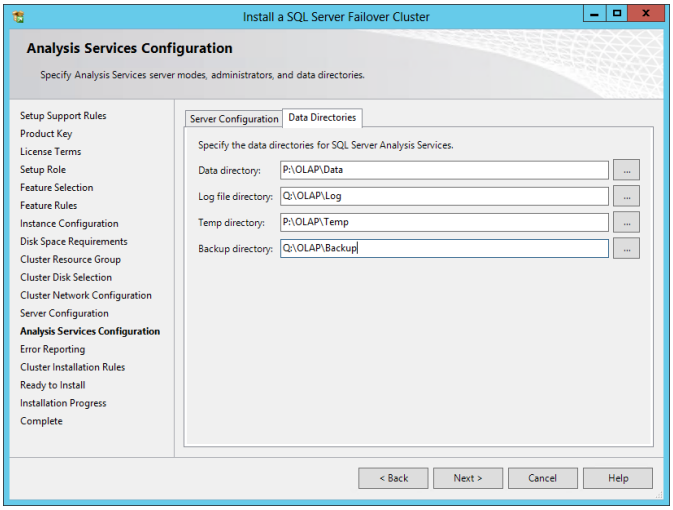


In instances that contain Analysis Services within the **Analysis Services Configuration** dialog, click the **Server Configuration** tab. In the Specify which users have administrative permissions for Analysis Services section, click Add Current User to add the current installation user. Click Add to select the following groups:
Service Manager instance:

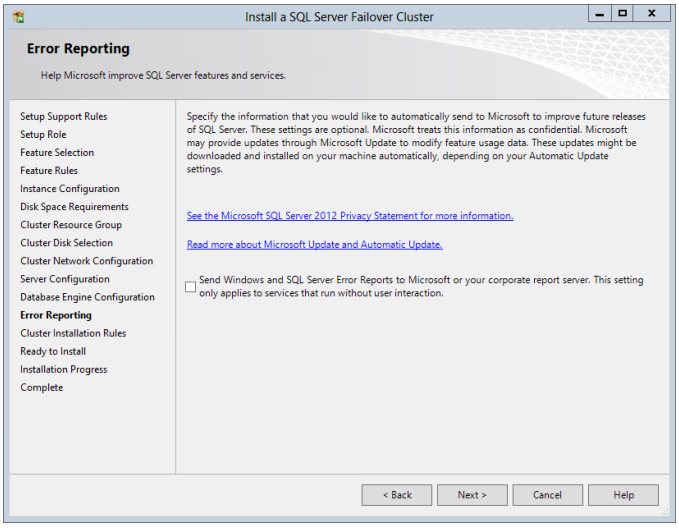
- Fast Track SQL Server Admins group
- Fast Track SQL Server Service account
- Fast Track SM Admins group
- Fast Track SM OLAP account

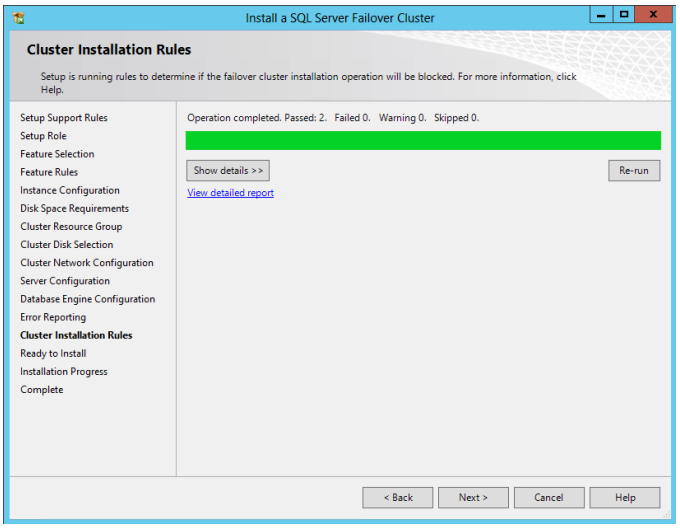
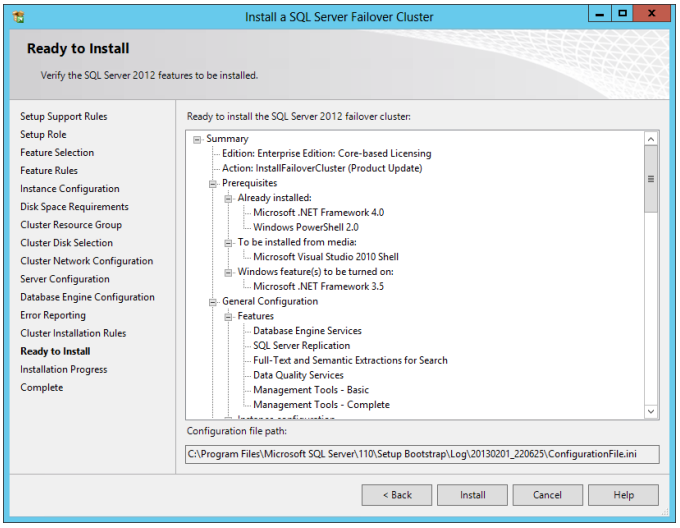
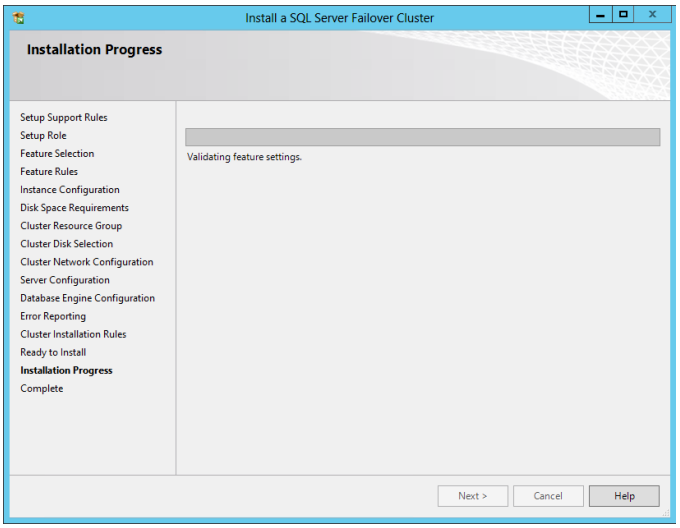


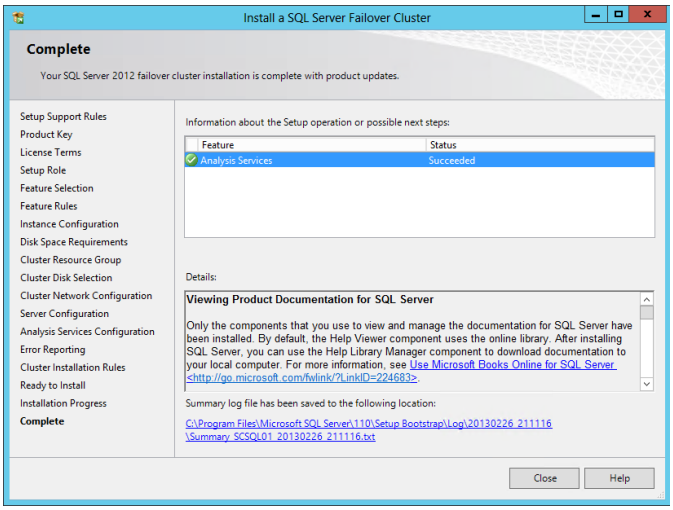
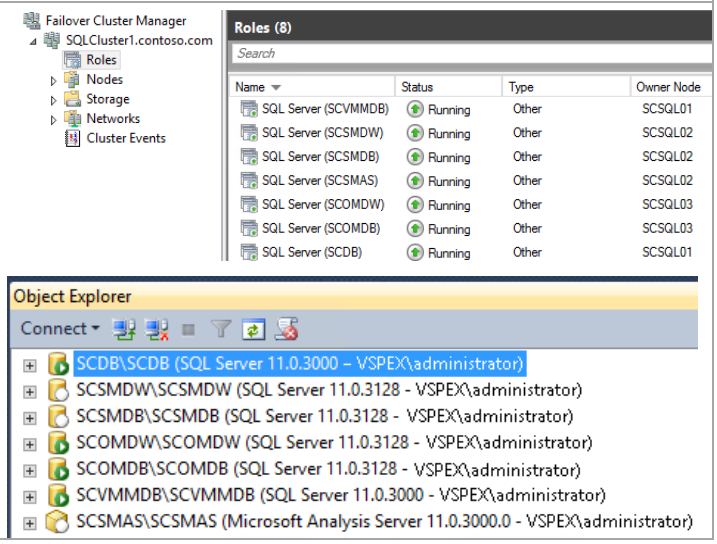
For instances with Analysis Services, use the following configuration:
On the **Data Directories** tab, set the Data directory, and Temp directory to the cluster disk configured for the database files. Set the Log file directory and the Backup directory to the cluster disk configured for the log files. Do not change the folder structure unless your organization has specific standards for this.
When complete, click **Next** to continue.



In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



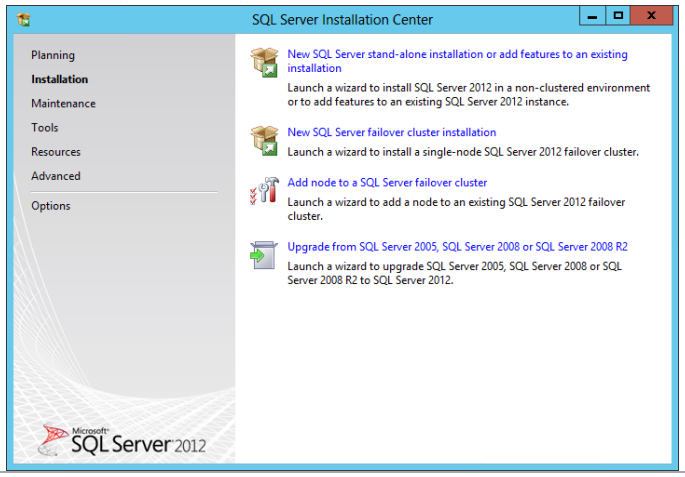
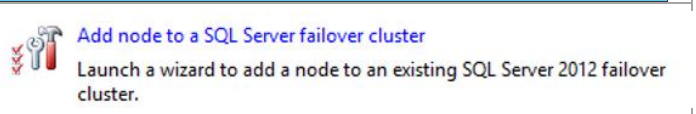
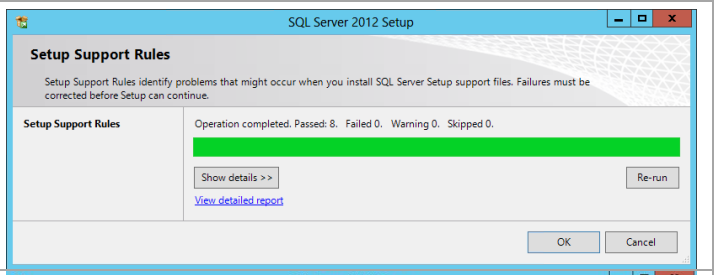
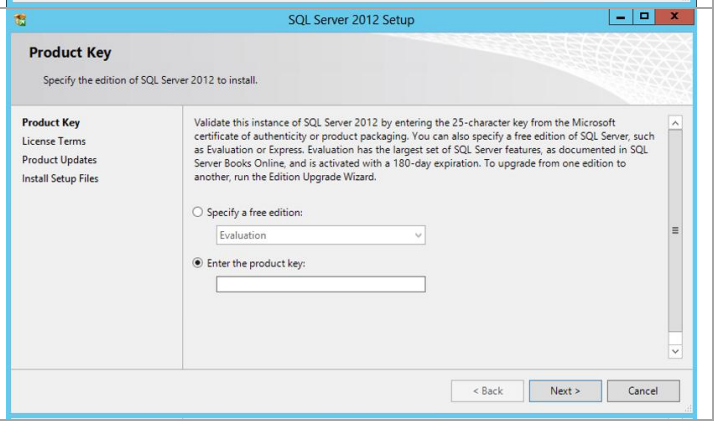
In the **Cluster Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.	
In the **Installation Progress** dialog, the installation progress will be displayed.	

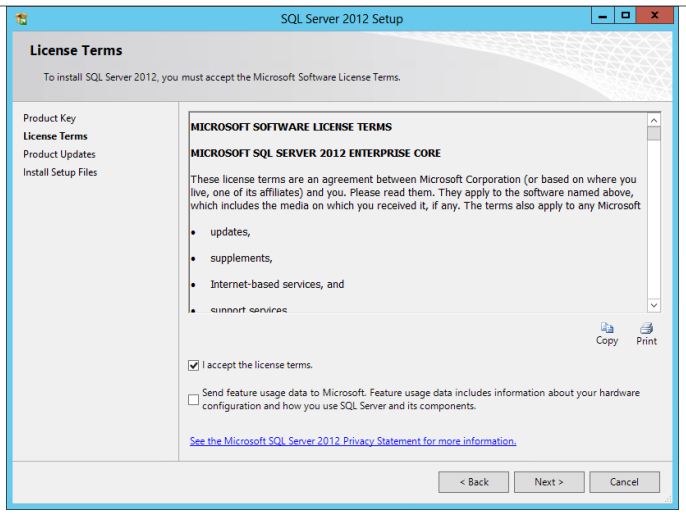
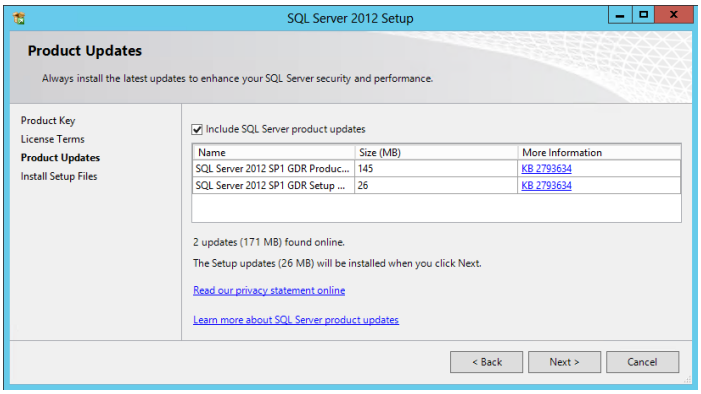
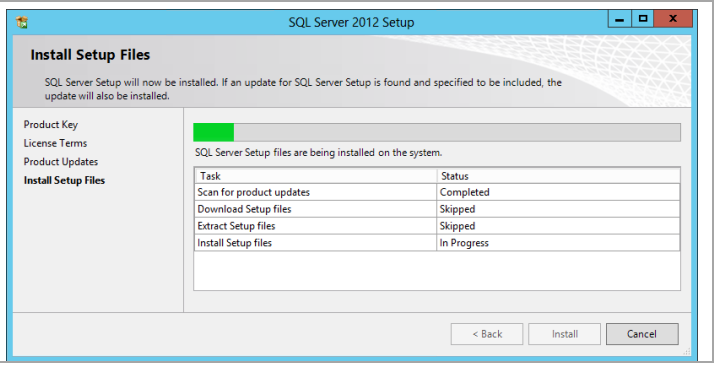
When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.	
Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).	
Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server® 2012 Management Studio (SSMS) prior to moving to the next step of installation.	

Install the SQL Named Instances on the Guest Cluster (Additional Nodes)

When completed with the creation of all required SQL instances on Node 1, additional nodes (Node 2 required, additional nodes are optional) can be added to each instance of the cluster. Follow the steps below to begin the installation of additional nodes of the cluster.

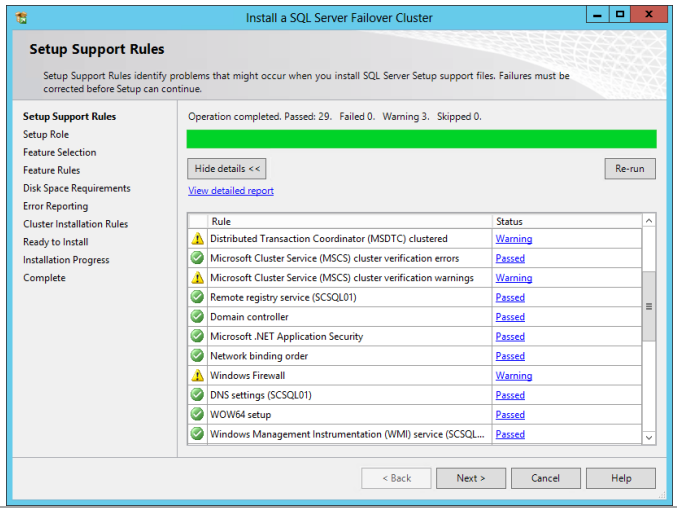
▶ Perform the following steps on **each additional fabric management SQL Server node** virtual machine.

From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear.	
From the **SQL Server Installation Center** click the **Add node to a SQL Server failover cluster** link.	
The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.	
In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue. **Note:** If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.	

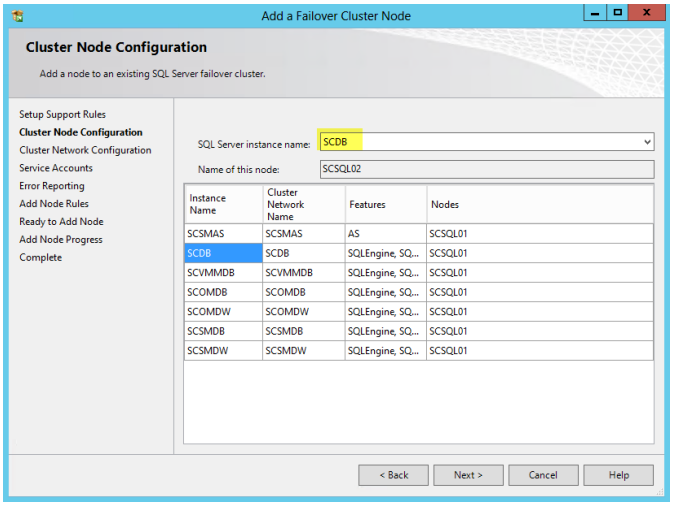
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.	
In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.	
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.	

In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Click **Next** to continue.

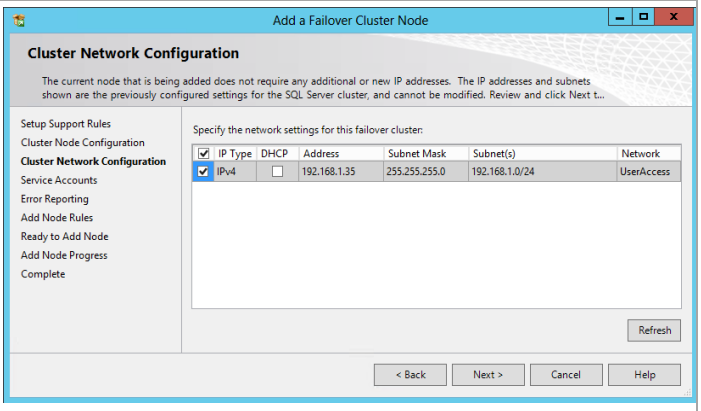
Note: The use of MSDTC is not required for the System Center 2012 SP1 environment.



In the **Cluster Node Configuration** dialog, select the desired instance name from the **SQL Server instance name** drop-down menu. Each instance will be listed along with the nodes currently assigned to each instance. Click **Next** to continue.

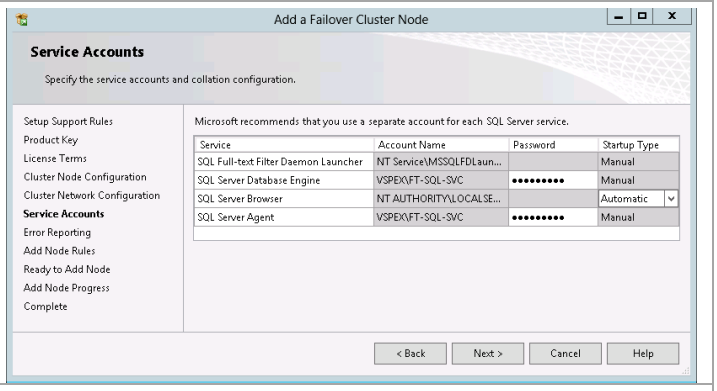


In the **Cluster Network Configuration** dialog, the network configuration values are displayed and set based on the existing failover cluster instance values from the first node and cannot be modified. Click **Next** to continue.

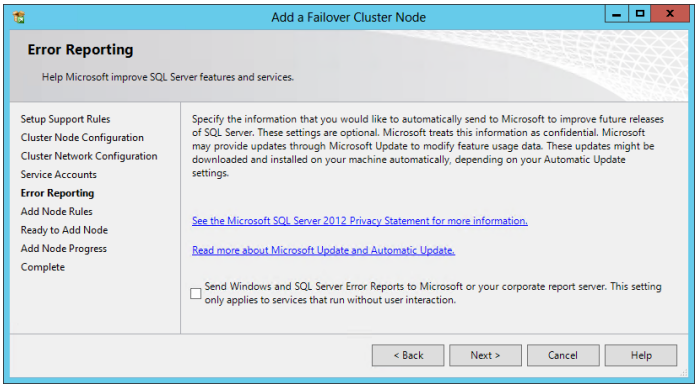


In the **Service Accounts** dialog, specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services. Once complete, click **Next** to continue.

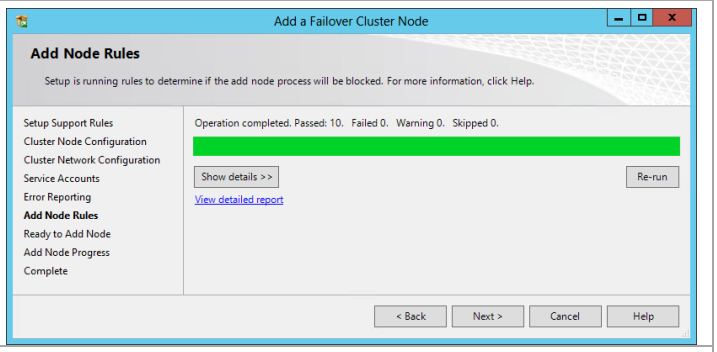
Note: For the SCSMAS instance only, an additional password must be supplied for the **SQL Server Analysis Services** service account.



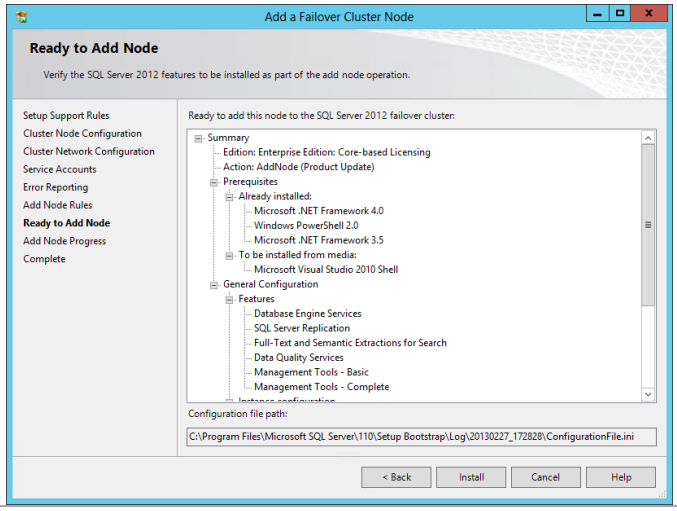
In the Error Reporting dialog, select or clear the Send Windows and SQL Server Error Reports to Microsoft or your corporate report server check box based on your organization's policies and click Next to continue.



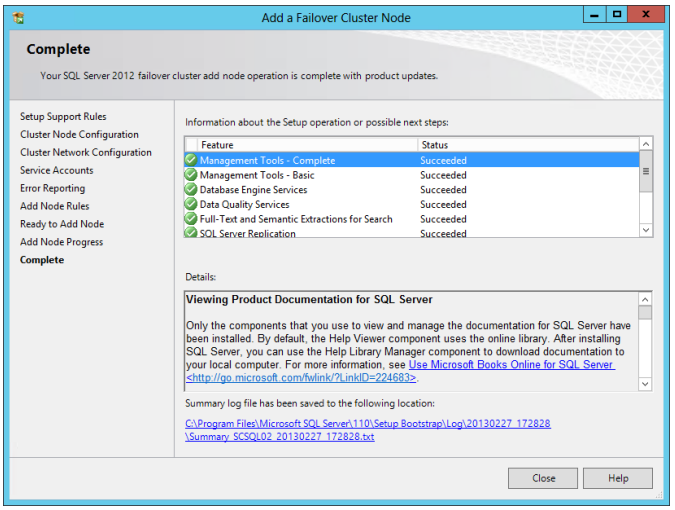
In the **Add Node Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



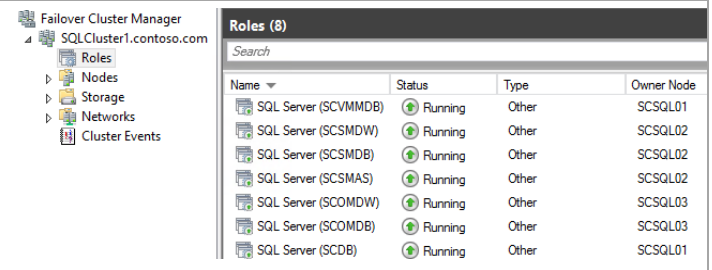
In the **Ready to Add Node** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the second SQL Server node for the selected instance.

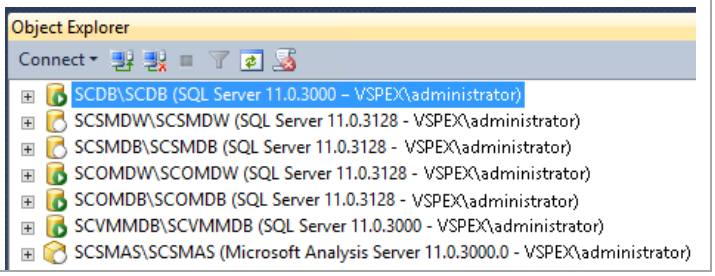


When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.
Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).



Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server® 2012 Management Studio (SSMS) prior to moving to the next step of installation.





Post-Installation Tasks

When the installation is complete, the following tasks must be performed to complete the installatioin of SQL Server.

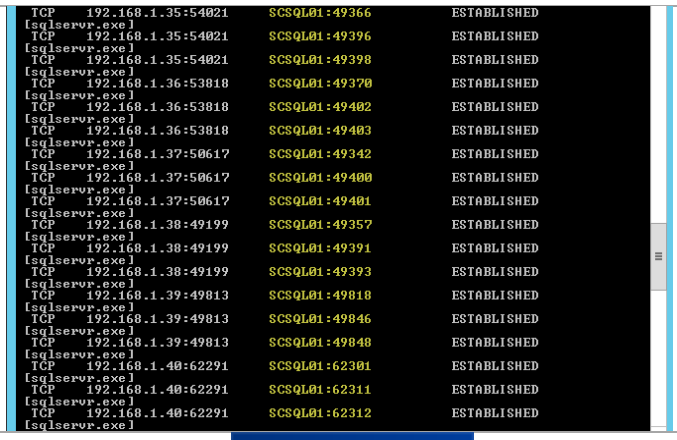
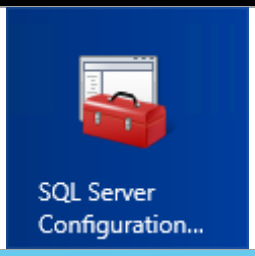
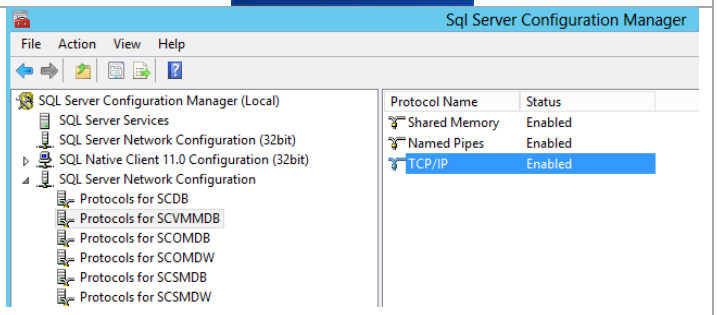
Configure Windows Firewall Setting for SQL Named Instances

To support the multi-instance cluster, you must configure each SQL instance to use a specific TCP/IP port for the database engine or analysis services. The default instance of the Database Engine uses port 1433, and named instances use dynamic ports. In order to configure the Firewall rules to allow access to each named instance static listening ports must be assigned. Note that the SCDB instance must be configured to use port 1433 if the Cloud Services Process Pack (CSPP) is intended to be used.

This process is described in TechNet[7] and instructions are provided in this document.

▶ Perform the following steps on **each fabric management SQL Server node** virtual machine.

[7] Configure a Server to Listen on a Specific TCP Port - http://technet.microsoft.com/en-us/library/ms177440(v=sql.110).aspx

Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt execute the following command: **`netstat -b`** Notice the existing dynamic ports used by the SQLSERVER.EXE sessions.	
On the first SQL Server node open **SQL Configuration Manager**.	
In the **SQL Server Configuration Manager** console pane, expand the **SQL Server Network Configuration** node and then expand the **Protocols for the <instance name>** node. Once selected, double-click **TCP/IP** from the available protocol names to observe its properties.	

In the **TCP/IP Properties** dialog, select the **IP Addresses** tab, several IP addresses appear in the format IP1, IP2, up to IPAll. Each address will include several values:

Active - *Indicates that the IP address is active on the computer. Not available for IPAll.*

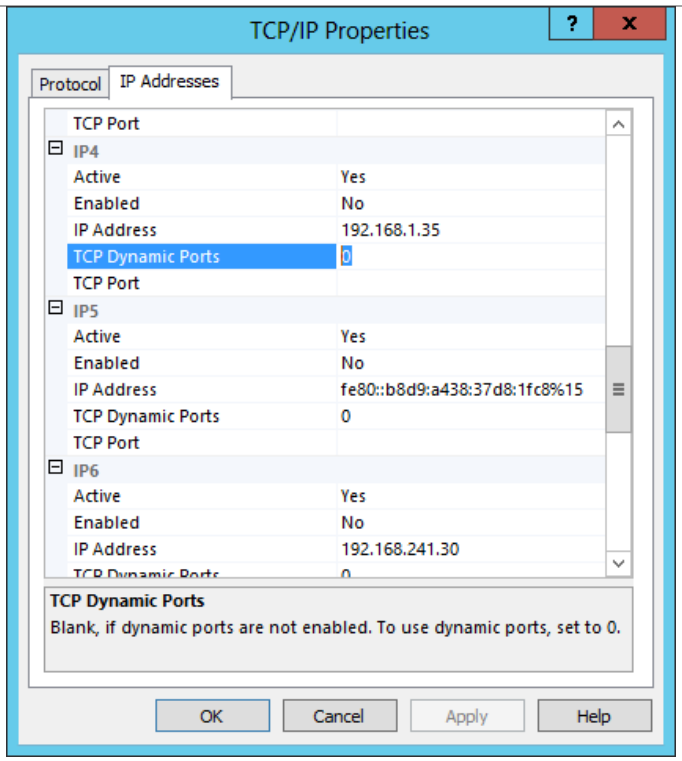
Enabled - *If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to No, this property indicates whether SQL Server is listening on the IP address. If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to Yes, the property is disregarded. Not available for IPAll.*

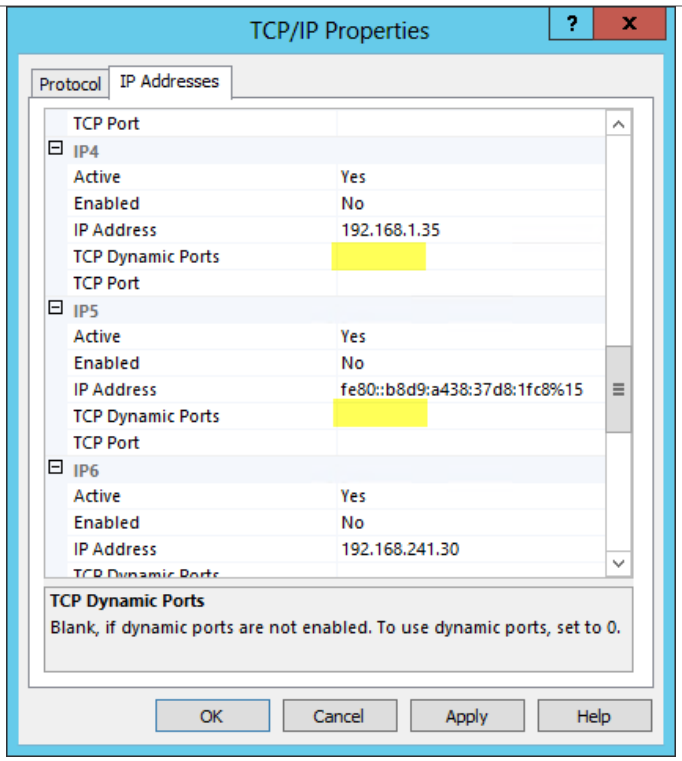
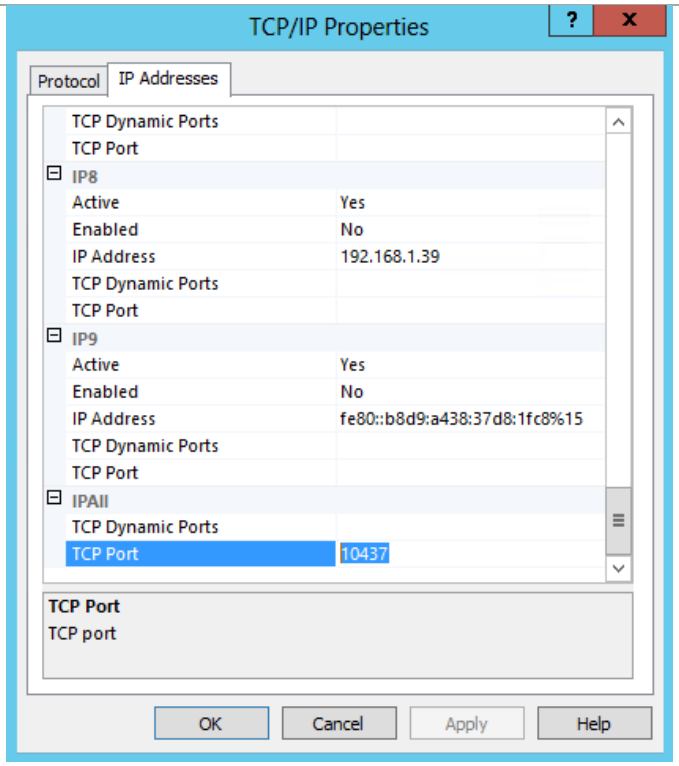
IP Address - *View or change the IP address used by this connection. Lists the IP address used by the computer, and the IP loopback address, 127.0.0.1. Not available for IPAll. The IP address can be in either IPv4 or IPv6 format.*

TCP Dynamic Ports - *Blank, if dynamic ports are not enabled. To use dynamic ports, set to 0. For IPAll, displays the port number of the dynamic port used.*

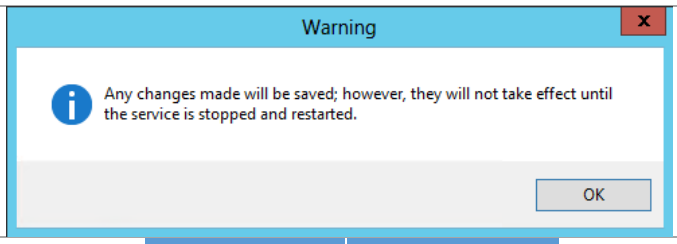
TCP Port - *View or change the port on which SQL Server listens. By default, the default instance of Database Engine listens on port 1433. Note that the SCDB database must use port 1433 if the Cloud Services Process Pack will be used.*

SQL Server Database Engine can listen on multiple ports on the same IP address, list the ports, separated by commas, in the format 1433,1500,1501. This field is limited to 2047 characters. To configure a single IP address to listen on multiple ports, the Listen All parameter must also be set to No, on the Protocols Tab of the TCP/IP Properties dialog box. For more information, see "How to: Configure the Database Engine to Listen on Multiple TCP Ports" in SQL Server Books Online.



Within the dialog, browse to each IP address section for the instance and delete the numerical value (0) from the **TCP Dynamic Ports** field.	
Scroll down to the **IPALL** section and delete the existing dynamic port value from **TCP Dynamic Ports** property. Assign static port value under **TCP Port** to one that is appropriate for the instance. For this example, port 10437 was specified. Click **Apply** to save the changes.	

A warning dialog will appear stating that the settings will not take effect until the SQL Server service has been restarted for that instance.



Repeat these steps to set a static port for each database service instance.
Reference the SQL settings table at the beginning of this section for the default values used in this guide.
Once all of the database instances are configured close **SQL Server Configuration Manager** and continue on to the next steps to change the SSAS instance listening port.

SQL Instance	Listening Port
SCDB	1433
SCVMMDB	10434
SCOMDB	10435
SCOMDW	10436
SCSMDB	10437
SCSMDW	10438
SCSMAS	10439

Note: The SCDB instance must use port 1433 if the Cloud Services Process Pack (CSPP) is used in the environment.

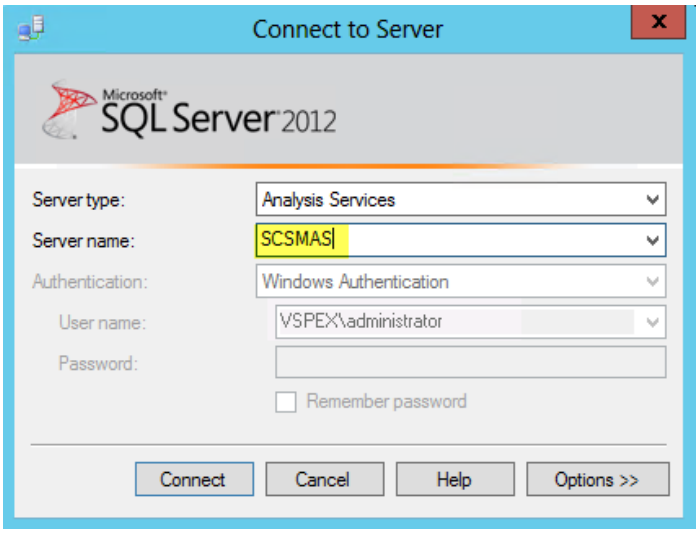
Open **SQL Server Management Studio**.

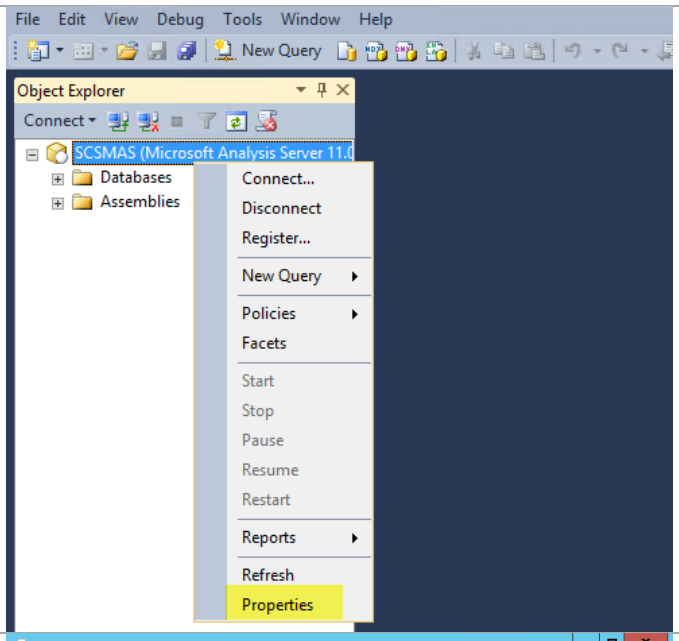
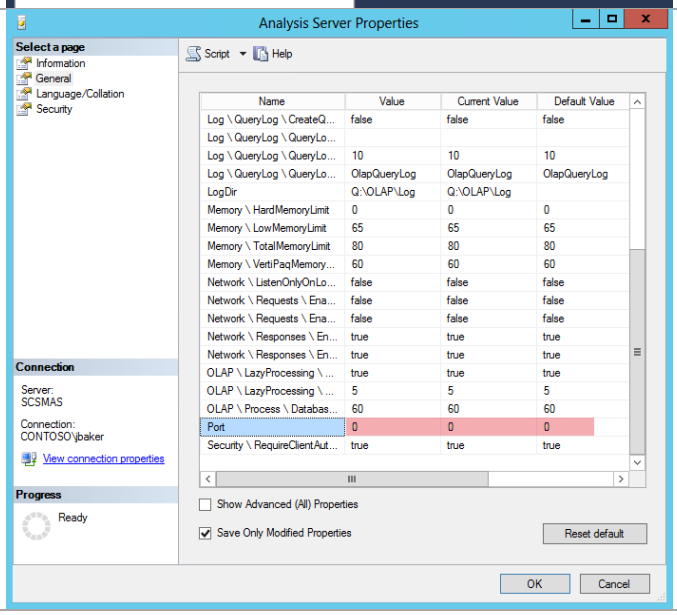


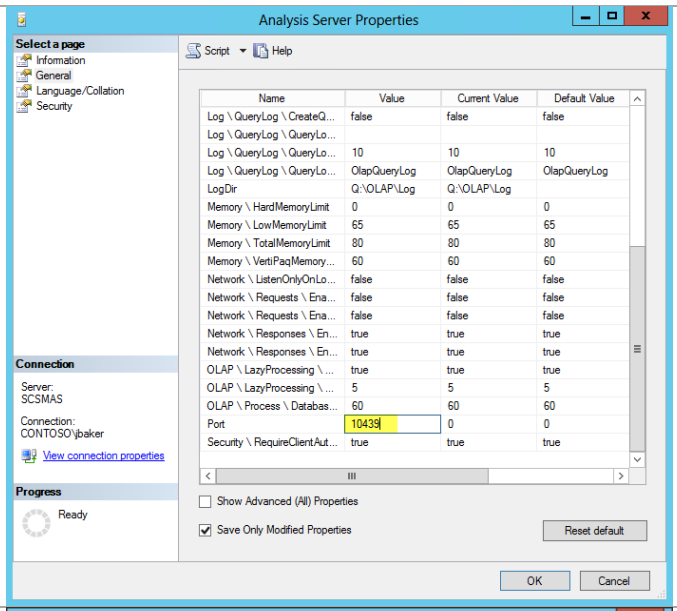
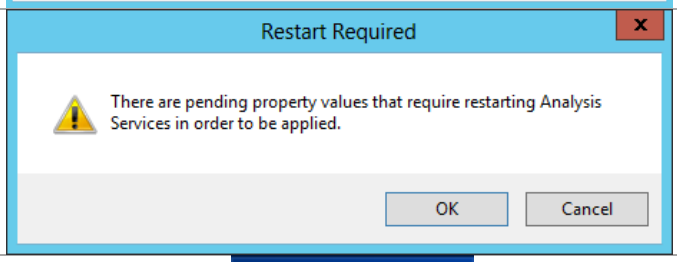
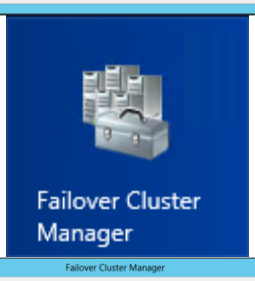
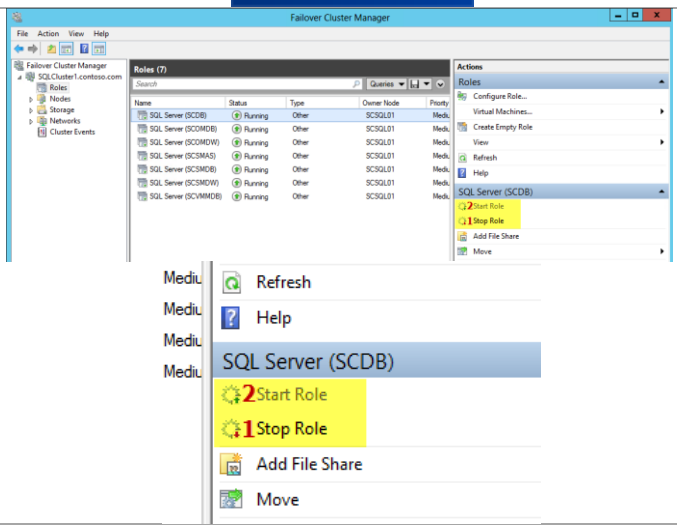
In the **Connect to Server** dialog, input the connection values for the SSAS instance. The default values of SCSMAS\SCSMAS for the analysis service are incorrect. You must use only the virtual computer object name (SCSMAS in this example) as shown here. Click **Connect** to connect to the instance.

Note: Be sure the account you are logged on with is a member of the FT-SQL-Admins domain group or has otherwise been defined as a SQL sysadmin for the instance.

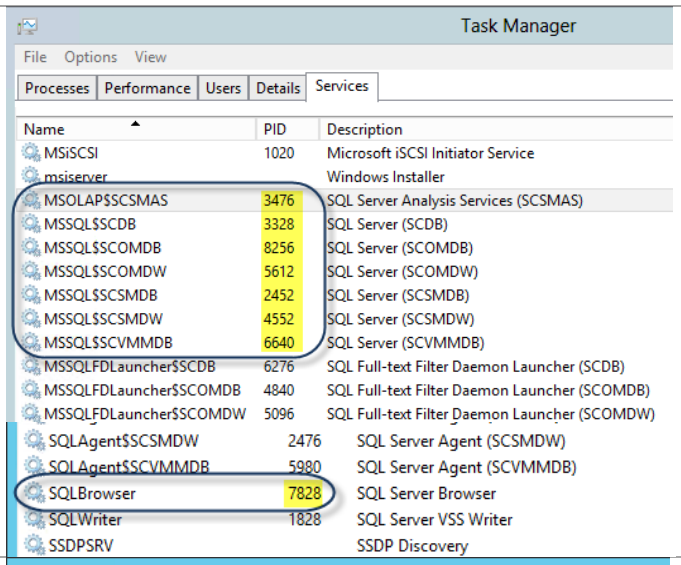




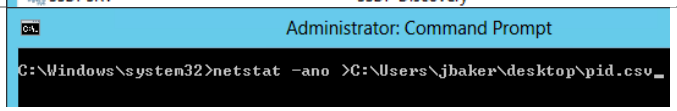
When connected to the instance in **SQL Management Studio**, right-click the SSAS instance and select **Properties**.	
In the Analysis Server Properties dialog, select the General tab and then select **Port** (SQL listening port) from the **Name** column. By default the value will be set to "0" (zero) to specify a dynamic port.	

In the same dialog, specify an appropriate static port value then click **OK** to save the changes.	
A dialog will appear outlining that a restart is required. Click **OK** and close SQL Management Studio.	
Open **Failover Cluster Manager** and expand the **Roles** node.	
To apply the new port settings, in **Failover Cluster Manager** select each SQL Server instance. In the action pane, select **Stop Role** to stop the service for each instance. Restart each instance by selecting **Start Role** from the action Pane. Close the **Failover Cluster Manager** console.	

To verify the port settings have been properly assigned, open **Task Manager** and select the **Services** tab. Review the list of services and note the PID numbers for each of the SQL Services.



Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt execute the following command: **`netstat -ano`** to export the output to a CSV file.



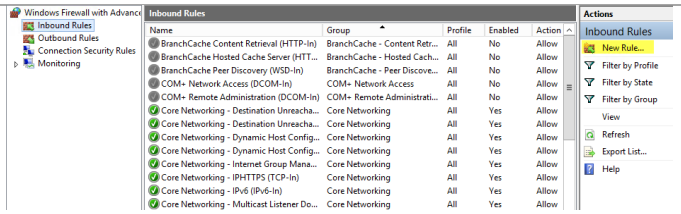
Import the CSV file into Excel and then format the data into a table.
Filter on the PID column, selecting only the PIDs you documented from the task manager step previously and then filter on the state column selecting only the listening and blank values.
The resulting table should confirm that all of the SQL instances are listening on only the static port assigned previously.
In addition to the static ports for each instance the 2382 TCP/UDP and 1434 TCP/UDP ports for SQL Browser will also be listed and will need to be opened in the firewall settings to support the Analysis and Database Engine instances.

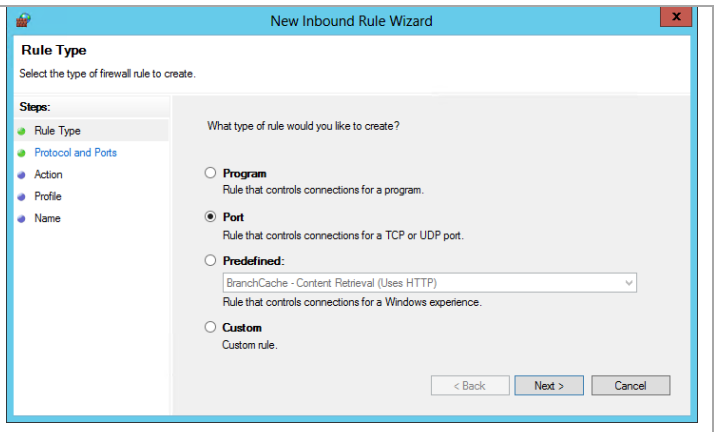
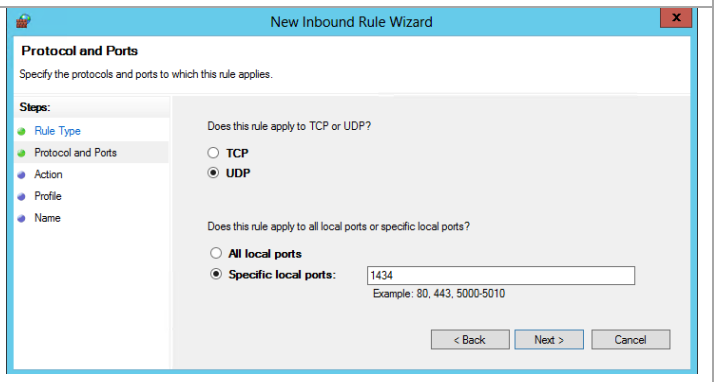
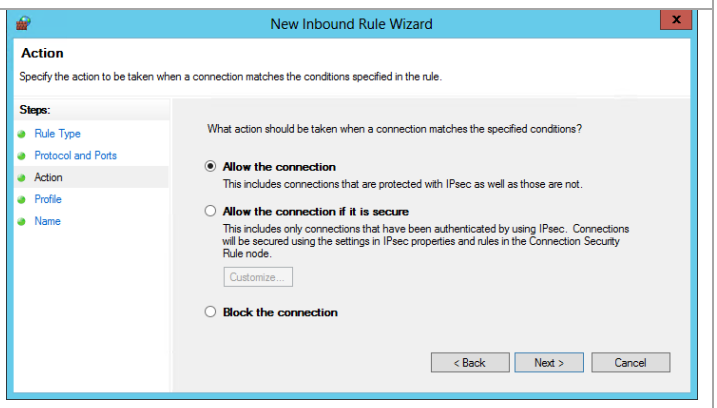
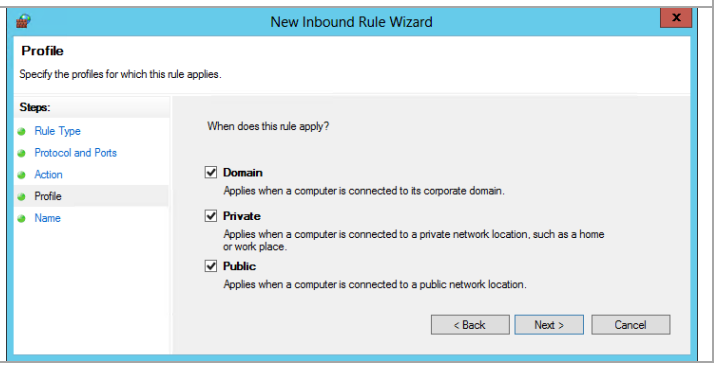
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING	7828
TCP	192.168.1.35:1433	0.0.0.0:0	LISTENING	3328
TCP	192.168.1.36:10434	0.0.0.0:0	LISTENING	6640
TCP	192.168.1.37:10435	0.0.0.0:0	LISTENING	8256
TCP	192.168.1.38:10436	0.0.0.0:0	LISTENING	5612
TCP	192.168.1.39:10437	0.0.0.0:0	LISTENING	2452
TCP	192.168.1.40:10438	0.0.0.0:0	LISTENING	4552
TCP	192.168.1.41:10439	0.0.0.0:0	LISTENING	3476
TCP	[::]:2382	[::]:0	LISTENING	7828
UDP	0.0.0.0:1434	*:*		7828
UDP	[::]:1434	*:*		7828

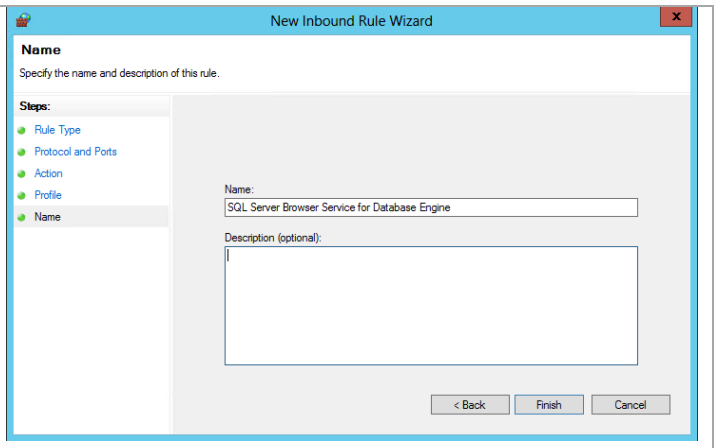
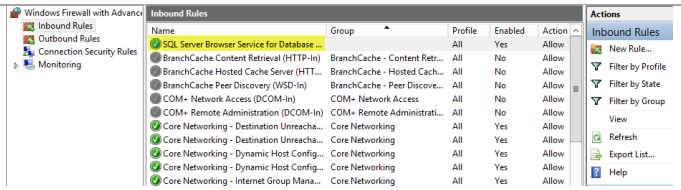
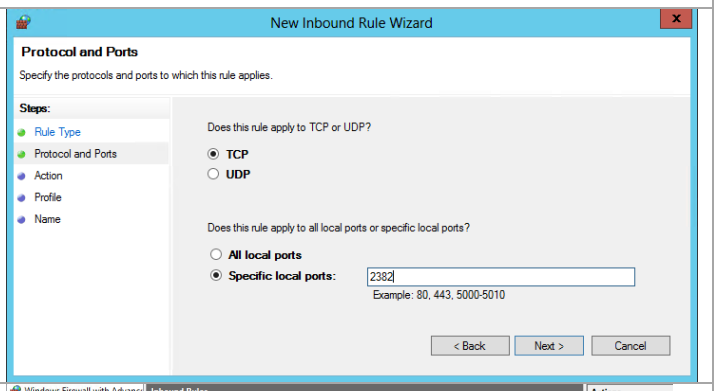
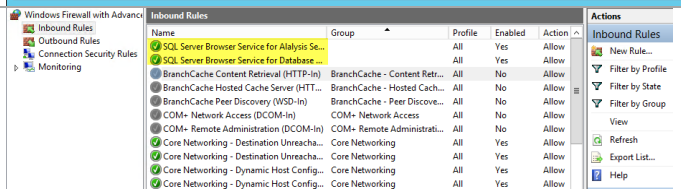
When completed, configure the Windows Firewall Rule for the SQL Browser Service. To perform this action, on each node in the Windows Failover Cluster that will host SQL instances, open the **Windows Firewall with Advanced Security** MMC console.

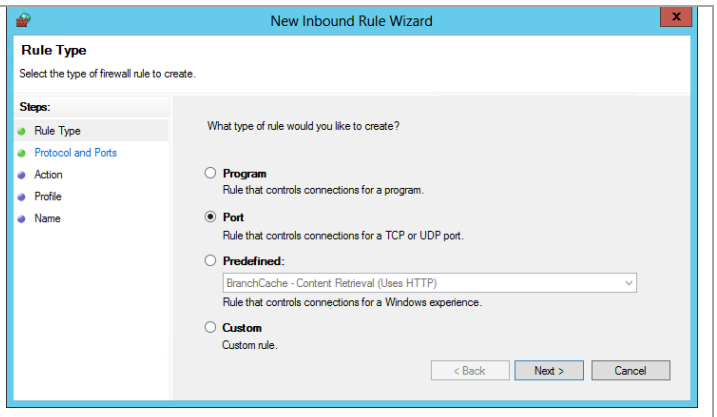
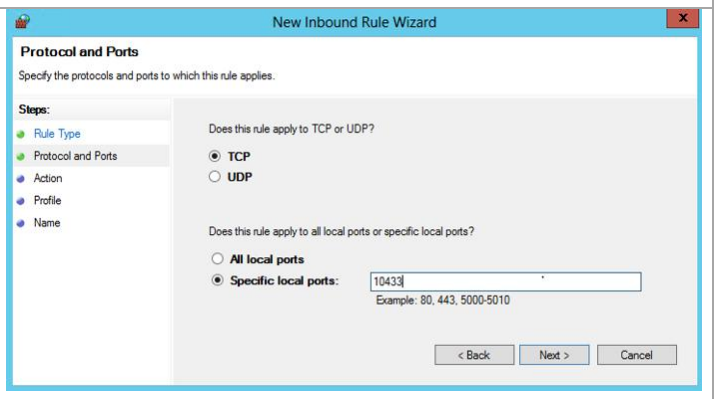
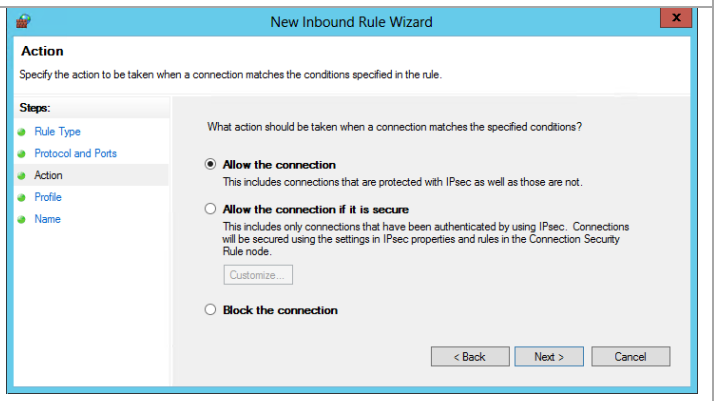


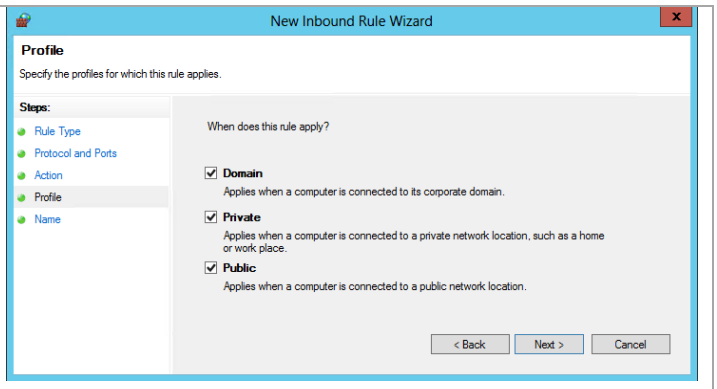
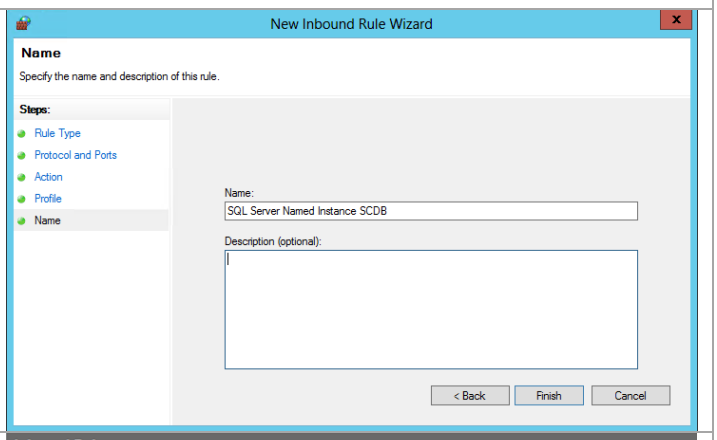
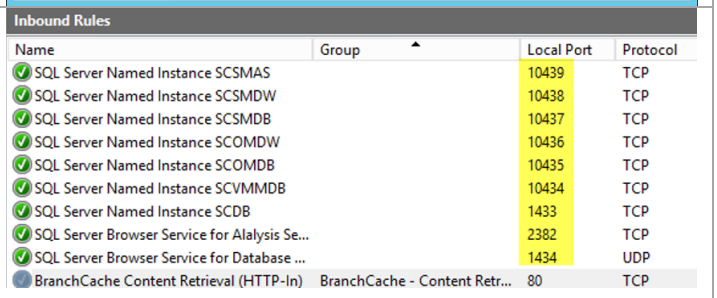
Within the **Windows Firewall with Advanced Security** MMC console, select the **Inbound Rules** node and select **New Rule** from the action pane.



In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.	
On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input 1434 to enable access to the SQL Browser service for Database Engine instances. Click **Next** to continue.	
On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.	
On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue. *Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.*	

Specify a name for the new rule such as "*SQL Server Browser Service for Database Engine*" and click **Finish**.	
The new rule listed in the Inbound Rules pane. Repeat this process by selecting **New Rule** once again from the action pane to create the **SQL Browser Service for Analysis Server** rule.	
Repeat the previously outlined steps to create the new rule, however on the **Protocol and Ports** page, select both the **TCP** and **Specific local ports** radio buttons. Specify the value of **2382** to enable access to the **SQL Browser service for the Analysis Server** instance.	
The additional new rule listed in the Inbound Rules pane. Next the inbound Windows Firewall rule for each of the SQL instances must be created and configured. From the same dialog, select **New Rule** from the action pane to create the firewall rule for the first named instance.	

In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.	
On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input the specific local TCP/IP port to enable access to the first named SQL instance. In this example to enable access to the SQL instance SCDB the port specified is 1433. Click **Next** to continue.	
On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.	

On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue. *Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.*	
Specify a name for the new rule such as "*SQL Server Named Instance SCDB*" and click **Finish**.	
Create an additional rule for each SQL instance. For the reference SQL architecture and instances the rule set would be configured similar to the following diagram.	
Alternatively, firewall rules can be created through PowerShell on the local server as shown in the following example. Be sure to replace the port number value with the correct value for your environment.	`New-NetFirewallRule -DisplayName "SQL Server Browser Service for Database Engine" -LocalPort 1434 -Protocol UDP -Action Allow`

To create the rules on the remote nodes through PowerShell, the following commands are provided as an example.
Note that the SCDB instance must be set to 1433 if the Cloud Services Process Pack will be used.

```
$RemoteSession = New-CimSession -ComputerName SCSQL02
New-NetFirewallRule -DisplayName "SQL Server Browser Service for Database Engine" -LocalPort 1434 -Protocol UDP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Browser Service for Analysis Server" -LocalPort 2382 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCDB" -LocalPort 1433 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCVMMDB" -LocalPort 10434 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCOMDB" -LocalPort 10435 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCOMDW" -LocalPort 10436 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMDB" -LocalPort 10437 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMDW" -LocalPort 10438 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMAS" -LocalPort 10439 -Protocol TCP -Action Allow -CimSession $RemoteSession
```

Assign Preferred Owners for SQL Instances in Failover Cluster Manager

To support the proper distribution of SQL instances across the multi-instance SQL Server cluster, you must configure Windows failover clustering to assign preferred owners for each SQL instance. The following steps are provided to assist with this configuration.

▶ Perform the following steps on **<u>one</u> fabric management SQL Server node** virtual machine.

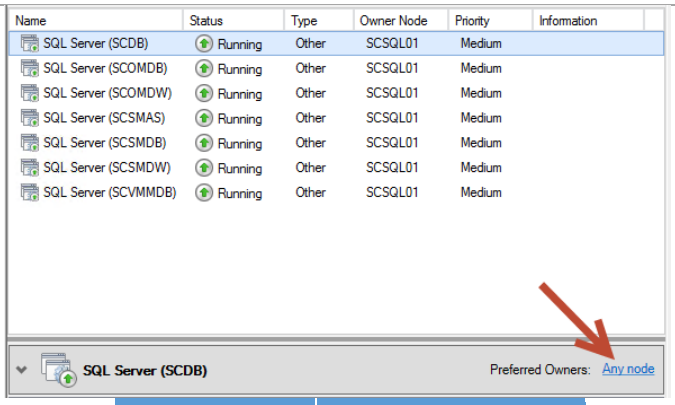
On any SQL Server cluster node, open **Failover Cluster Manager** and expand the **Roles** node.



During the installation of SQL Server, all instances were installed on the first failover cluster node and then added to each additional node. By default every failover cluster node is now a *Possible Owner* and a *Preferred Owner* of every SQL Server instance.

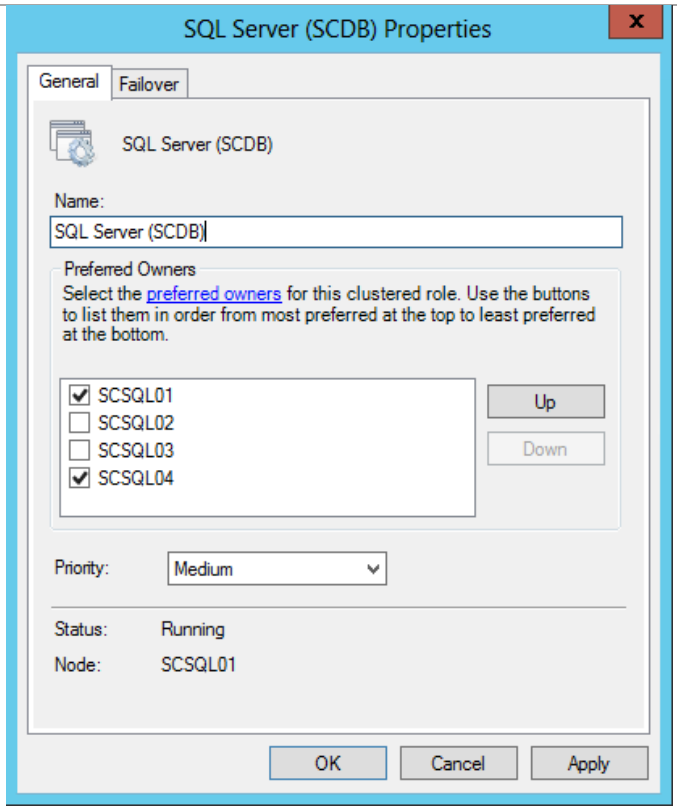
In order to better control failover behavior and distribution of the instances the **Preferred Owners** list must be modified and the owner node must be assigned by failing over the SQL Server instance to that node. Refer to the list created previously.

To perform this configuration, select the first SQL Server instance under the **Roles** node. With the first SQL Server instance selected, click on the **Any Node** link next to **Preferred Owners**.

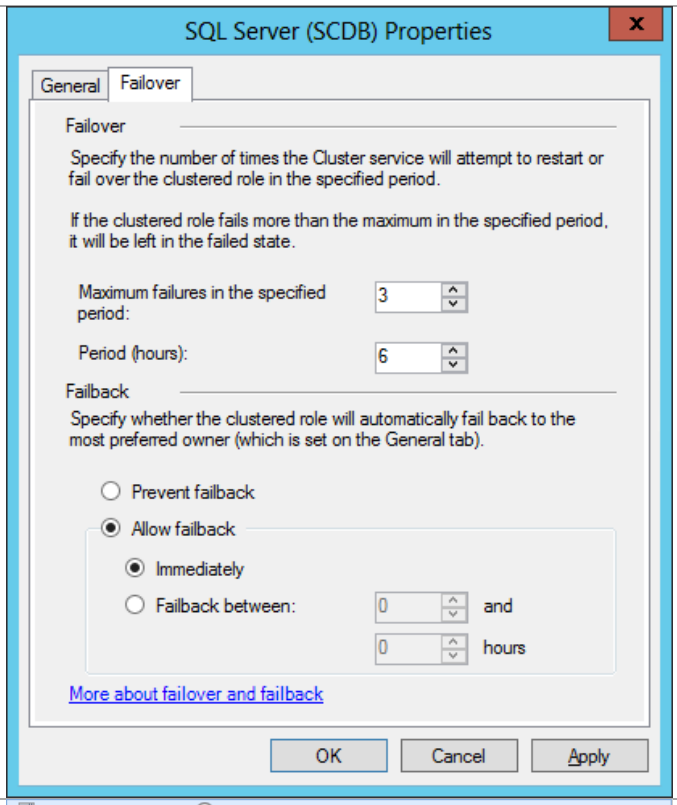


SQL Instance	Preferred Owners
SCDB	Node1, Node4
SCVMMDB	Node1, Node4
SCOMDB	Node3, Node4
SCOMDW	Node3, Node4
SCSMDB	Node2, Node4
SCSMDW	Node2, Node4
SCSMAS	Node2, Node4

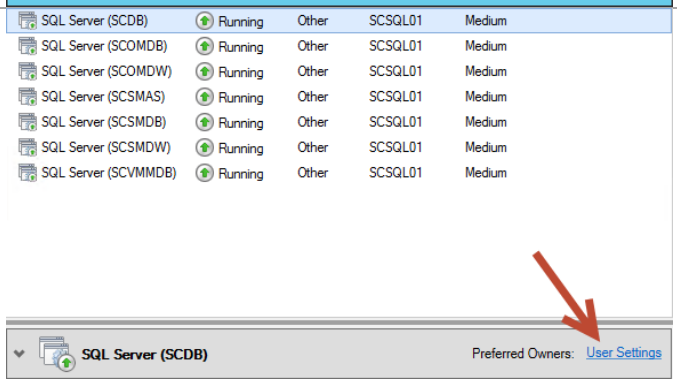
In the **SQL Server Properties** dialog, select the **General** tab, select the two preferred nodes for the instance. It is not required to adjust the order as this will be automatically adjusted when the process is completed.



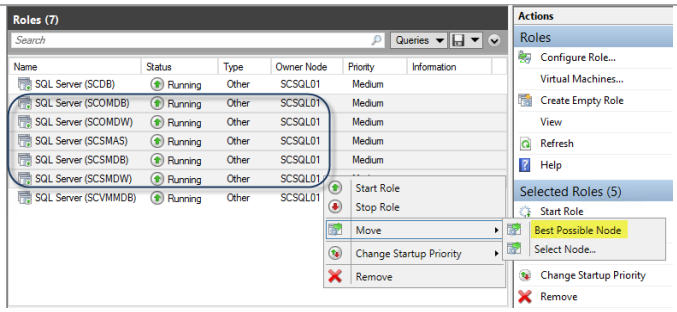
In the **SQL Server Properties** dialog, select the **Failover** tab. In the **Failback** section, select the **Allow failback** and **Immediately** radio buttons. Click **OK** to save the changes.



The value for the **Preferred Owners** link now displays a value of *User Settings*.
Repeat this process for each SQL Server instance.

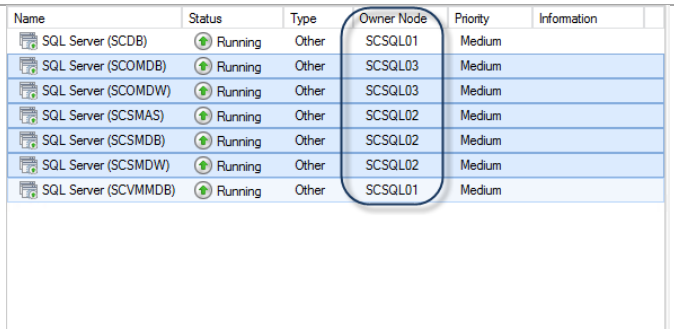


When all instances have been configured correctly for Preferred Owners you must initiate a planned failover to balance the SQL Server instances across nodes.
In **Failover Cluster Manager**, select the roles for each of the five SQL Instances that should not run on Node1 (SCOMDB, SCOMDW, SCSMDB, SCSMDW, SCSMAS). Right click on the selection of SQL Instances and select Move and then Best Possible Node from the context menu.



When the moves are completed, all Instances should be distributed across Node1, Node2 and Node 3. Node4 is reserved as the passive node.

Note: With all nodes configured as Possible Owners, failover to nodes not listed as a Preferred Owner can still occur when the preferred owners are not available. However, with Failback enabled the SQL Server instances should always be reassigned on their preferred node when availability returns. This configuration supports a primary dedicated passive node plus two additional active/passive nodes in the case of a failure of two nodes. It is important to note however, that Failback only applies to automatic failover events and not to user initiated moves.

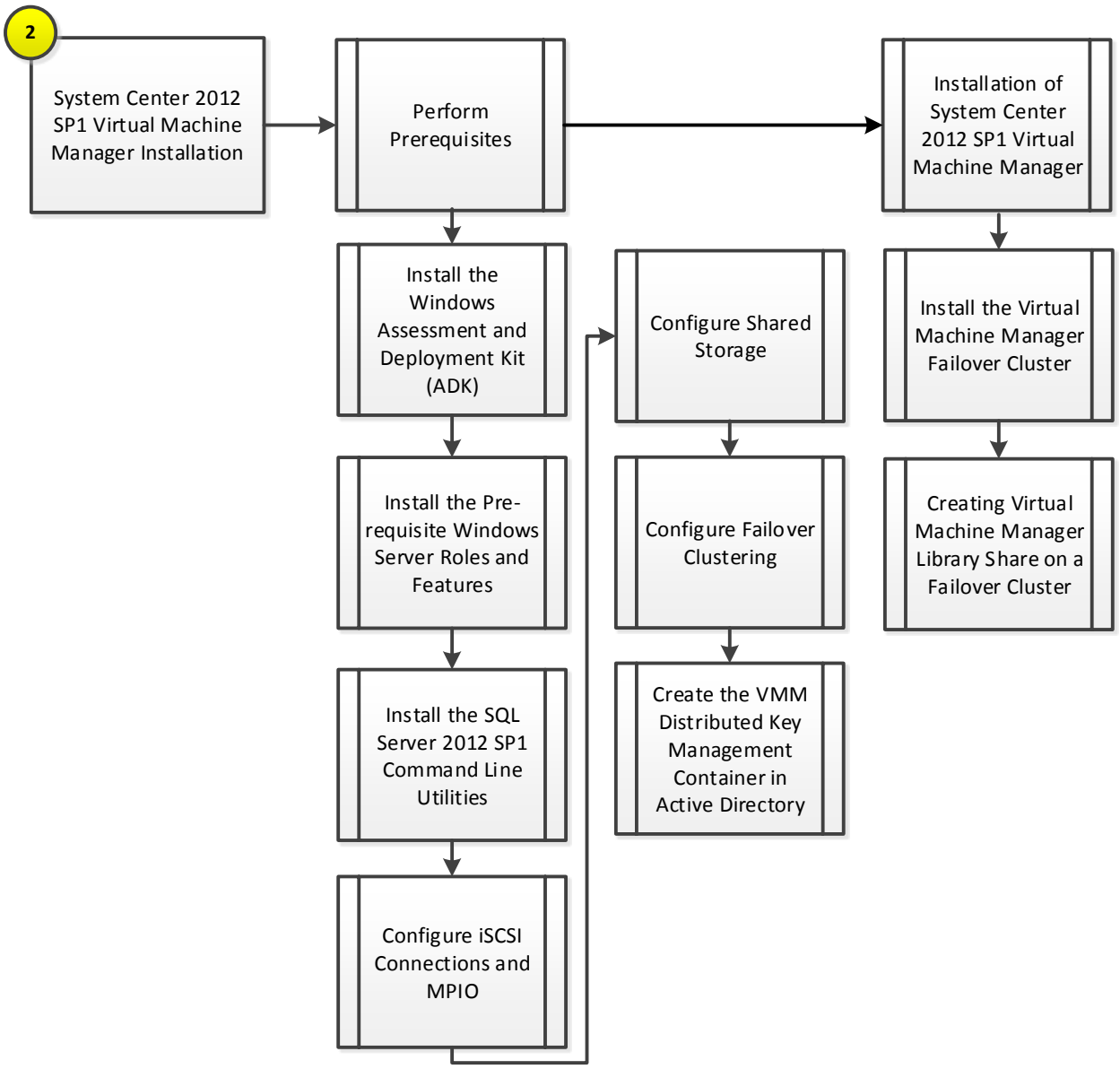


Name	Status	Type	Owner Node	Priority	Information
SQL Server (SCDB)	Running	Other	SCSQL01	Medium	
SQL Server (SCOMDB)	Running	Other	SCSQL03	Medium	
SQL Server (SCOMDW)	Running	Other	SCSQL03	Medium	
SQL Server (SCSMAS)	Running	Other	SCSQL02	Medium	
SQL Server (SCSMDB)	Running	Other	SCSQL02	Medium	
SQL Server (SCSMDW)	Running	Other	SCSQL02	Medium	
SQL Server (SCVMMDB)	Running	Other	SCSQL01	Medium	

9 System Center Virtual Machine Manager

The System Center 2012 SP1 Virtual Machine Manager Installation process is comprised of the following high-level steps:

Figure 11 Virtual Machine Manager Installation Process



9.1 Overview

This section provides high-level walkthrough on deploying Virtual Machine Manager into the Fast Track fabric management architecture. The following assumptions are made prior to the installation:

- Two base virtual machines running Windows Server 2012 have been provisioned and configured as a Windows Failover Cluster.
  - The selected operating system installation type during install must be Full Installation.
  - Requires at least two shared storage LUNs or one shared storage LUN and a file share witness
  - Requires a dedicated virtual network adapter for cluster communication
  - Using SMB 3.0, implement two dedicated virtual network adapters for SMB communications.

- The Microsoft .NET Framework 4 feature will be installed by default.
- The target virtual machines must have the Windows Assessment and Deployment Kit (ADK) for Windows 8 and Windows Server 2012 installed.
- The target virtual machine must have the Windows Server Update Services (WSUS) 4.0 console installed (available on Windows Server 2012).
    - Virtual Machine manager can use either a WSUS root server or a downstream WSUS server. VMM does not support using a WSUS replica server. The WSUS server can either be dedicated to VMM or can be a WSUS server that is already in use.
- A Microsoft SQL Server instance dedicated to Virtual Machine Manager as outlined in previous steps must be available.
    - The Virtual Machine Manager SQL Server instance must be case-insensitive (default on SQL Server 2012).
    - The SQL Server name must not exceed 15 characters.
    - The account used to install Virtual Machine Manager must have the rights needed to connect to the remote SQL Server instance and create databases.
- The installation account must have rights to create the Distributed Key Management container in AD DS or this container must already exist prior to running Virtual Machine Manager setup.

9.2 Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following user accounts have been created:

Table 26 Prerequisite Accounts

User name	Purpose	Permissions
<DOMAIN>\FT-VMM-SVC	Virtual Machine Manager Service Account	This account will need full admin permissions on the Virtual Machine Manager server virtual machine and runs the Virtual Machine Manager service.

Groups

Verify that the following security groups have been created:

Table 27 Prerequisite Security Groups

Security group name	Group scope	Members
<DOMAIN>\FT-SCVMM-Admins	Global	FT-VMM-SVC
<DOMAIN>\FT-SCVMM-FabricAdmins	Global	Virtual Machine Manager Delegated Administrators

Security group name	Group scope	Members
<DOMAIN>\FT-SCVMM-ROAdmins	Global	Virtual Machine Manager Read Only Admins
<DOMAIN>\FT-SCVMM-TenantAdmins	Global	Virtual Machine Manager Tenant Administrators who manage Self-Service users
<DOMAIN>\FT-VMM-AppAdmins	Global	Virtual Machine Manager Self-Service users

Additional information on these roles can be found on TechNet[8].

Required Networks

VMaccess, ClusComm, iSCSI-A, iSCSI-B (optionally can use SMB-A and SMB-B to access a file share witness).

If deploying the Nexus 1000V, the VSM network is required.

Install the Windows Assessment and Deployment Kit

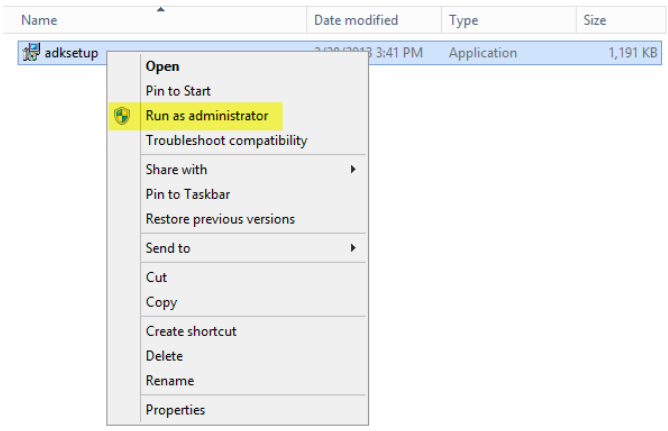
The Virtual Machine Manager installation requires that the Windows Assessment and Deployment Kit (ADK) be installed on the Virtual Machine Manager management server. The Windows ADK can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=30652.

During installation, only the Deployment Tools and the Windows Preinstallation Environment features will be selected. This installation also assumes the VMM servers have internet access. If that is not the case an offline installation can be performed and information for this installation option along with complete installation details can be found at http://msdn.microsoft.com/en-us/library/hh825494.aspx.

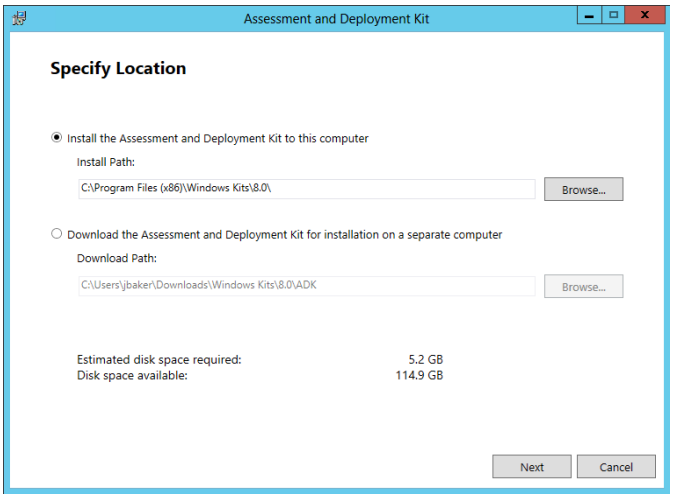
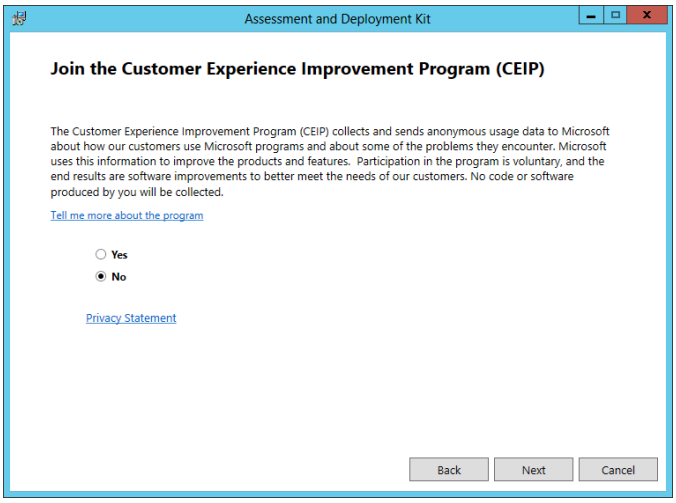
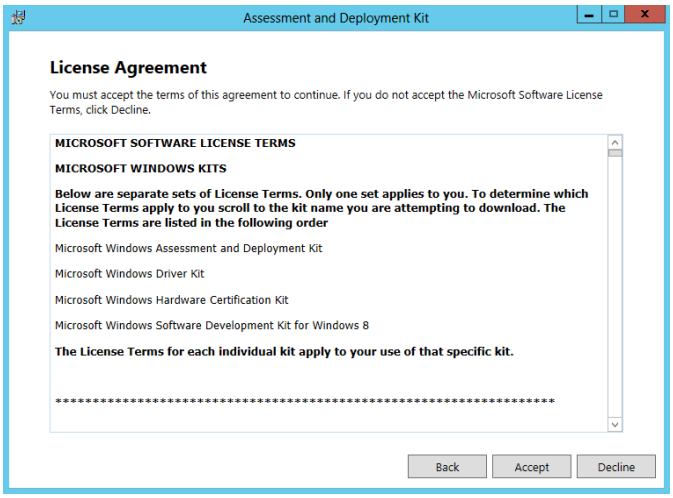
The following steps detail how to install the Windows ADK on the Virtual Machine Manager management server.

▶ Perform the following steps on both **Virtual Machine Manager** virtual machines.

From the Windows ADK installation media source, right-click **adksetup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



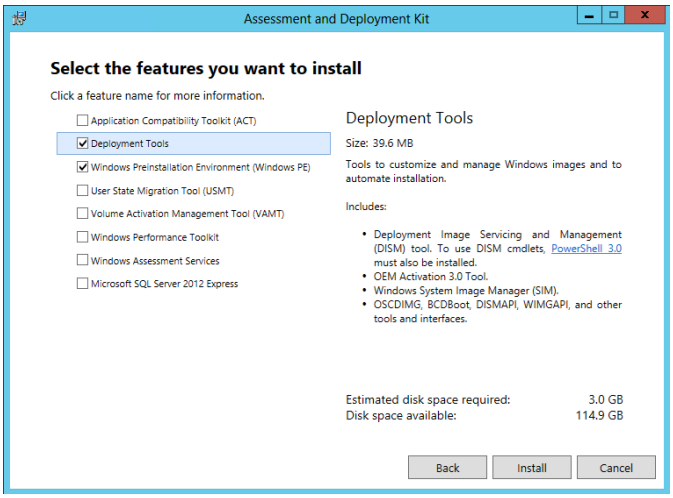
[8] Creating User Roles in VMM - http://technet.microsoft.com/en-us/library/gg696971.aspx

A splash screen will appear. In the **Specify Location** dialog, accept the default folder location of *%ProgramFiles%\Windows Kits\8.0* and click **Next** to continue.	
In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
In the **License Agreement** dialog, click **Accept** to continue.	

In the **Select the features you want to install** dialog, select the following option checkboxes:

- **Deployment Tools**
- **Windows Preinstallation Environment (Windows PE)**

Ensure all other option checkboxes are deselected. Click **Next** to begin the installation.



Once installation is complete deselect the **Launch the Getting Started Guide** checkbox and click **Close** to exit the installation wizard.

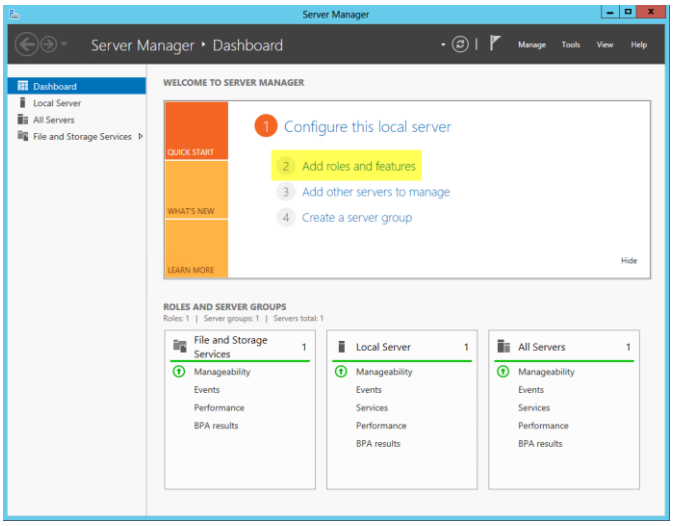


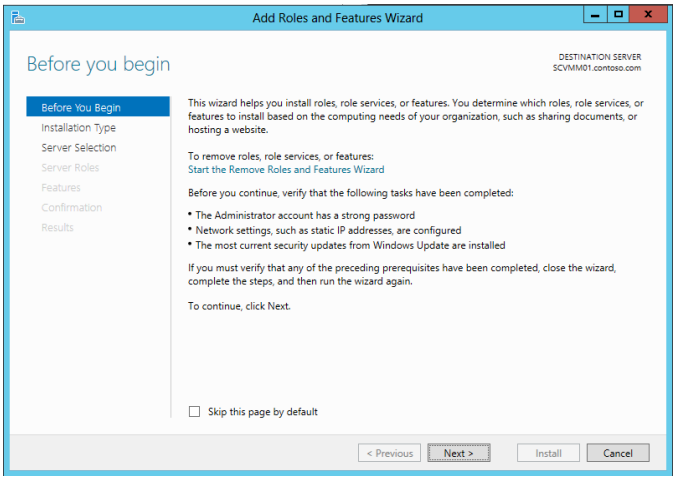
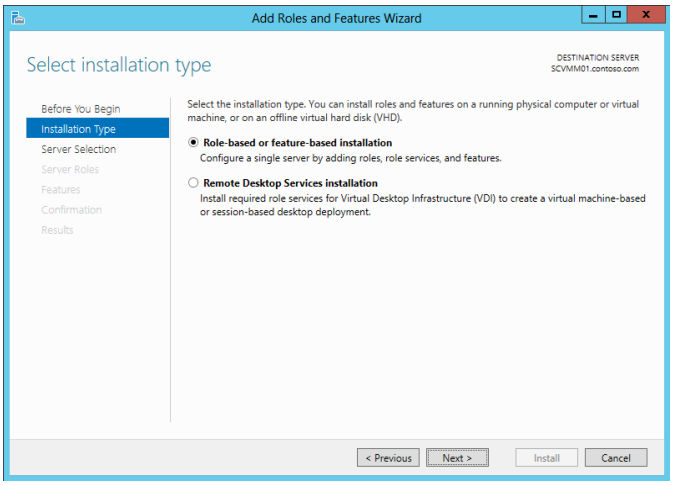
Install the Prerequisite Windows Server Roles and Features

The Virtual Machine Manager installation requires the WSUS Administration Tools to be installed on the Virtual Machine Manager management servers. In addition, the Failover Clustering Features must be installed. Follow the steps below to install the pre-requisite roles and features on the Virtual Machine Manager management servers.

▶ Perform the following steps on each **Virtual Machine Manager** virtual machine.

Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, click **Next** to continue.	
In the **Select Installation Type** dialog, you are presented with two options: • *Role-based or Feature-based installation* – Traditional installation of roles and features to enable discrete functionality on the operating system. • *Remote Desktop Services scenario-based installation* – Installation of a pre-determined combination of roles, features and configurations to support a Remote Desktop (Session Virtualization) or VDI scenario Select the **Role-based or Feature-based installation** radio button and click **Next** to continue.	

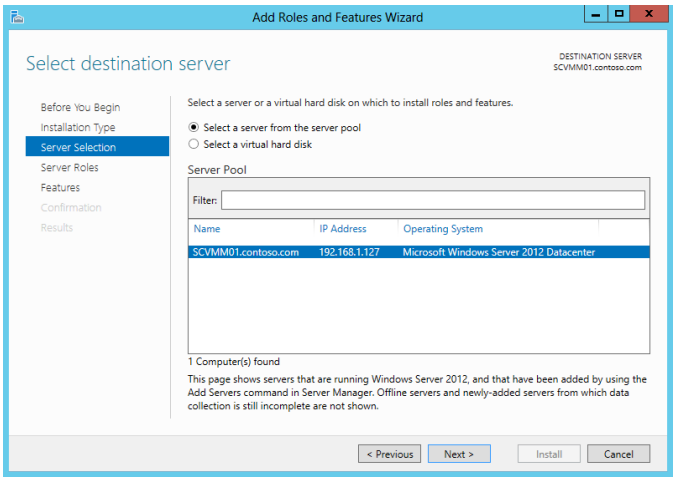
In the **Select destination server** dialog, you are presented with two options:

- *Select a server from the server pool* – This option allows you to select a server from the managed pool of systems defined within Server Manager.

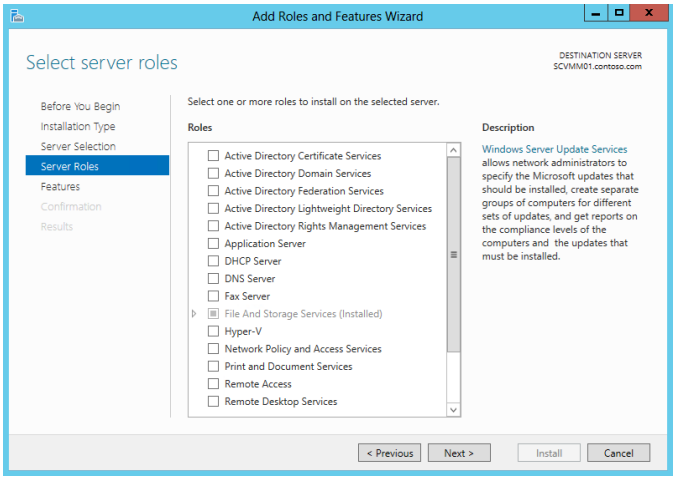
- *Select a virtual hard disk* – This option allows for roles to be installed to staged VHD files for offline servicing purposes.

For this installation, select the **Select a server from the server pool** radio button, select the local server and click **Next** to continue.

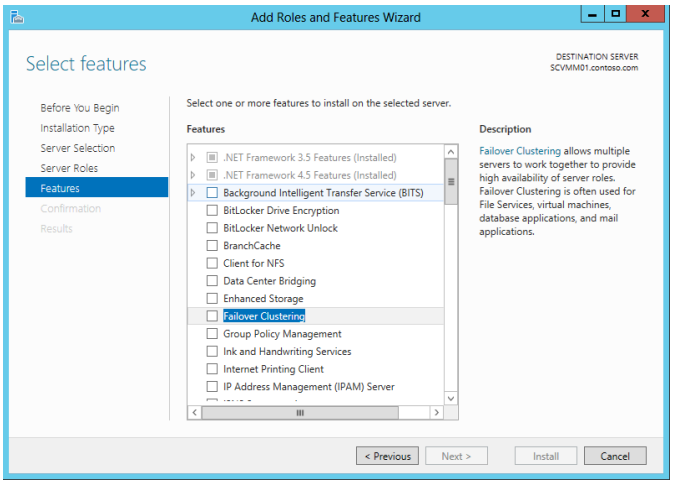
Note: While many servers may be presented in the Select a server from the server pool option, only one can be selected at a time for role and feature installation operations. To enable installs across multiple hosts, the configuration can be saved at the end of the wizard and applied to multiple systems via Server Manager PowerShell cmdlets.

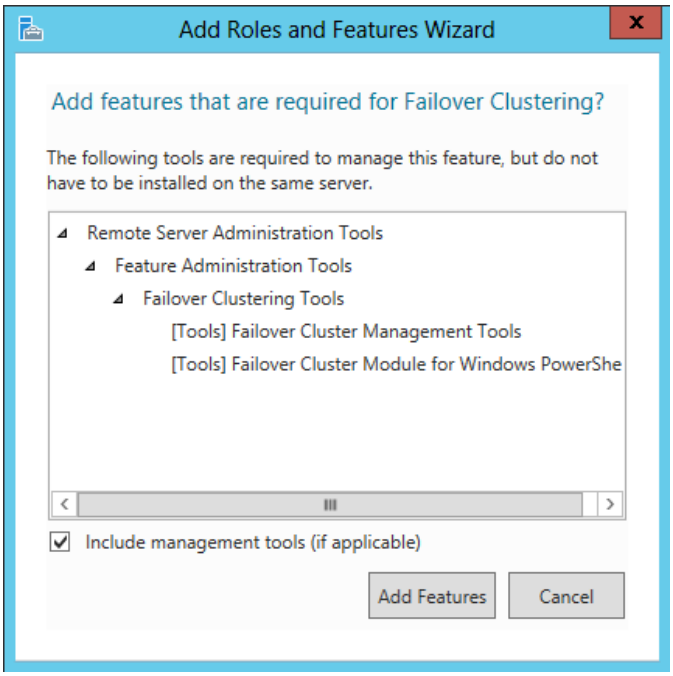
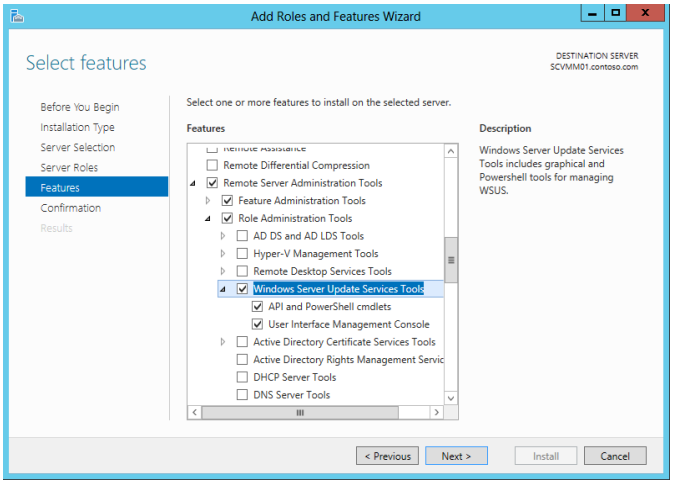


In the **Select Server Roles** dialog, do not make any additional selections and click **Next** to continue.



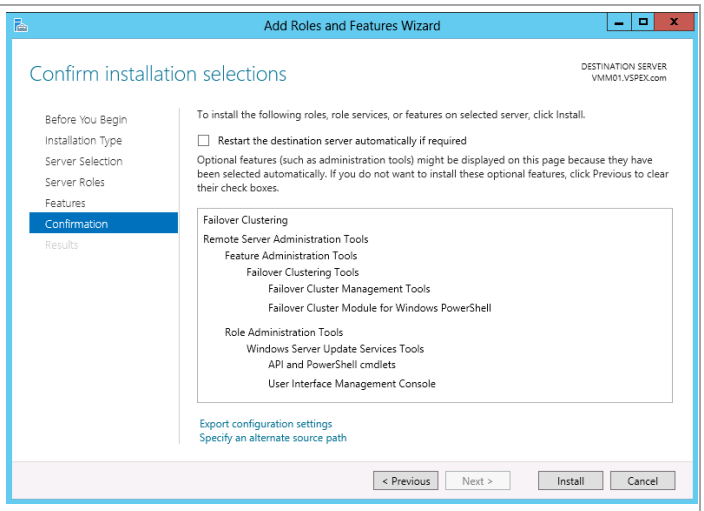
In the **Features** dialog, select **Failover Clustering**.



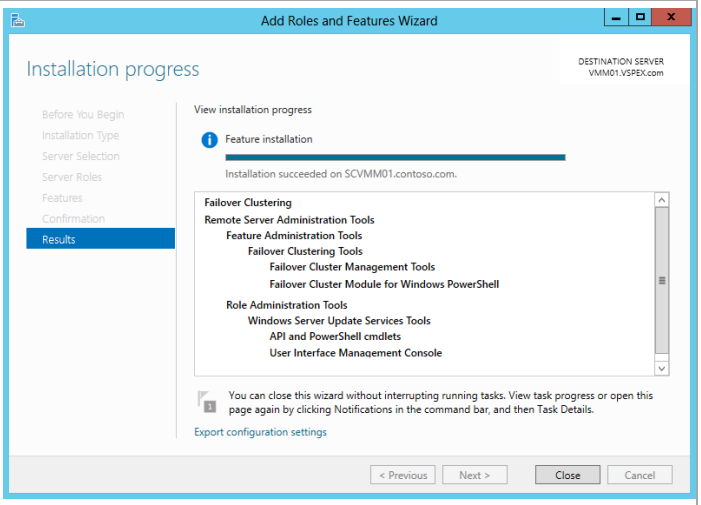
The **Add features that are required for Failover Clustering** dialog will appear. Check the **Include management tools (if applicable)** checkbox, then click the **Add Features** button.	
Next select **Windows Server Update Services Tools** top level features. Click **Next** to continue.	

In the **Confirm installation selections** dialog, Failover Clustering and Windows Server Update Services features are selected.
Click **Install** to begin installation.

Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. Once exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.

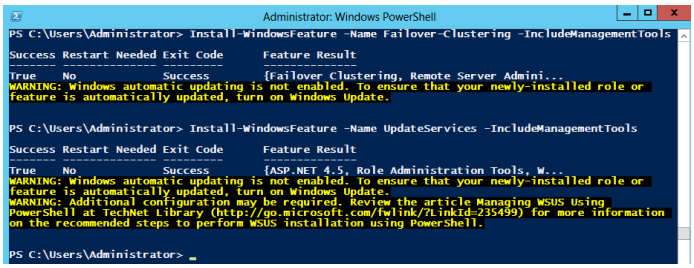


The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



Note that while the following installation was performed interactively, the installation of roles and features can be automated using the PowerShell.

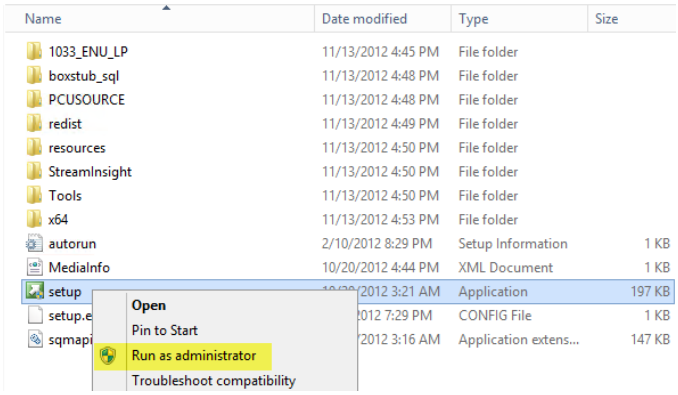
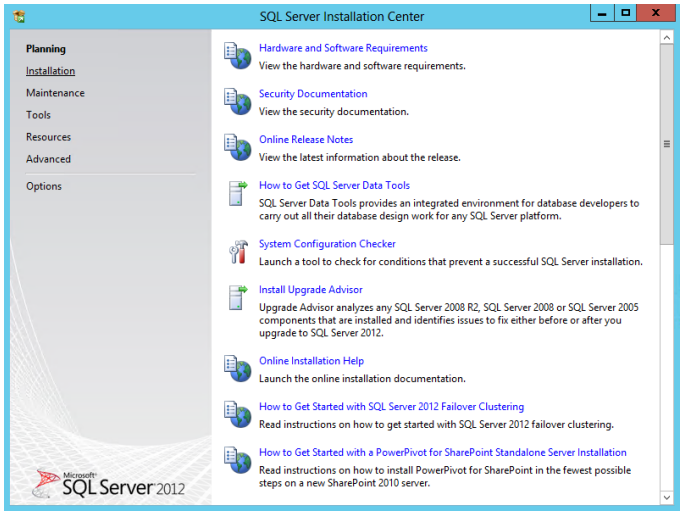
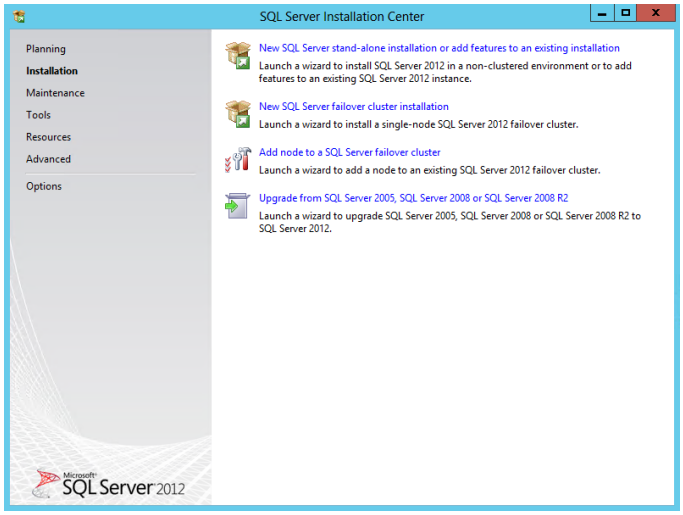
```
Install-WindowsFeature –Name
Failover-Clustering –
IncludeManagementTools
Install-WindowsFeature –Name
UpdateServices –
IncludeManagementTools
```



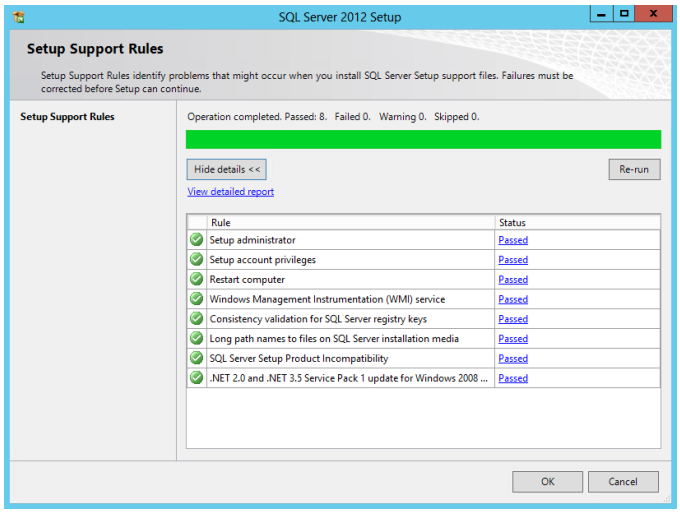
Install the SQL Server 2012 SP1 Command Line Utilities

The Virtual Machine Manager installation requires that the SQL Server 2012 Command Line Utilities and Management Tools be installed on the Virtual Machine Manager Management server. Follow the steps below to install the Command Line Utilities and Management Tools on the Virtual Machine Manager Management server.

▶ Perform the following steps on each **Virtual Machine Manager** virtual machine.

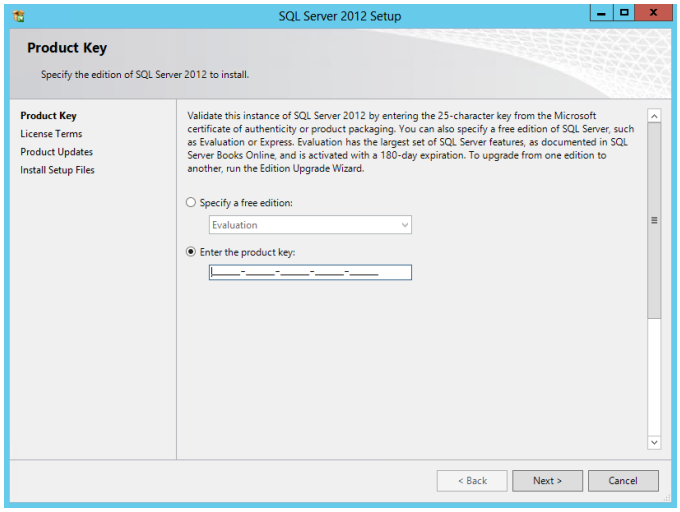
From the SQL Server 2012 with SP1 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The **SQL Server Installation Center** will appear. Select **Installation**.	
From the **SQL Server Installation Center**, click the **New SQL Server stand-alone installation or add features to an existing installation** link.	

The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check.
Click **OK** to continue.

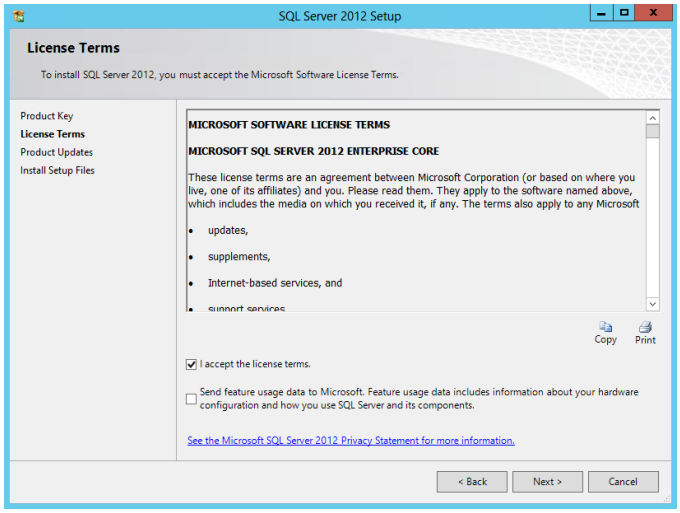


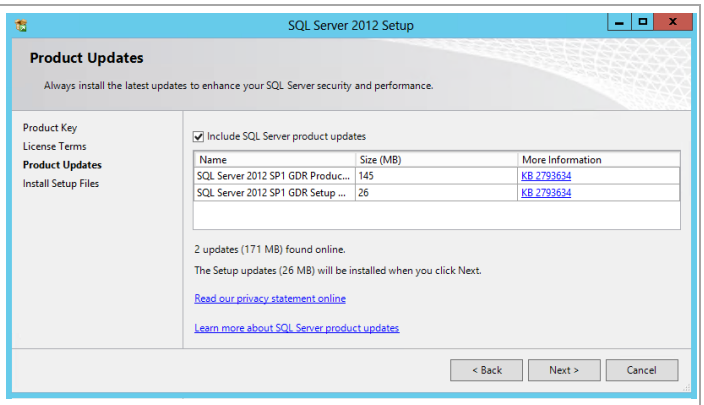
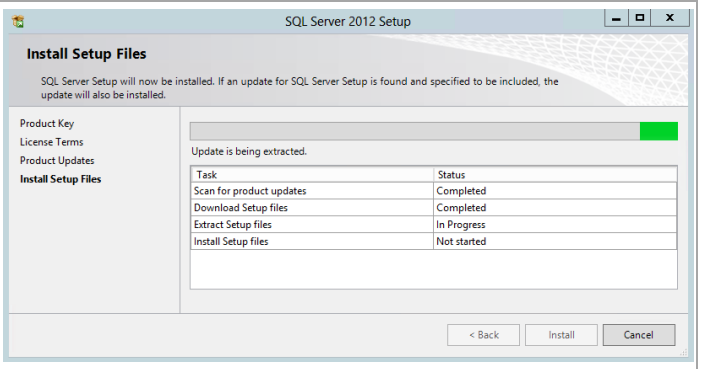
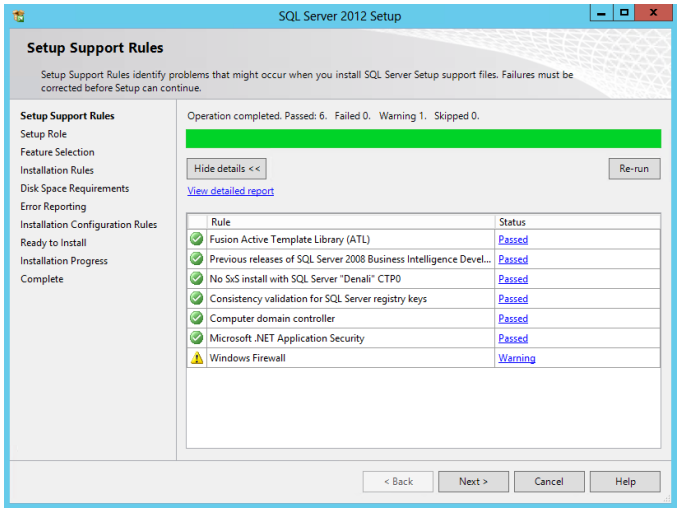
In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box.
Click **Next** to continue.

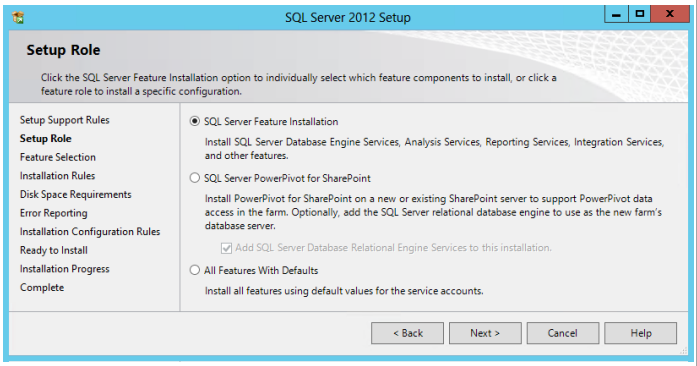
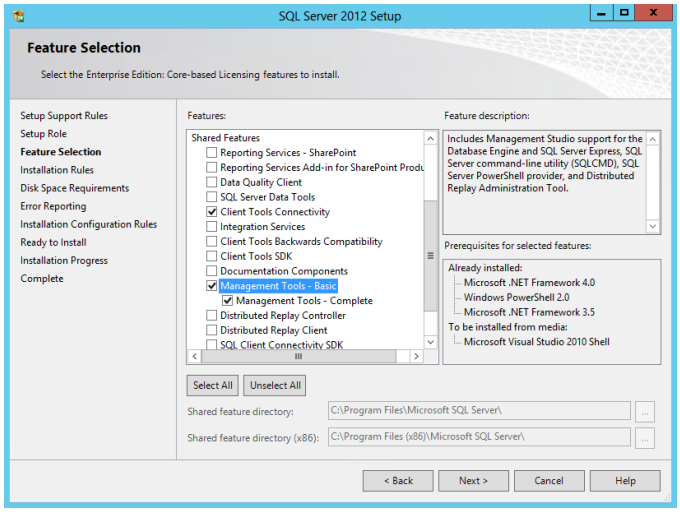
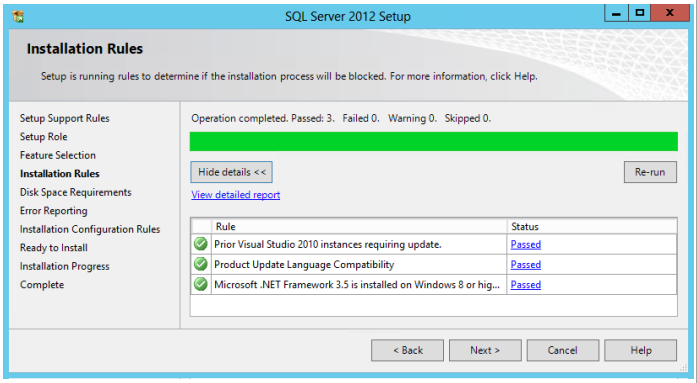
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.

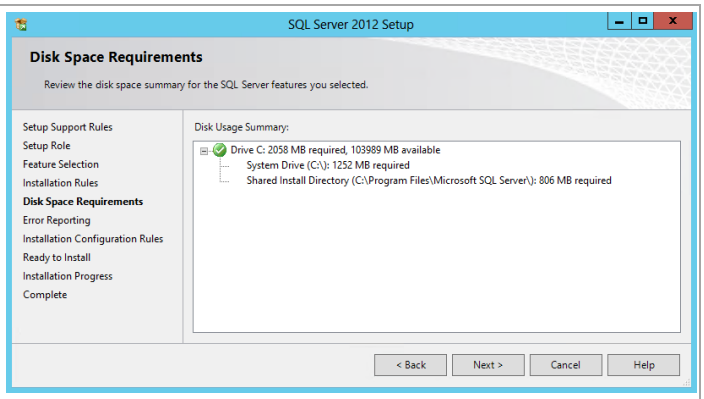
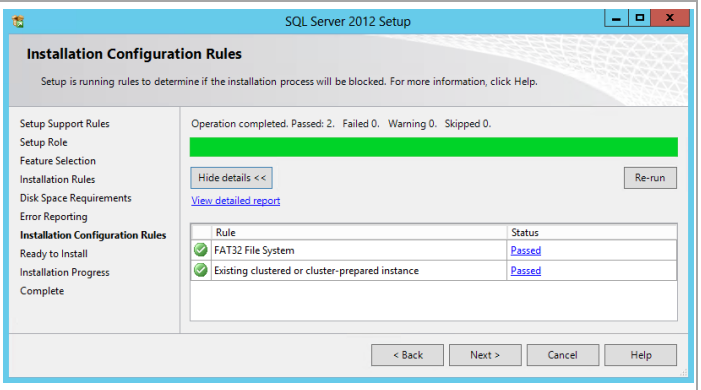


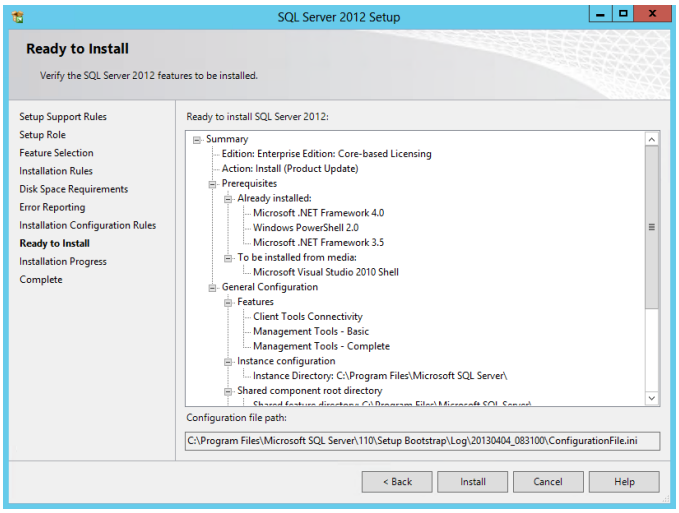
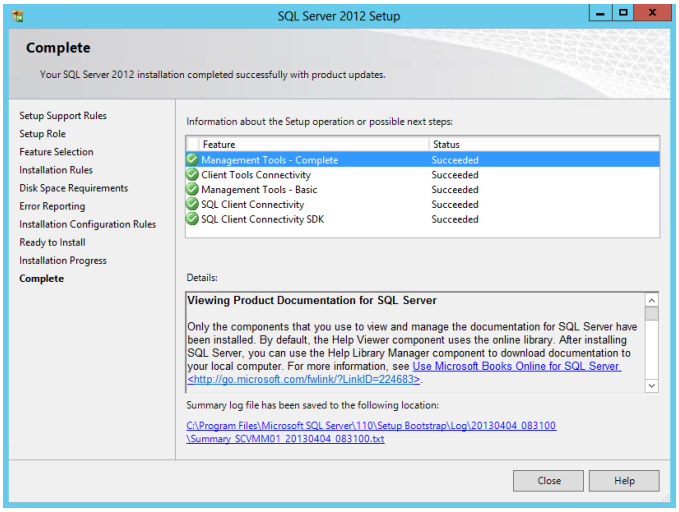
In the **License Terms** dialog, select **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.



In the Product Updates dialog, leave the **Include SQL Server product updates**, selection checked and click **Next**.	
On the **Install Setup Files** dialog the update and install process will be displayed.	
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

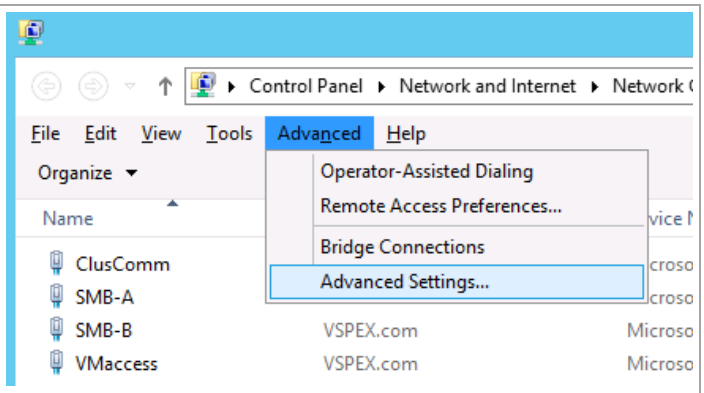
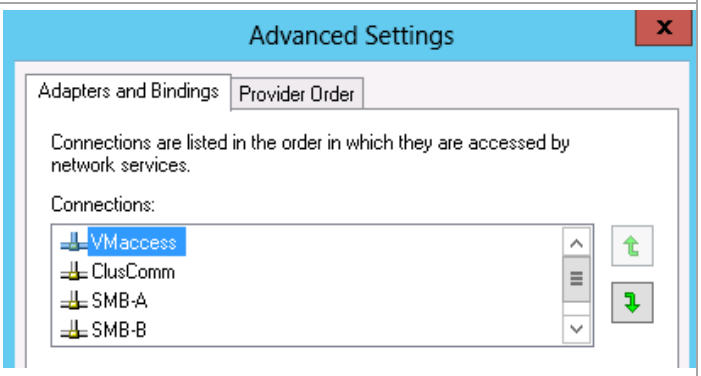
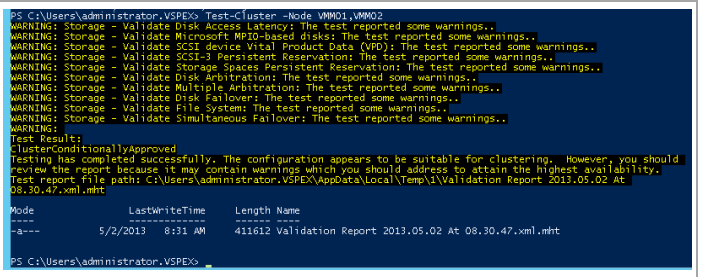
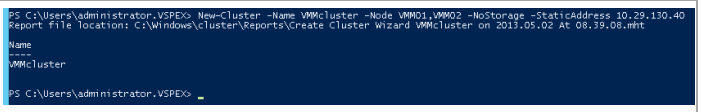
In the **Setup Role** dialog, select the **SQL Server Feature Installation** option and click **Next** to continue.	
In the **Feature Selection** dialog, select the **Client Tools Connectivity, Management Tools – Basic** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.	
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

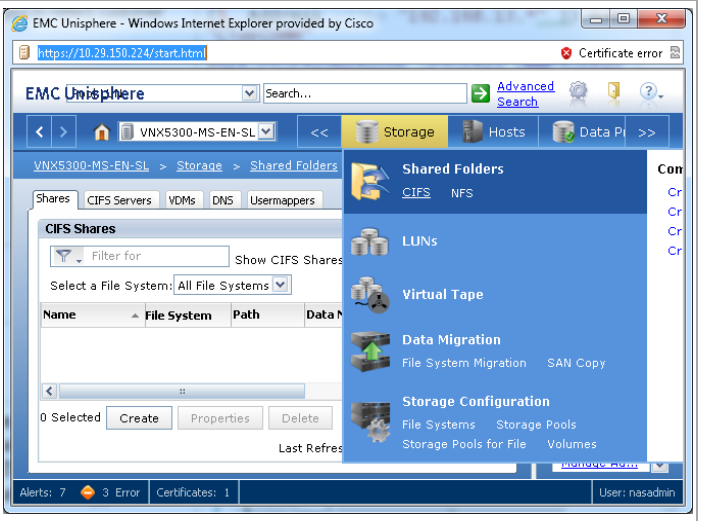
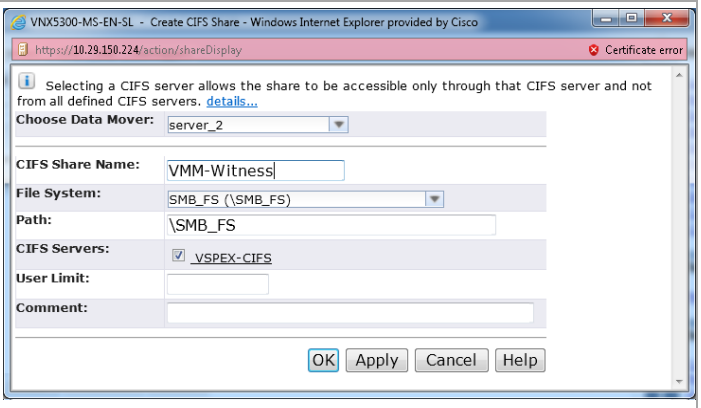
In the **Disk Space Requirements** dialog, verify that the installation has enough space on the target drive and click **Next** to continue.	
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.	
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

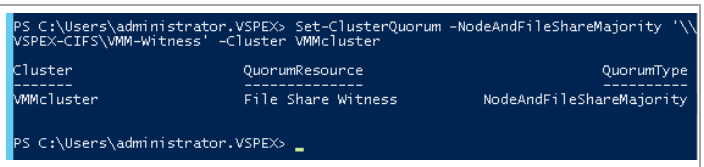
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.	
Once complete, the **Complete** dialog will appear. Click **Close** to complete the installation of SQL Server tools.	

Configure Failover Clustering with SMB 3.0 Shared Storage

If you have included the SMB 3.0 feature of the VNX5500 array, it is very convenient to use its capability to provide a highly available File Share Witness for the cluster. Otherwise, you can go through the previously defined process of creating a LUN on the VNX5500 array and presenting it via iSCSI and MPIO to the VMM cluster. The same process defined for creating the LUNs and presenting them to the SQL Server cluster would be followed, except only a single LUN would be created to work as the Disk Witness for the VMM cluster. Both work equally well; it is a lot quicker and easier to set up a file share witness if you have that option available.

Ensure that the network binding order is correct on both nodes. From Network Connections, press the **Alt** key to display the menu bar. Click **Advanced** and select **Advanced Settings…**	
It is most important for the VM access network to appear first in the list. The order of the other networks is not important. Use the arrows on the right to move the network order up and down. Click **OK** when the order is correct.	
From a PowerShell window, issue the following command: `Test-Cluster -Node VMM01,VMM02` Since no storage is available yet, you will see a series of storage related warnings. The last line of warnings provides the name of the validation report file. You should display that report in Internet Explorer to ensure that only storage related warnings exist. If errors exist, they must be corrected. Other warnings must be reviewed to ensure they are acceptable or fixable.	
Create the cluster with no storage with the following PowerShell command: `New-Cluster -Name VMMcluster -Node VMM01,VMM02 -NoStorage -StaticAddress 10.29.130.40`	

Previously illustrated methods for renaming the cluster's network adapters to reflect actual usage instead of generic names can be used to rename the clusters, or the commands at right can be used. **Note:** Values should be changed to reflect customer naming and IP addressing.	(Get-ClusterNetwork -Cluster VMMCluster | ? {$_.Address -like "10.29.130.*" }).Name = "VMaccess" (Get-ClusterNetwork -Cluster VMMCluster \| ? {$_.Address -like "192.168.16.*" }).Name = "SMB-A" (Get-ClusterNetwork -Cluster VMMCluster | ? {$_.Address -like "192.168.17.*" }).Name = "SMB-B" (Get-ClusterNetwork -Cluster VMMCluster \| ? {$_.Address -like "192.168.13.*" }).Name = "ClusComm" (Get-ClusterNetwork -Cluster VMMCluster -Name VMaccess).Role = 3 (Get-ClusterNetwork -Cluster VMMCluster -Name SMBnet1).Role = 0 (Get-ClusterNetwork -Cluster VMMCluster -Name SMBnet2).Role = 0 (Get-ClusterNetwork -Cluster VMMCluster -Name ClusComm).Role = 1
In Unisphere, navigate to **Storage > Shared Folders > CIFS**. Click **Create** to create a files share to be used as the witness for the cluster.	
Enter a name for the share in the **CIFS Share Name** field. Check the box by the **CIFS Servers** to select the defined CIFS server that will be used. Click **OK** to continue.	

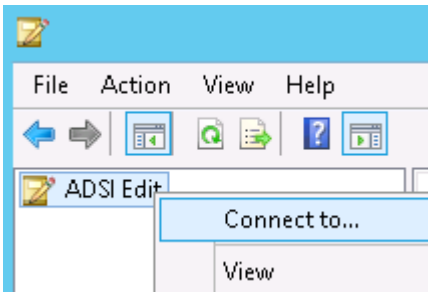
Issue the following PowerShell command to add the created file share as the witness disk to the VMM cluster. `Set-ClusterQuorum -NodeAndFileShareMajority '\\VSPEX-CIFS\VMM-Witness' -Cluster VMMcluster` Alternatively, you can add it through the Failover Cluster Manager console.	

Create the Virtual Machine Manager Distributed Key Management Container in Active Directory Domain Services

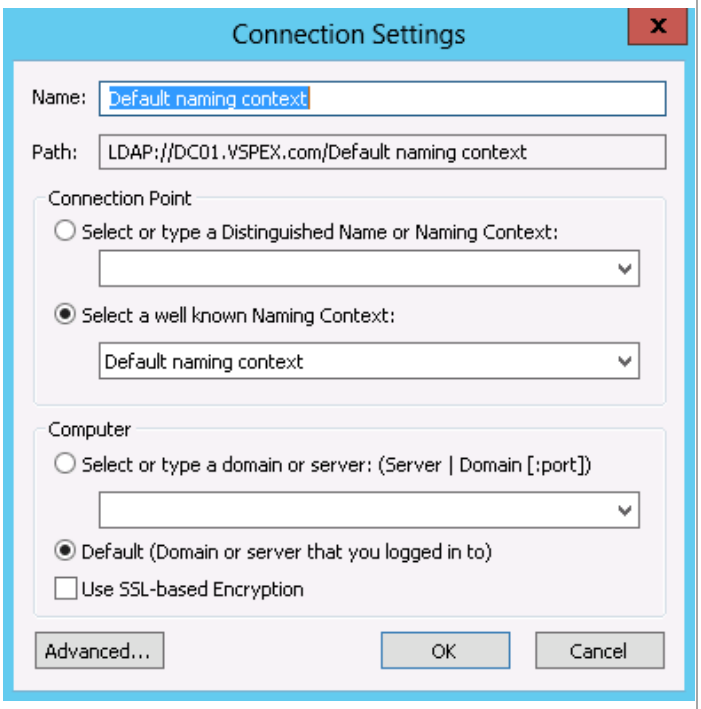
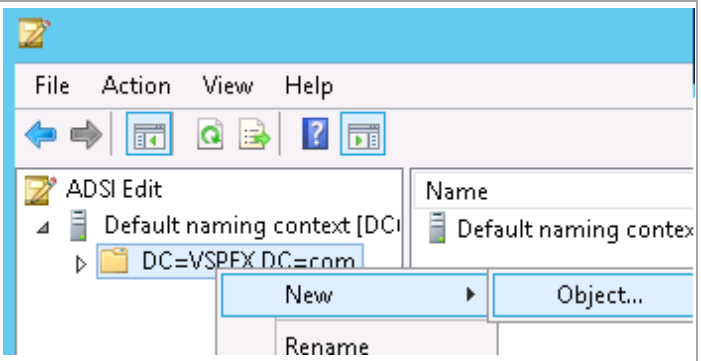
The Virtual Machine Manager installation requires that an Active Directory container be created to house the distributed key information for Virtual Machine Manager[9].

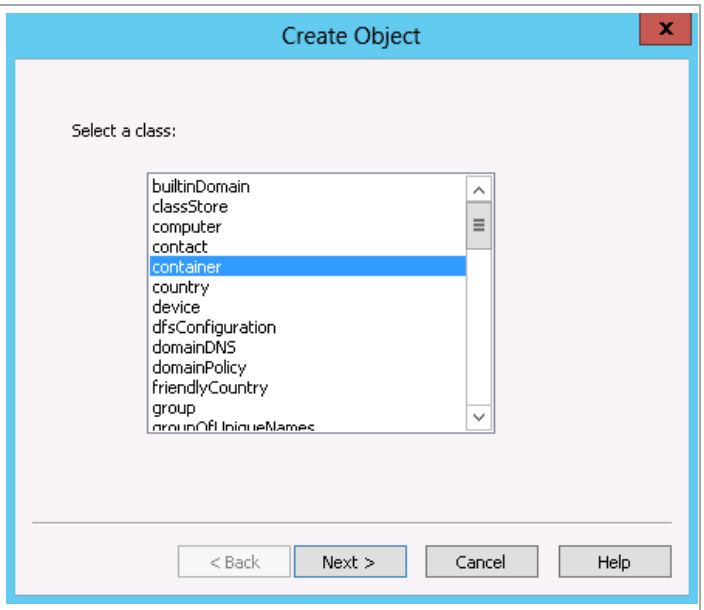
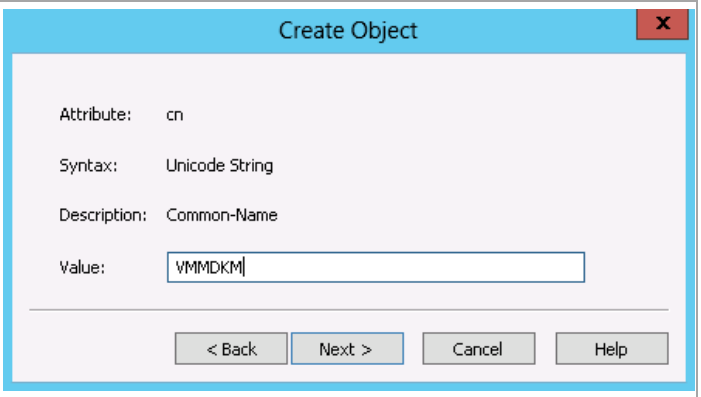
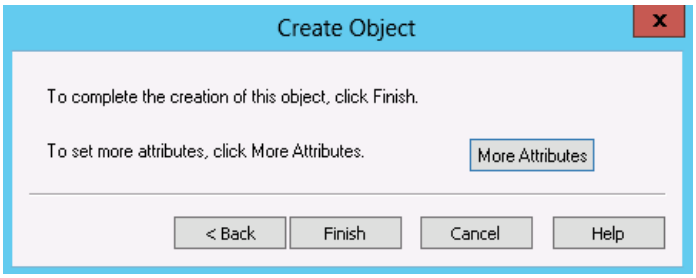
Note: If Virtual Machine Manager will be deployed using an account with rights to create containers in AD DS this step can be skipped.

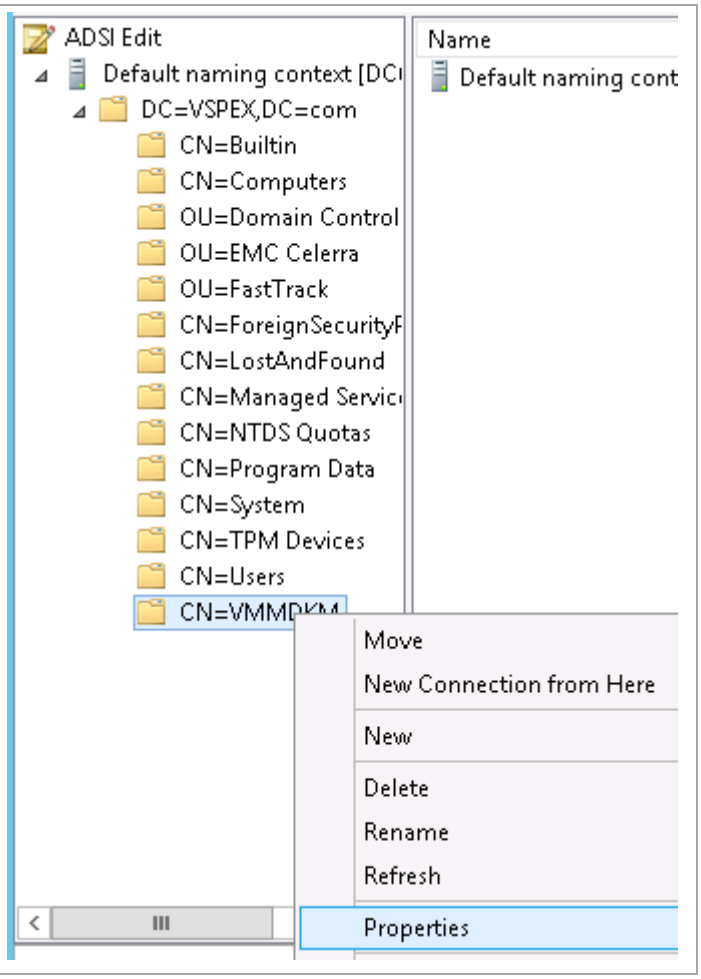
Perform the following steps to create an AD DS container to house the distributed key information. These instructions assume a Windows Server 2008 R2 domain controller is in use, similar steps would be followed for other versions of Active Directory including Windows Server 2008 and Windows Server 2012.

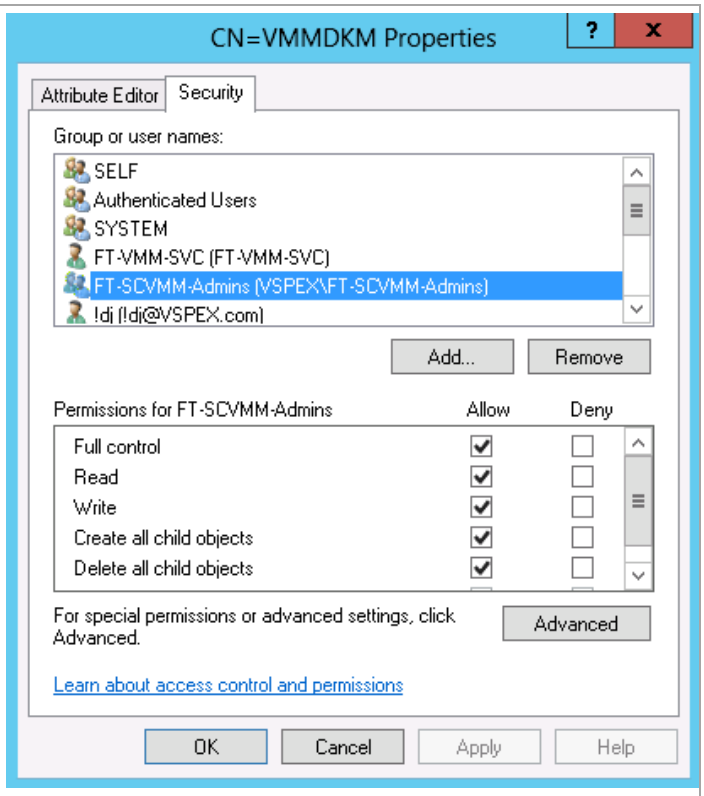
▶ Perform the following steps on a **Domain Controller** in the domain where Virtual Machine Manager is to be installed.	
Log in to a Domain Controller with a user that has Domain Admin privileges and run **adsiedit.msc.**	
Right-click the **ADSI Edit** node and select **Connect to…** from the context menu.	

[9] Configuring Distributed Key Management in VMM - http://technet.microsoft.com/library/gg697604.aspx.

In the **Connections Settings** dialog, in the **Connection Point** section, click the radio button by the **Select a well known Naming Context**. Select **Default naming context** from the drop-down menu and click **OK**.	
Expand **Default naming context [<computer fully qualified domain name>]**, expand **<distinguished name of domain>**, right-click the root node and select **New – Object...** from the context menu.	

In the **Create Object** dialog box, select **Container** and then click **Next.**	
In the **Value** text box, type *<VMMDKM>* and then click **Next**.	
Click **Finish** to create the container object.	

Within ADSI Edit, right-click the new **VMMDKM** object and then click **Properties.**	

In the **VMMDKM Properties** dialog box, click the **Security** tab. Click **Add** to add the **VMM Service account** and **VMM Admins group**. Grant the security principles **Full Control** permissions. Click **OK** three times and close ADSI Edit.	

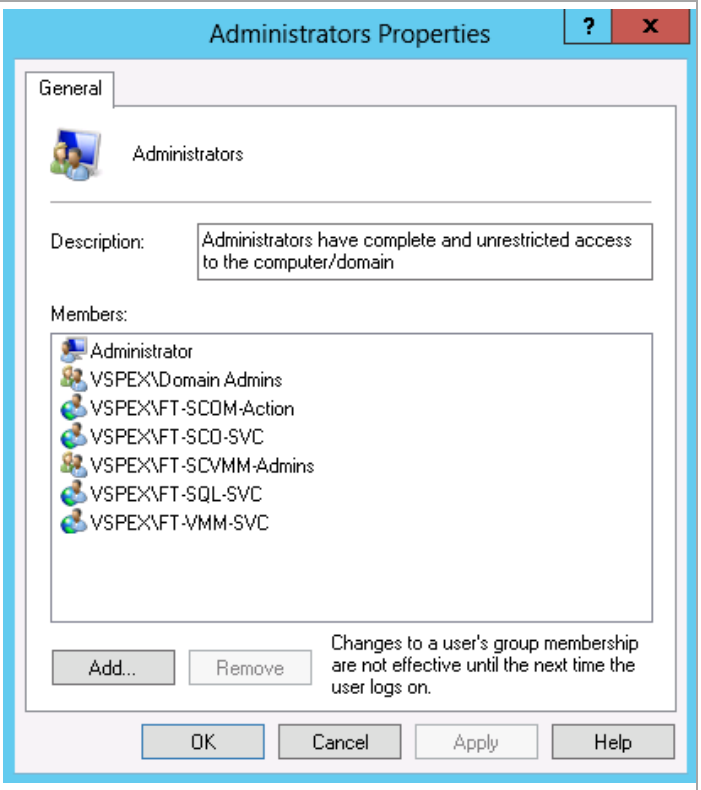
9.3 Installation – SCVMM Management Server

Install the Virtual Machine Manager Failover Cluster

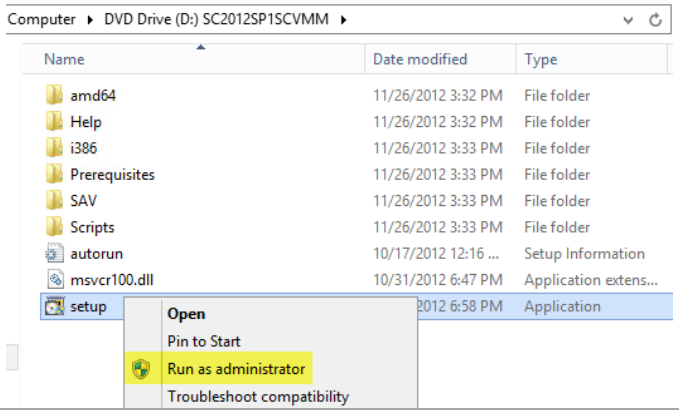
▶ Perform the following steps on the **first Virtual Machine Manager** virtual machine.

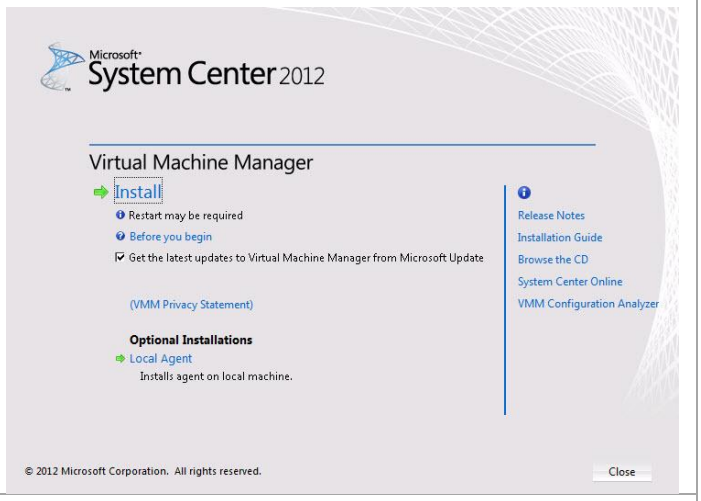
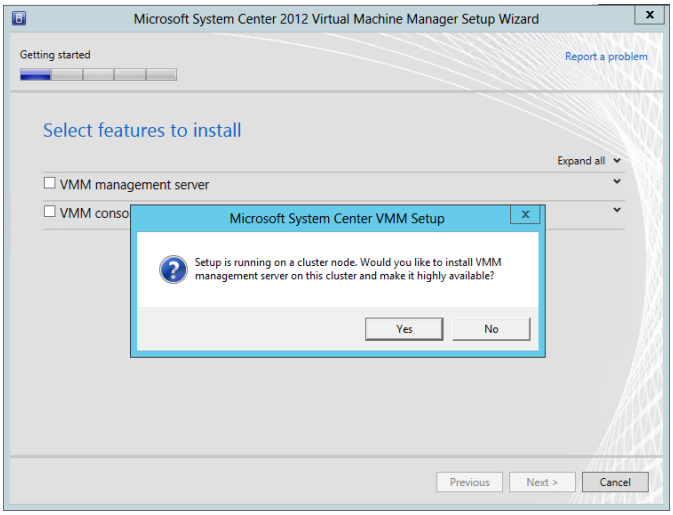
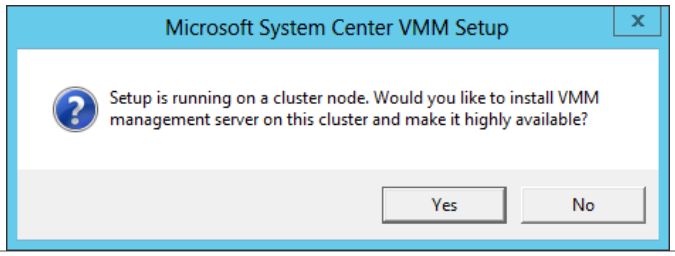
Log on to the Virtual Machine Manager virtual machine with a user with local admin rights.
Verify the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager virtual machine:

- Orchestrator service account.
- Operations Manager action account.
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.
- SQL Server service account.

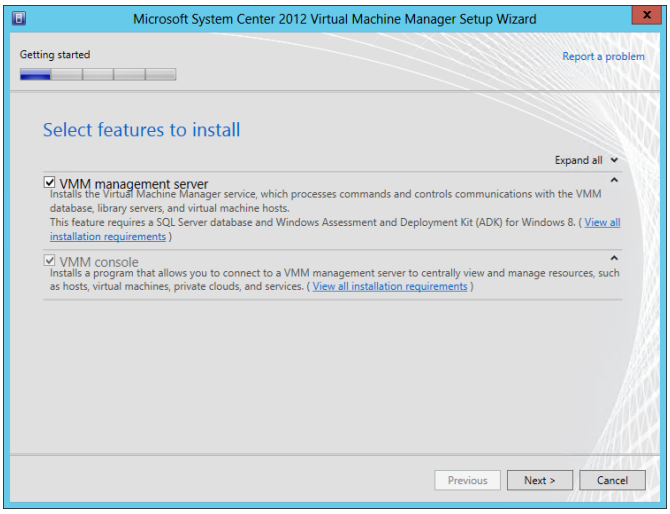


From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.	
Attempting to select any feature will cause the cluster management server notice to appear. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard.	 

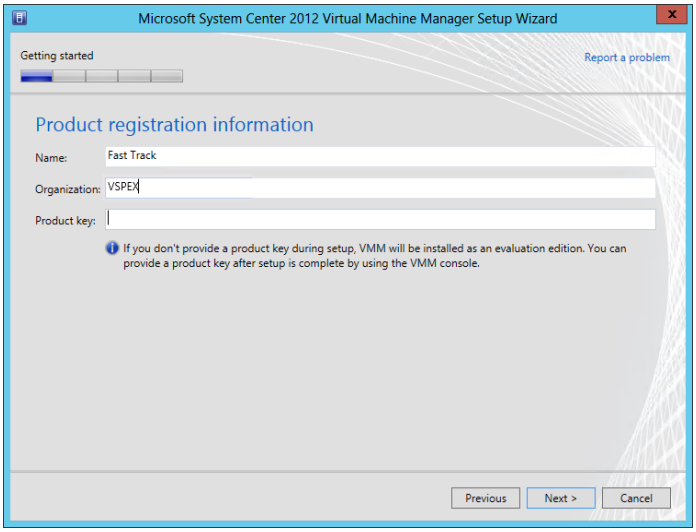
In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **VMM console** installation option check box will be selected by default.
Click **Next** to continue.



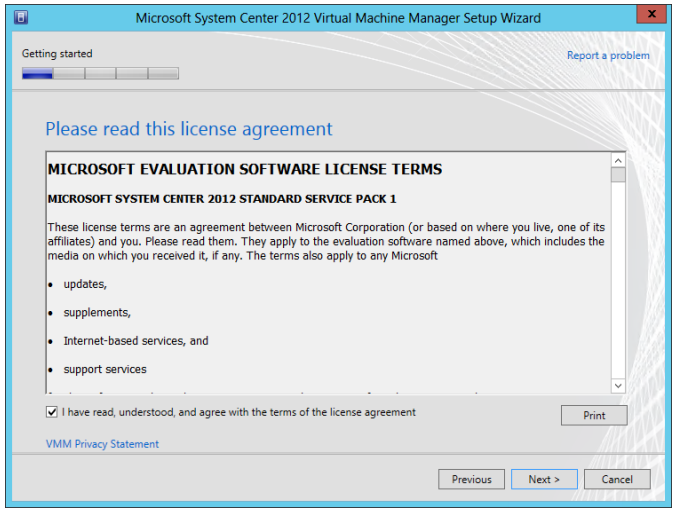
In the **Product registration information** dialog, enter the following information in the provided text boxes:

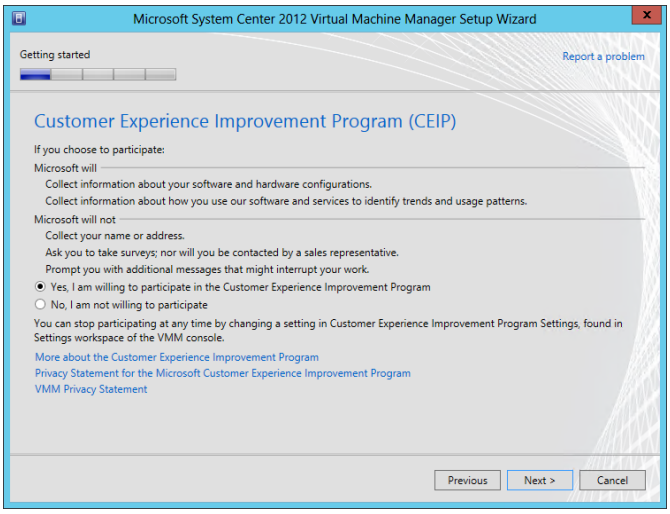
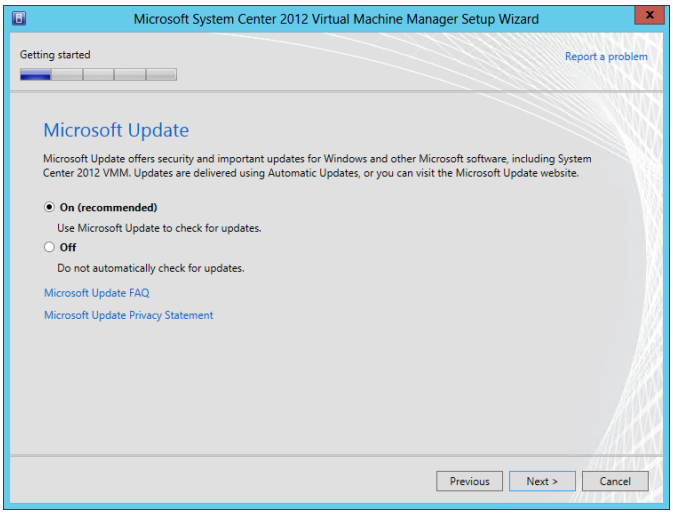
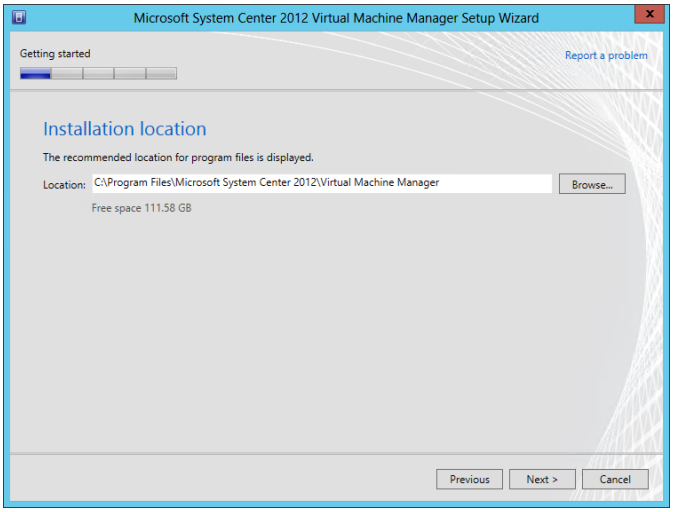
- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** - *specify the name of the licensed organization*.
- **Product key** – *provide a valid product key for installation of Virtual Machine Manager. If no key is provided, Virtual Machine Manager will be installed in evaluation mode*.

Click **Next** to continue.



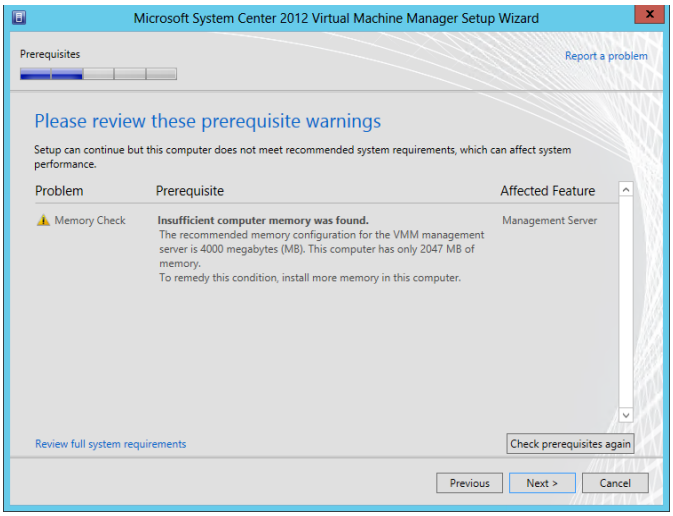
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement installation** option check box is selected and click **Next** to continue.



In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.	

Note: The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy.

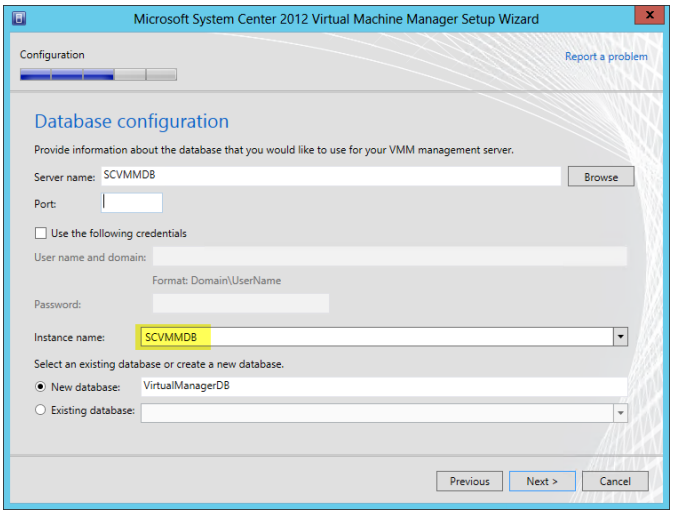
The following is just an example of that UI.
If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



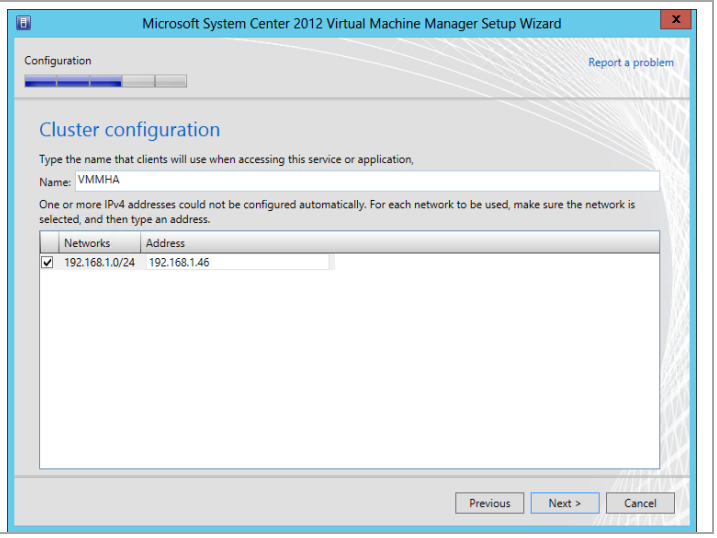
In the **Database configuration** dialog, enter the following information in the provided text boxes:

- **Server name** – *specify the name of the SQL Server cluster created in the steps above.*
- **Port** - *specify the TCP port used for the SQL Server, as configured in the steps above.*

Verify that the **Use the following credentials** check box is clear. In the **Instance name** drop-down menu, select the Virtual Machine Manager database instance deployed earlier in the SQL Server cluster.
In the **Select an existing database or create a new database** option, select the **New database** option and accept the default database name of *VirtualManagerDB*.
Click **Next** to continue.



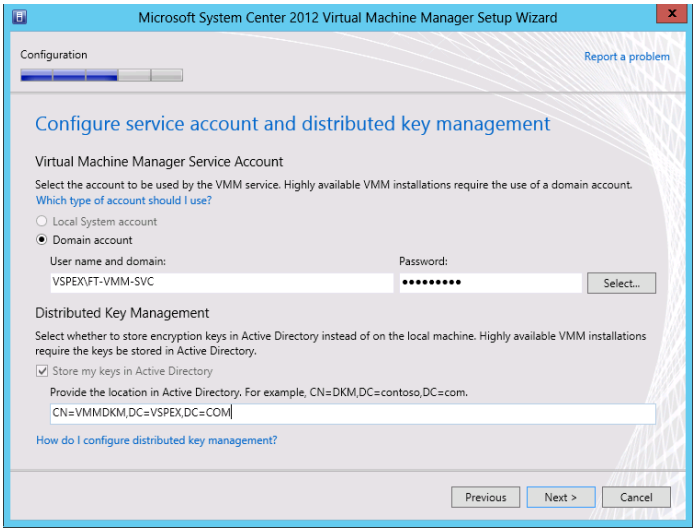
In the **Cluster Configuration** dialog, in the **Name** field, provide a name for the Virtual Machine Manager cluster service.
If the cluster node you are installing is configured with static IP addresses you will also need to provide an IP address for the Virtual Machine Manager cluster service. If the cluster node is configured to use DHCP, no additional information is required.



In the **Configure service account and distributed key management** dialog, in the **Virtual Machine Manager Service account** section, select the **Domain account** option. Enter the following information in the provided text boxes:

- **User name and domain** – *specify the Virtual Machine Manager service account identified in the section above in the following format: <DOMAIN>\<USERNAME>.*
- **Password** – *specify the password for the Virtual Machine Manager service account identified above.*

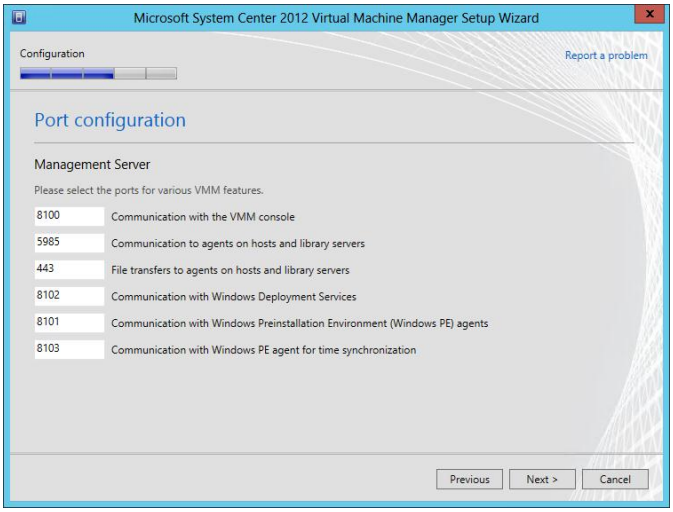
In the **Distributed Key Management** section, select the **Store my keys in Active Directory** check box. In the provided text box, type the distinguished name (DN) location created earlier within Active Directory: *cn=VMMDKM,DC=domain,…*
Click **Next** to continue.

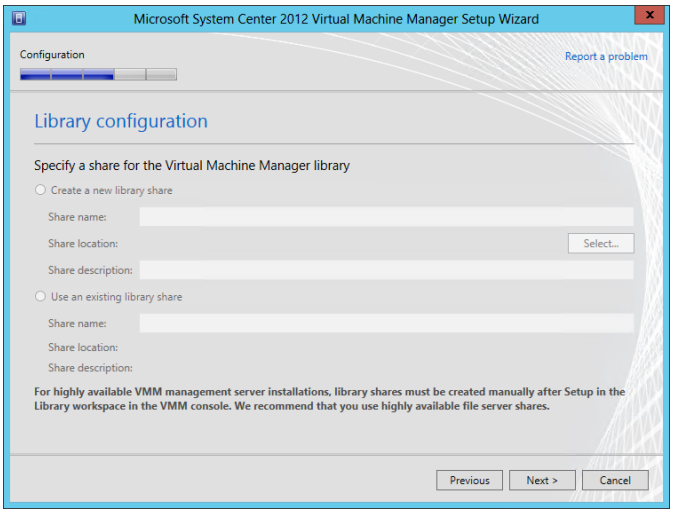
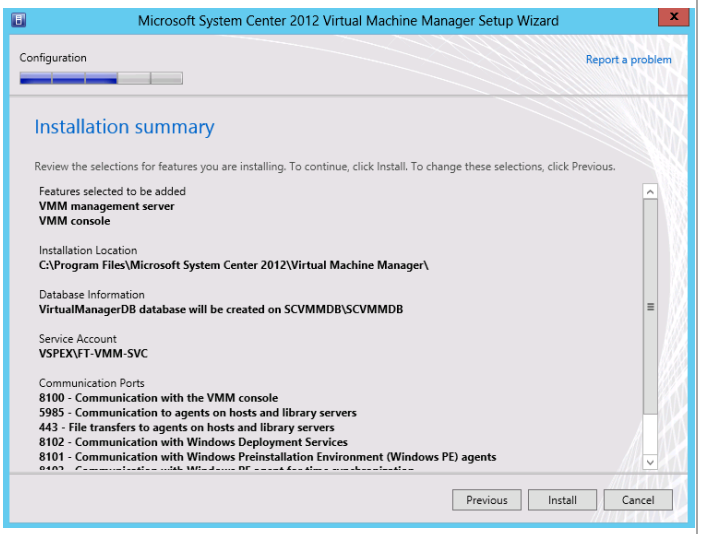
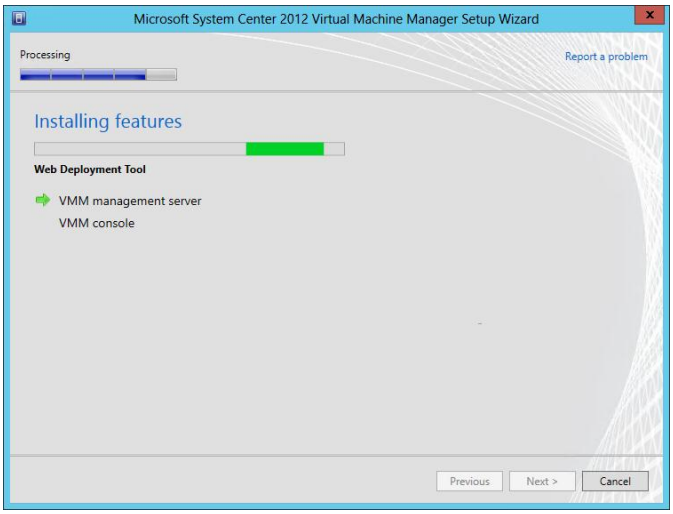


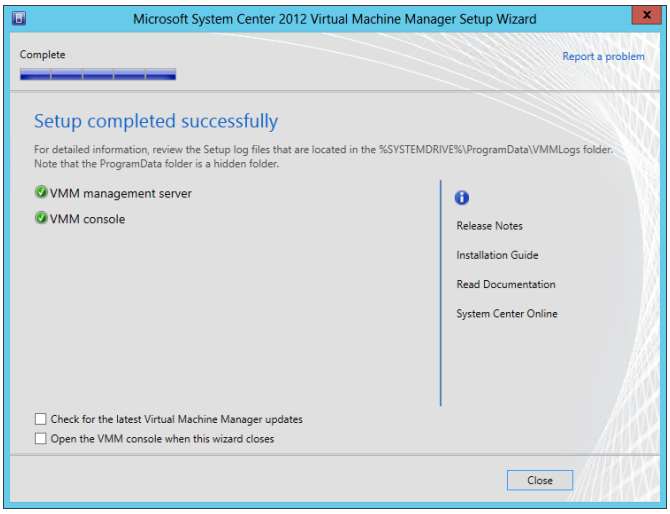
In the **Port configuration** dialog, accept the default values in the provided text boxes:

- **Communication with the VMM console** – *default: 8100.*
- **Communication to agents on hosts and library servers** – *default: 5985.*
- **File transfers to agents on hosts and library servers** – *default: 443.*
- **Communication with Windows Deployment Services** – *default: 8102.*
- **Communication with Windows Preinstallation Environment (Windows PE) agents** – *default: 8101.*
- **Communication with Windows PE agent for time synchronization** – *default: 8103.*

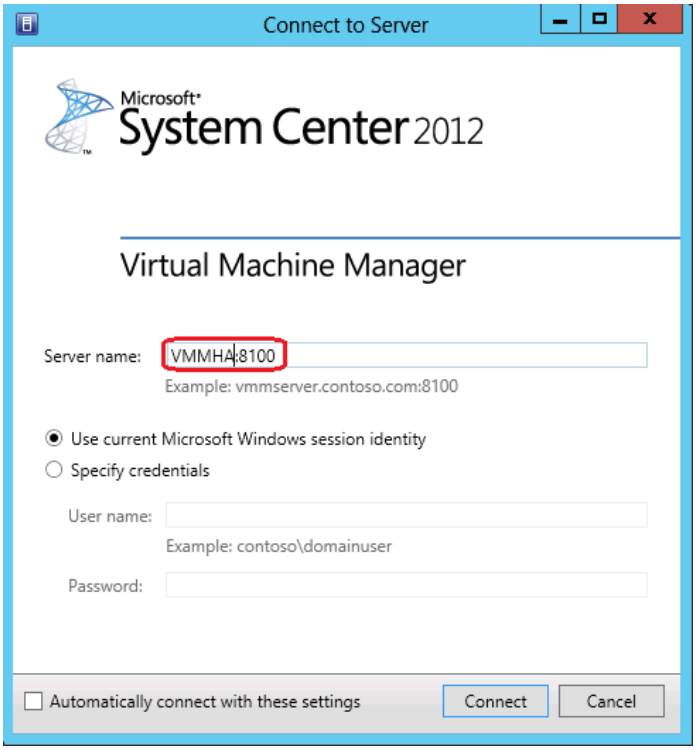
Click **Next** to continue.

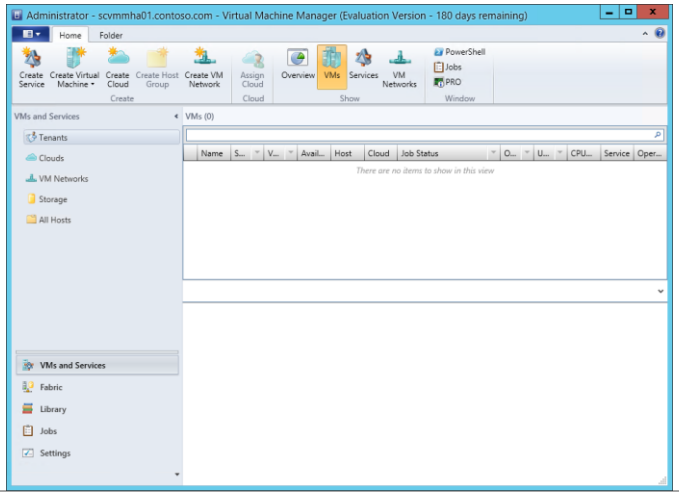


In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
The wizard will display the progress while installing features.	

Once the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

Once complete, launch the **Virtual Machine Manager** console to verify the installation occurred properly. Set the Server name value to match the name that was provided for the Cluster Resource name during setup (for example, VMMHA: 8100).
Verify that the console launches and connects to the Virtual Machine Manager instance installed.

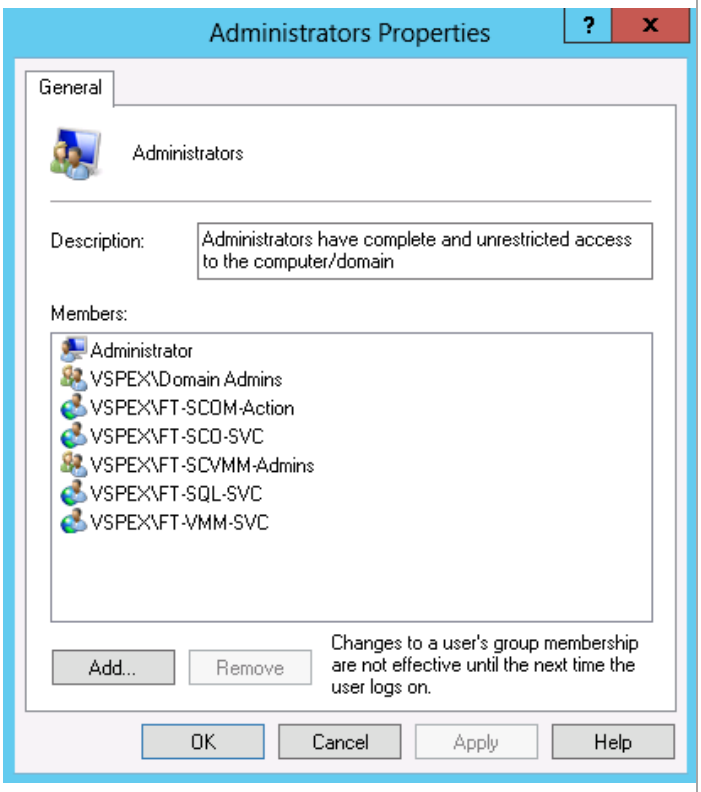




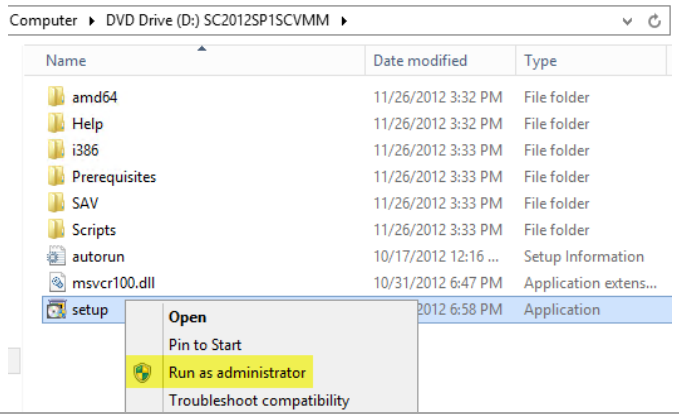
▶ Perform the following steps on the **second Virtual Machine Manager** virtual machine.

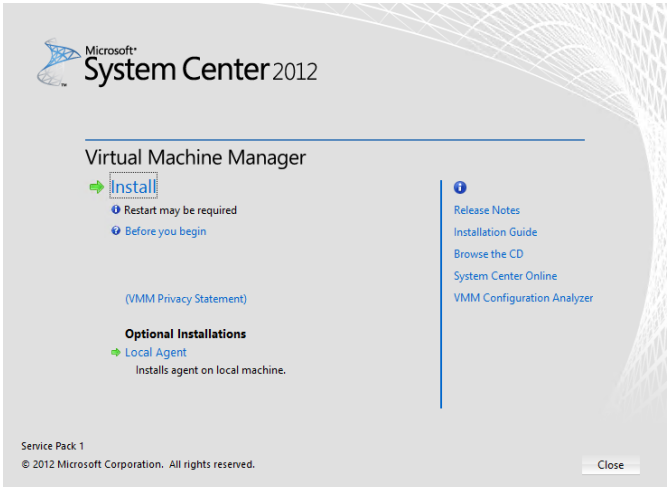
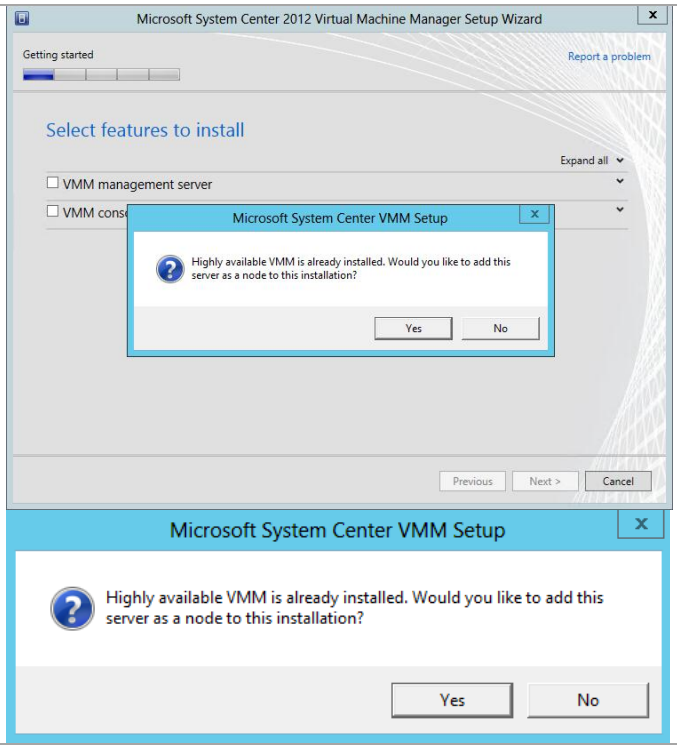
Log on to the **second** Virtual Machine Manager virtual machine with a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager Virtual Machine:

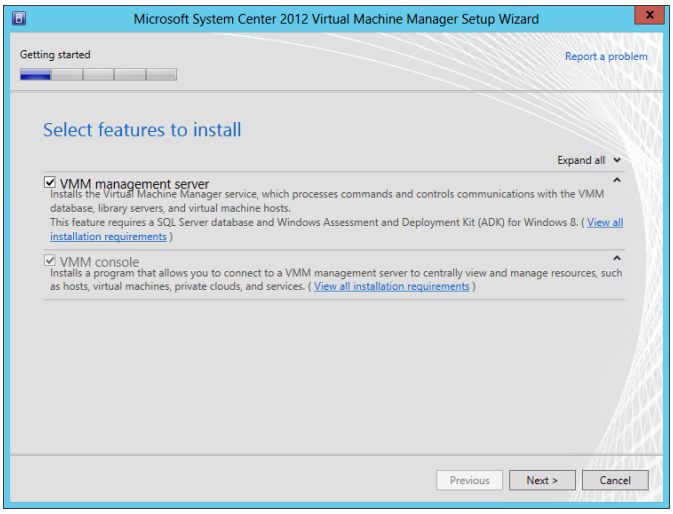
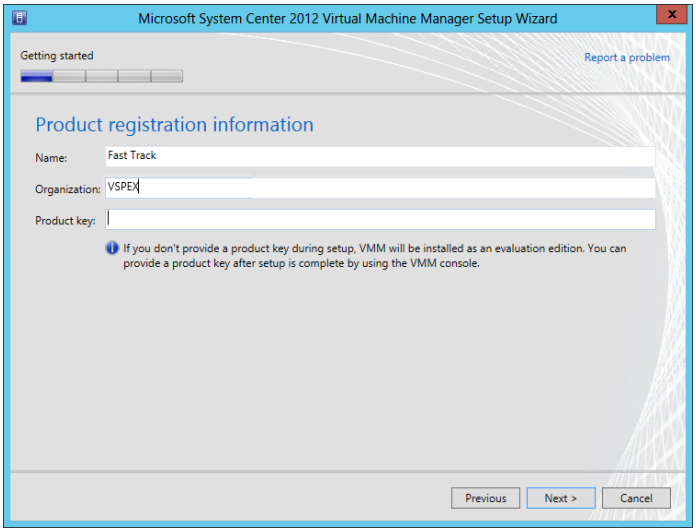
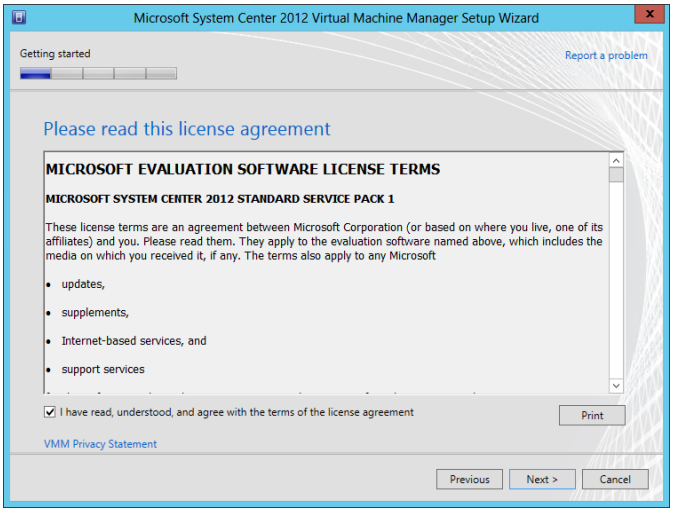
- Orchestrator service account.
- Operations Manager action account.
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.
- SQL Server service account.

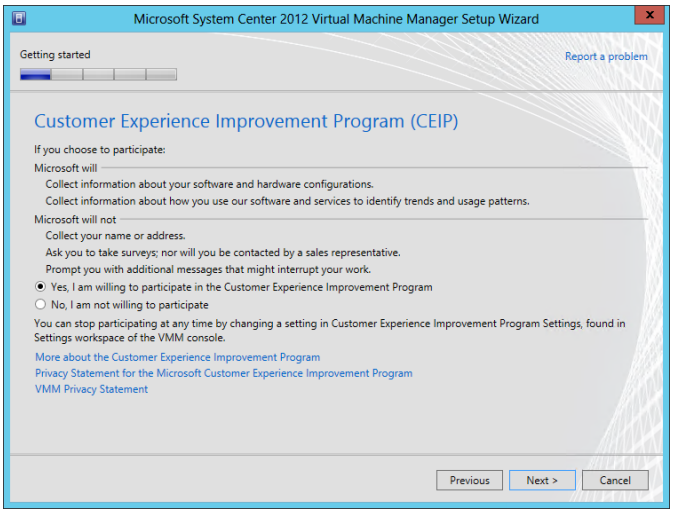
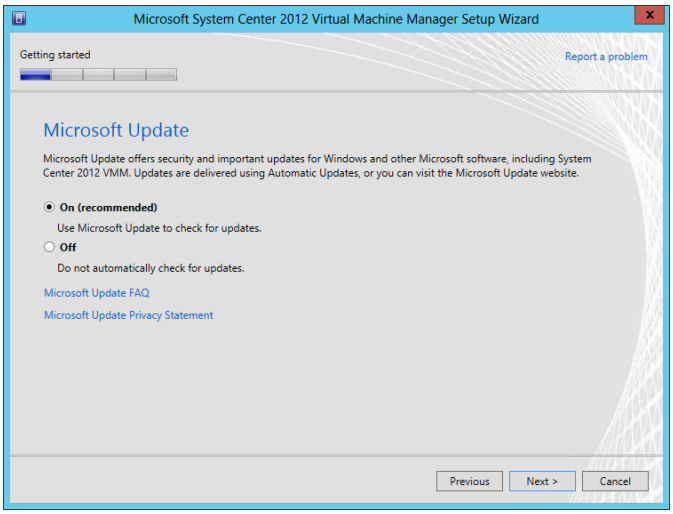
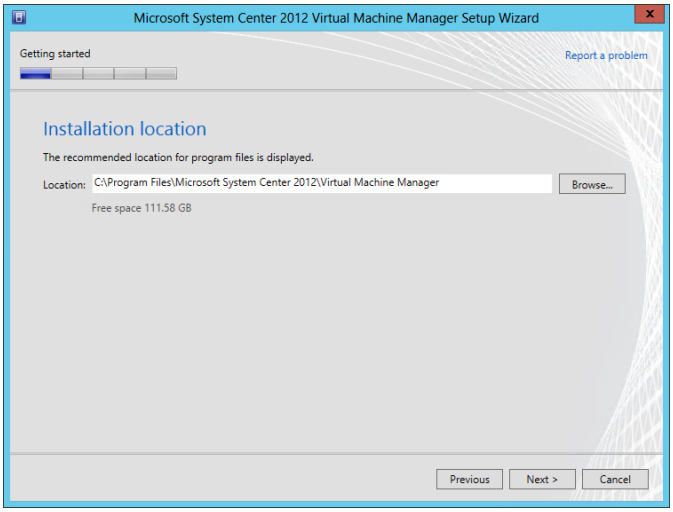


From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



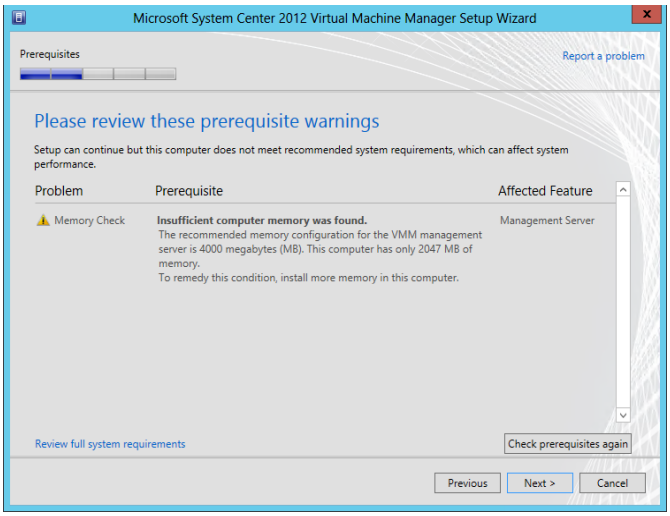
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.	
Attempting to select any feature will cause the cluster management server notice to appear. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard and add the second node. **Note:** Virtual Machine Manager can be deployed on up to 16 cluster nodes but only a single node can be active at any time.	

In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **Virtual Machine Manager console** installation option check box will be selected by default. Click **Next** to continue.	
In the **Product registration information** dialog, enter the following information in the provided text boxes: • **Name** – *specify the name of the primary user or responsible party within your organization*. • **Organization** – *specify the name of the licensed organization*. • **Product key** – *provide a valid product key for installation of Virtual Machine Manager. If no key is provided, Virtual Machine Manager will be installed in evaluation mode*. Click **Next** to continue.	
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.	

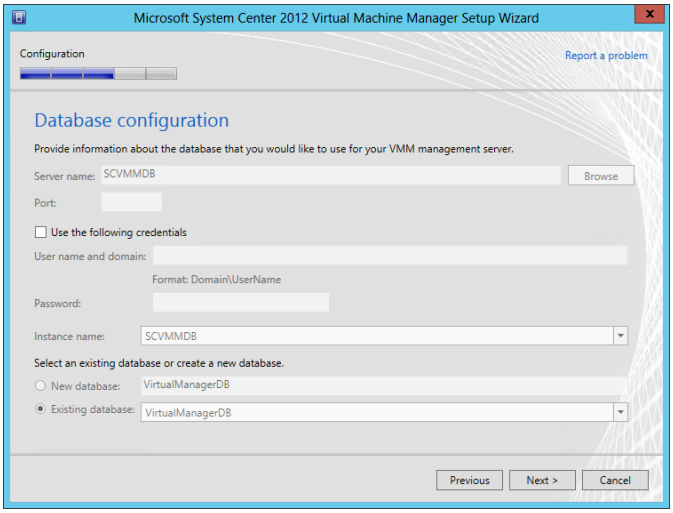
In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.	
In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.	

Note: The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy.

The following is just an example of that UI.
If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



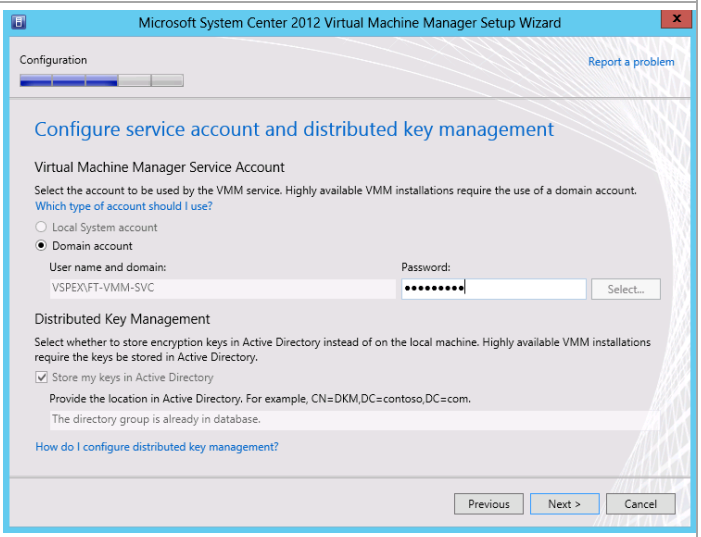
In the **Database configuration** dialog, all options are greyed out when adding an additional node to an existing Virtual Machine Manager cluster.
Click **Next** to continue.

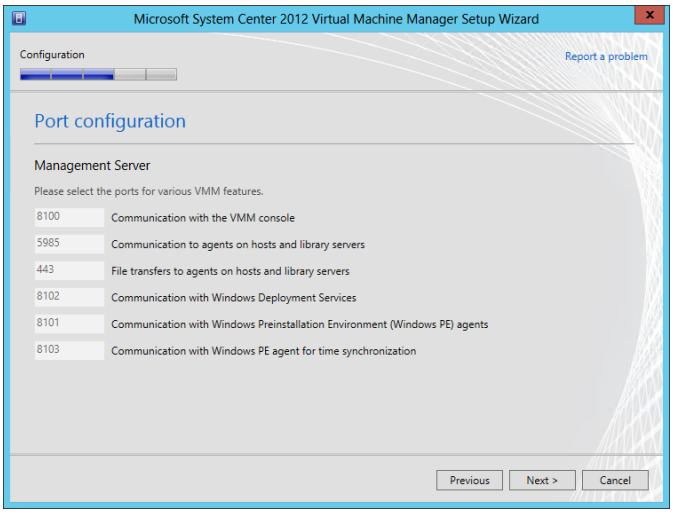
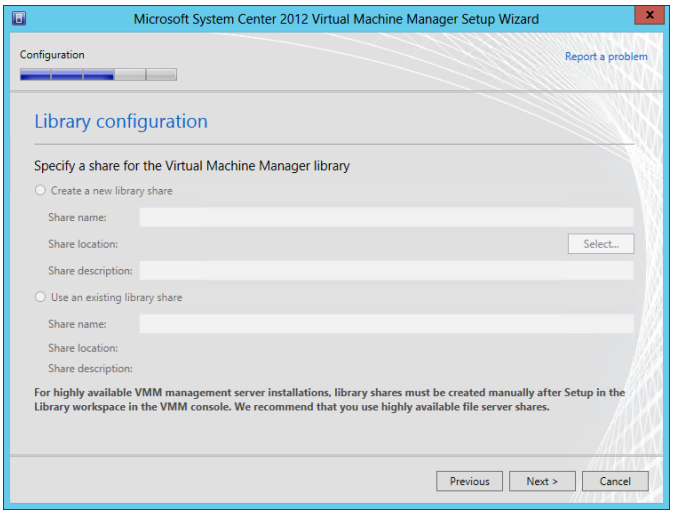
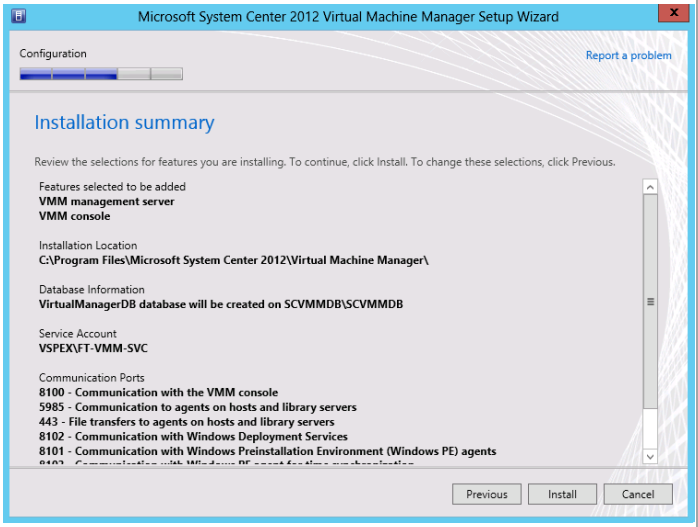


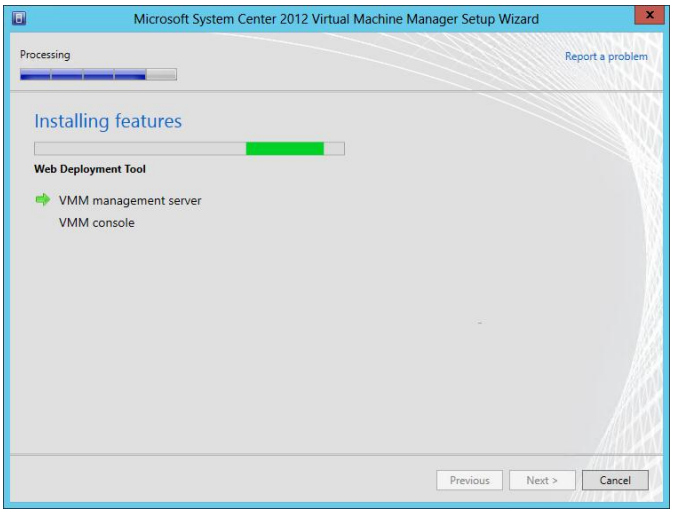
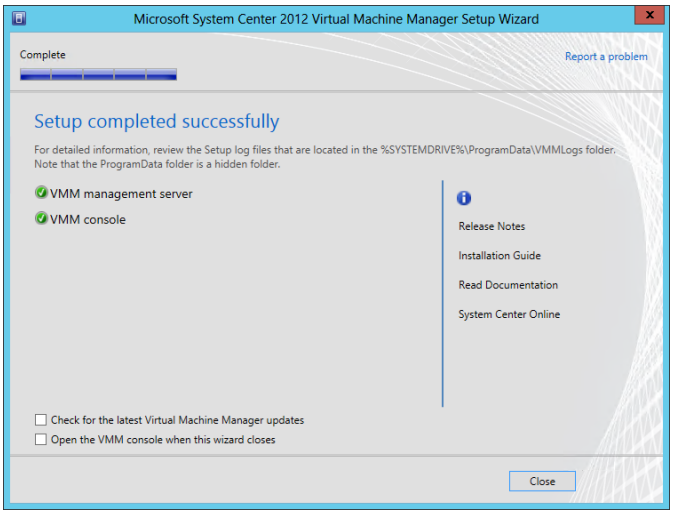
In the **Configure service account and distributed key management** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields other than **Password** are greyed out.

- **Password** – *specify the password for the Virtual Machine Manager service account identified above.*

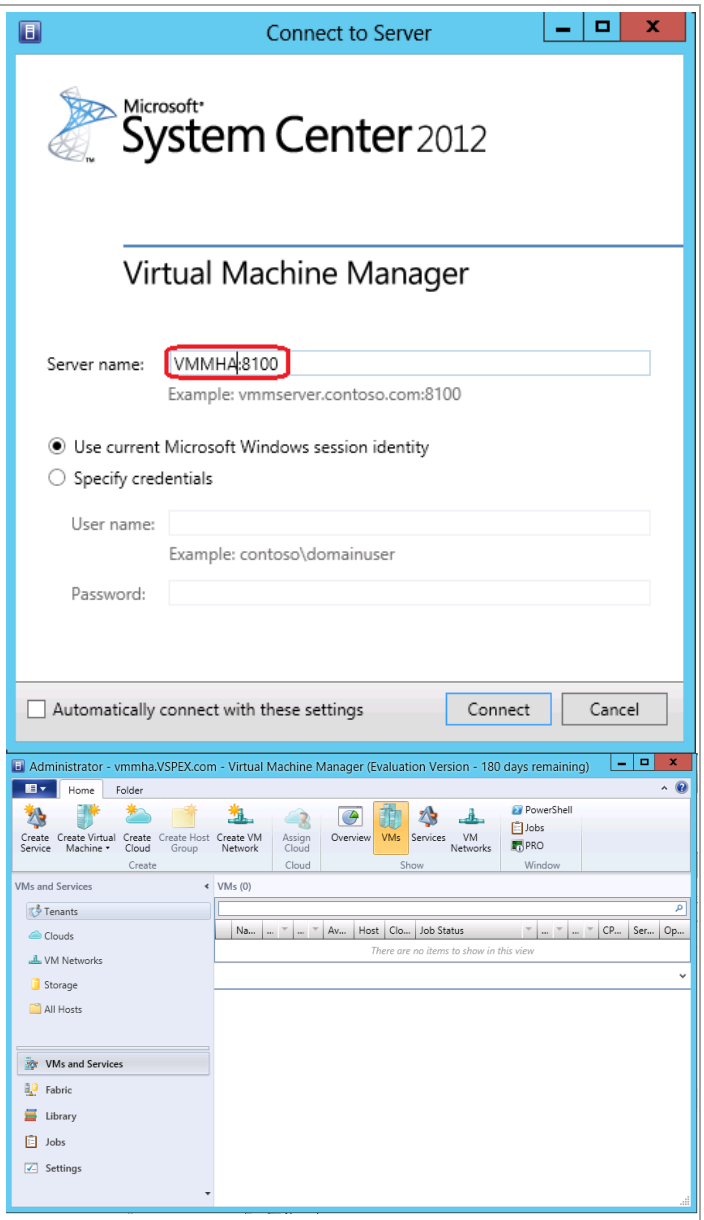
Click **Next** to continue.

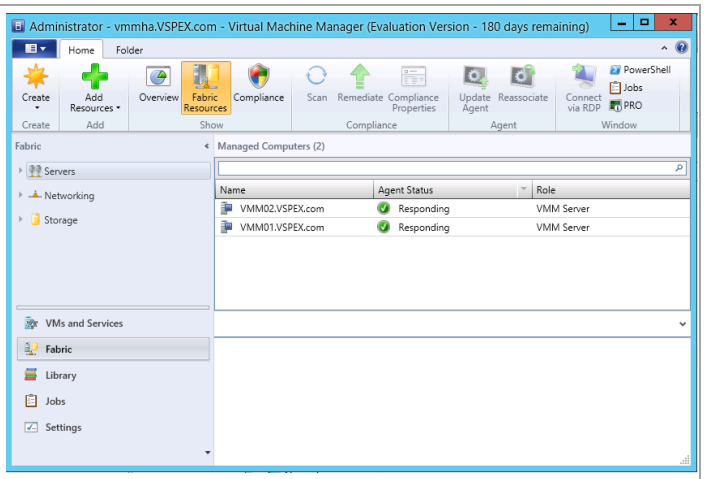


In the **Port configuration** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields are greyed out. Click **Next** to continue.	
In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

The wizard will display the progress while installing features.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

When complete, launch the Virtual Machine Manager console to verify the installation occurred properly. Set the **Server** Name value to match the name that was provided for the **Cluster Resource** name during setup (for example, HAVMM: 8100). Verify that the console launches and connects to the Virtual Machine Manager instance installed.

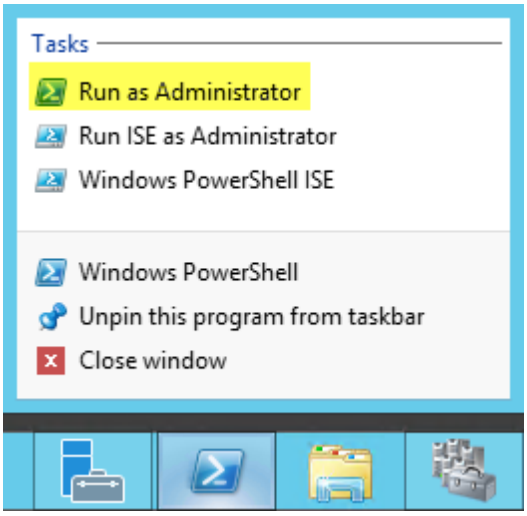
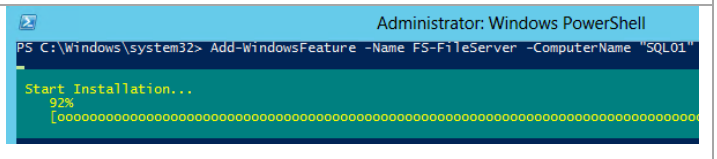


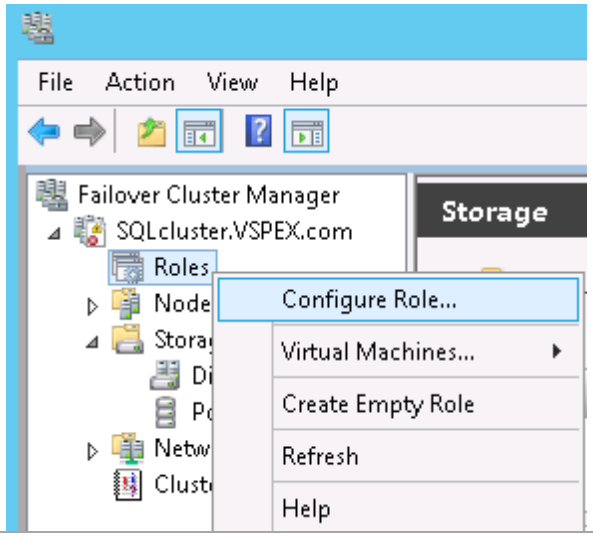
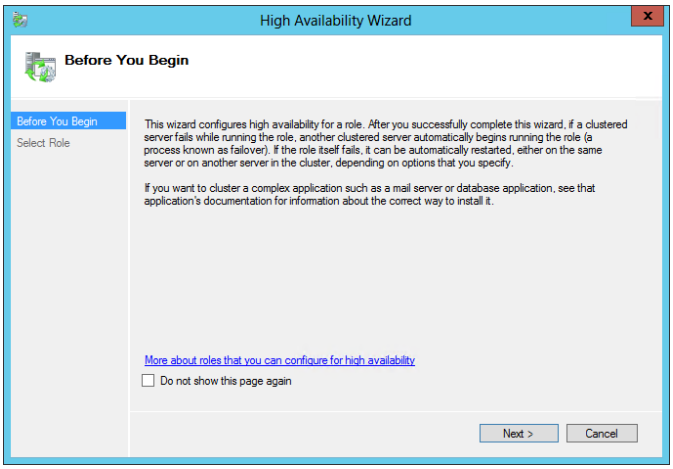
In the **Virtual Machine Manager** console, expand **Servers** and select VMM Server. Verify that both cluster nodes are listed as *VMM Servers* under Role and that both nodes are listed as *Responding* under Agent Status.	

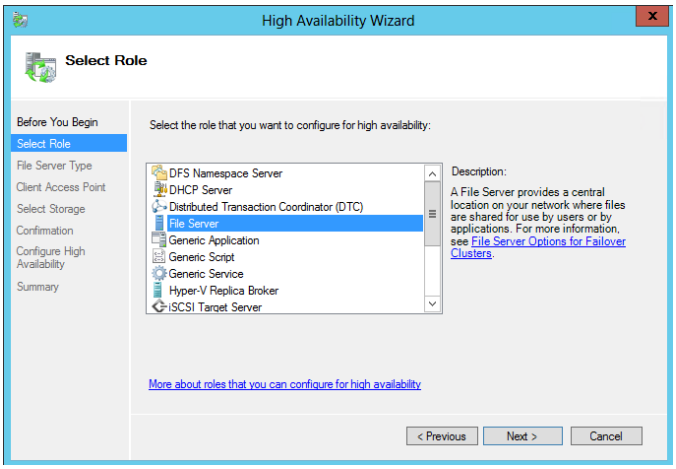
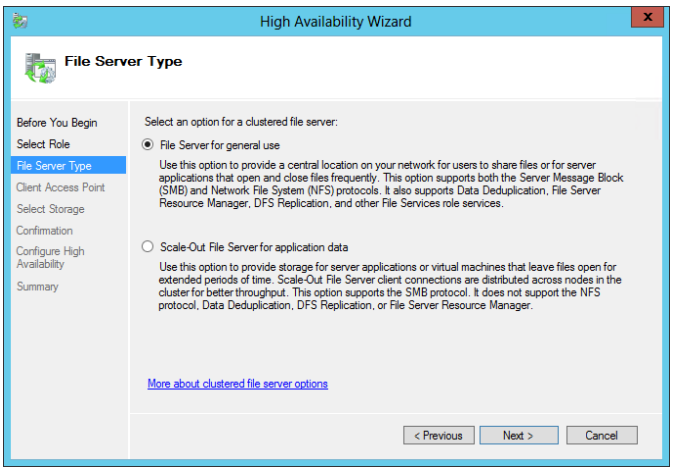
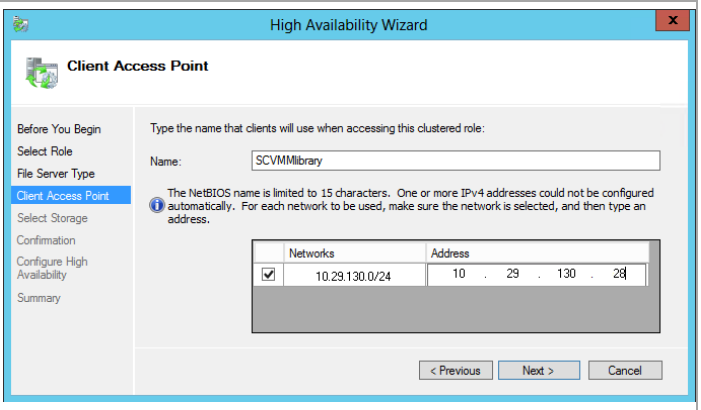
9.4 Creating Virtual Machine Manager Library Share on the VNX5500

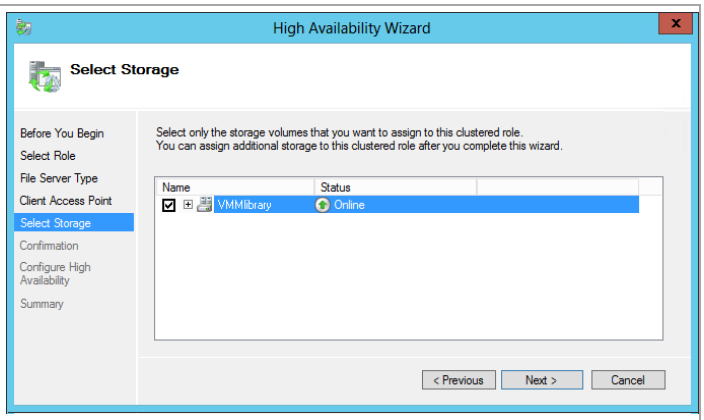
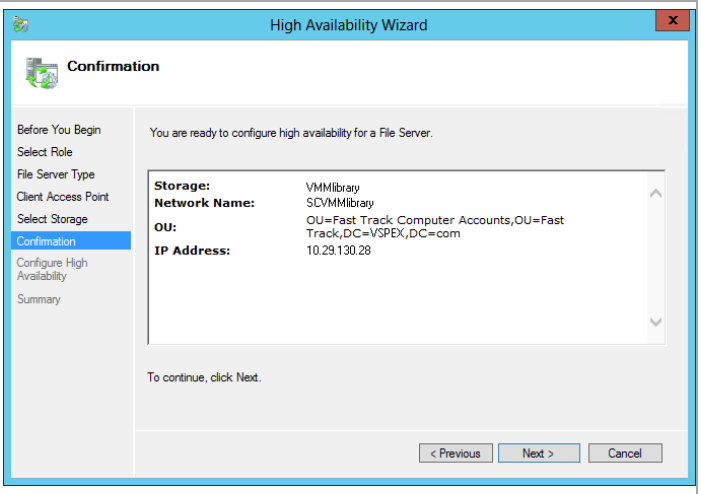
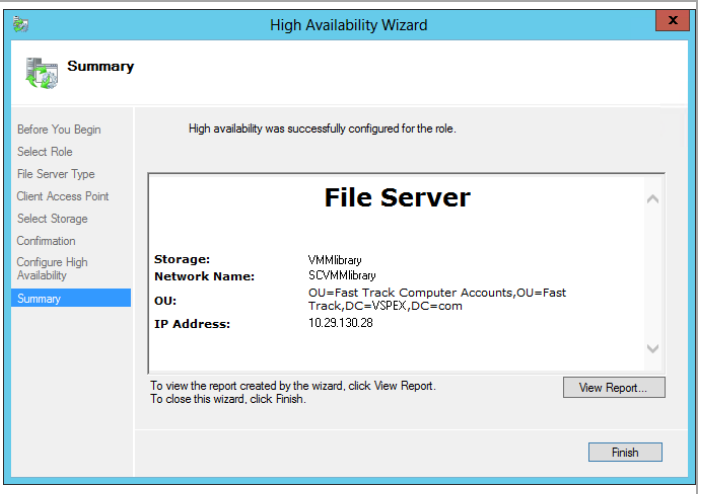
In a highly available installation of Virtual Machine Manager, the Virtual Machine Manager Library must reside on a Windows Server outside of the Virtual Machine Manager Cluster infrastructure; it is not a supported configuration to reside upon the Virtual Machine Manager cluster or its nodes. In addition, making the Virtual Machine Manager Library highly available is a recommended practice given that the Virtual Machine Manager servers themselves are highly available. The Private Cloud Fast Track physical architecture makes no recommendations on where the Virtual Machine Manager Library resides, other than that it should be as highly available as other aspects of the installation. While any Windows Server file server cluster will suffice, this document will detail the steps required to host the Virtual Machine Manager Library upon the SQL Server Cluster created in earlier portions of this document.

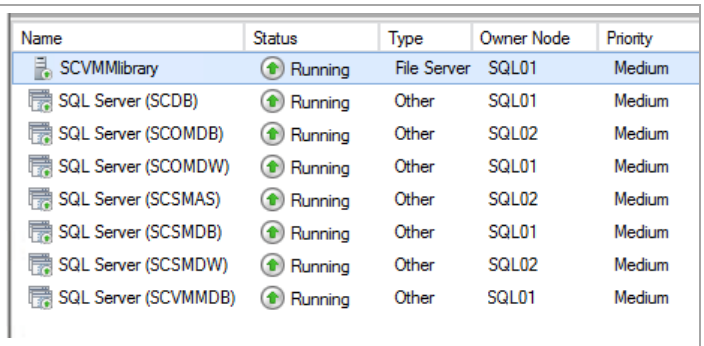
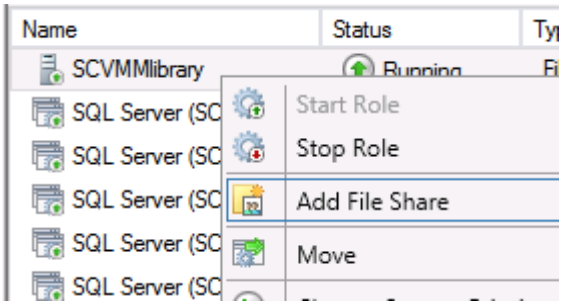
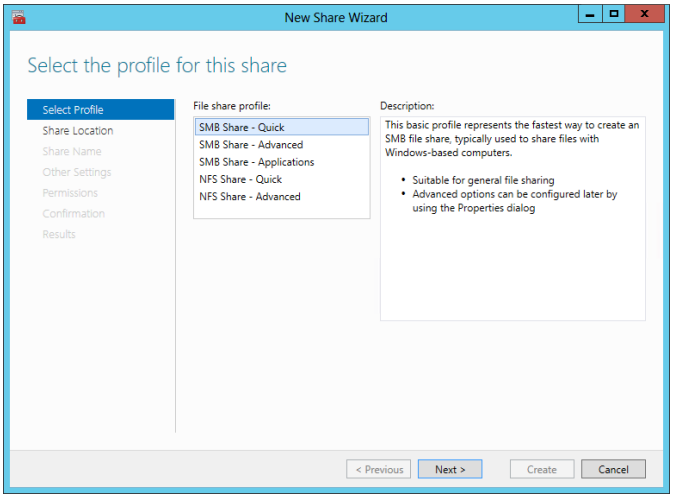
▶ Perform the following steps on each **SQL Server** virtual machine.

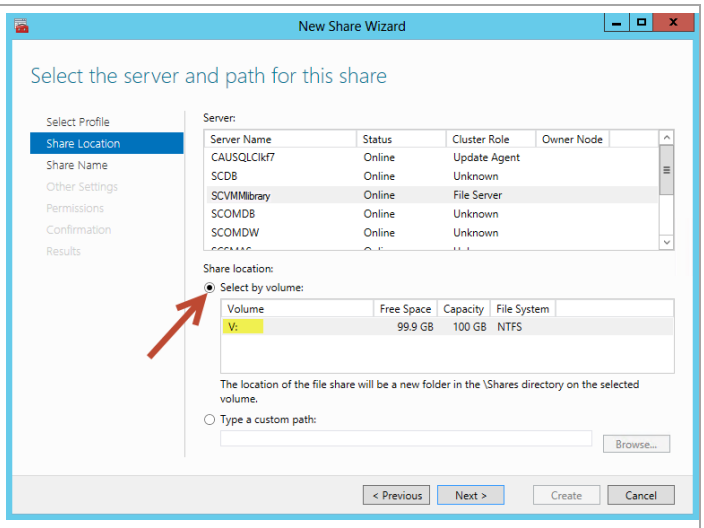
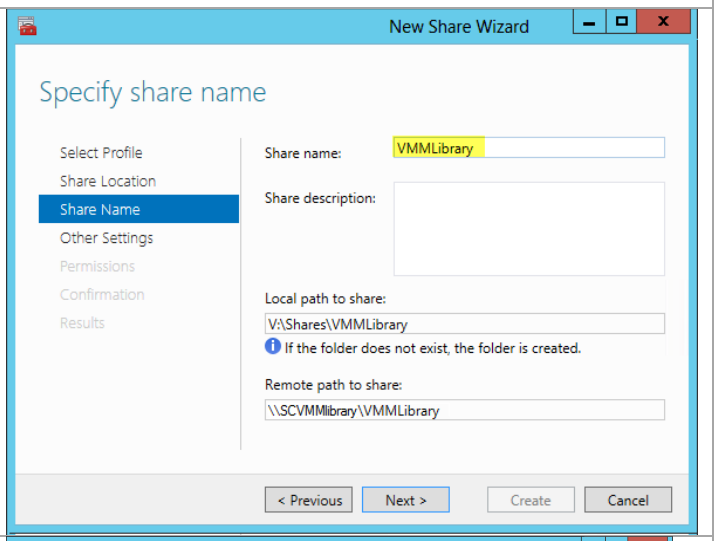
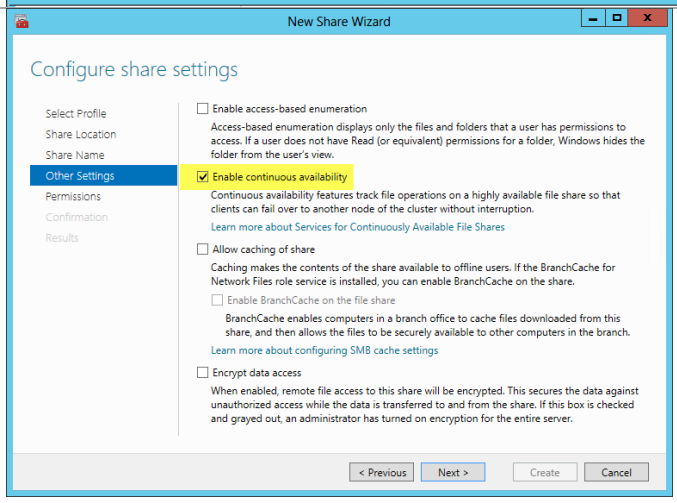
Open a PowerShell session as an administrator.	
From the administrator PowerShell session run the following command once for each SQL cluster node changing the ComputerName value each time to that of a different SQL cluster node. `Add-WindowsFeature -Name FS-`	

`FileServer -ComputerName "SQL01"`	
Add an additional iSCSI or Fibre Channel LUN and prepare it as described in previous steps. This should appear as available storage in the **Failover Cluster Manager Storage** node.	
▶ Perform the following steps on the **first SQL Server** cluster node.	
Within **Failover Cluster Manager**, right-click on **Roles** and select **Configure Role…** from the context menu.	
The **High Availability Wizard** will appear. In the **Before You Begin** dialog click **Next** to begin the wizard.	

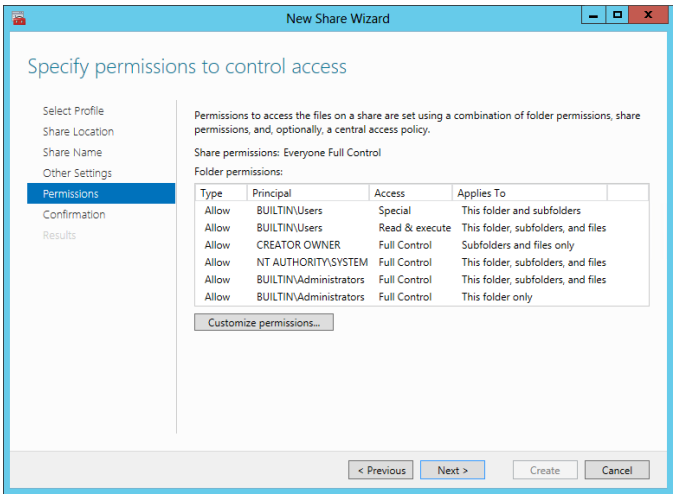
In the **Select Role** dialog, from the available services and applications, select **File Server** and click **Next** to continue.	
In the **File Server Type** dialog, select the **File Server for general use** radio button and click **Next** to continue.	
In the **Client Access Point** dialog, specify a unique name for the clustered file server in the **Name** text box. Additionally, for static IP configurations, select the appropriate network and assign a unique IP address to the service. Click **Next** to continue.	

In the **Select Storage** dialog, from the available storage, select the Cluster Disk that will be used for the Virtual Machine Manager Library and click **Next** to continue.	
In the **Confirmation** dialog, verify the options selected and click **Next** to continue.	
When complete, the **Summary** dialog will show a report of the actions taken by the wizard. Verify success and click **Finish** to complete the wizard.	

The new highly available file server is available as a new service in Failover Cluster Manager.	
Within **Failover Cluster Manager**, right-click the newly created file server service and select **Add File Share** from the context menu.	
The **New Share Wizard** will appear. In the **Select Profile** dialog, select **SMB Share – Quick** and click **Next** to continue.	

In the **Shared Folder Location** dialog, in the **Server** pane select the File Server cluster role object name created earlier. In the **Share location** pane, choose the **Select by volume** radio button option and click **Next** to continue.	
In the **Share Name** dialog, type the value of "VMMLibrary" in the **Share name** field and then click **Next** to continue.	
On the **Other Settings** page, select only the **Enable continuous availability** option and then click **Next**.	

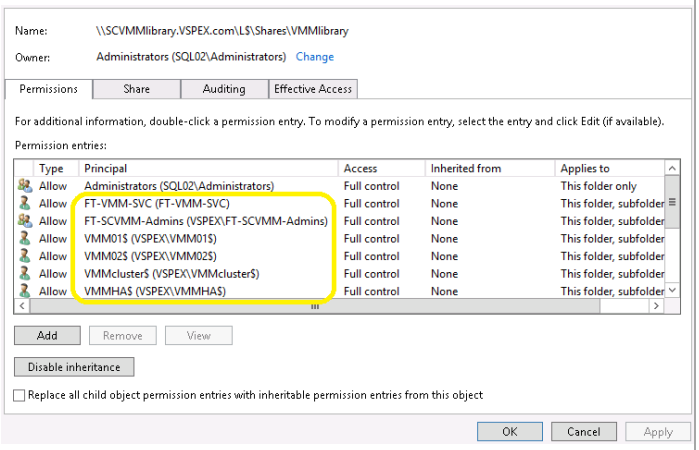
In the **Permissions** dialog, click the **Customize Permissions…** button.



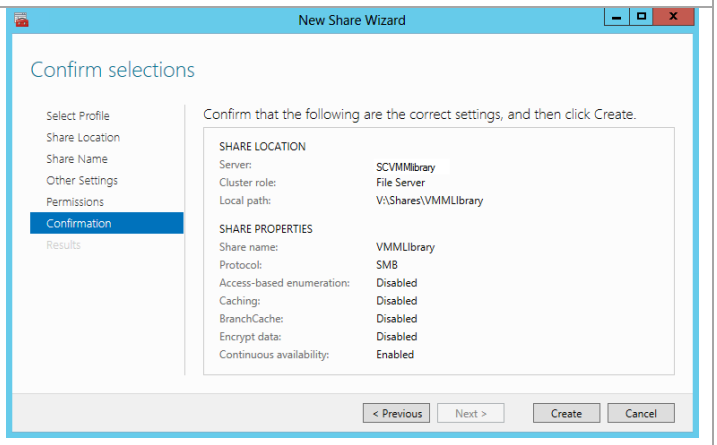
In the **Permissions for VMMLibrary** dialog, add the following accounts with NTFS Full Control permissions over the folder:

- The VMM service account.
- The VMM Admins group.
- Both VMM computer accounts.
- The VMM CNO computer account.
- The VMM VCO computer account.

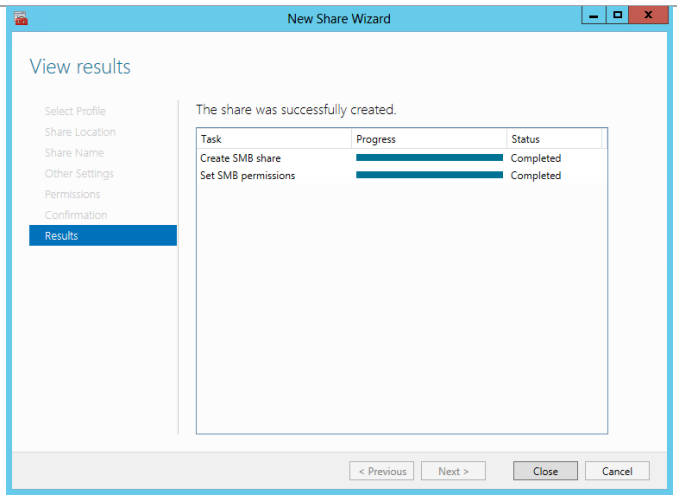
Click **OK** to save the changes and **Next** to continue in the wizard.



Review the settings on the **Confirmation** dialog and click **Create**.

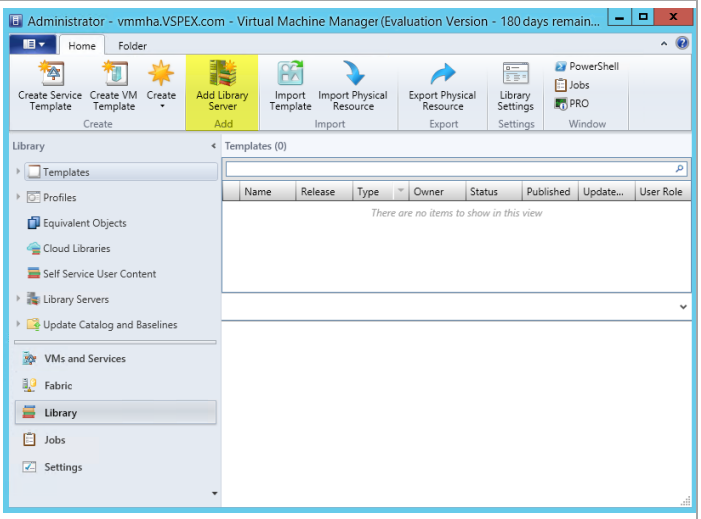


In the **Results** dialog, verify that the shared folder was provisioned properly and click **Close**.

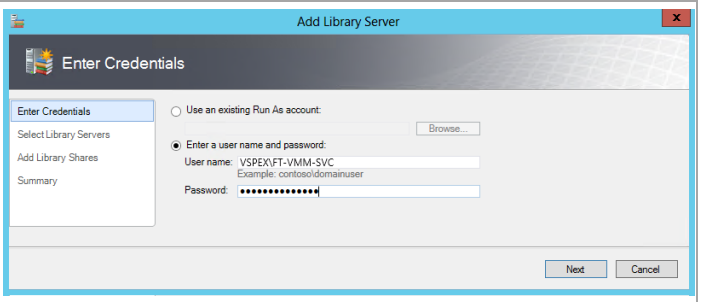


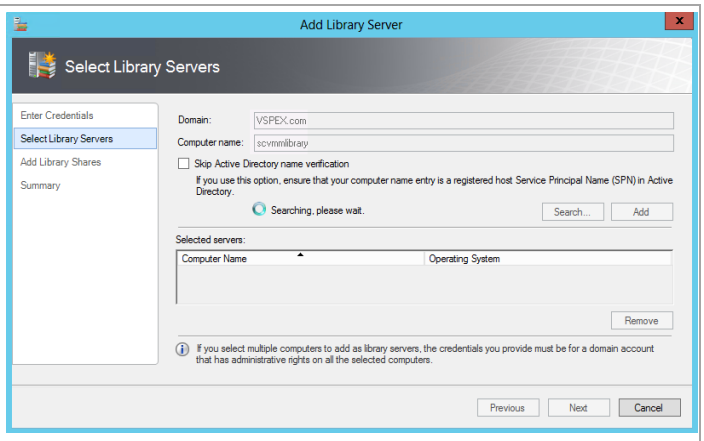
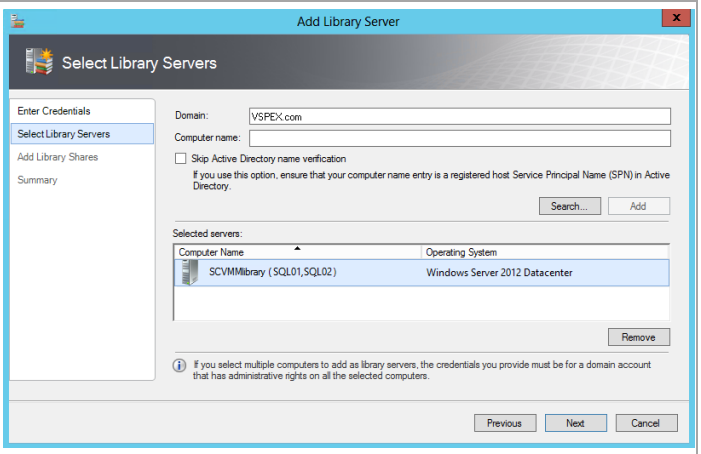
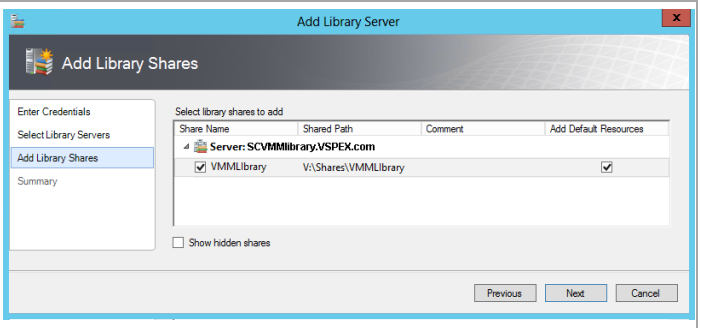
▶ Perform the following steps on the **Virtual Machine Manager** virtual machine.

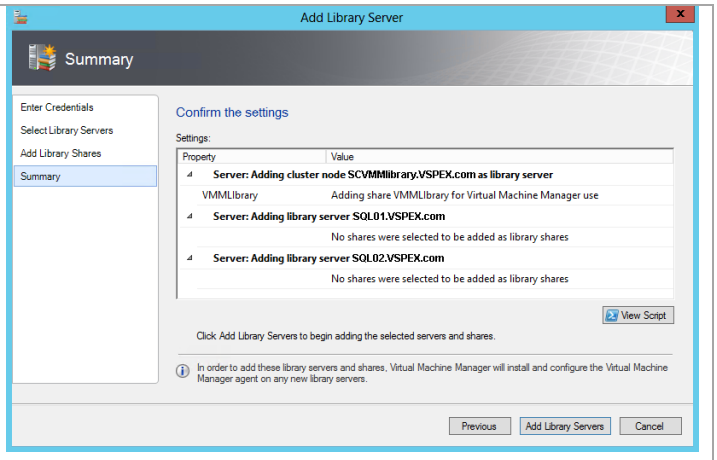
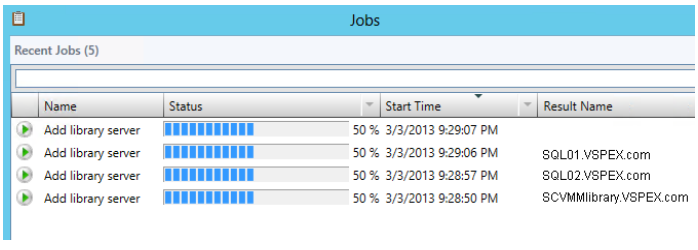
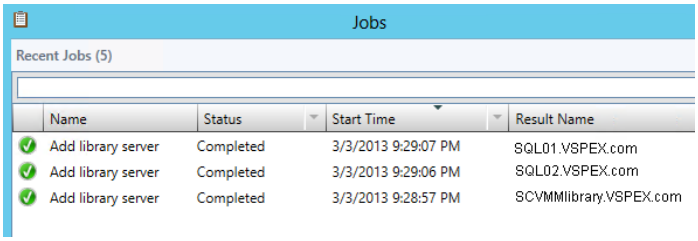
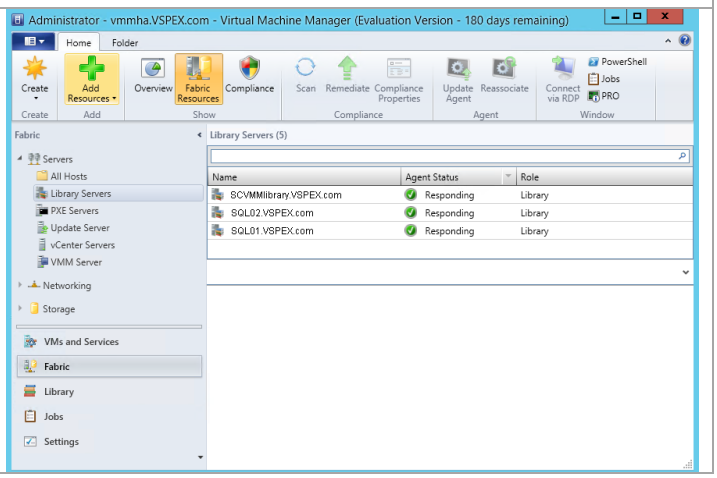
In the **Virtual Machine Manager** console, select the **Library** node. In the **Home** tab, click the **Add Library Server** button from the ribbon.

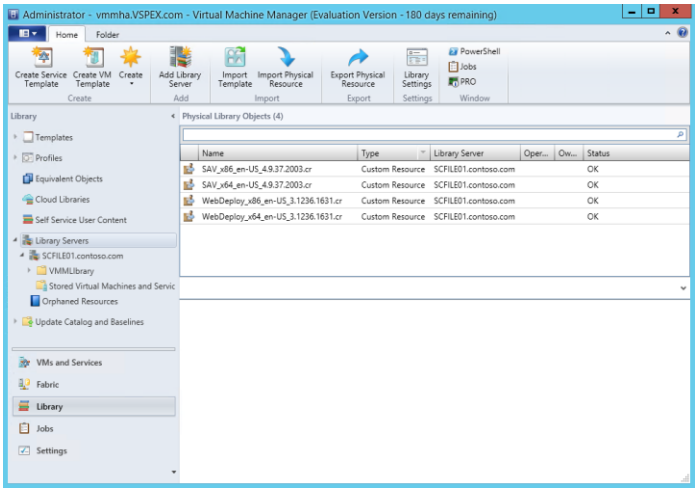


The **Add Library Server** wizard will appear. In the **Enter Credentials** dialog, select the **Enter a user name and password** option. In the **User name** and **Password** text boxes, enter credentials that have administrative rights over each of the target servers where the new HA Virtual Machine Manager Library share will reside.
Click **Next** to continue.

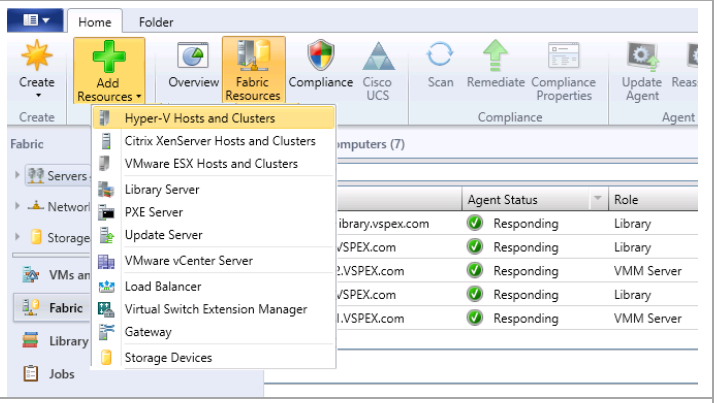
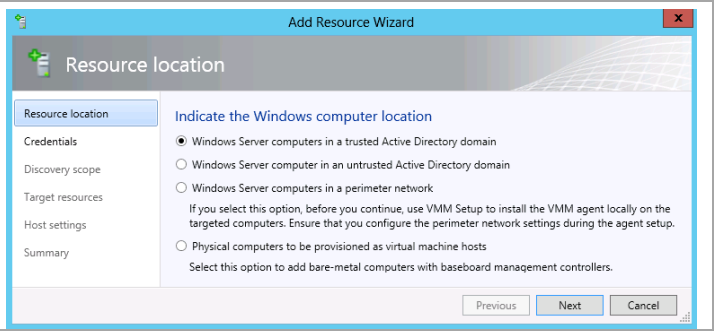


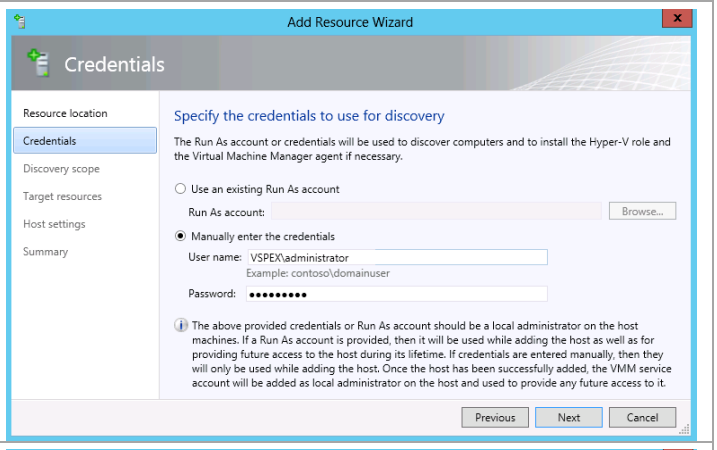
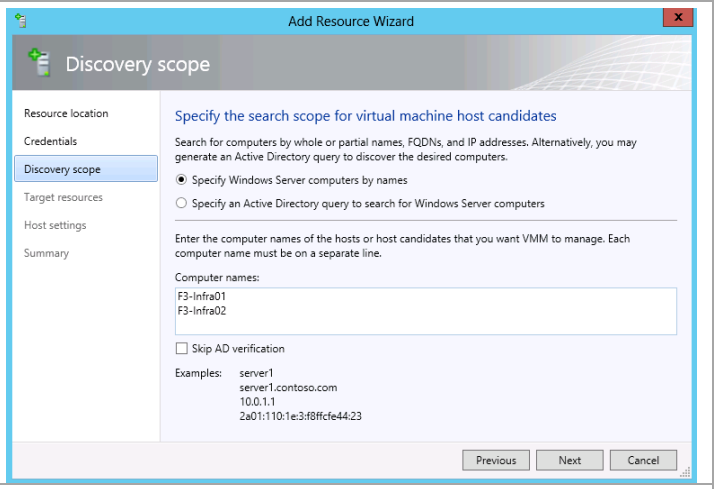
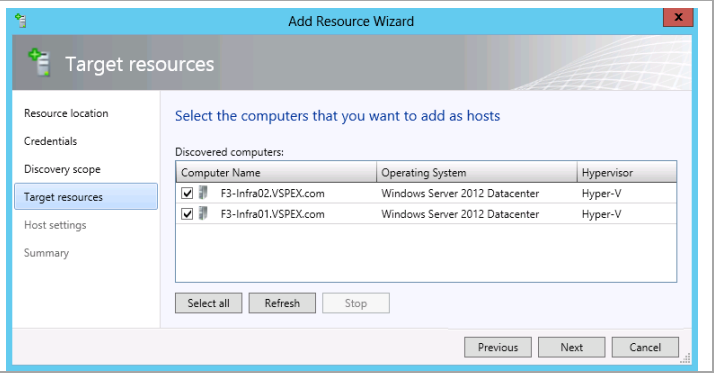
In the **Select Library Servers** dialog, specify the FQDN of the target domain in the **Domain** text box. In the **Computer name** text box, type the name of the newly created HA File Server CNO and click **Add**.	
In the **Specified Servers** pane, the cluster object will appear in the dialog. Click **Next** to continue.	
In the **Add Library Shares** dialog, select the check box associated with the VMMLibrary share created earlier. Verify that the **Add Default Resources** check box is selected and click **Next** to continue.	

Review the **Summary** dialog and click **Add Library Servers** to continue.	
The **Jobs** dialog will appear showing the progress of the Add Library Server action. In the **Jobs** dialog, verify that all steps have completed.	 
In the **Virtual Machine Manager** console, expand, select Fabric, and navigate to the **Library Servers** node. Verify that all cluster nodes are listed along with the cluster object name and that all servers are listed as Responding under **Agent Status**.	

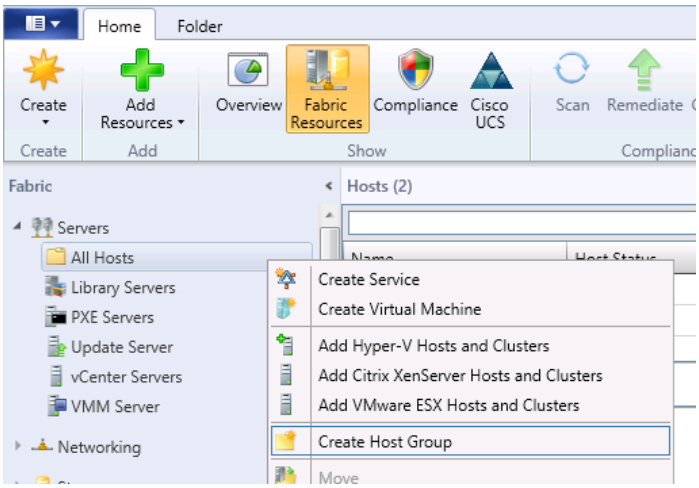
In the **Virtual Machine Manager** console, navigate to the **Library Servers** node and verify that all of the correct objects are created. When verified, exit the console.	

9.5 Add Hyper-V Hosts to VMM

From the console, select **Fabric** and click on the down arrow on **Add Resources** in the menu ribbon. Select **Hyper-V Hosts and Clusters**.	
In the **Resource location** dialog window, click the radio button by **Windows Server computers in a trusted Active Directory domain**. Click **Next** to continue.	

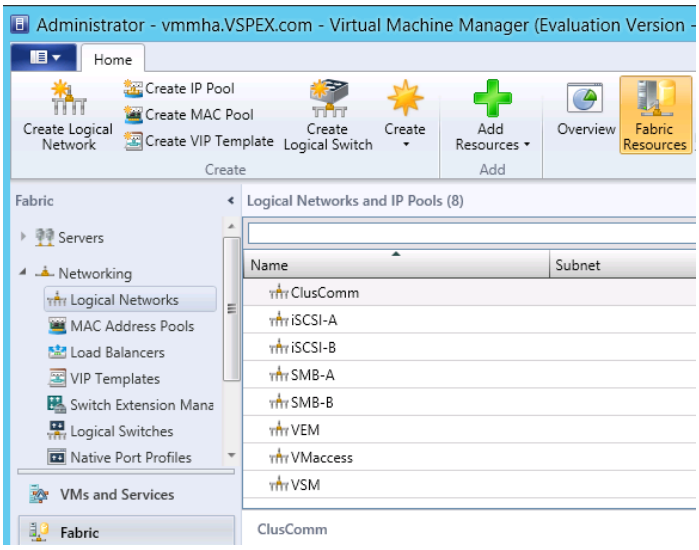
In the **Credentials** dialog window, select the radio button by **Manually enter the credentials**. Enter the credentials for the domain administrator. Click **Next** to continue.	
In the **Discovery scope** dialog window, select the radio button by **Specify Windows Server computers by names**. Enter the names of your Hyper-V hosts, one per line. Click **Next** to continue.	
On the **Target resources** dialog window, click **Select all** to select all the found machines. Click **Next** through the remainder of the dialog windows to add the Hyper-V hosts to VMM.	

Expand **Servers** in the console. Right-click **All Hosts** and select **Create Host Group**.
Expand **All Hosts** to show the clustered Hyper-V hosts. Click on the cluster name and drag it onto the newly created Host Group.

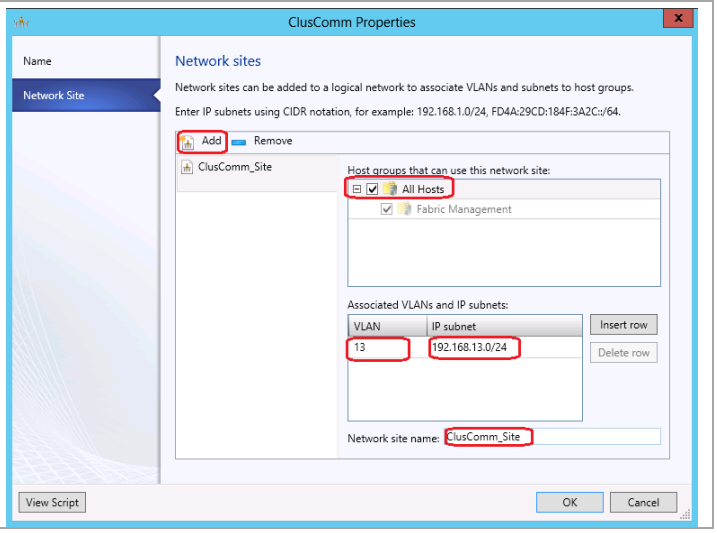


9.6 Configure Logical Networks

Select **Fabric** within the VMM console. Then select **Networking** and **Logical Networks**.
Double click on one of the networks, except VEM, to open the **Properties**.



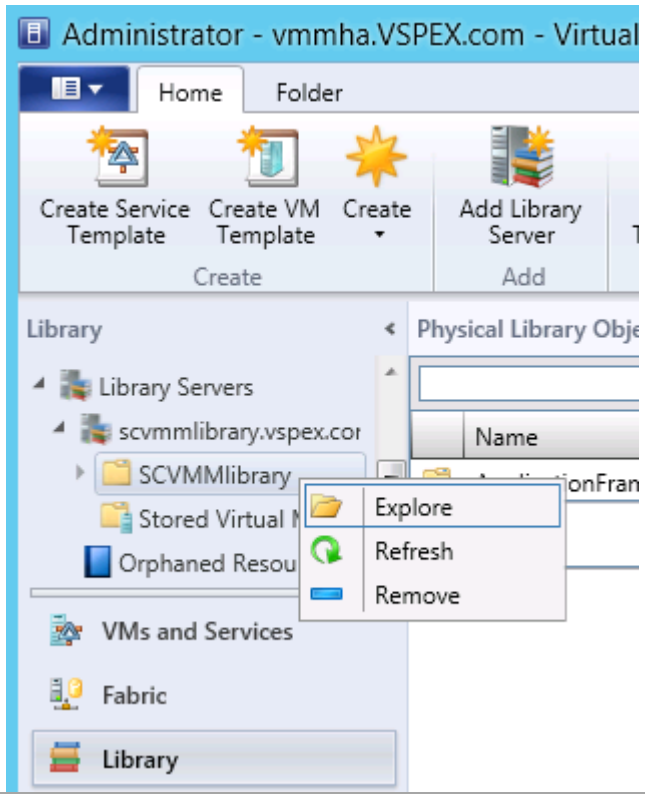
On the **Properties** window, click **Network Site**.
Click **Add** to start the configuration of the network site.
Select the Hyper-V **hosts** that will be able to offer this network site via a virtual switch definition.
Enter the **VLAN** tag value for this network.
Enter the **IP subnet** definition in CIDR notation for this network.
Optionally, rename the **site name**.
Click **OK** to continue.
Repeat for all networks except VEM.



9.7 Configure Library Subdirectories (optional)

Having a library as part of VMM provides a handy location for storage of many items that are used regularly in the management and maintenance of the cloud. It can be helpful to create subdirectories within the standard SCVMMlibrary share that was just created for storage of items, such as distribution media in the form of ISO files.

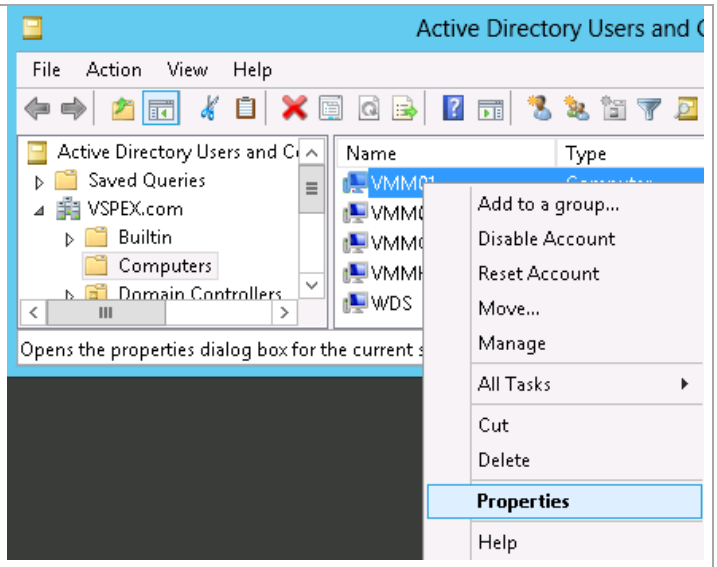
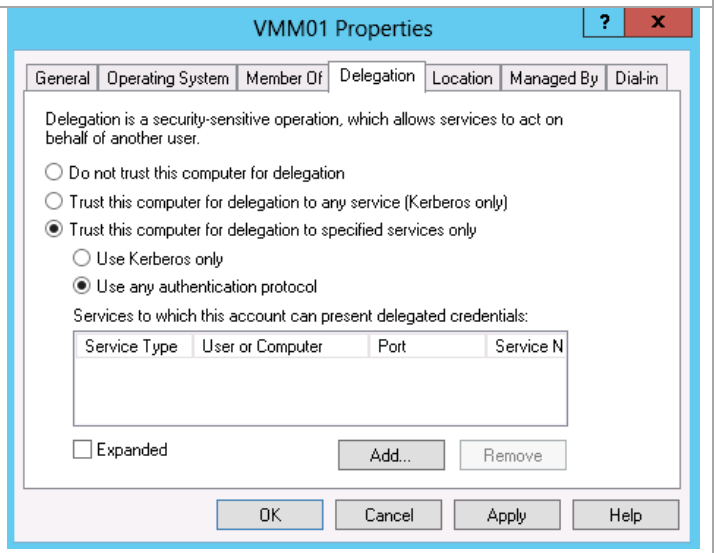
In the SCVMM console, select **Library**. Right-click on the library just created above, and select **Explore**.
This launches a familiar Windows Explorer window that allows you to create whatever directories you may find useful, such as a **Software** directory to be used for storing ISO files. Another useful directory would be PowerShell scripts.
Once the directories are created, they can be used as regular UNC paths under the share created previously, allowing you to copy information into them from any location, as long as the individual copying information has the privileges to do so.

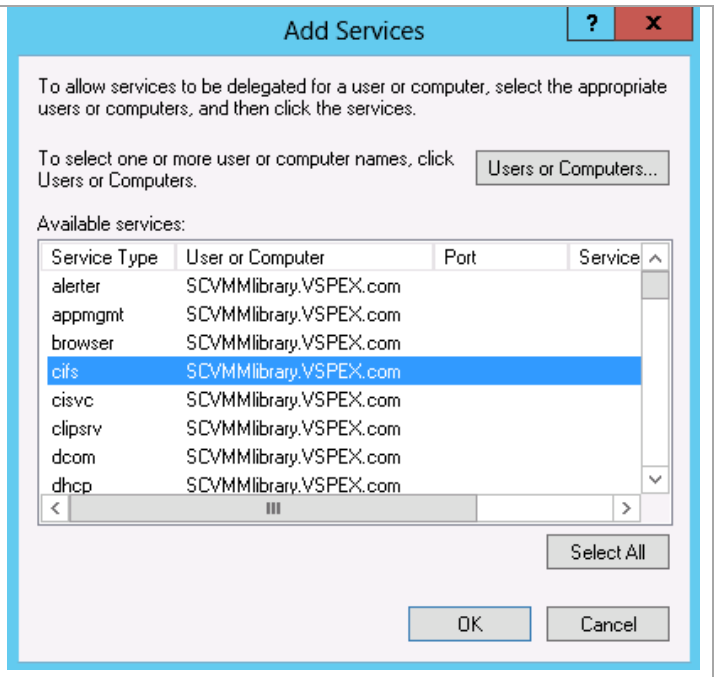


9.8 Configure Constrained Delegation (optional)

By default, when VMM is creating a virtual machine, and you are using an ISO file from the library for installation purposes, the ISO file is copied and made part of the virtual machine's definition. This wastes time copying the file and it takes extra space. Not to say that different versions of installation media may end up getting stored all over. Sharing ISO items across nodes requires additional configuration of the VMM hosts. This is called *constrained delegation* which allows the VMM host to operate on behalf of the virtual machine being created.

This is a security change to a default installation, so it should be reviewed with your security department before deployment.

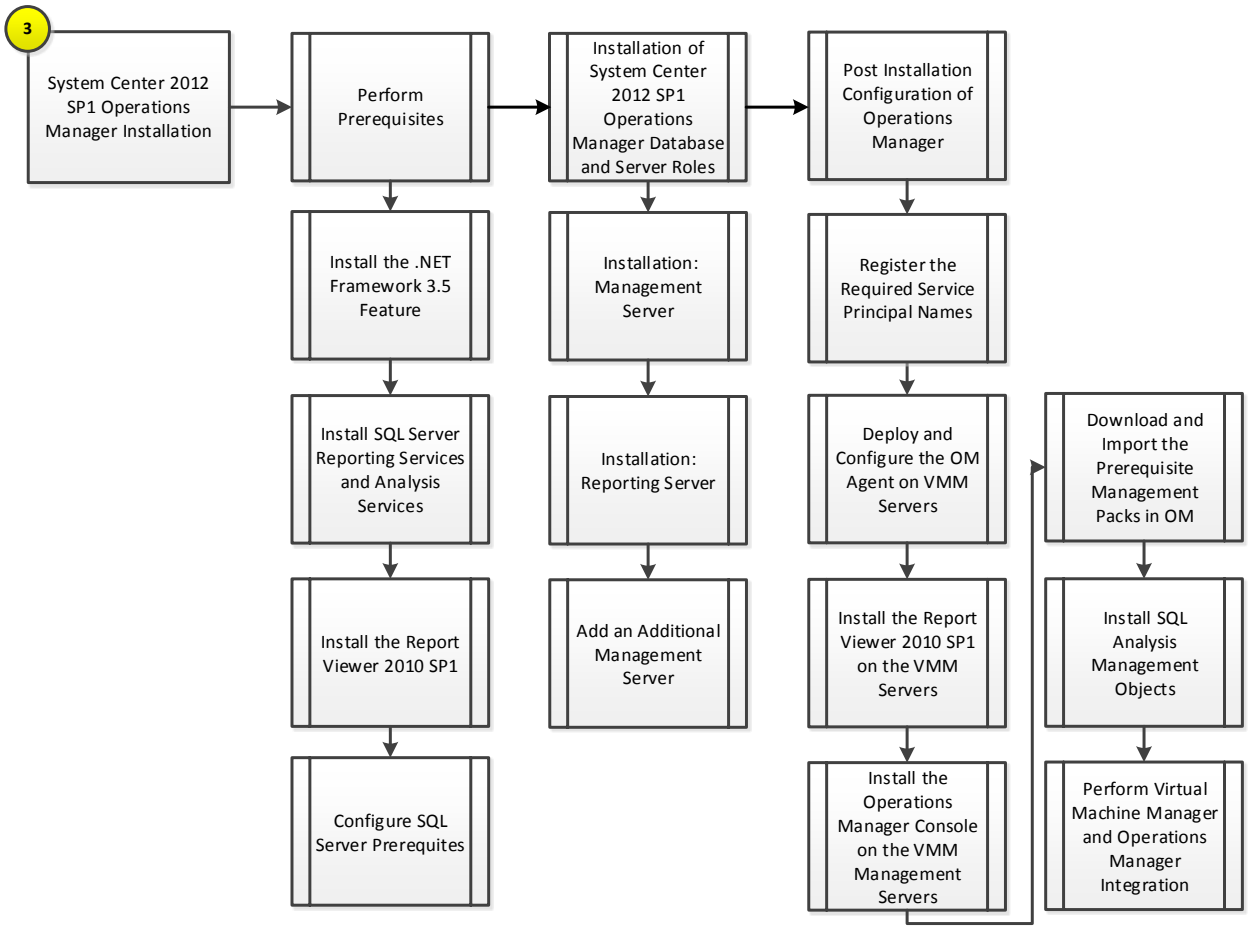
On your domain controller (or from a system that has the proper Remote Server Administration Tools installed), launch **Active Directory Users and Computers**. Expand your domain and expand **Computers**. Right-click on your VMM host and select **Properties**.	
Select the **Delegation** tab on the Properties sheet. Click the radio button by **Trust this computer for delegation to specified services only**. Click the radio button by **Use any authentication protocol**. Click the **Add...** button.	

In the **Add Services** dialog window, click the **Users or Computers…** button. Select the name of the server offering the SCVMM library. In this configuration, there is a highly available cluster service named SCVMMlibrary that is offering the share. Select the **cifs** entry. Click **OK** to continue. Click **OK** in the server Properties window to accept the changes. Repeat this process for every VMM host.	

10 System Center Operations Manager

The Operations Manager installation process is comprised of the following high-level steps:

Figure 12 Operations Manager Installation Process



10.1 Overview

This section provides high-level walkthrough on deploying Operations Manager into the Fast Track fabric management architecture. The following assumptions are made:

- A base virtual machine running Windows Server 2012 has been provisioned for Operations Manager
- A SQL Server 2012 cluster with dedicated instances has been established in previous steps:
  - The default SQL Server collation settings are required - SQL_Latin1_General_CP1_CI_AS.
  - SQL Server Full Text Search is required.
- The installation will follow a remote SQL Server configuration with multiple SQL Server instances:
  - SQL Server Reporting Services and SQL Server Analysis Services and associated databases will run on one instance locally on the Operations Manager management server.
  - The Operations Manager databases on will run on a separate SQL Server instance on the Fabric Management SQL cluster.

10.2 Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created[10]:

Table 28 Prerequisite Accounts

User name	Purpose	Permissions
<DOMAIN>\FT-SCOM-SVC	System Center configuration service and System Center data access service account (sdk_user role)	Domain account with local admin permissions on all Operations Manager management servers and local admin rights on all SQL Server nodes as well as sysadmin rights on all Operations Manager SQL Server instances.
<DOMAIN>\FT-SCOM-Action	Operations Manager action account	This account will need full admin permissions on all target systems that will be managed using the action account.
<DOMAIN>\FT-SCOM-DR	Operations Manager data reader account	Domain account with local admin permissions on all Operations Manager management servers, local admin rights on all SQL Server nodes.
<DOMAIN>\FT-SCOM-DW	Operations Manager, Data Warehouse write account	Domain account with local admin permissions on all Operations Manager management servers and local admin rights on all SQL Server nodes.

Groups

Verify that the following security groups have been created:

Table 29 Prerequisite Security Groups

Security Group Name	Group Scope	Members
<DOMAIN>\FT-SCOM-ADMINS	Global	<DOMAIN>\FT-SCOM-Action <DOMAIN>\FT-SCOM-SVC <DOMAIN>\FT-SCOM-DR <DOMAIN>\FT-SCOM-DW Operations Manager Administrators' privileged admin account

[10] Specific rights for Operations Manager are outlined in http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin

Security Group Name	Group Scope	Members
		Operations Manager computer account <DOMAIN>\FT-VMM-SVC
<DOMAIN>\FT-SCOM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>\FT-SCOM-AdvOperators	Global	Operations Manager Advanced Operators privileged admin accounts

Required Networks

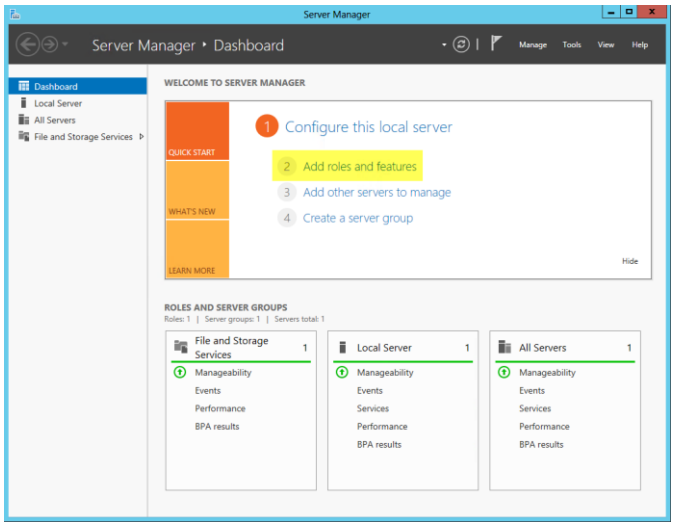
VMaccess

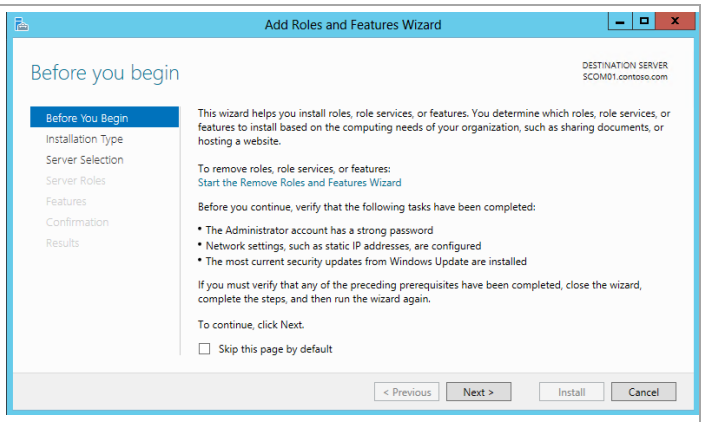
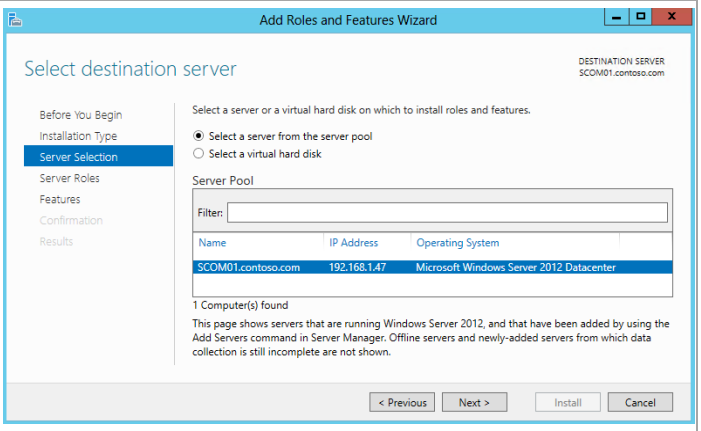
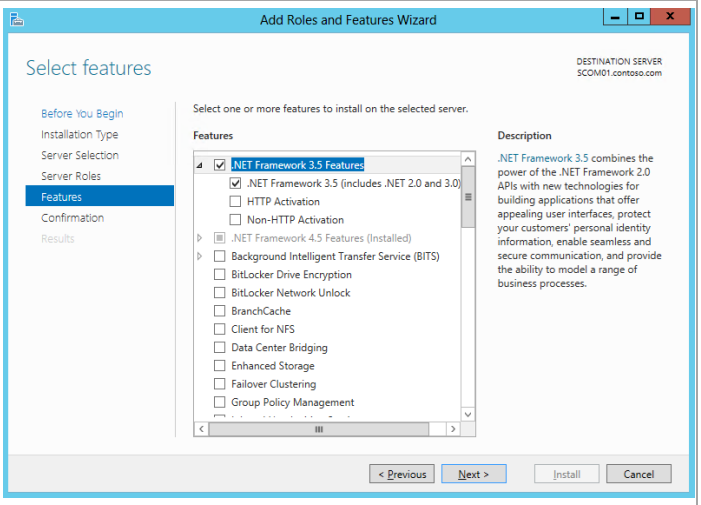
Add the .NET Framework 3.5 Feature

If you did not include this feature in your sysprepped base VHD, you will need to add the .NET Framework 3.5 feature. The Operations Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on all **Operations Manager** virtual machines.

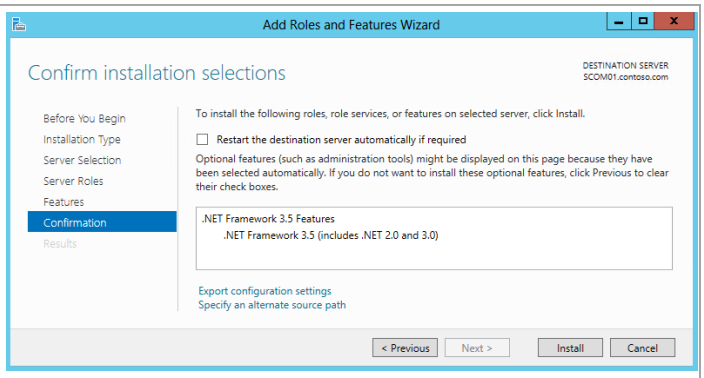
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



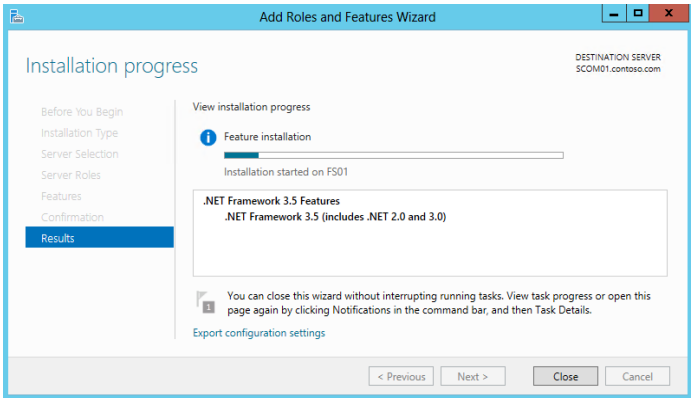
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.	
In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next - for** this installation, click the **Features** menu option to continue.	
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.	

In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

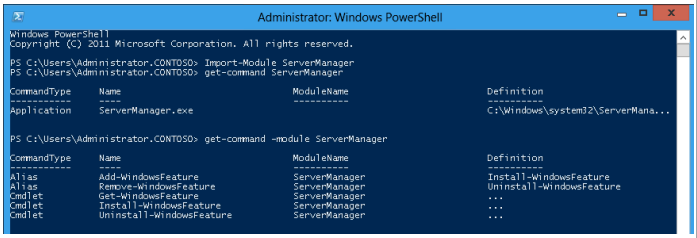
Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. Once exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.



The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



While the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.



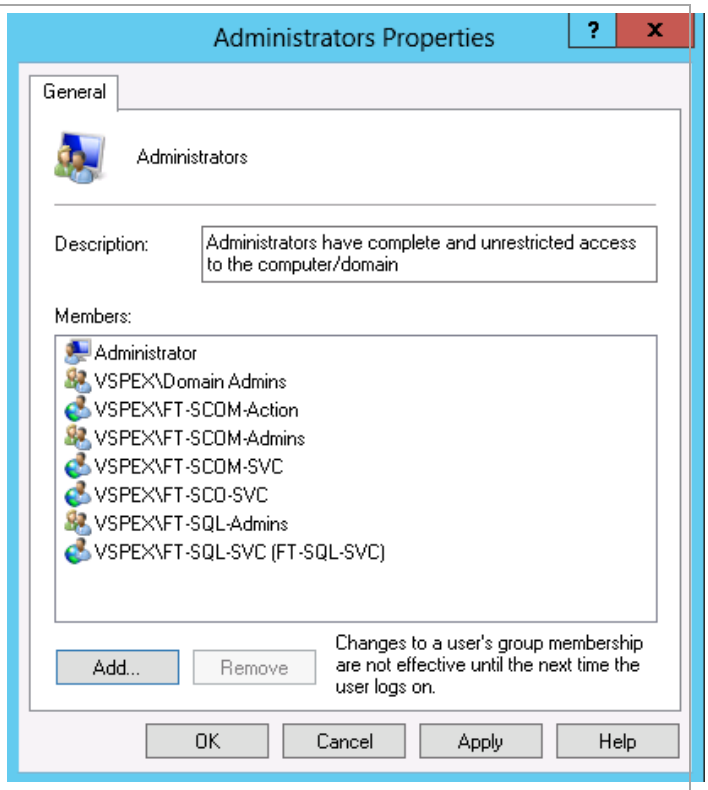
Install the SQL Server Reporting Services and Analysis Services (Split Configuration)

The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the provided steps to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

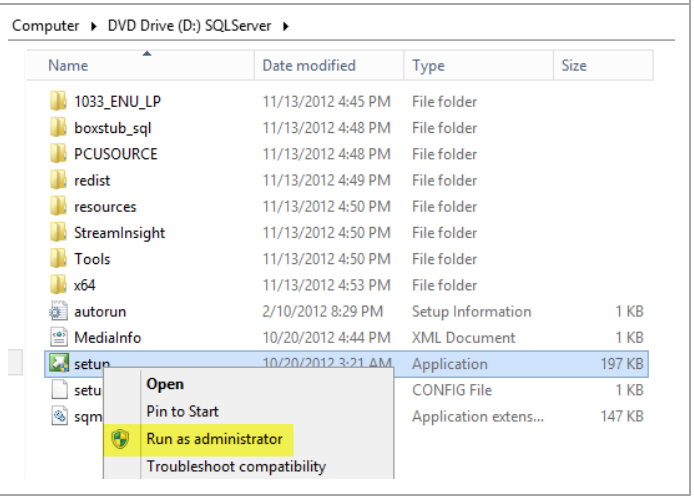
▶ Perform the following steps on the **Operations Manager Reporting Server** virtual machine only.

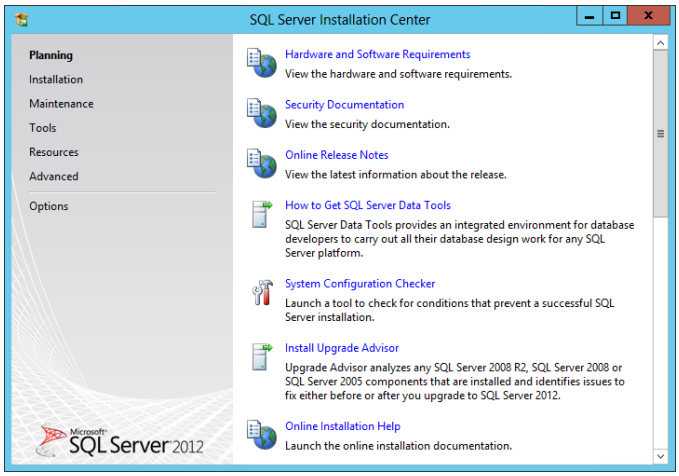
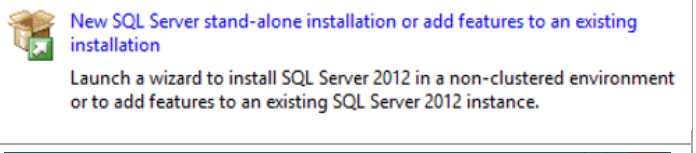
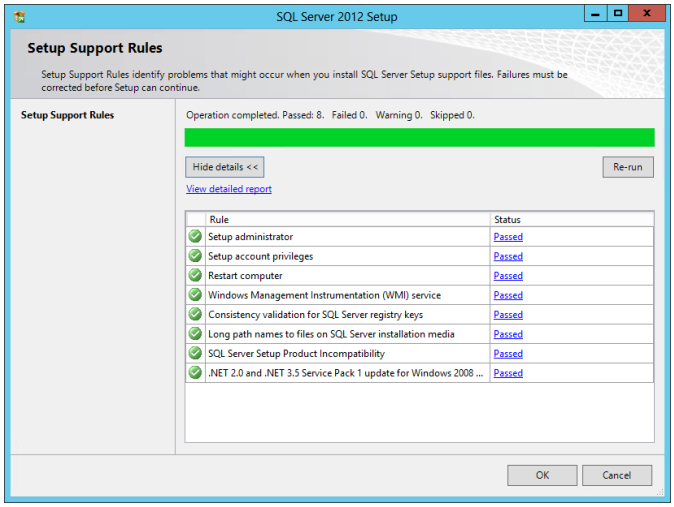
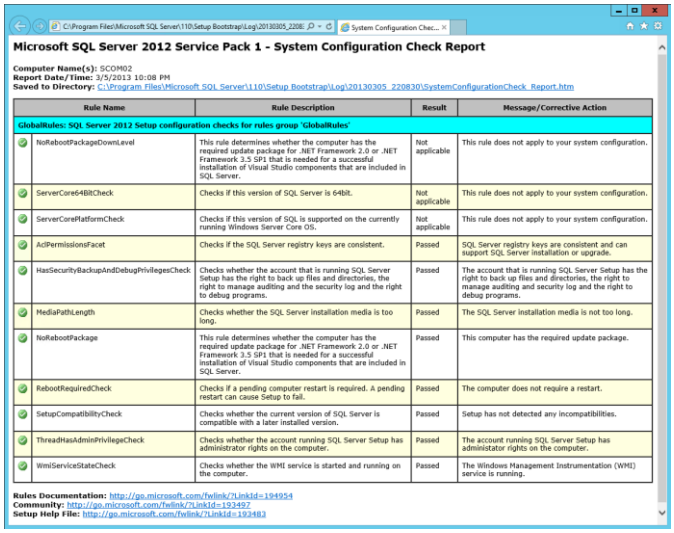
Log on to the Operations Manager Reporting Server virtual machine with a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager reporting server virtual machine:

- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.
- SQL Server service account.
- SQL Server Admins group.



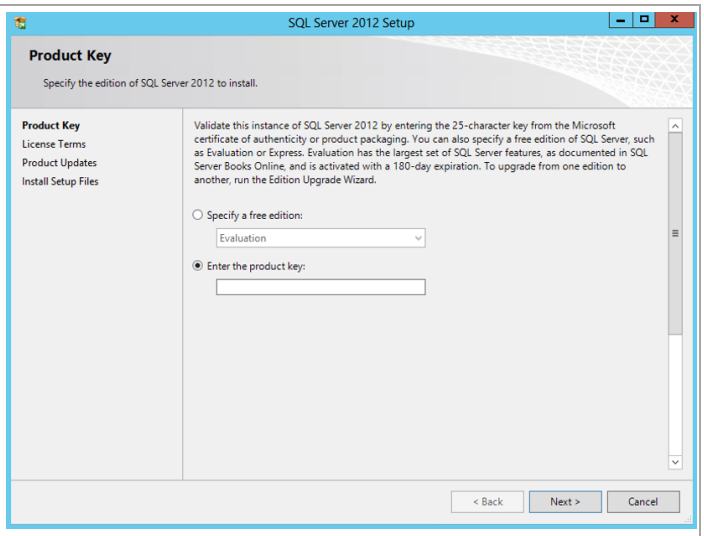
From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



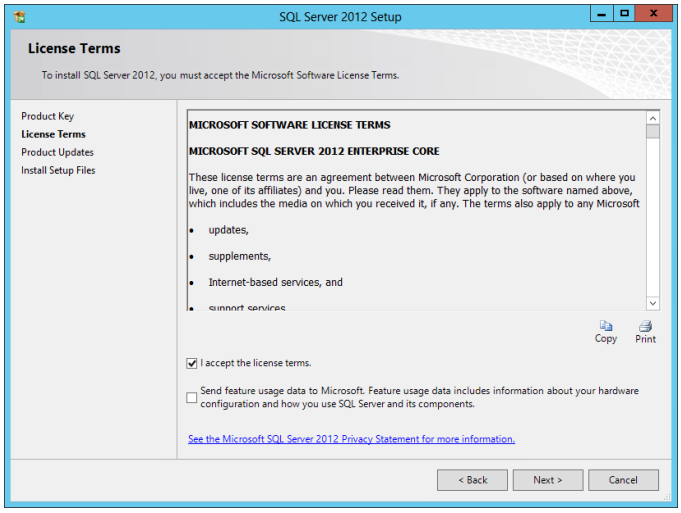
The **SQL Server Installation Center** will appear. Select the **Installation** menu option.	
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.	
The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.	
If the **View detailed report** link is selected, the following report is available.	

In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box.
Click **Next** to continue.

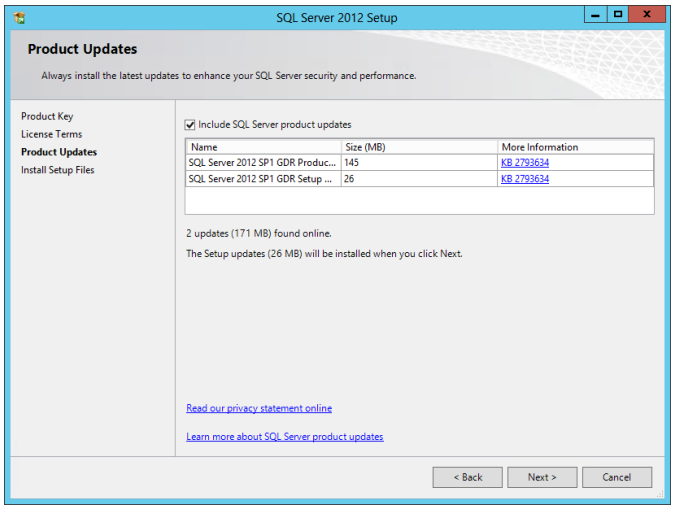
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.

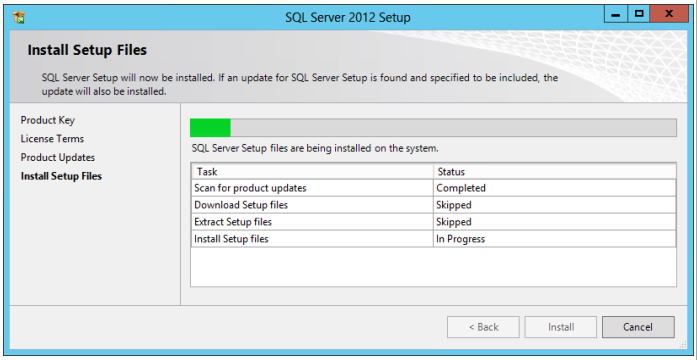
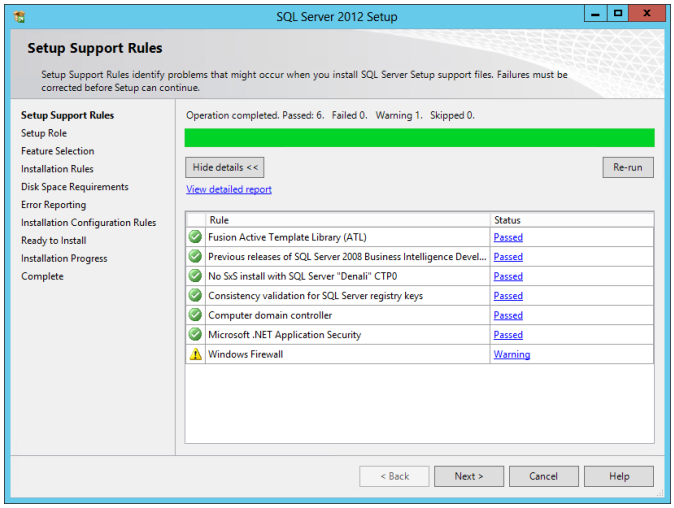
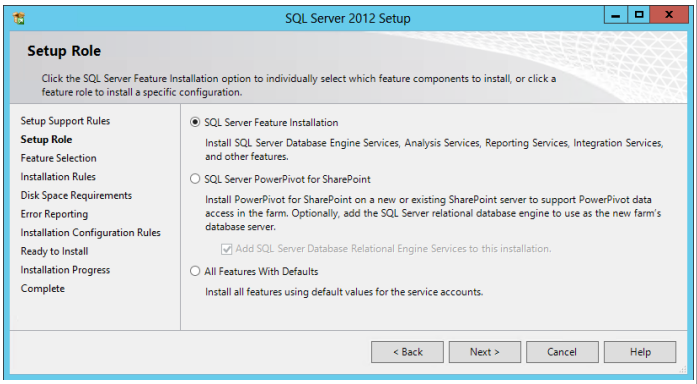


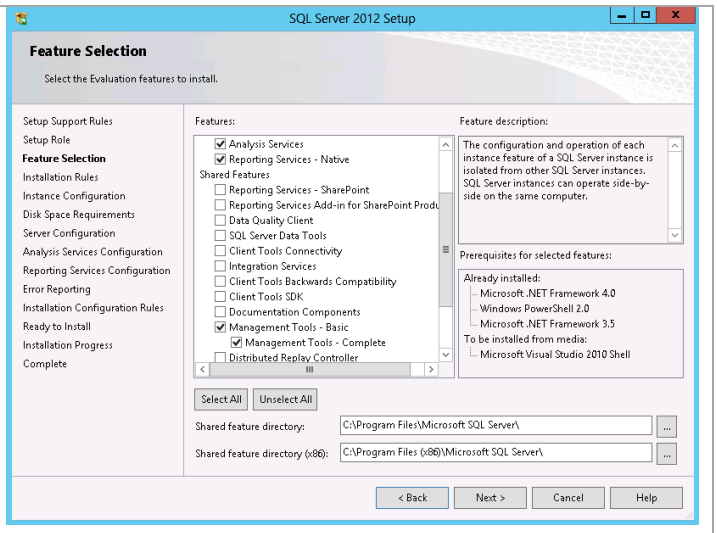
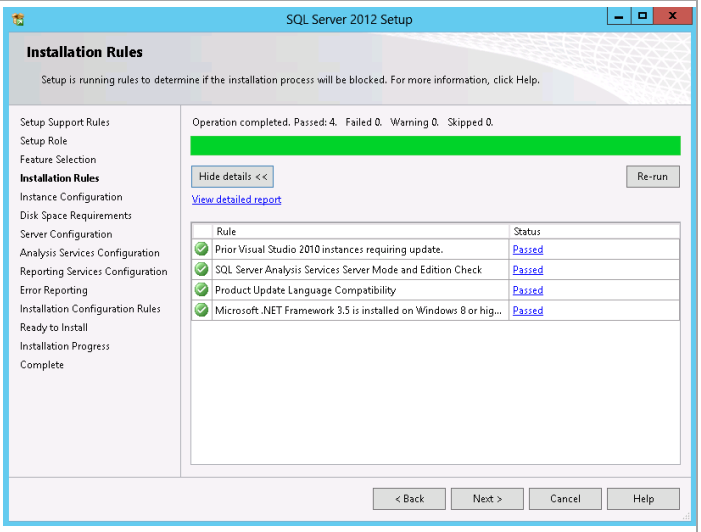
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.



In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.



In the **Install Setup Files** dialog, click **Install** and allow the support files to install.	
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment. Click **Next** to continue.	
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.	

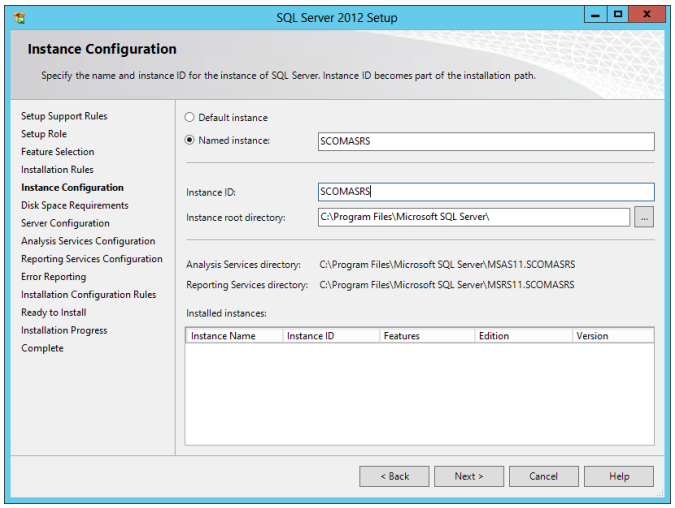
In the **Feature Selection** dialog, select the **Analysis Services, Reporting Services - Native, Management Tools – Basic,** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.	
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

In the **Instance Configuration** dialog, select the **Named instance** option. In the provided text box, specify the instance name being installed.

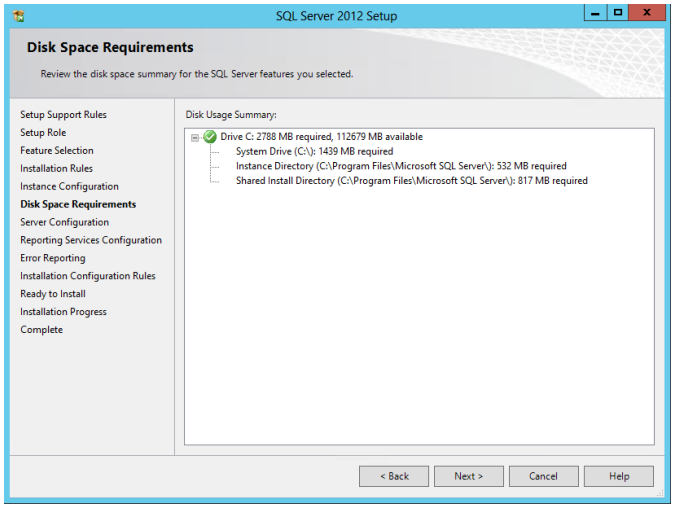
- **Instance ID** –*Select the Named instance option and specify SCOMASRS in the provided box. Verify the Instance ID is listed as SCOMASRS in the associated box. Keep the default Instance root directory values, and then click Next to continue.*

- **Instance root directory** – *accept the default location of %ProgramFiles%\Microsoft SQL Server*.

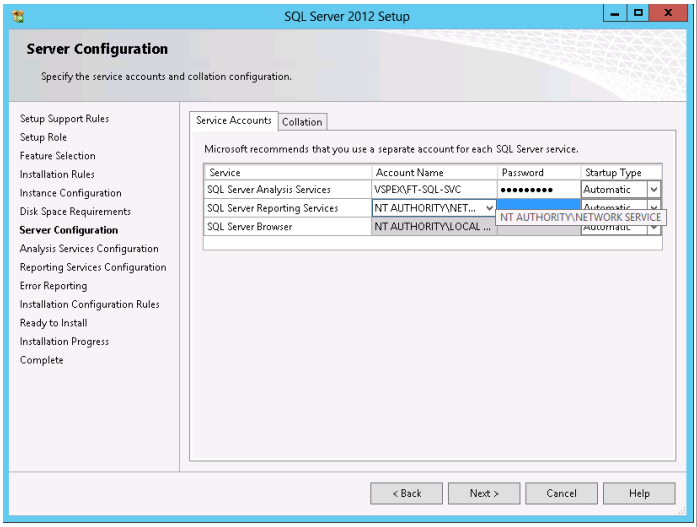
Note: A post-installation configuration process will occur to configure the reporting server database within the Operations Manager Data Warehouse SQL Server instance.



In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.



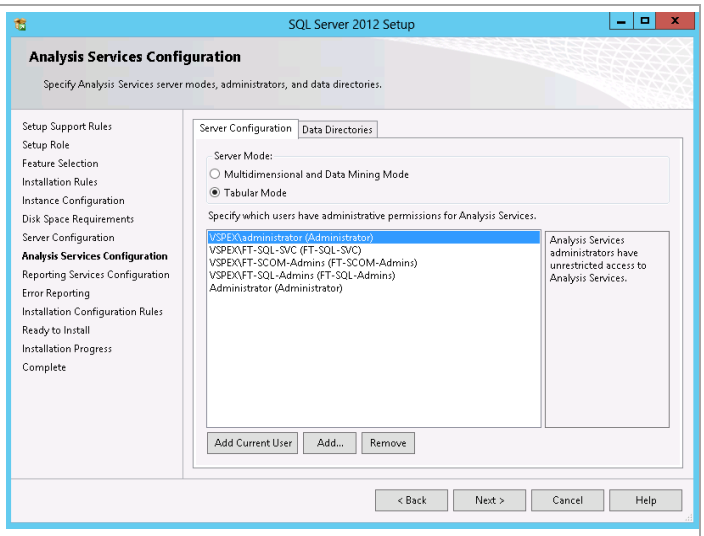
In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the domain SQL Server service account account for the **SQL Server Analysis Services** service. Specify the **NT AUTHORITY\NETWORK SERVICE** account for the **SQL Server Reporting Services** service.
Click **Next** to continue.



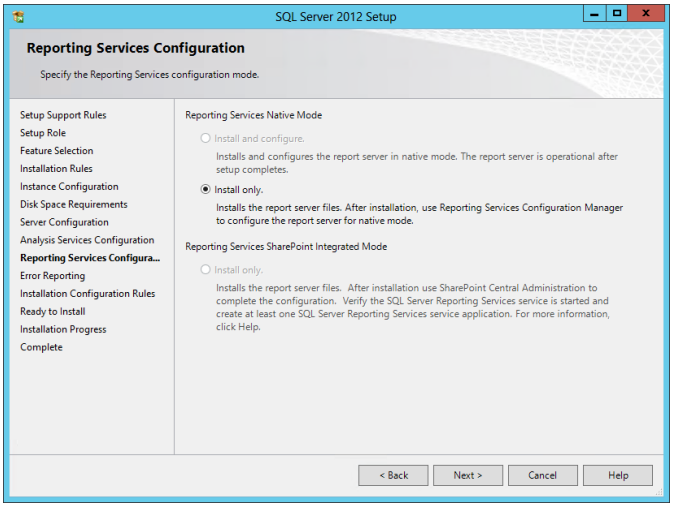
In the Analysis Services Configuration dialog, select the Account Provisioning tab. In the Specify which users have administrative permissions for Analysis Services section, click the Add Current User button to add the current installation user. Click the Add… button to select the following groups:

- Operations Manager Admins group
- Operations Configuration service and Data Access service account
- SQL Server Service account
- SQL Server Admins group
- BUILTIN\Administrators

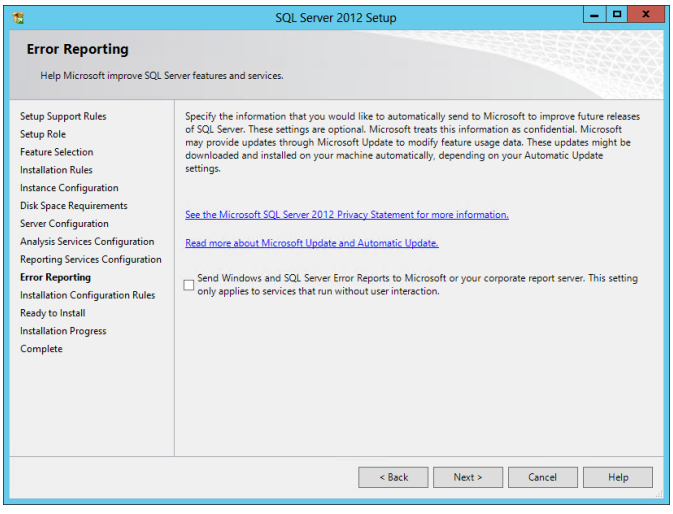
Click Next to continue.

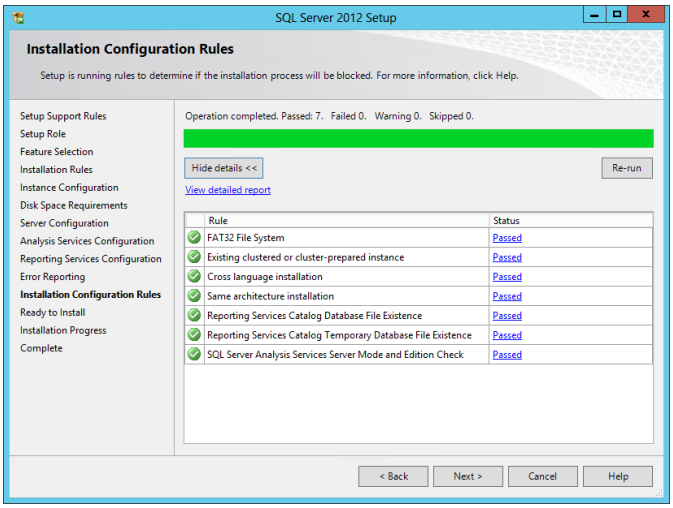
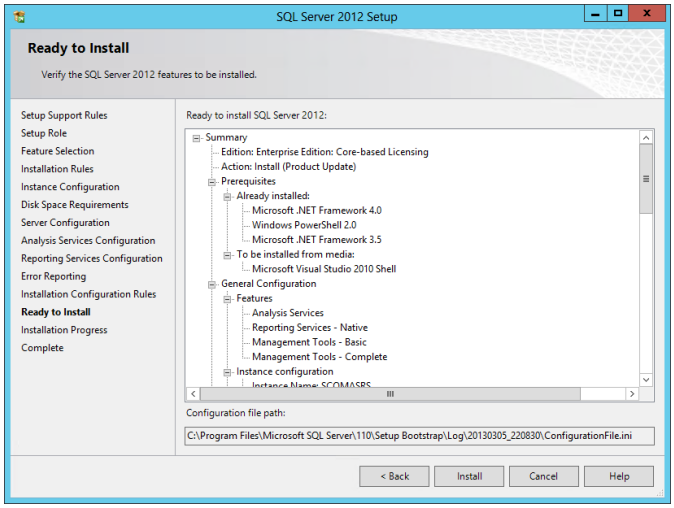
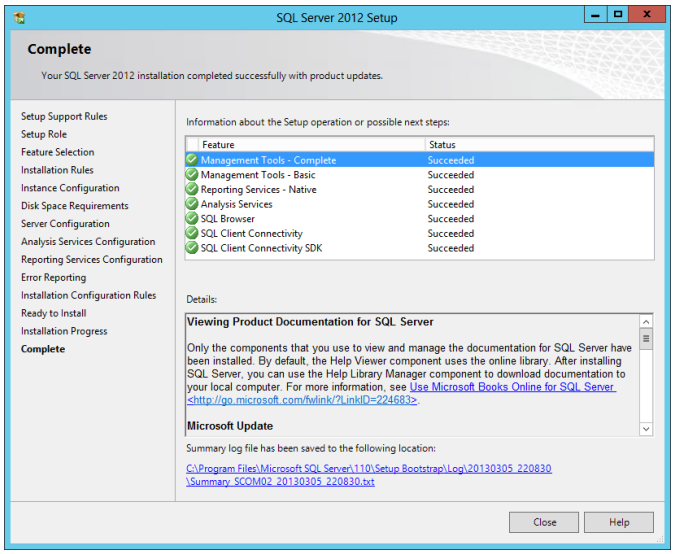


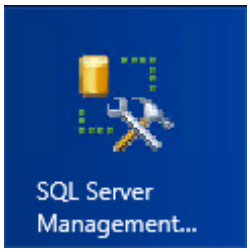
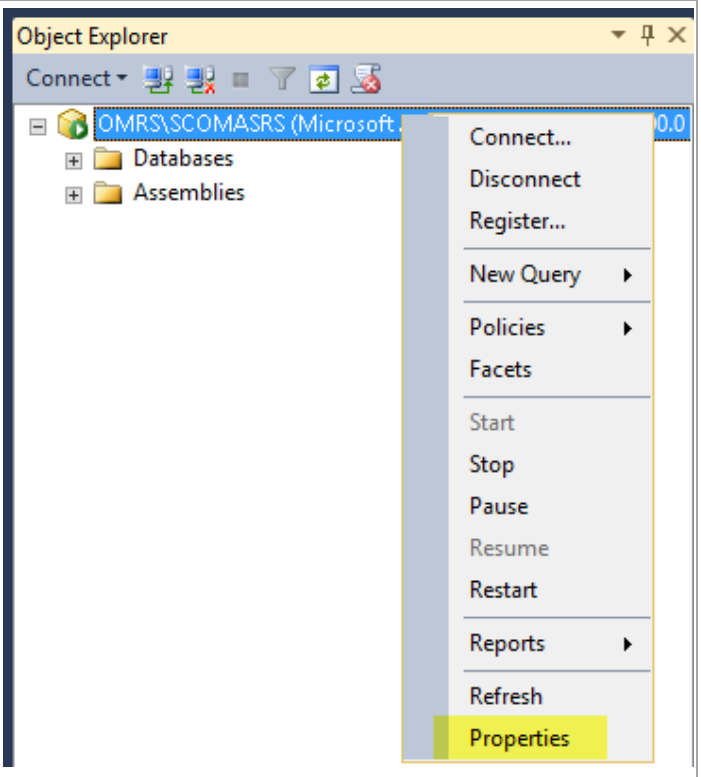
In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation.
Click **Next** to continue.

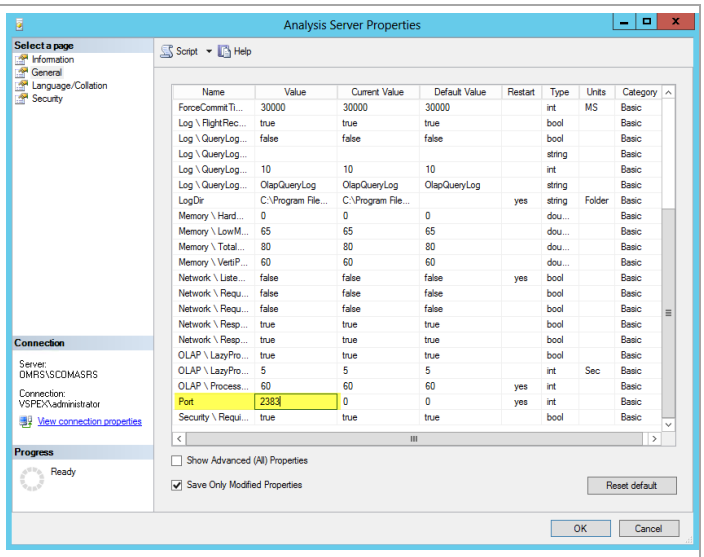
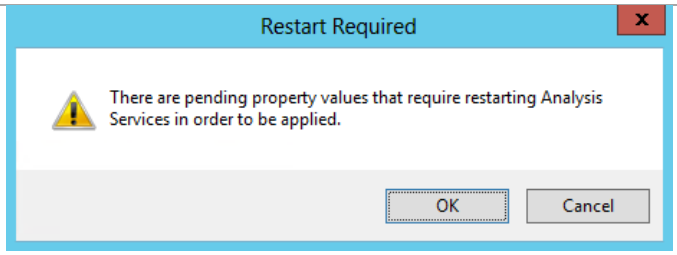
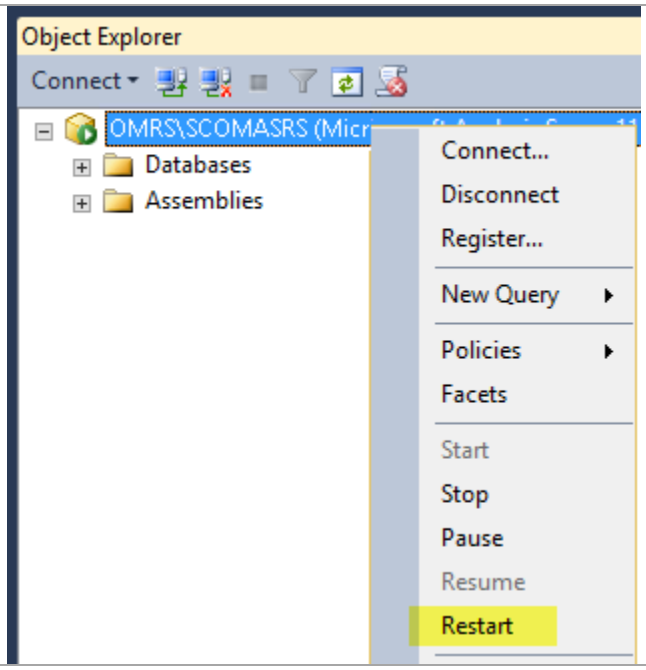


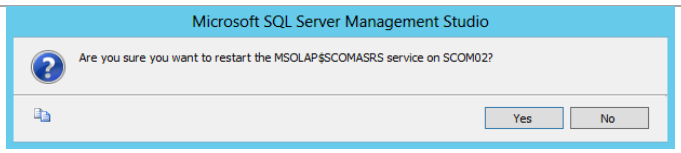
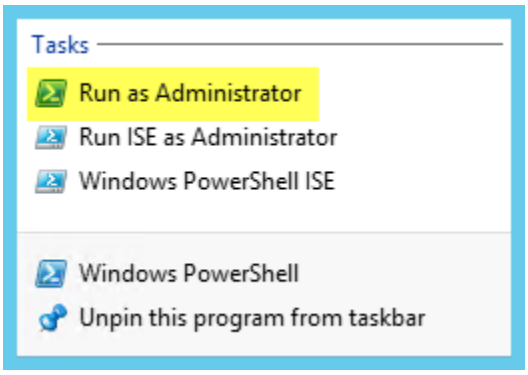
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.

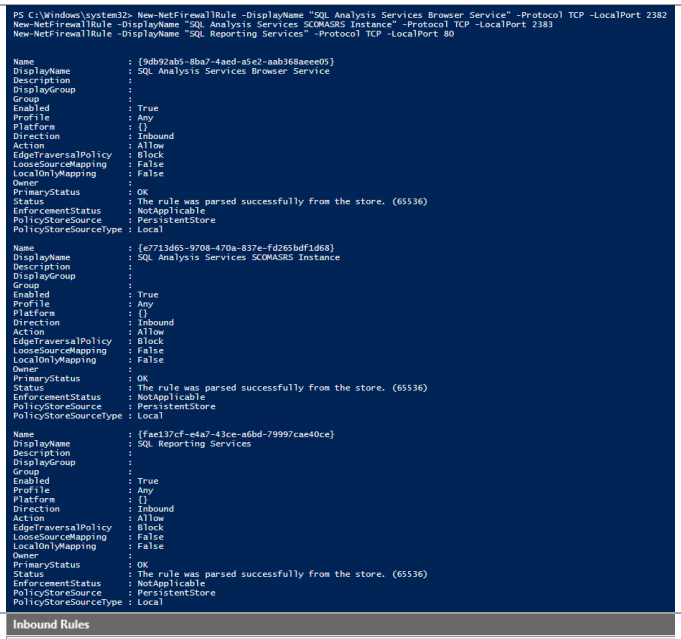


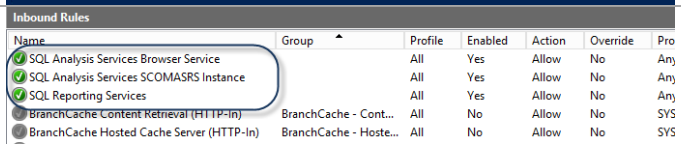
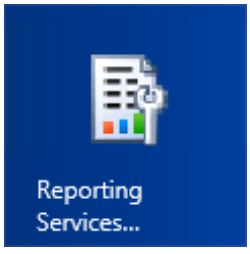
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.	
When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.	

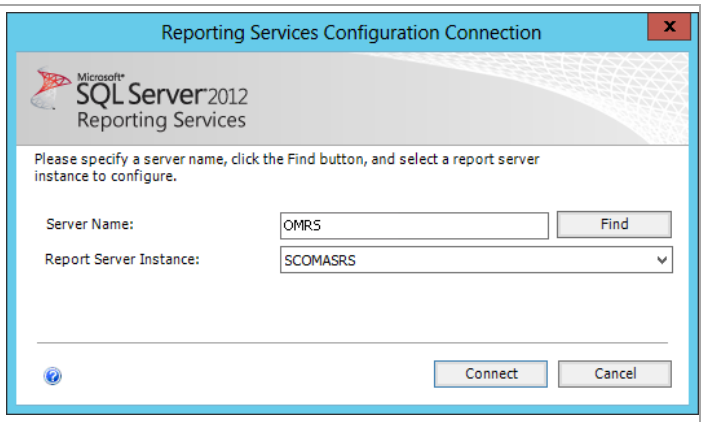
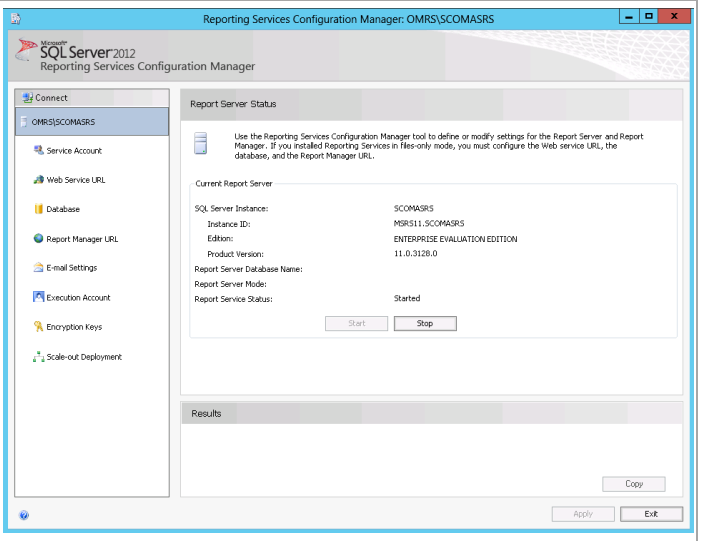
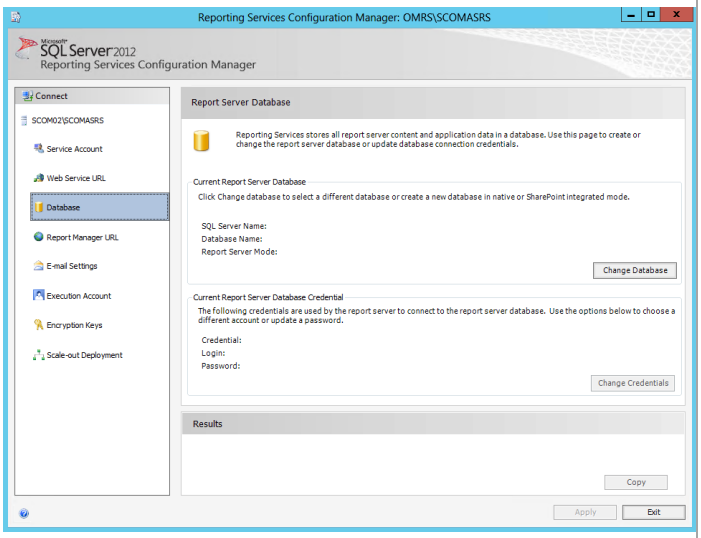
Verify the installation in SSMS prior to moving to the next step of installation. Launch **SQL Server Management Studio** and connect to Analysis Services at **ServerName\InstanceName**.	 
By default, named instances will use dynamic ports. In order to achieve better compatibility with firewalls the instance port should be set to static. Select the SSAS instance. Right-click the instance and select **Properties**.	

In the **Properties** dialog select the **General** tab. Scroll down to the **Port** value under the **Name** column. Select the value and change the value of 0 (zero) to 2383 or a port value of your choice. When complete, click **OK** to continue.	
When prompted by the Restart Required dialog, click **OK**.	
Within **SQL Server Management Studio**, in **Object Explorer**, select the SSAS instance, right-click and select **Restart** from the context menu.	

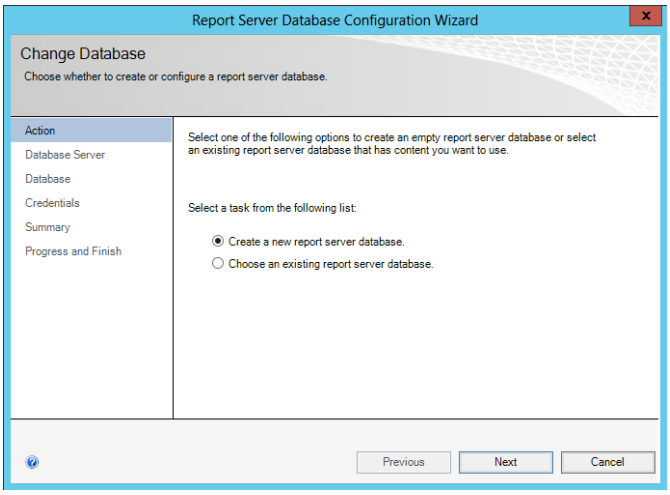
On the confirmation screen, click **Yes**. Close **SQL Server Management Studio**.	
By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled. Open an administrative session of PowerShell.	

Execute the following commands to create the needed Firewall Rules:
`New-NetFirewallRule -DisplayName "SQL Analysis Services Browser Service" -Protocol TCP -LocalPort 2382`
`New-NetFirewallRule -DisplayName "SQL Analysis Services SCOMASRS Instance" -Protocol TCP -LocalPort 2383`
`New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80`
Adjust the display names and ports based on organizational requirements.
	

Open the **Windows Firewall with Advanced Security** MMC console to verify the results. Once verified, close the MMC console.	
When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start Menu**, navigate and select the **Reporting Services Configuration Manager** tile.	

The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Operations Manager server. In the **Report Server Instance** text box, use the default **SCOMASRS** drop-down menu value. Click **Connect**.	
The **Reporting Services Configuration Manager** tool will appear.	
In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.	

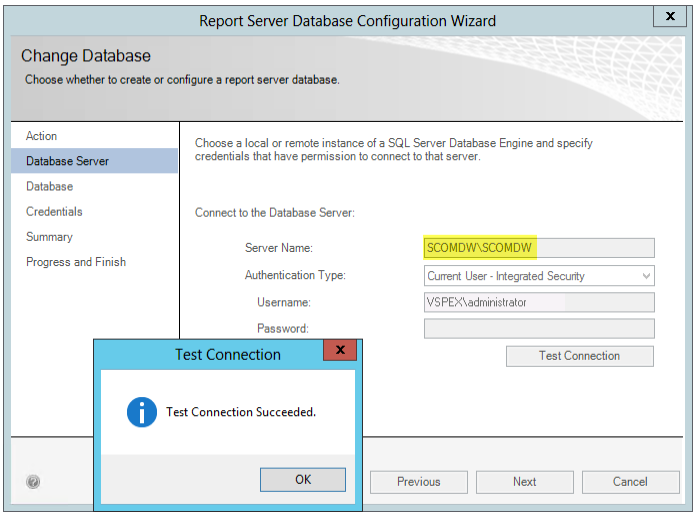
The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – *specify the name of the SQL Server CNO and the database instance created for the Operations Manager installation.*
- **Authentication Type** – *specify **Current User – Integrated Security** from the drop-down menu.*

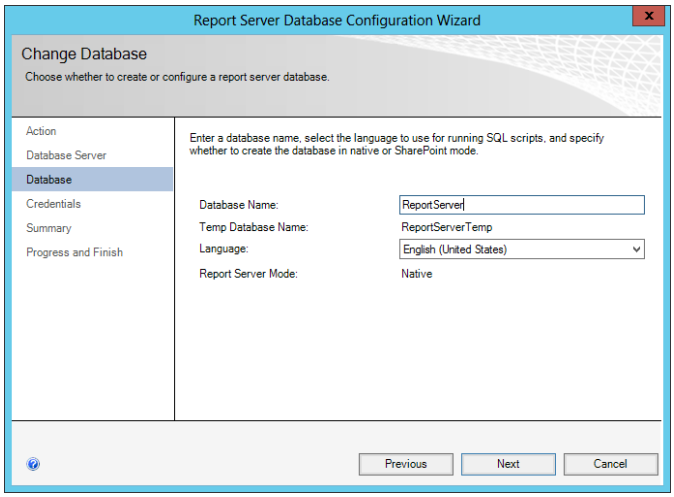
Click the **Test Connection** button to verify the credentials and database connectivity.
When verified, click **Next** to continue.

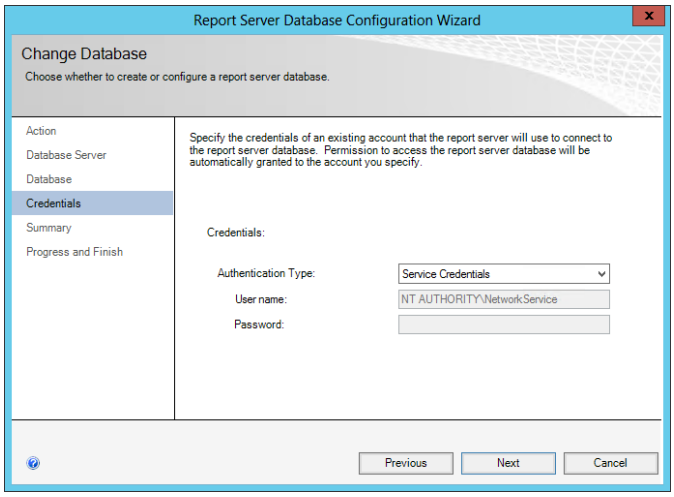
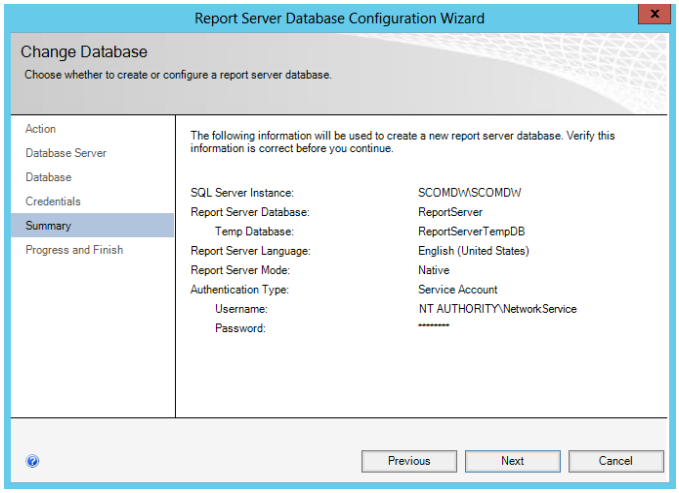
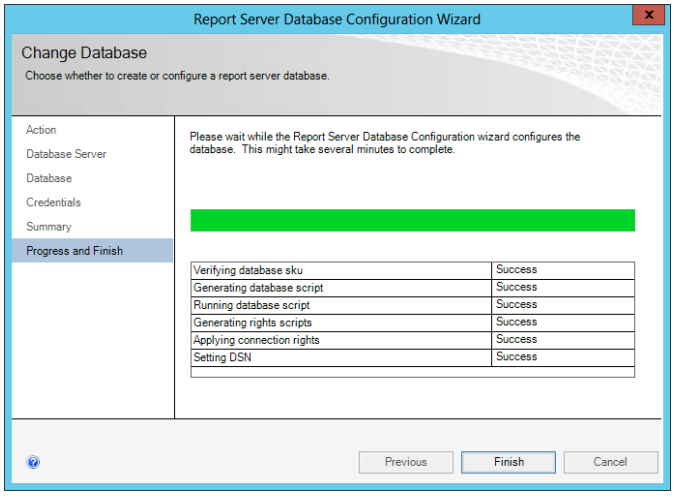


In the **Database** section, specify the following values:

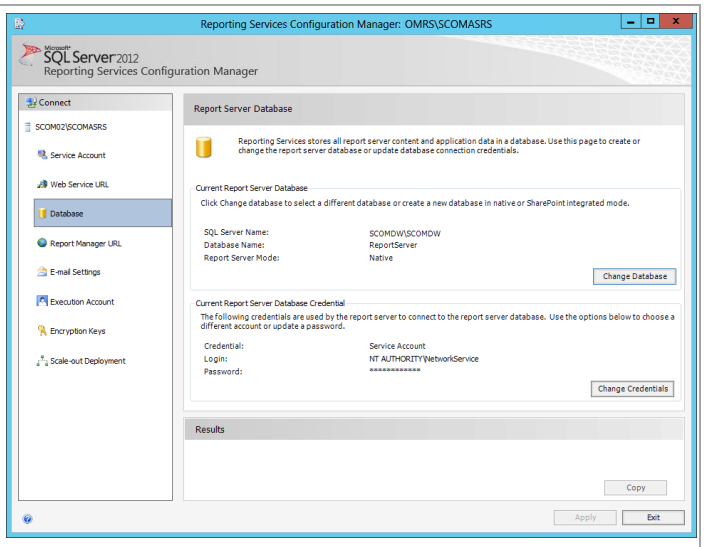
- **Database Name** – *accept the default value of ReportServer.*
- **Language** – *specify the desired language option from the drop-down menu.*
- **Report Server Mode** – *select the **Native Mode** option.*

Click **Next** to continue.



In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.	
In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.	
The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.	

In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.



In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer_SCOMASRS** in the provided text box.

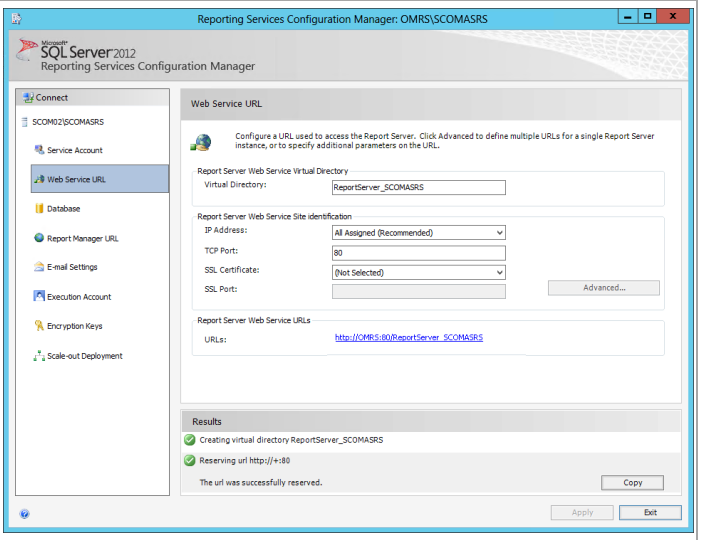
- In the **Report Server Web Service Site Identification** section, set the following values**:**

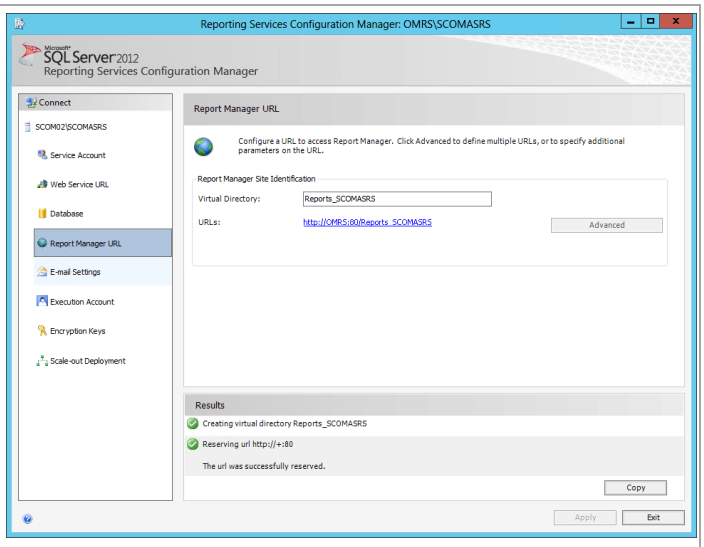
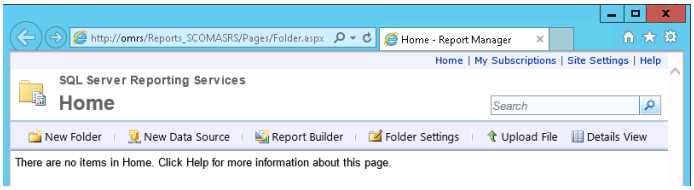
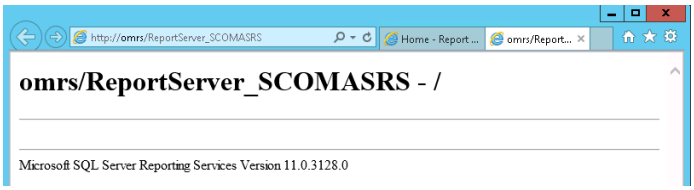
    - **IP Address** – *set the **All Assigned** drop-down menu value.*

    - **TCP Port** – *specify the desired TCP Port (default 80).*

    - **SSL Certificate** – *select the available certificate or choose the default of (Not Selected).*

Click the **Apply** button to save the settings and create the Web Service URL.



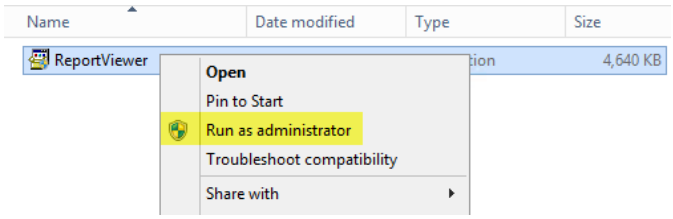
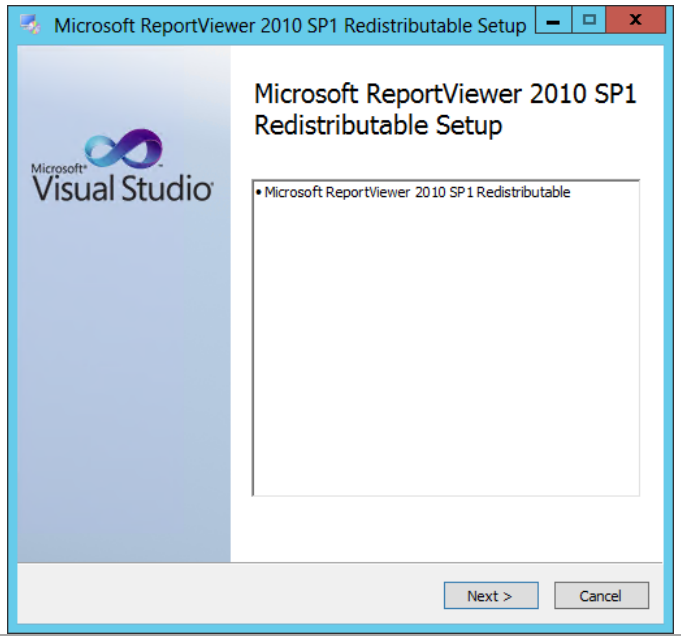
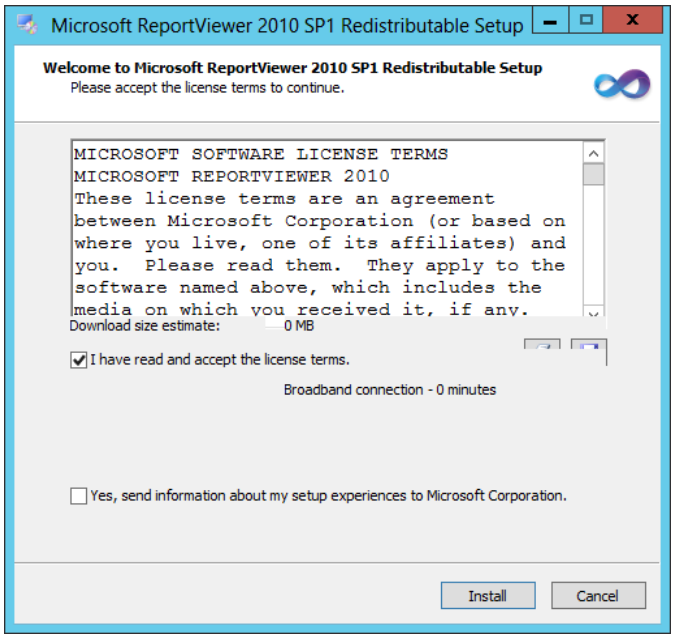
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value: • In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports_SCOMASRS** in the provided text box. Click the **Apply** button to save the settings and create the Report Manager URL.	
Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.	
Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly. **Note:** In order to test the URL directory from the Operations Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.	
Close the Reporting Server Configuration Manager.	

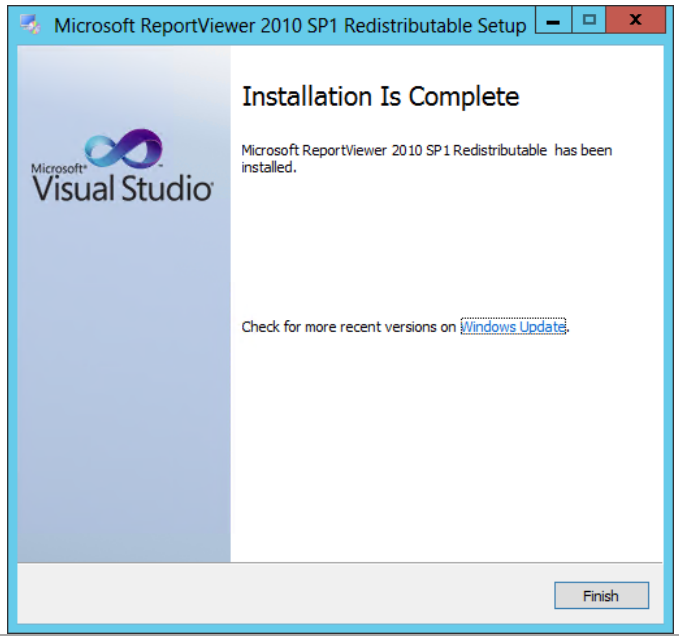
Install Microsoft Report Viewer 2010 SP1

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package to be installed prior to the installation of Operations Manager[11]. Follow the provided steps to install Microsoft Report Viewer 2010 SP1.

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

[11] Microsoft Report Viewer 2010 SP1 Redistributable Package - http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.	
Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.	
Select the **I have read and accept the license terms** check box and click **Install**.	

The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.	

Configuration of Operations Manager SQL Server Prerequisites

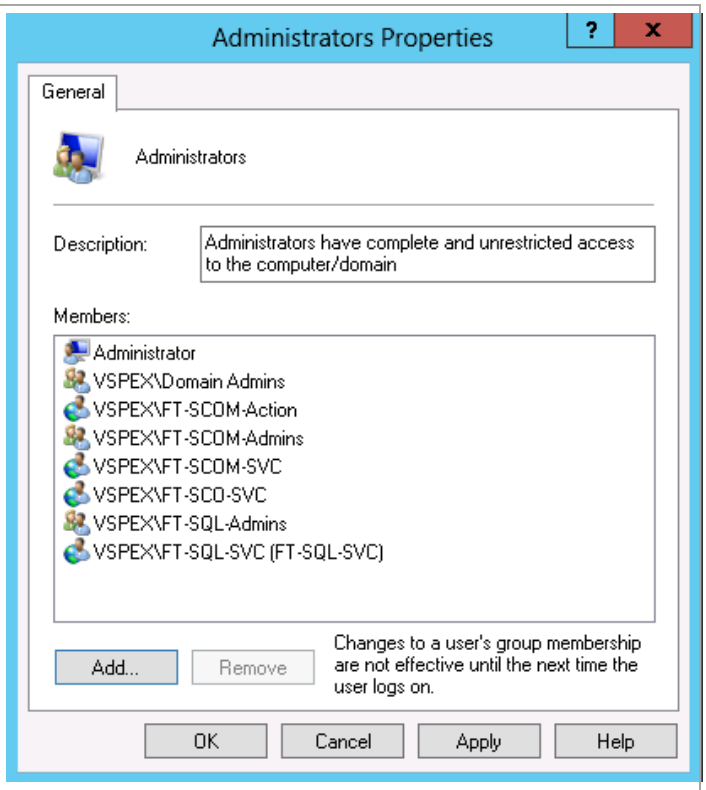
The following prerequisite steps must be completed prior to the installation of Operations Manager roles[12].

- Perform the following steps on the **Operations Manager management server** virtual machines.

[12] Deploying System Center 2012 - Operations Manager - http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin.

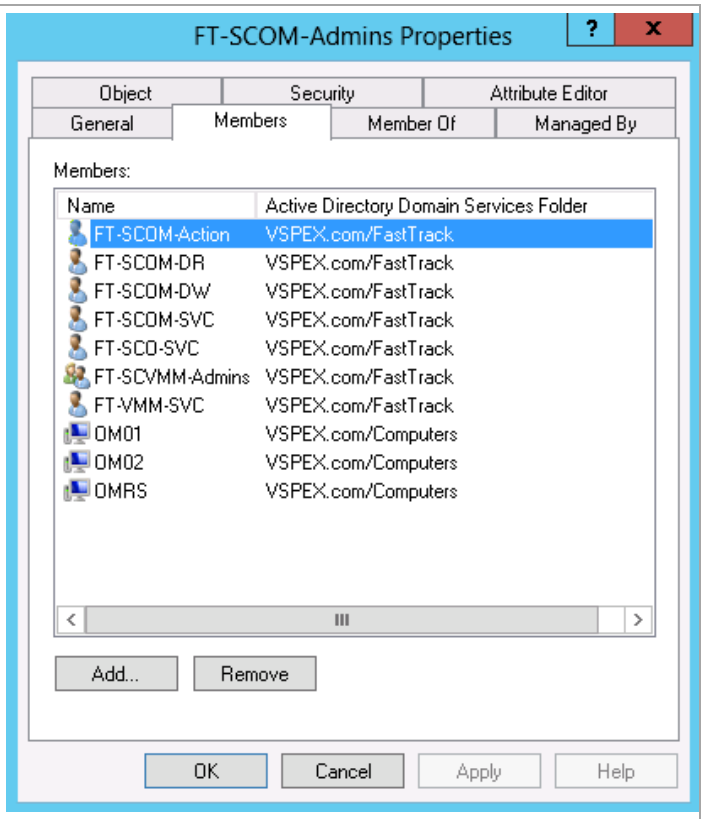
Log on to the Operations Manager virtual machine as a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager virtual machine:

- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.



▶ Perform the following step on an **Active Directory Domain Controller** in the target environment.

In the domain where Operations Manager will be installed, verify that the Operations Manager computer account and the groups outlined in the table above are members of the OM Admins group created earlier.

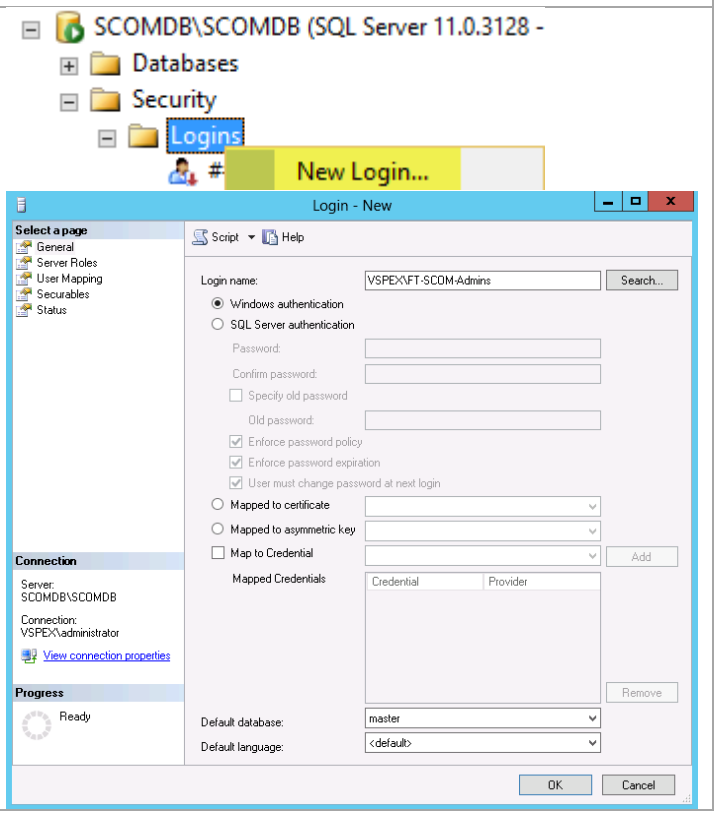


▶ Perform the following steps on the **primary SQL Server cluster node**.

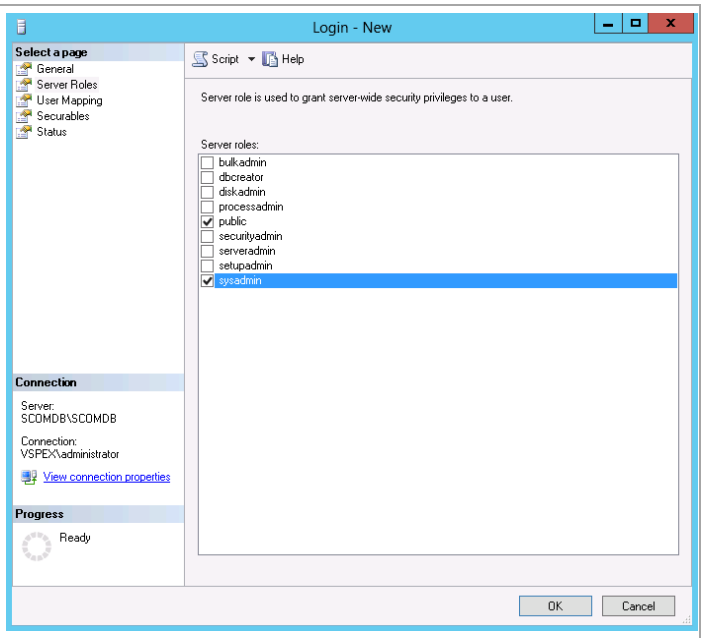
Using Administrative credentials, log on to the first SQL Server and open SSMS. Connect to the Operations Manager SQL Server instance using the values specified earlier. Create a new login by navigating to the **Logins** node under **Security** within SQL Management Studio. Right-click the **Logins** node and select **New Login…** from the context menu.

In the **Login – New** dialog, specify the Operations Manager Admins group created earlier as the new **Login name**.

Before clicking **OK** to create the new login, perform the next step.



While still in the **Login – New** dialog, select the **Server Roles** page. Select the **sysadmin** role and click **OK** to add this login to the sysadmin role of the instance.



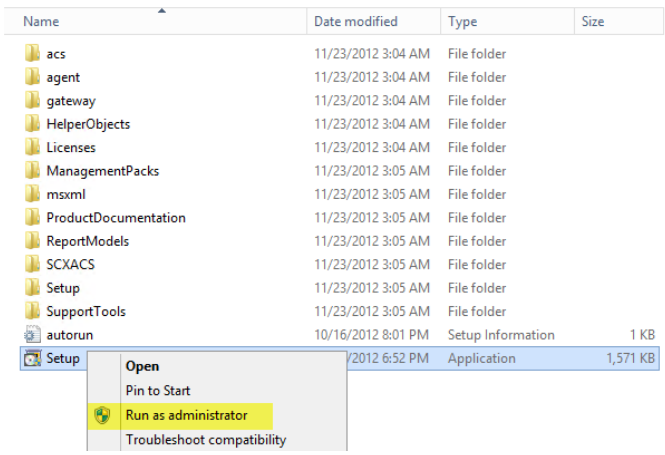
10.3 Installation

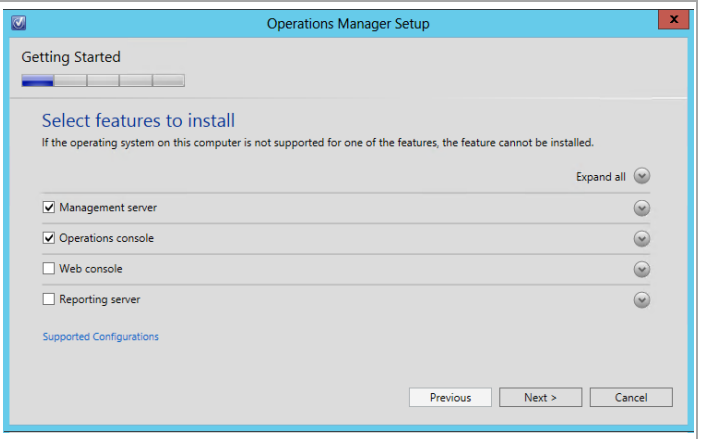
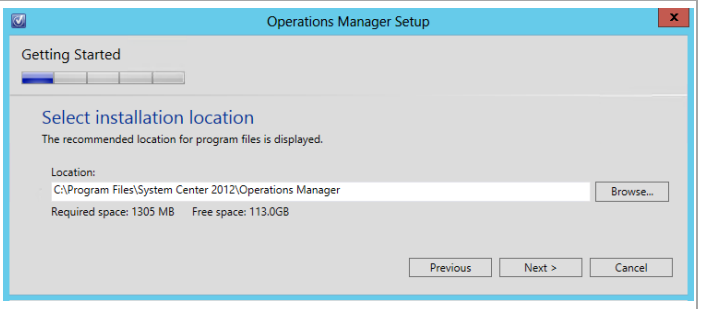
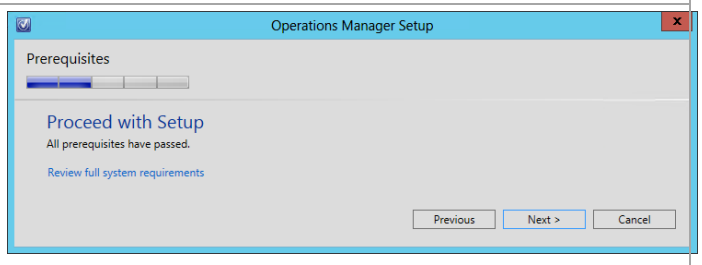
Install the Operations Manager Management Server

The following steps must be completed in order to install and configure the Operations Manager database and server roles.

▶ Perform the following steps on the first **Operations Manager management server** virtual machine.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

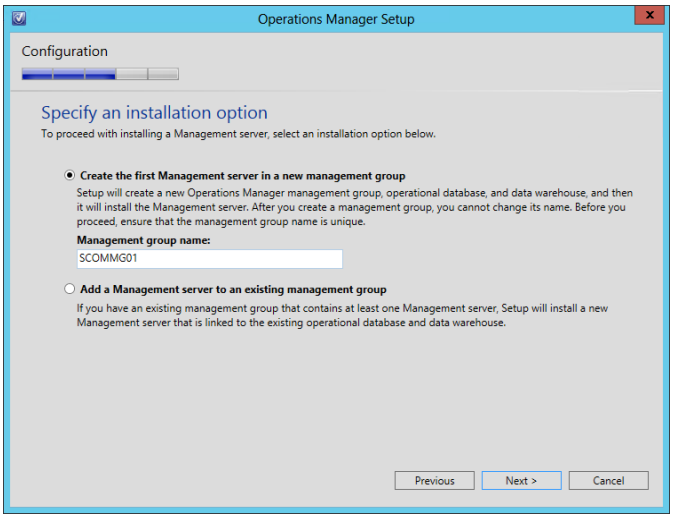


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.	
In the **Select features to install** dialog, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.	
The setup will verify that all system pre-requisites are met in the **Proceed with Setup** dialog. If any pre-requisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.	

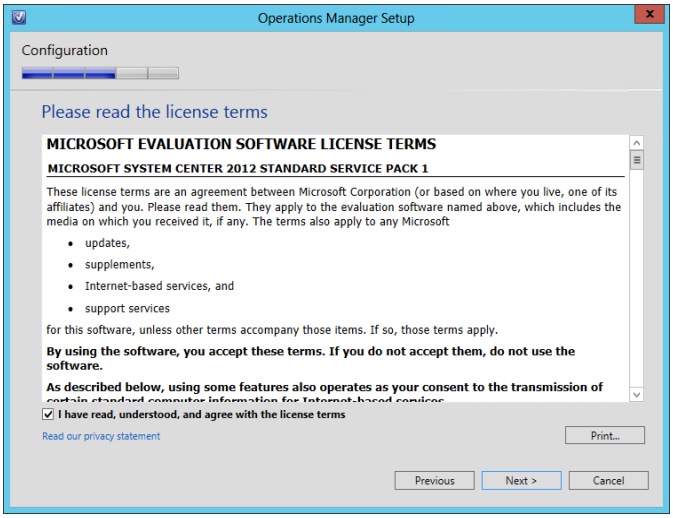
In the **Specify an installation option** dialog, two installation options are provided:

- **Create the first management server in a new management group**.
- **Add a Management server to an existing management group**.

Select the **Create the first Management server in a new management group** option and supply a unique name in the **Management group name** text box. Note that this name must be unique across System Center products.
Click **Next** to continue.



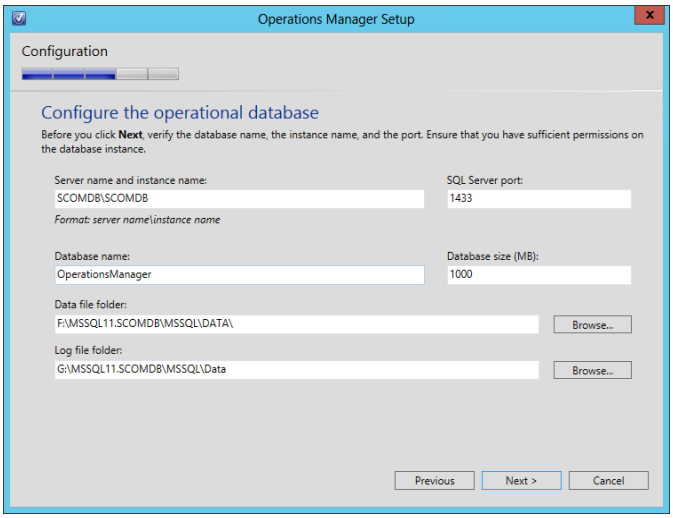
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the terms of the license agreement installation** option check box is selected and click **Next** to continue.



In the **Configure the operational database** dialog, Specify the following information in the provided text boxes:

- **Server name and instance name** – *specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.*
- **SQL Server port** – *specify the TCP port used for SQL Server connectivity (1433 is the default, however this may be different based on instance requirements outlined earlier).*
- **Database name** – *specify the name of the Operations Manager database. In most cases the default value of OperationsManager should be used.*
- **Database size (MB)** – *specify the initial database size.* [13] *The following values can be used as a general guideline:*
    - *Up to 500 agents: 12 GB.*
    - *Up to 1000 agents: 24 GB.*
- **Data file folder** – *specify the drive letter associated in the SQL Server cluster for the database data files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.*
- **Log file folder** – *specify the drive letter associated in the SQL Server cluster for the log files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.*

Click **Next** to continue.

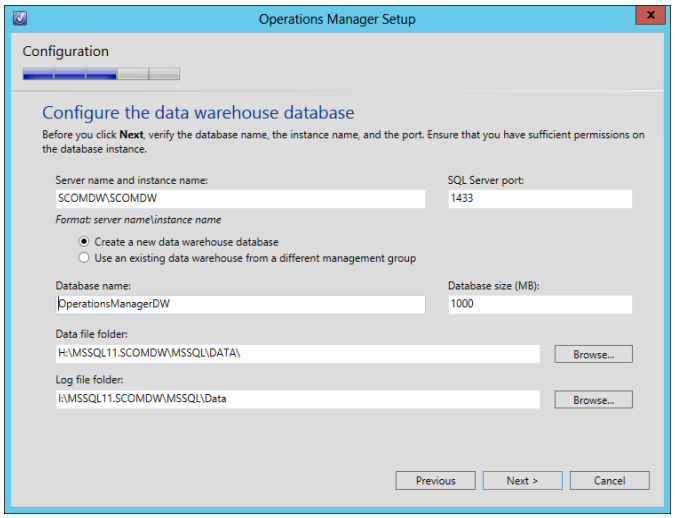


[13] System Center 2012 - Operations Manager Component Add – On - http://www.microsoft.com/en-us/download/details.aspx?id=29270 provides general guidance for database sizing.

In the **Configure the data warehouse database** dialog, specify the following information in the provided text boxes:

- **Server name and instance name** – *specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.*
- **SQL Server port** – *specify the TCP port used for SQL Server connectivity (1433 by default, however this may be different based on instance requirements outlined earlier).*
- **Database name** – *specify the name of the Operations Manager Data Warehouse database. In most cases the default value of OperationsManagerDW should be used.*
- **Database size (MB)** – *specify the initial database size. [14] The following values can be used as a general guideline:*
    - *Up to 500 agents: 356 GB.*
    - *Up to 1000 agents: 720 GB.*
- **Data file folder** – *specify the drive letter associated in the SQL Service cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.*
- **Log file folder** – *specify the drive letter associated in the SQL Server cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.*

Click **Next** to continue.

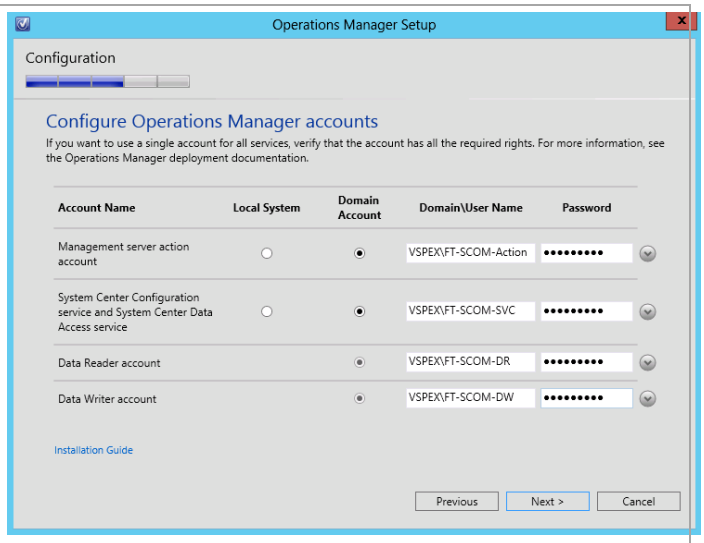


[14] System Center 2012 - Operations Manager Component Add – On - http://www.microsoft.com/en-us/download/details.aspx?id=29270 provides general guidance for database sizing.

In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- **Management server action account.**
- **System Center Configuration service and System Center Data Access service.**
- **Data Reader account.**
- **Data Writer account.**

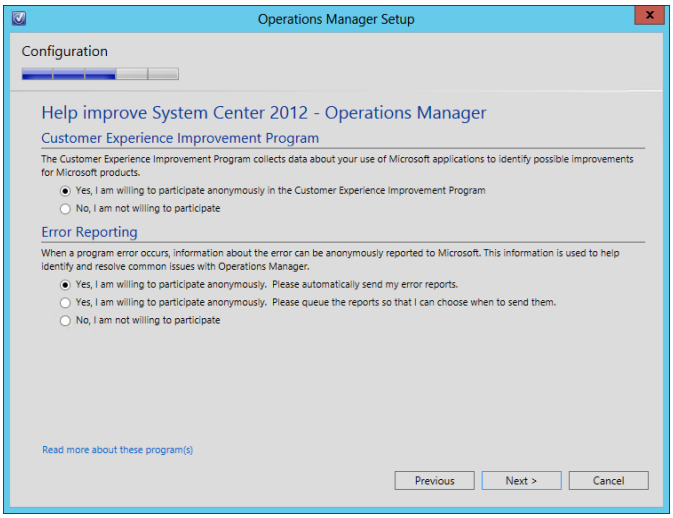
If the use of a Domain Account is specified, enter the user account information as *<DOMAIN>\<USERNAME>* and enter the appropriate password.
Once completed, click **Next** to continue.



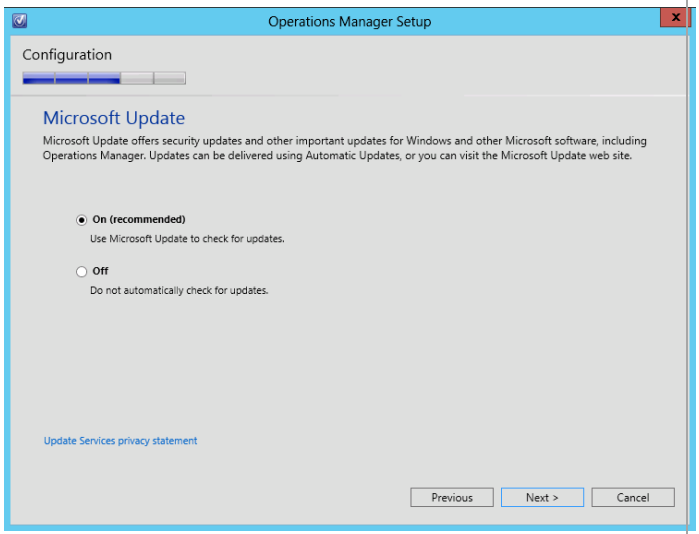
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

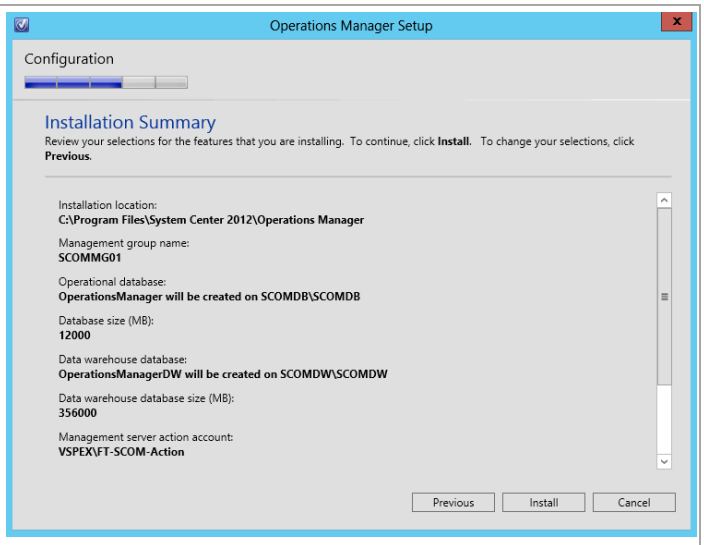
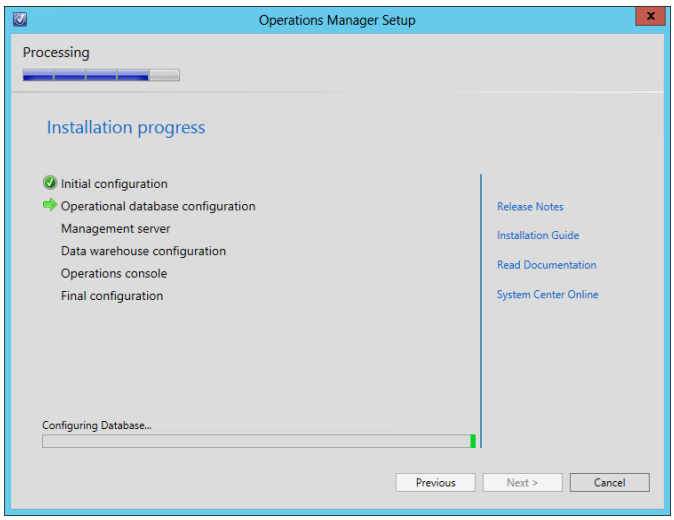
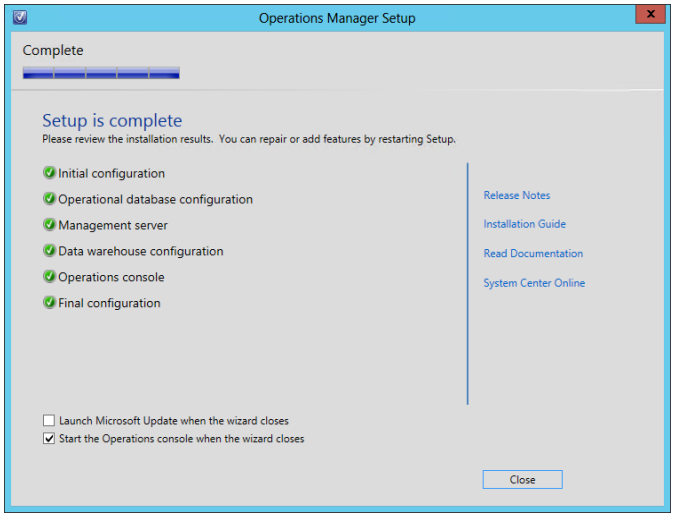
- **Customer Experience Improvement Program.**
- **Error Reporting.**

Select the appropriate option based on your organization's policies and click **Next** to continue.

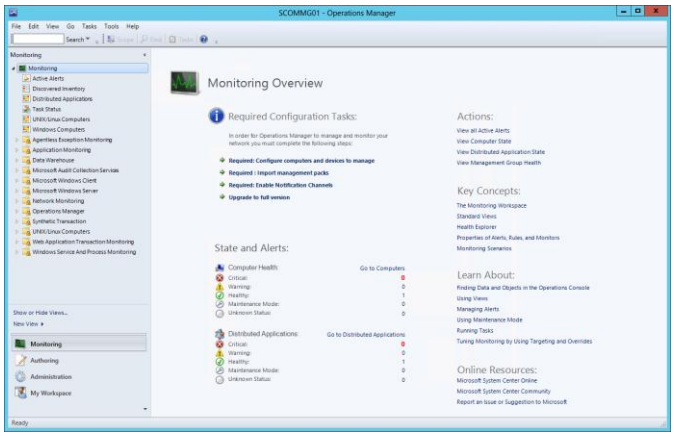


The **Microsoft Update** dialog provides options for setting automatic updating**.** Select the appropriate option based on your organization's policies and click **Next** to continue.



The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue. **Note:** Ensure you set the database sizes appropriately for your particular deployment.	
The wizard will display the progress while installing features.	
When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.	

When completed, the **Operations Manager** console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.

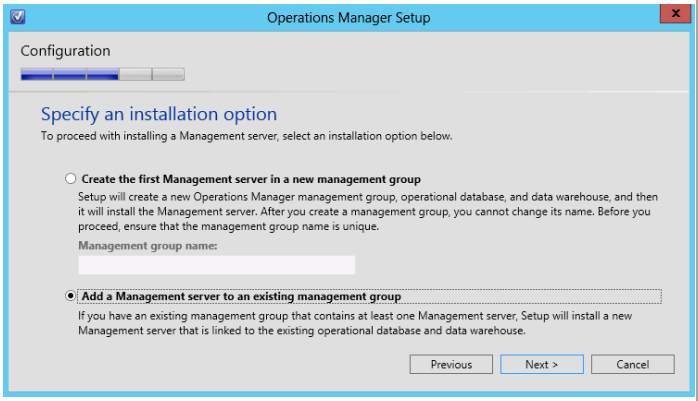


Install the Second Operations Manager Management Server

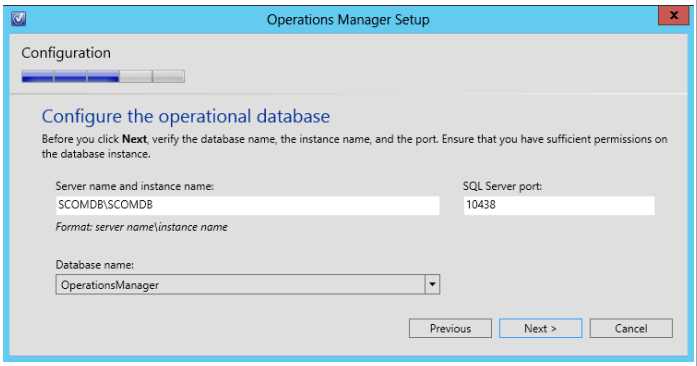
Installation of the second Operations Manager management server is almost identical to installing the first server. The following steps show which setup entries are different during installation.

▶ Perform the following steps on the second **Operations Manager management server** virtual machine.

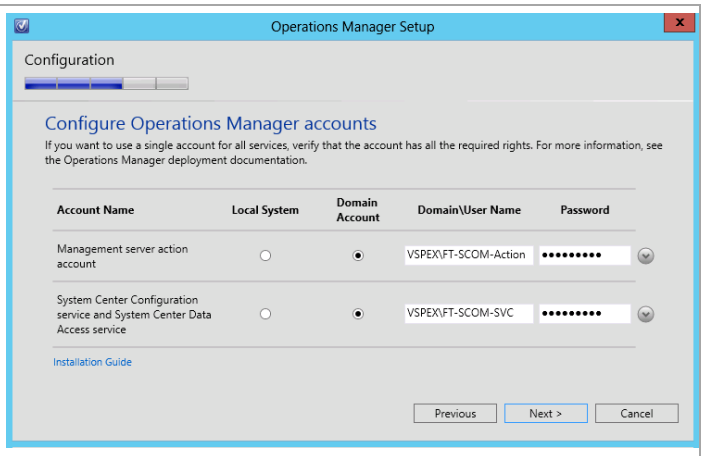
On the **Configuration/Specify and installation** option screen of setup, select the **Add a Management server to an existing management group** radio button.
Click **Next** to continue.



On the **Configuration/Configure the operational database** screen of setup, specify the CNO and database instance name of the Operations Manager database. Specify the port number that you assigned to this instance. From the dropdown list of the Database name field, select the OperationsManager database.
Click **Next** to continue.



On the **Configuration/Configure Operations Manager accounts** screen of setup, specify the Management server action account and Configuration service and data access accounts with the appropriate passwords.
Click **Next** to continue.

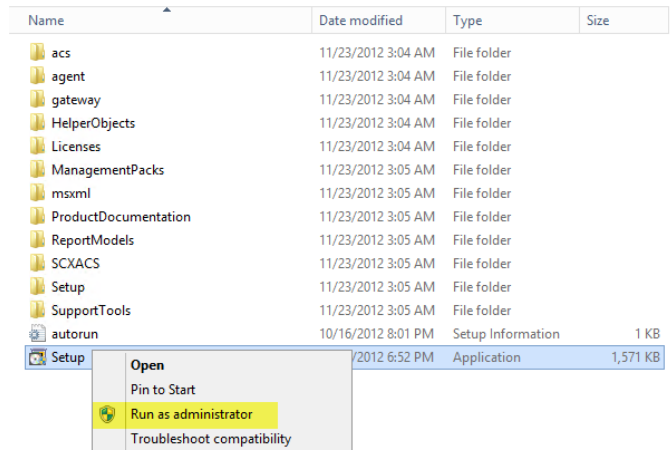


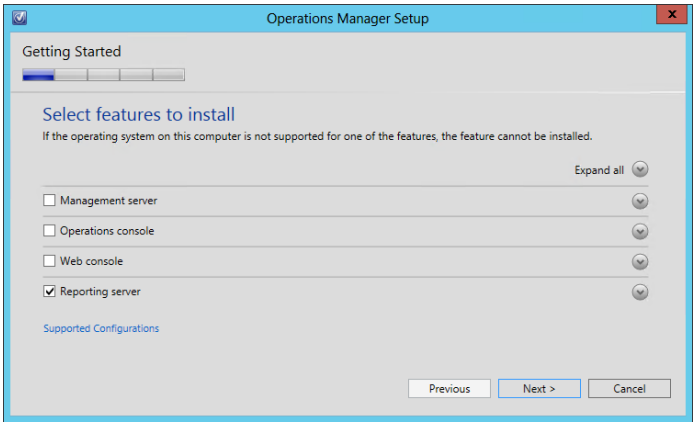
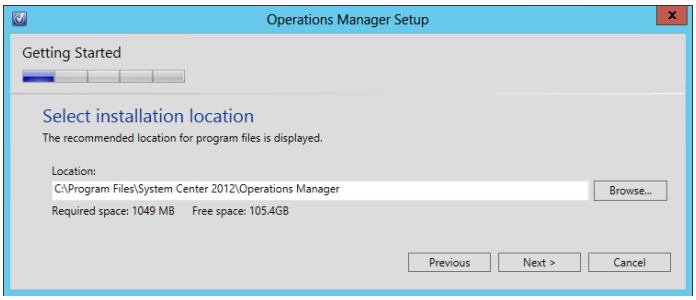
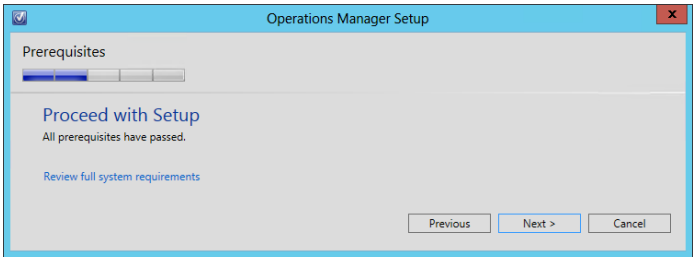
Install the Operations Manager Reporting Server

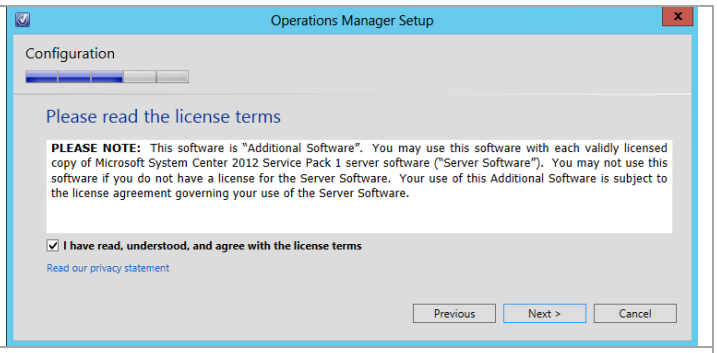
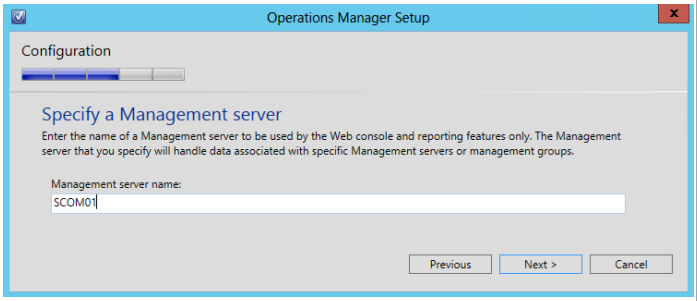
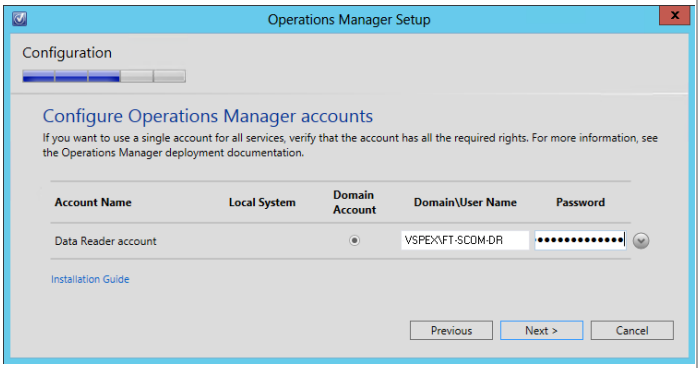
The following steps must be completed in order to install and configure the Operations Manager reporting server role.

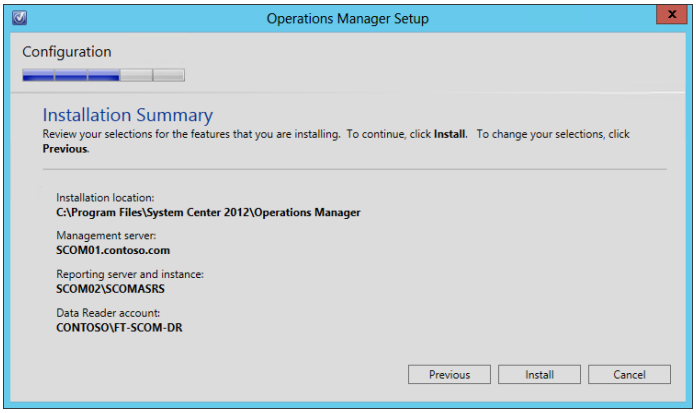
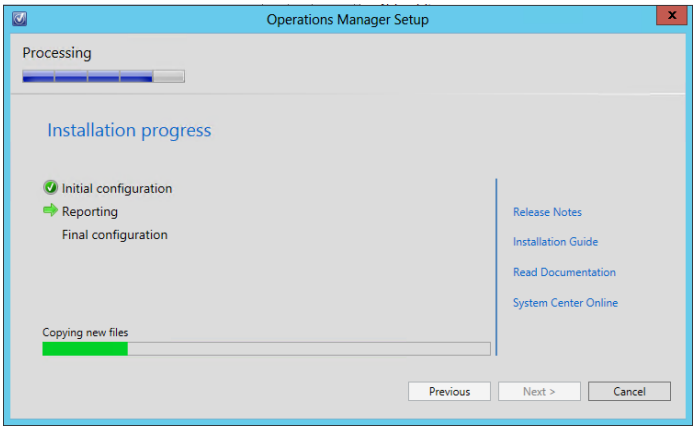
▶ Perform the following steps on the **Operations Manager reporting server** virtual machine.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

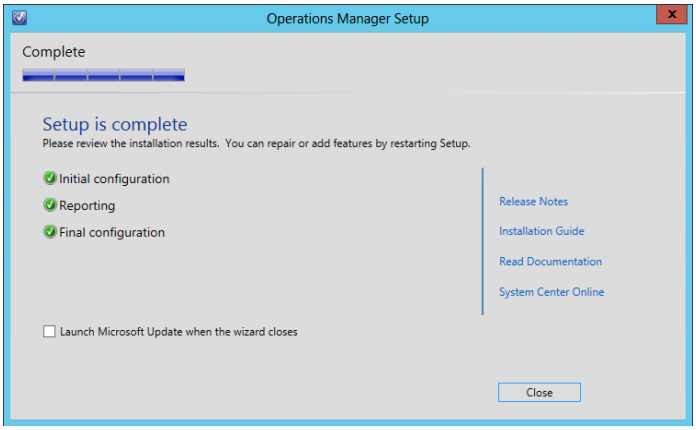


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.	
In the **Select features to install** dialog, verify that the **Reporting server** check boxes are selected. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.	
The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.	

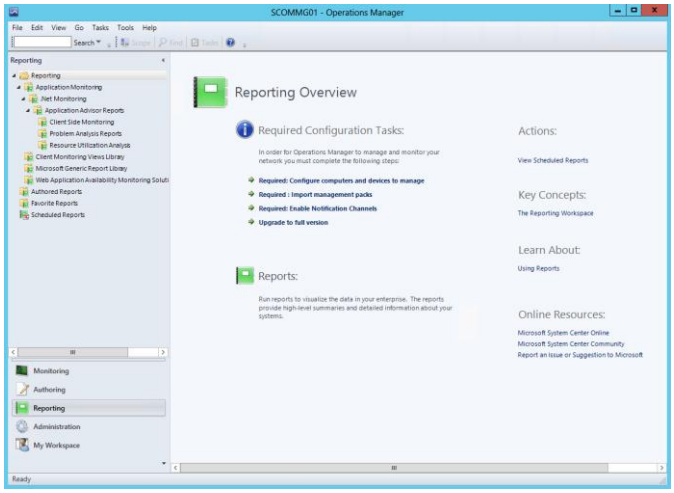
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.	
In the **Specify a Management server** dialog, type the name of the previously installed management server in the **Management server name** text box. Click **Next** to continue.	
In the **SQL Server instance for reporting services** dialog, select the SQL Server instance hosting the local SQL Server Reporting Services and SQL Server Analysis Services from the drop-down menu created during earlier steps. Click **Next** to continue.	
In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options: • **Data Reader account.** If the use of a Domain Account is specified, enter the user account information as *<DOMAIN>\<USERNAME>* and enter the appropriate password. When completed, click **Next** to continue.	

The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. This includes: • **Operational Data Reporting (ODR).** Select the appropriate option based on your organization's policies and click **Next** to continue.	
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
The wizard will display the progress while installing features.	

When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch Microsoft Update when the wizard closes** check box is selected and click **Close** to complete the installation.



When completed, open the Operations Manager console from the first management server. From this console, the installation can be validated by noting that the **Reporting** node is now visible in the console.



10.4 Post-Installation Tasks

When the installation is complete, the following tasks must be performed to complete Operations Manager and Virtual Machine Manager Integration.

Register Service Principal Names for the Operations Manager Management Servers

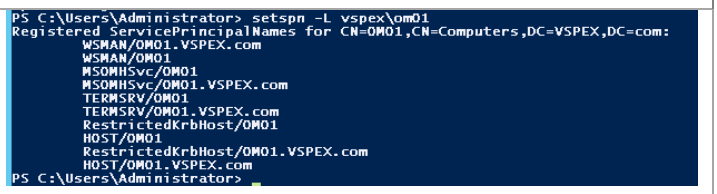
The following steps must be performed on a Domain Controller or one of the Operations Manager servers using a domain admin account or an account with permissions to create SPNs.

▶ Perform the following steps on a **Domain Controller** in the domain where Operations Manager is installed.

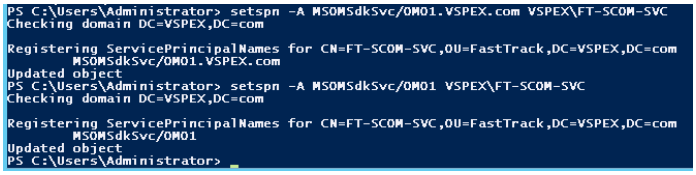
The Operations Manager Health Service SPN's should be set automatically by the Management Server's computer account. To confirm the SPN's set correctly open an administrative command prompt and execute the following command:

`SETSPN -L <DOMAIN>\<SERVERNAME>`

Where <DOMAIN> is the Active Directory domain name where the Operations Manager management server is installed and <SERVERNAME> is the name of the Operations Manager Management

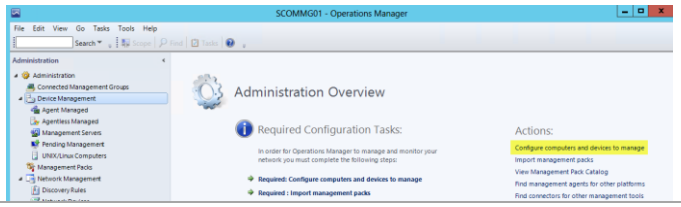


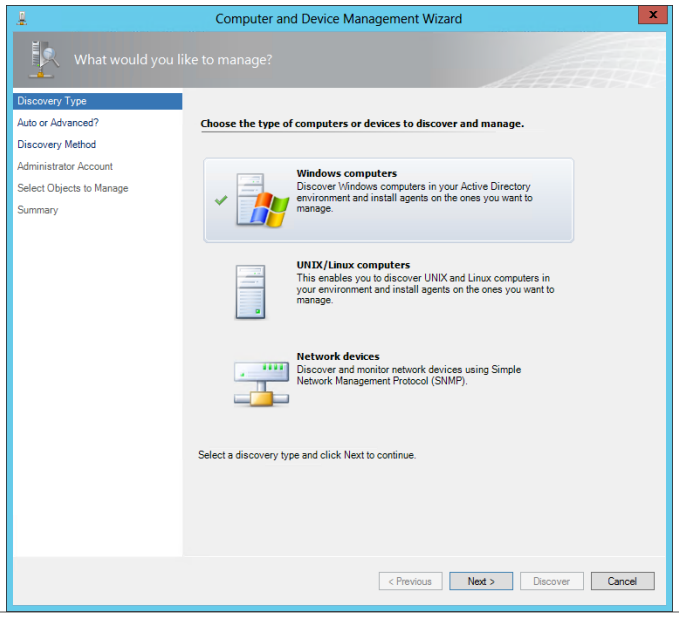
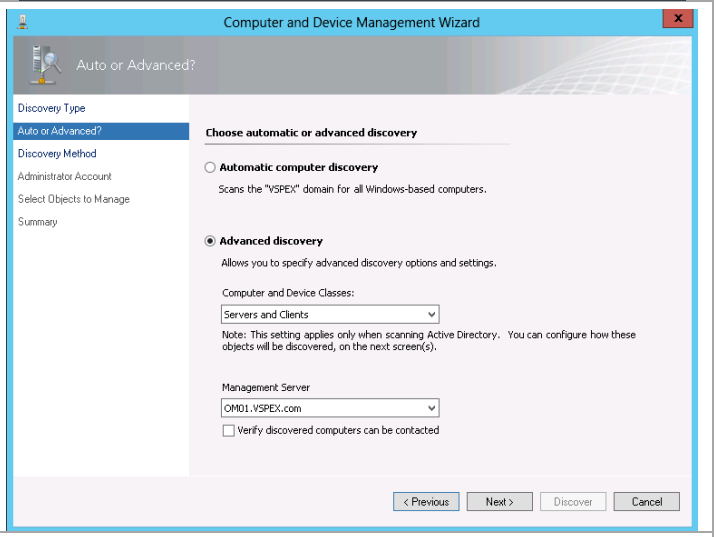
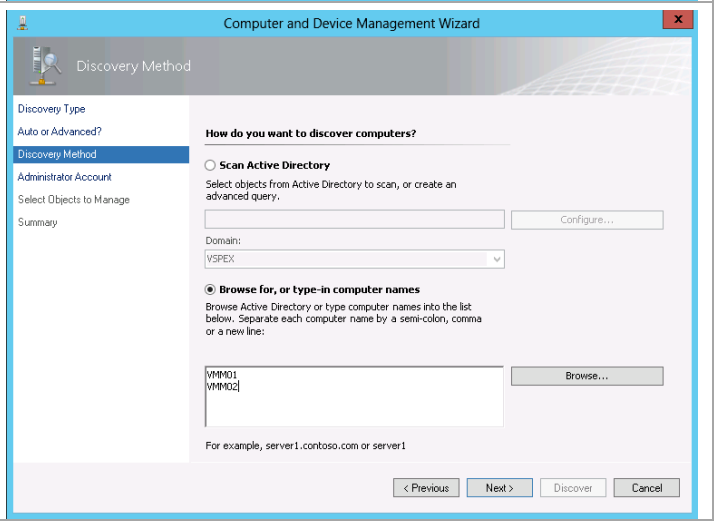
Server.	

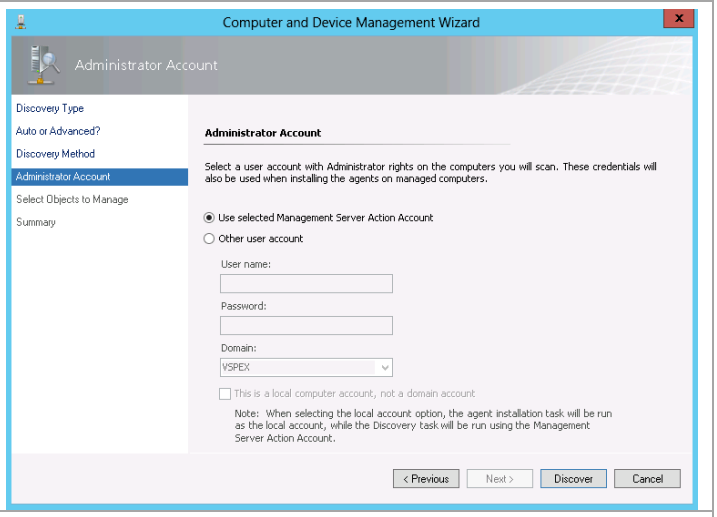
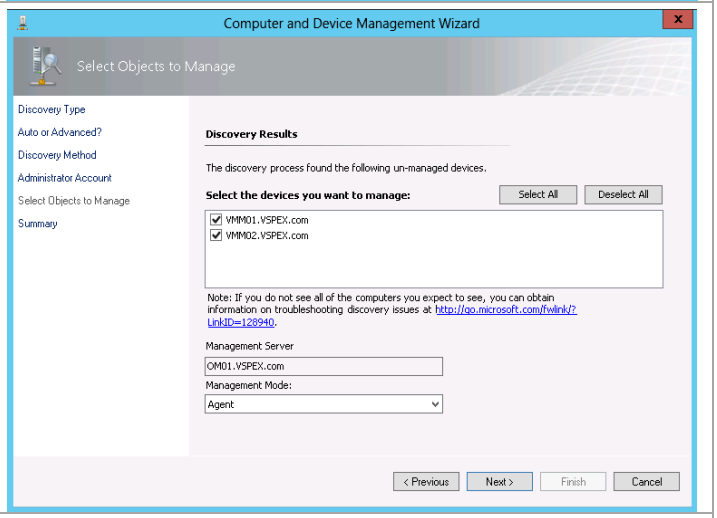
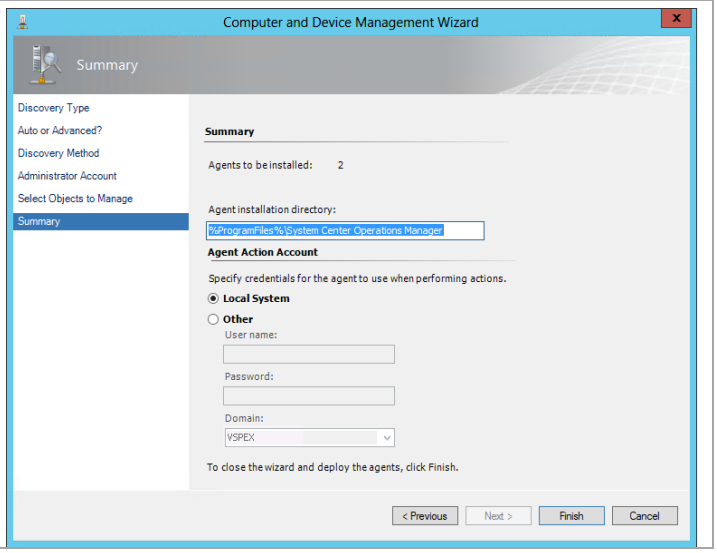
The Data Access Service account runs under a domain user account context and is not able to create the appropriate SPNs in Active Directory. The following command must be executed by a domain admin account or an account with delegated permissions to user objects.
To set the SPN run the following commands from an administrative command prompt:
`SETSPN.exe -A MSOMSdkSvc/<ManagementServerFQDN> <domain>\<SDKServiceAccount>`
`SETSPN.exe -A MSOMSdkSvc/<ManagementServerNetBIOS> <domain>\<SDKServiceAccount>`
Where <ManagementServerFQDN> is the name of the Operations Manager management server and <SDKServiceAccount> is the name of the Operations Manager Service Account.
If there is more than one Management Server being deployed then these commands must be run for each Management Server.
	

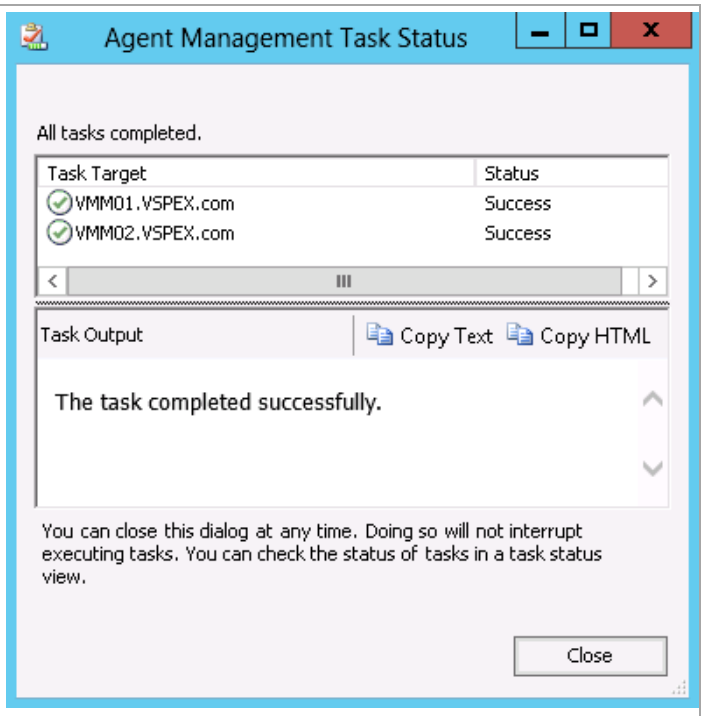
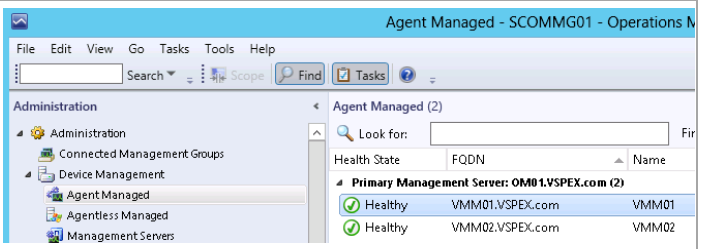
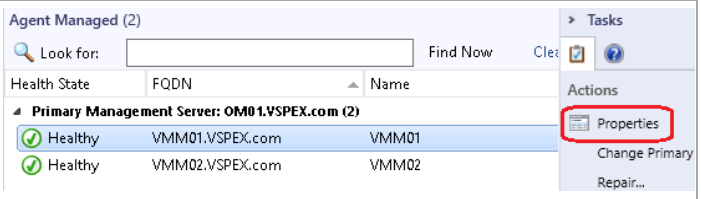
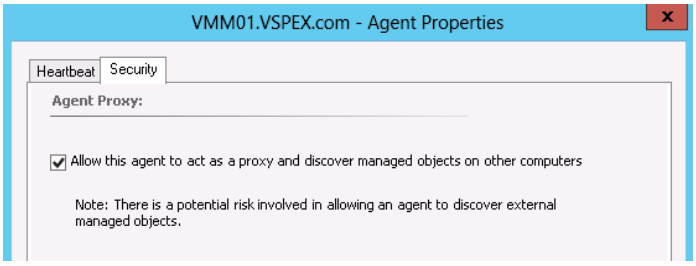
Once complete the SPNs can be confirmed with the following command: `SETSPN -L <DOMAIN>\<SDKServiceAccount>`	

Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Servers

▶ Perform the following steps on the **Operations Manager management server** virtual machine.	
In **Operations Manager** console, navigate to the **Administration** workspace. Under **Actions**, select **Configure computers and devices to manage**.	

The **Computer and Device Management Wizard** will appear. In the **Discovery Type** dialog, select **Windows computers** from the available options and click **Next** to continue.	
In the **Auto or Advanced?** dialog, select the **Advanced discovery** option. Click **Next** to continue.	
In the **Discovery Method** dialog box, under **Browse for, or type-in computer names**, input the names of both VMM servers. Click **Next** to continue.	

In the **Administrator Account** dialog, select the **Use selected Management Server Action Account**. Click **Discover** to start the discovery process.	
In the **Select Objects to Manage** dialog, review the Discovery Results and select the VMM servers. From the **Management Mode** drop-down menu, select **Agent** and click **Next** to continue.	
In the **Summary** dialog, accept the default **Agent installation directory** as *%ProgramFiles%\System Center Operations Manager*. In the **Agent Action Account** section, select the **Local System** option. Once complete, click **Finish** to perform the agent installation.	

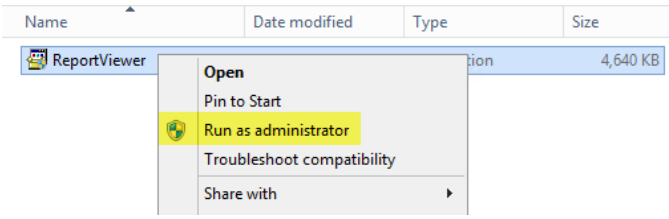
In the **Agent Management Task Status** dialog, verify that the agent installation completes successfully. Once successful, click **Close** to complete the operation.	
The next step is to enable the Operations Manager agent deployed to the Virtual Machine Manager management server to be a proxy agent. In **Operations Manager** console, navigate to the **Administration** workspace, expand the **Device Management** node and select the **Agent Managed** view. **Note:** It can take a few minutes for the Health State to transition from Not Monitored to Healthy.	
In the **Agent Managed** pane, select the agent associated with the VMM Management Server and click **Properties** in the task pane.	
In the **Agent Properties** dialog, select the **Security** tab. Verify that the **Allow this agent to act as a proxy and discover managed objects on other computers** check box is selected. Click **OK** to save the changes. Repeat this process for the second VMM server.	

Install Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server

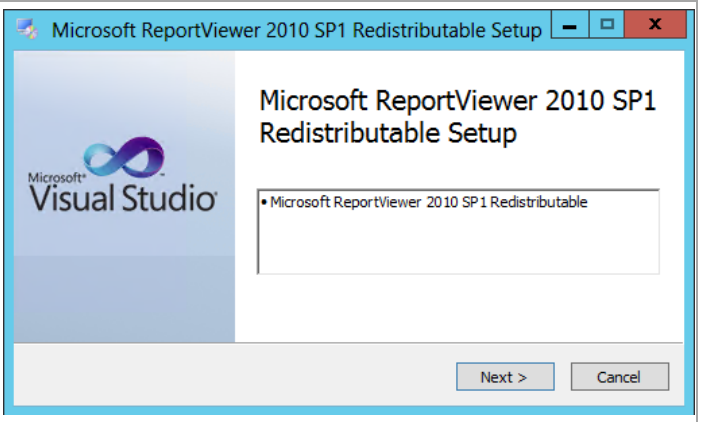
Additionally, the Operations Manager console installation requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation. Follow the provided steps to install the Microsoft Report Viewer 2010 SP1 package.

▶ Perform the following steps on each **Virtual Machine Manager** virtual machine.

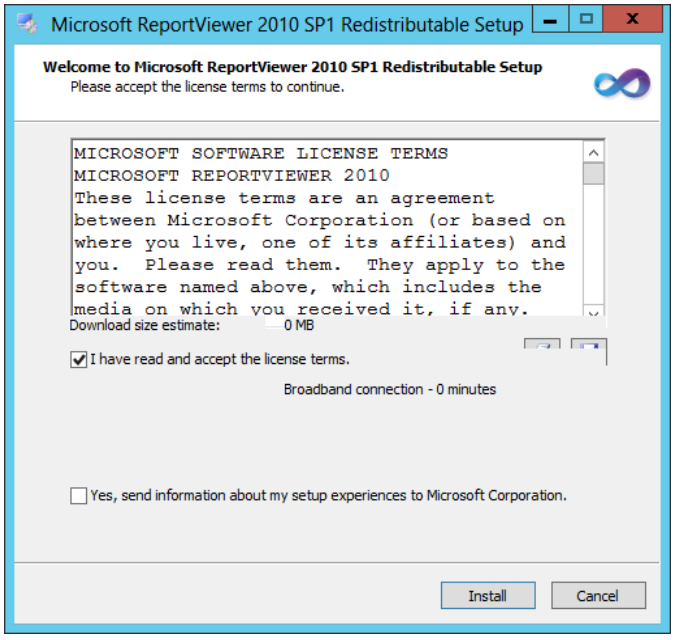
From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



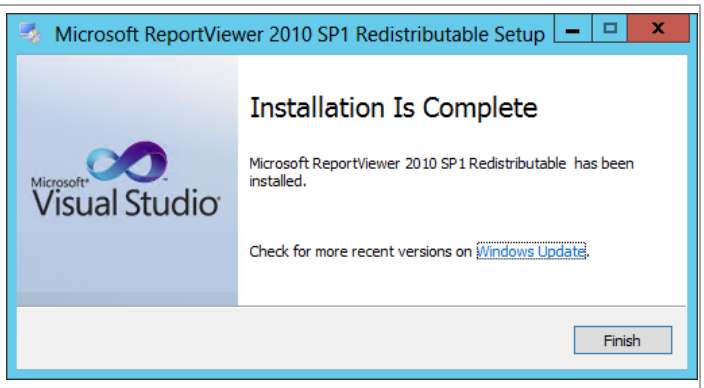
Within the Microsoft ReportViewer 2010 SP1 Redistributable Setup dialog, select Next to begin the installation.



Select **I have read and accept the license terms** check box and click **Install**.



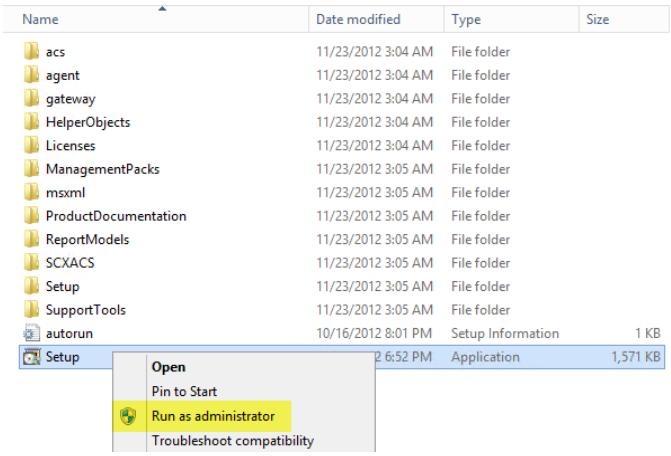
The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.



Install Operations Manager Console on the VMM Management Server

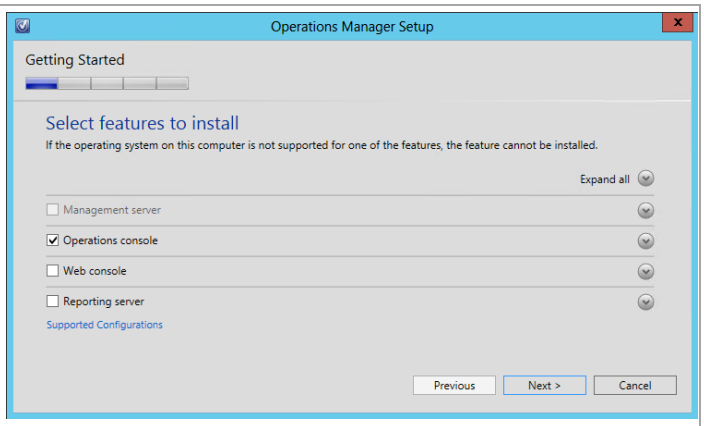
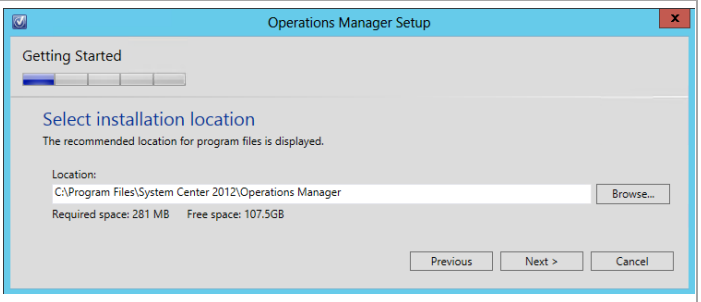
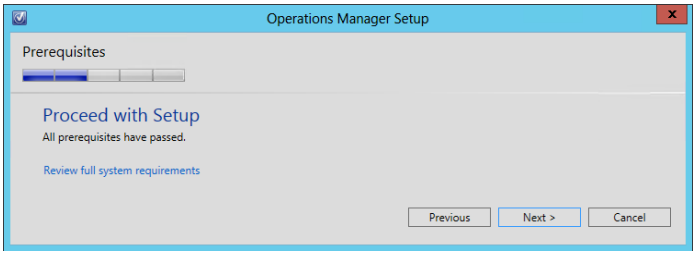
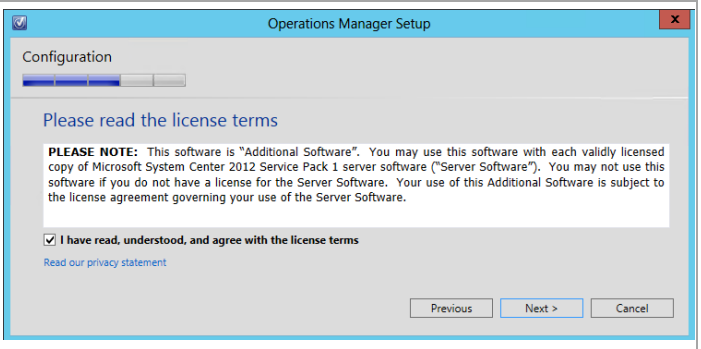
▶ Perform the following steps on each **Virtual Machine Manager** virtual machine.

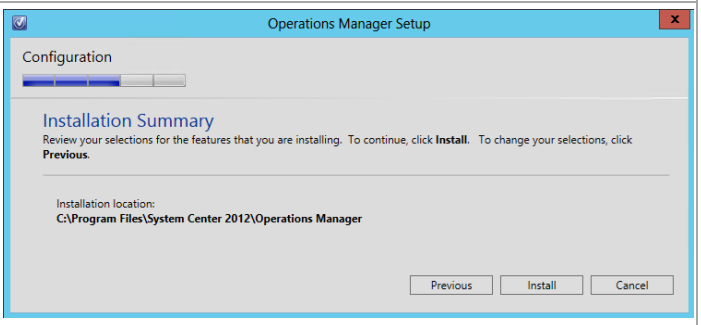
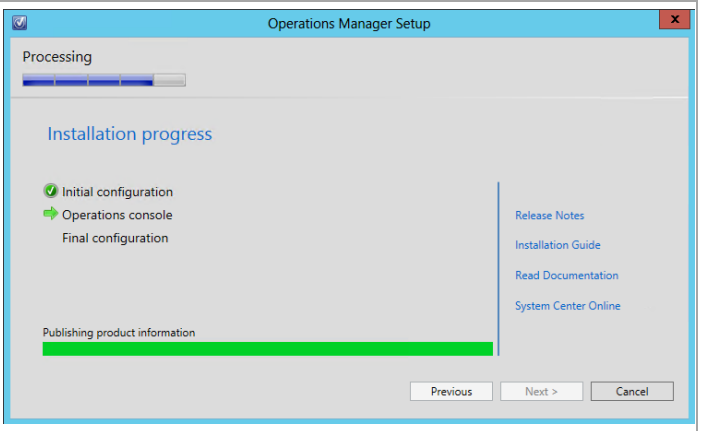
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

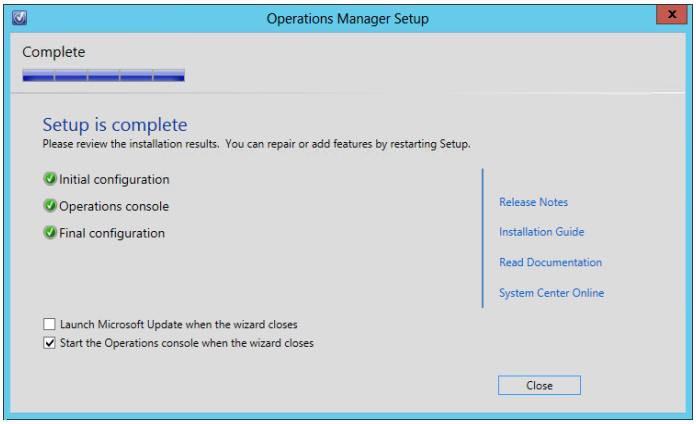
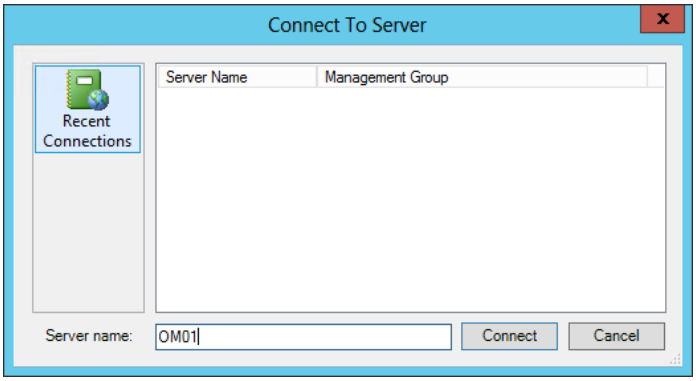
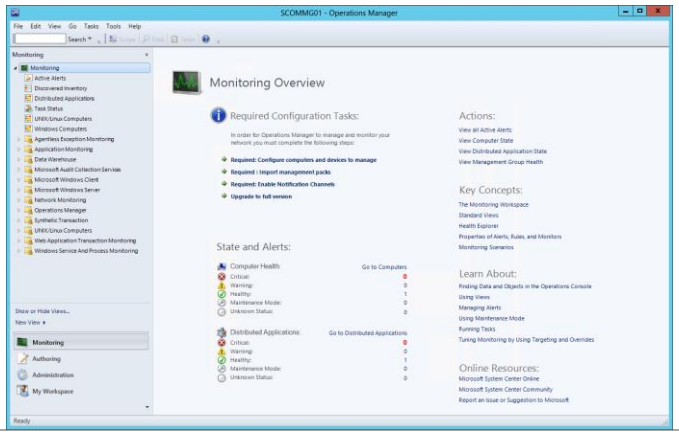


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.	
The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.	
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.	

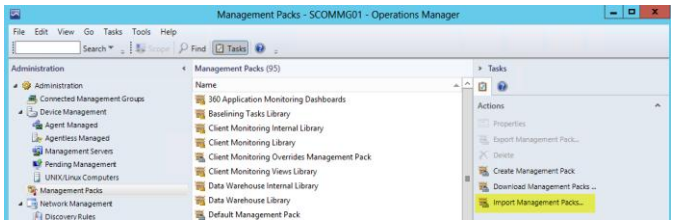
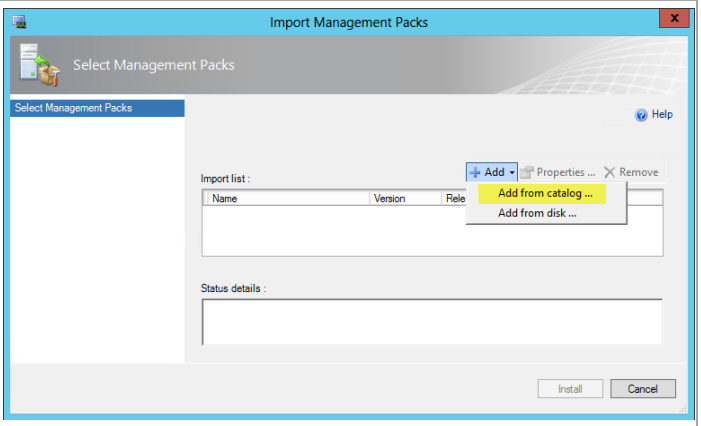
The **Help Improve System Center 2012 – Operations Manager** dialog provides options for participating in various product feedback mechanisms. These include: • **Customer Experience Improvement Program.** • **Error Reporting.** Select the appropriate option based on your organization's policies and click **Next** to continue.	
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
The wizard will display the progress while performing the installation.	

When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Management console when the wizard closes** check box is selected and click **Close** to complete the installation.	
When completed, the **Operations Manager console** will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.	 

Download and Import the Prerequisite Operations Manager Management Packs in Operations Manager

In order to start monitoring the environment with Operations Manager, some prerequisite management packs need to be downloaded and imported.

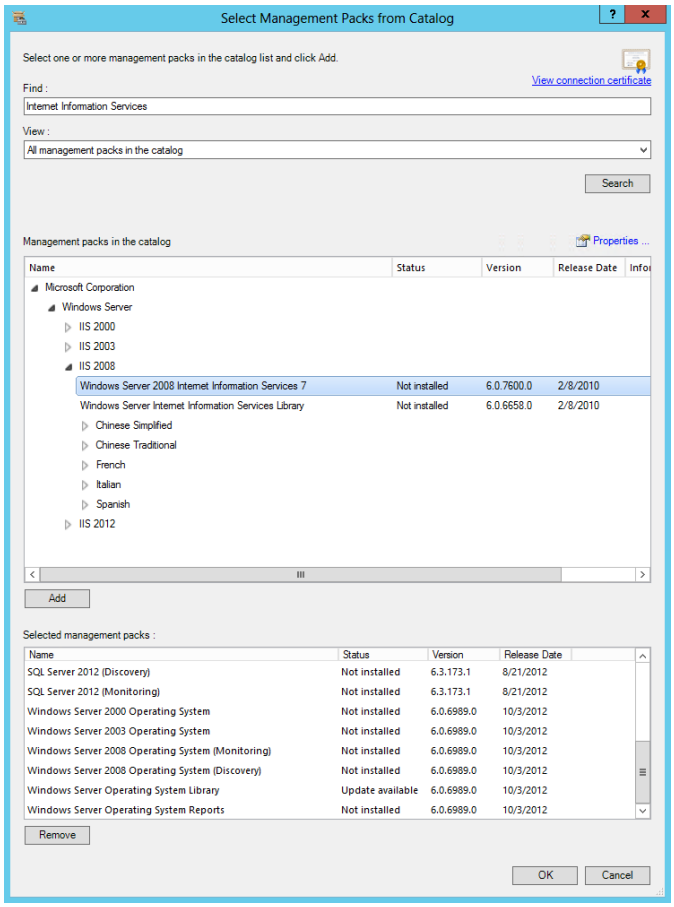
▶ Perform the following steps on the **Operations Manager** virtual machine.

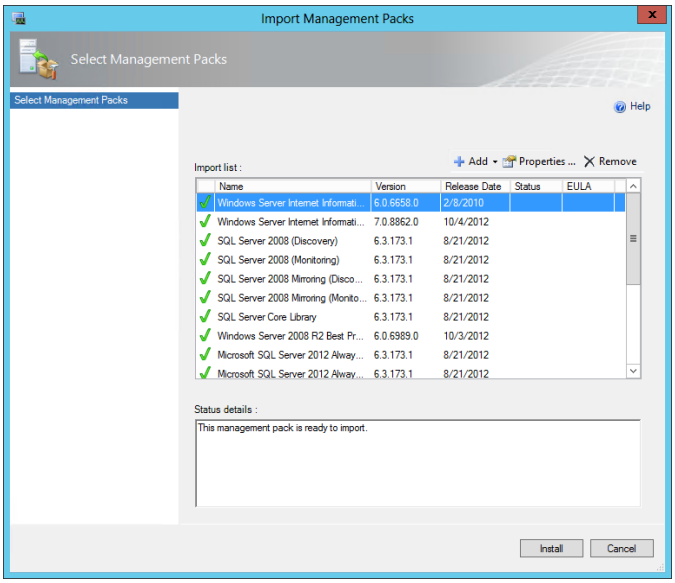
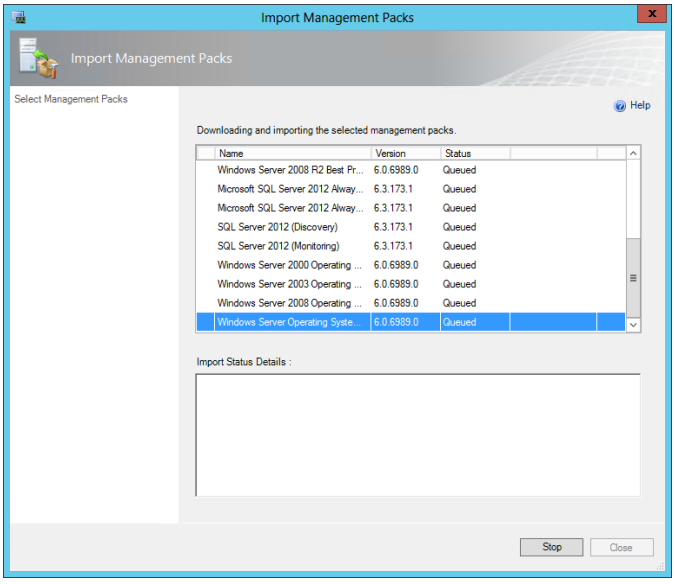
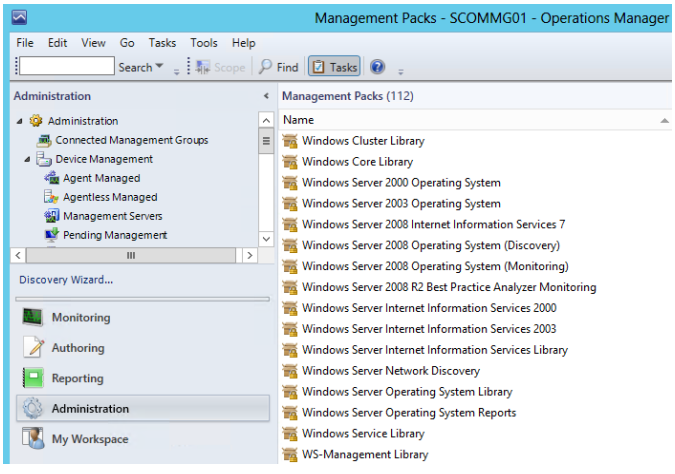
In the **Operations Manager** console, navigate to the **Administration** pane and select the **Management Packs** node. In the **Actions** pane, click **Import Management Packs…**	
In the **Select Management Packs** dialog, click the **Add** button and select **Add from catalog…** in the drop-down menu. **Note:** If you have already downloaded the management packs to disk, you can select **Add from disk…**	

In the **Select Management Packs from Catalog** dialog, find and add the following management packs:

- Windows Server Internet Information Services Library Version 6.0.6658.0
- Windows Server Internet Information Services Library Version 7.0.8862.0
- Windows Server Internet Information Services 2000 Version 6.0.6658.0
- Windows Server Internet Information Services 2003 Version 6.0.6658.0
- Windows Server 2008 Internet Information Services 7 Version 6.0.6658.0
- SQL Server 2008 (Discovery) version 6.3.173.1
- SQL Server 2008 (Monitoring) version 6.3.173.1
- SQL Server 2008 Mirroring (Discovery) version 6.3.173.1
- SQL Server 2008 Mirroring (Monitoring) version 6.3.173.1
- SQL Server Core Library version 6.3.173.1
- SQL Server 2012 (Discovery) version 6.3.173.1
- SQL Server 2012 (Monitoring) version 6.3.173.1
- Windows Server 2008 R2 Best Practice Analyzer Monitoring version 6.0.6989.0
- Windows Server 2000 Operating System version 6.0.6989.0
- Windows Server 2003 Operating System version 6.0.6989.0
- Windows Server 2008 Operating System (Discovery) version 6.0.6989.0
- Windows Server 2008 Operating System (Monitoring) version 6.0.6989.0
- Windows Server Operating System Library version 6.0.6989.0
- Windows Server Operating System Reports version 6.0.6989.0
- Windows Server 2012 Operating System (Discovery) version 6.0.6989.0
- Windows Server 2012 Operating System (Monitoring) version 6.0.6989.0

Once added, click **OK** to continue.



At the **Select Management Packs** dialog, click **Install** to import the selected management packs.	
The management packs will download and import into Operations Manager. Once complete, verify that the imports were successful and click **Close** to exit the **Import Management Packs** wizard.	
In the **Operations Manager** console, go to the Administration workspace and verify the previously selected management packs are now installed.	

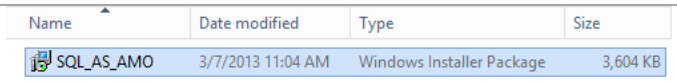
Install SQL Analysis Management Objects

For full functionality of Virtual Machine Manager 2012 SP1 integration with Operations Manager 2012 SP1, SQL Server 2008 R2 SP1 AMO and SQL Server 2012 SP1 AMO must be installed on all VMM management servers.

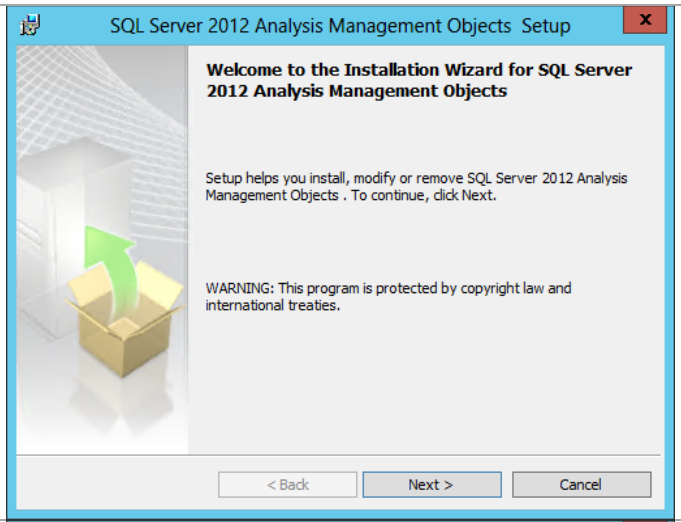
▶ Perform the following steps on both **Virtual Machine Manager** virtual machines.

From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.

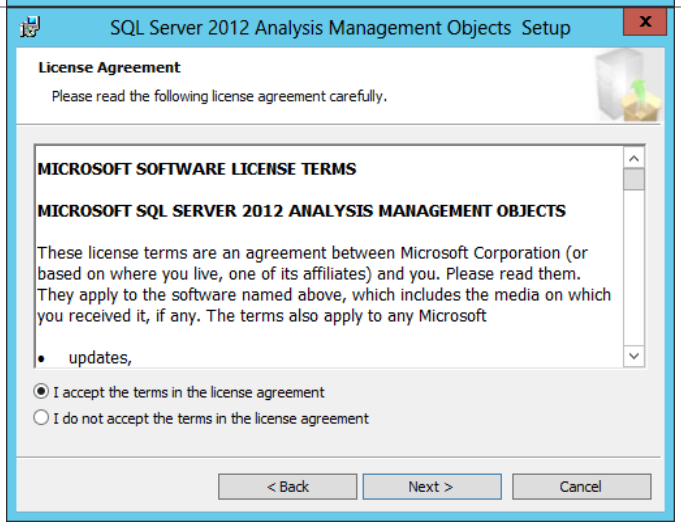
Note: The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580.

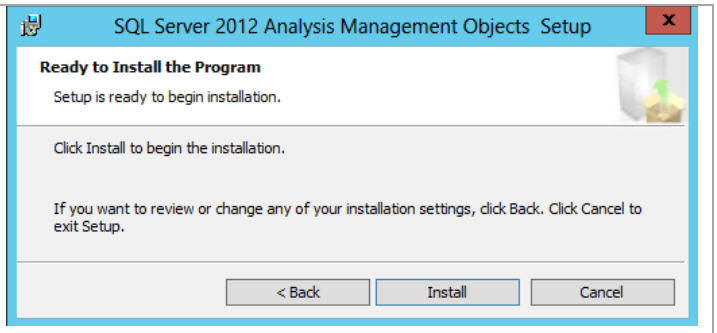
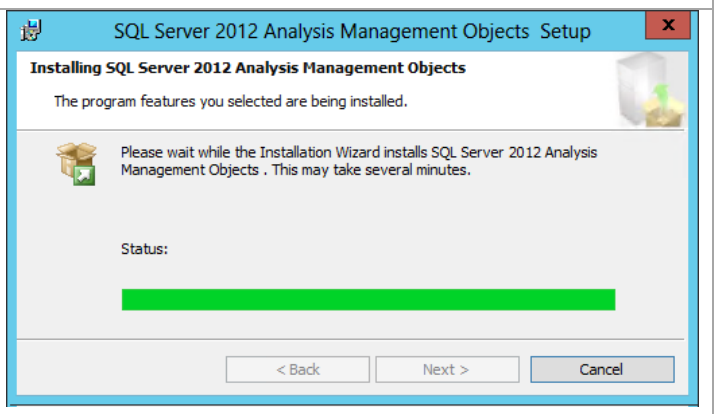
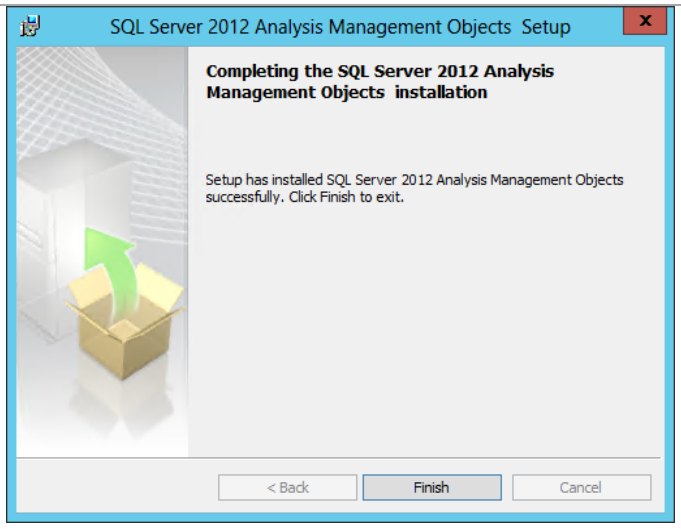


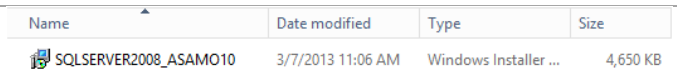
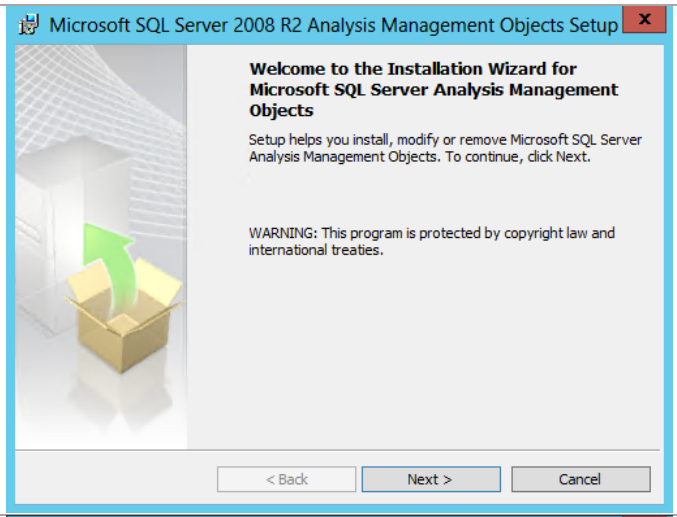
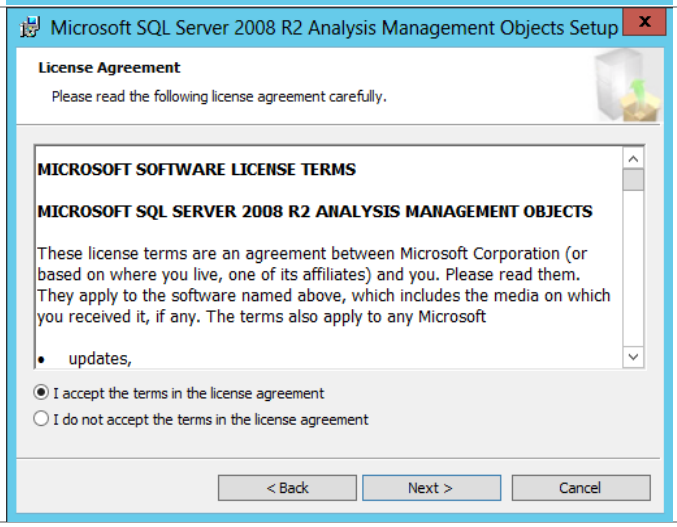
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.

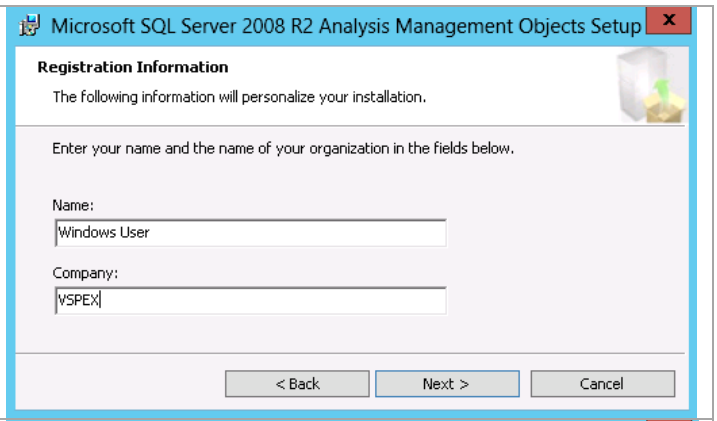
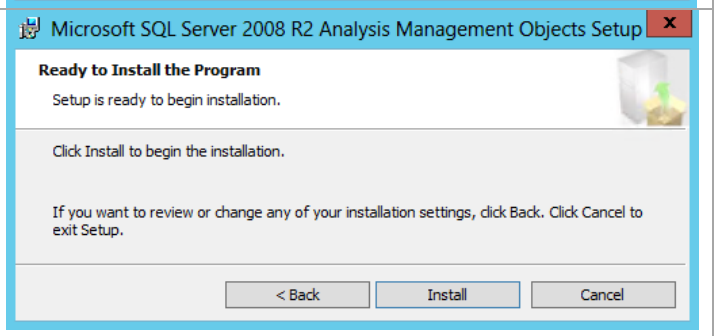
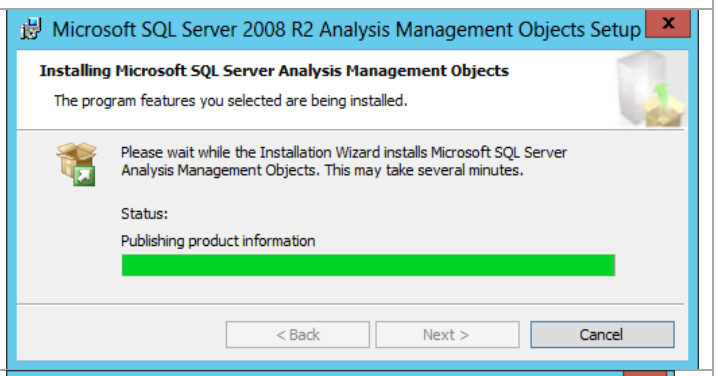
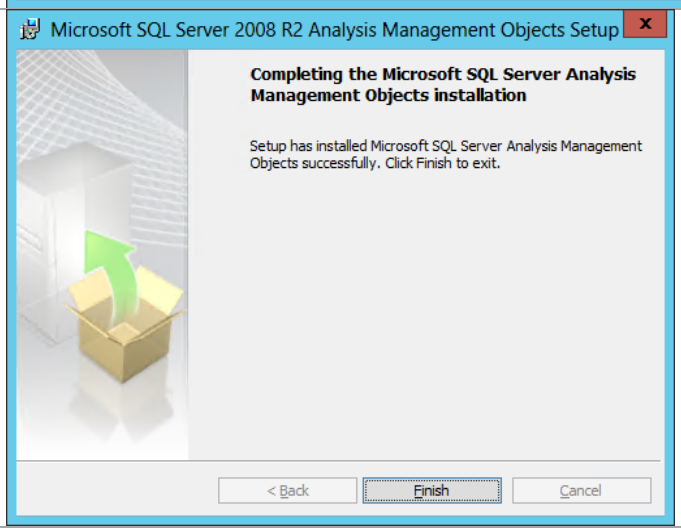


In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.



In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
The installation process may take several minutes to complete. The progress is displayed on the status dialog.	
In the **Completing the SQL Server 2012 Analysis Management Objects** installation dialog, click **Finish** to exit the installation.	

The SQL Server 2008 R2 SP1 Analysis Management Objects package must be installed as well to allow for the integration wizard to complete. From the **SQL Server 2008 R2 SP1 Analysis Management Objects** installation media source, double-click **SQLSERVER2008_ASAMO10.MSI** to begin setup. **Note:** The SQL Server 2008 R2 SP1 Analysis Management Objects installer, **1033\x64\SQLSERVER2008_ASAMO10.msi,** can be downloaded from http://www.microsoft.com/download/en/details.aspx?id=26728.	
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.	
In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.	

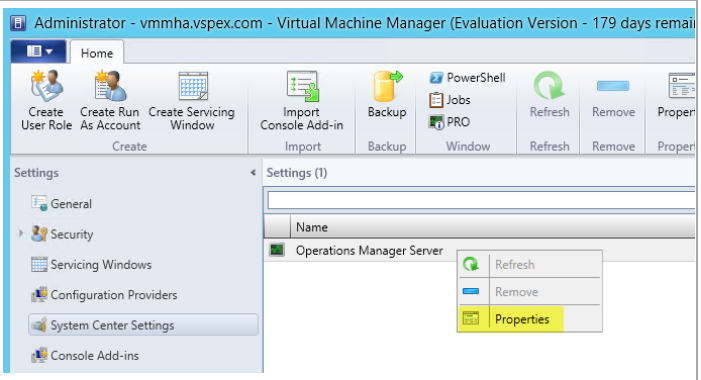
In the **Registration Information** dialog, provide values in the **Name** and **Company** textboxes and then click **Next** to continue.	
On the **Ready to Install the Program** screen, click **Install** to begin the installation.	
The installation process may take several minutes to complete. The progress is displayed on the Status screen.	
On the **Completing the SQL Server 2008 Analysis Management Objects** installation screen, click **Finish** to exit the installation.	

Perform Virtual Machine Manager and Operations Manager Integration

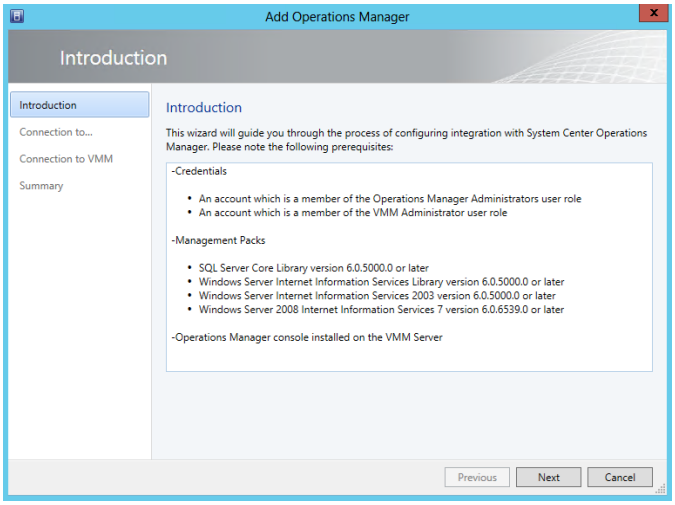
When all pre-requisite configurations and installations are performed, the integration of Virtual Machine Manager and Operations Manager can be completed.

▶ Perform the following steps on the **Virtual Machine Manager** virtual machine.

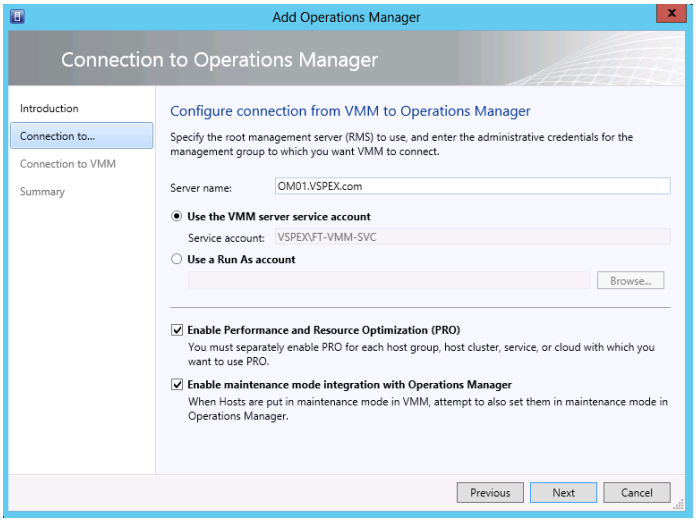
In the Virtual Machine Manager console, navigate to **Settings** pane and select **System Center Settings**, right-click **Operations Manager Server** and select **Properties** from the context menu.

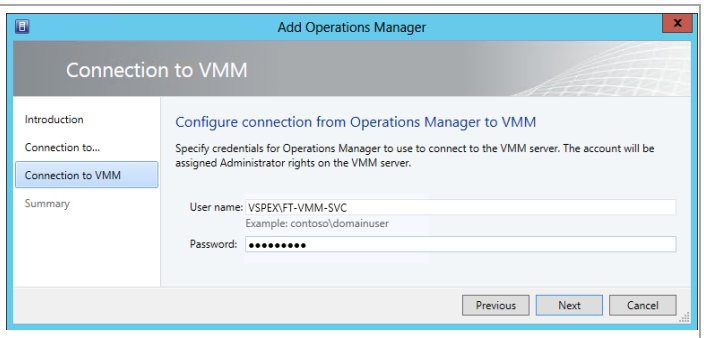
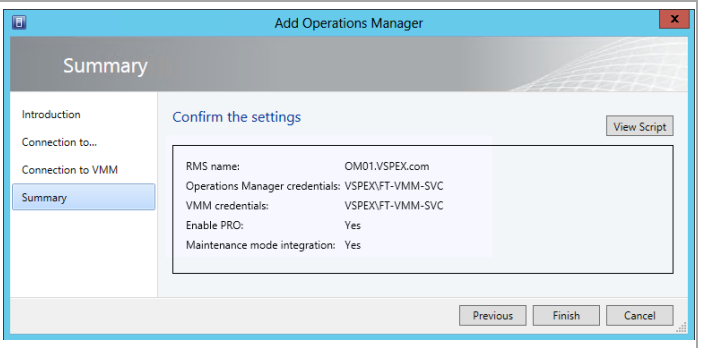
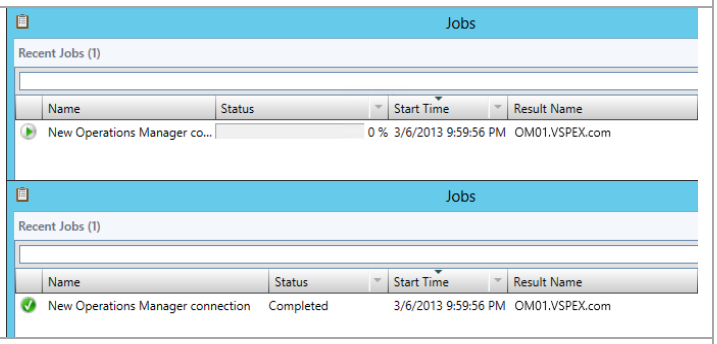
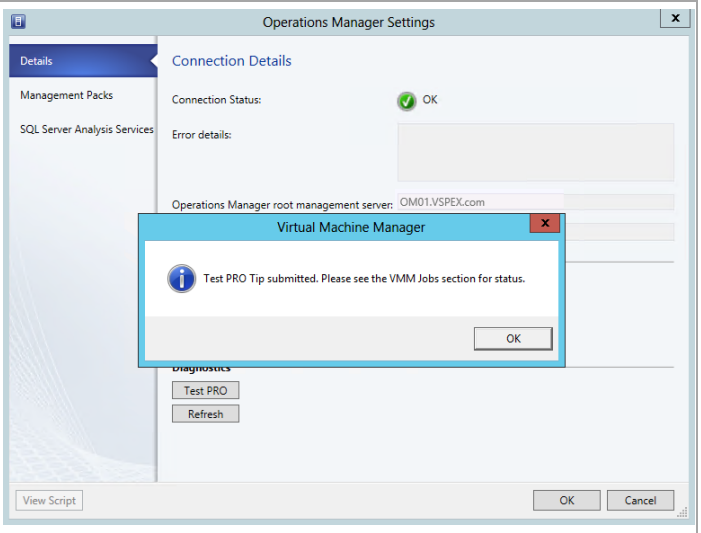


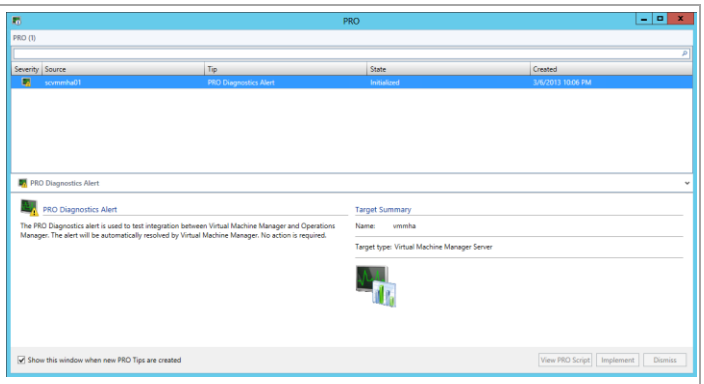
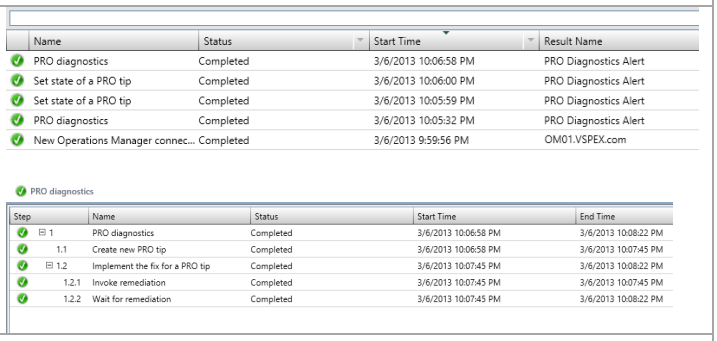
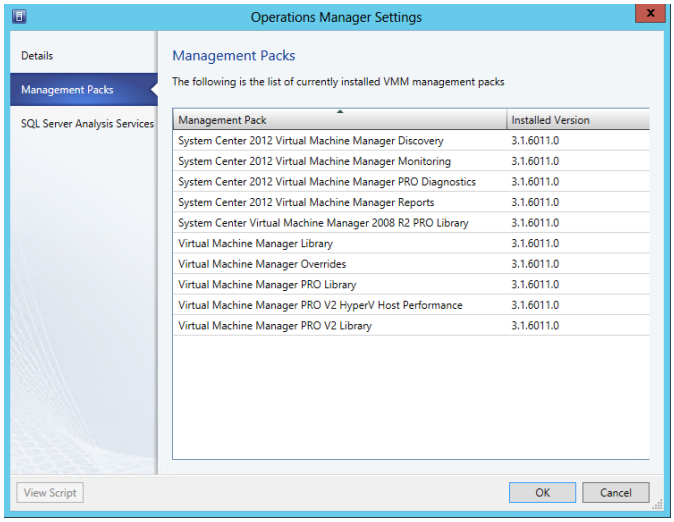
The **Add Operations Manager** dialog will appear. In the **Introduction** dialog, verify the prerequisites have been met and click **Next** to continue.



In the **Connection to Operations Manager** dialog, type the FQDN of the Operations Manager server in the Server name text box. Select the **Use the VMM server service account** option. Select the **Enable Performance and Resource Optimization (PRO)** and **Enable maintenance mode integration with Operations Manager** check boxes.
When complete, click **Next** to continue.



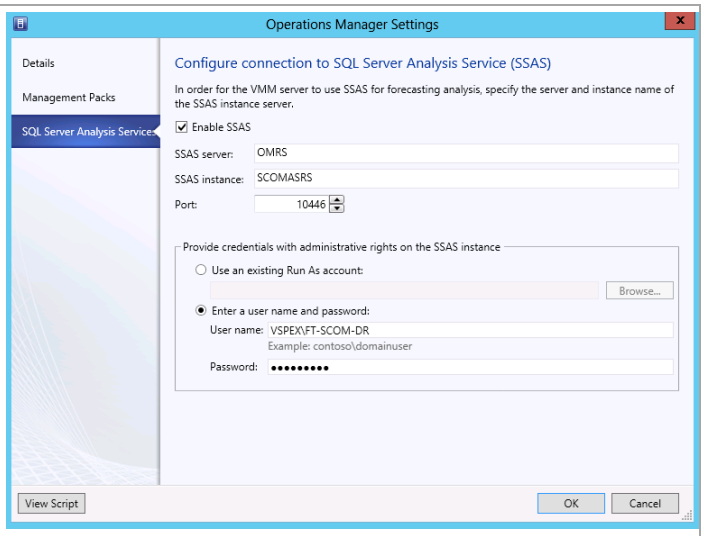
In the **Connection to VMM** dialog, specify the VMM service account credentials in the **User name** and **Password** text boxes and click **Next** to continue.	
In the **Summary** dialog, verify the options selected click **Finish** to begin the Operations Manager integration process.	
The **Jobs** pane will appear. Before moving forward, wait for the job to complete successfully.	
In the Virtual Machine Manager console, navigate back to **Settings** then select **System Center Settings** and double-click **Operations Manager Server.** The Operations Manager Settings dialog will appear. In the **Details** pane, click the **Test PRO** button.	

As part of the test, PRO will generate a diagnostics alert.	
After a few minutes, verify that the PRO test is successful. Navigate to the Jobs pane and verify the PRO jobs completed successfully.	
In the **Management Packs** dialog, verify all Virtual Machine Manager Management Packs were successfully installed.	

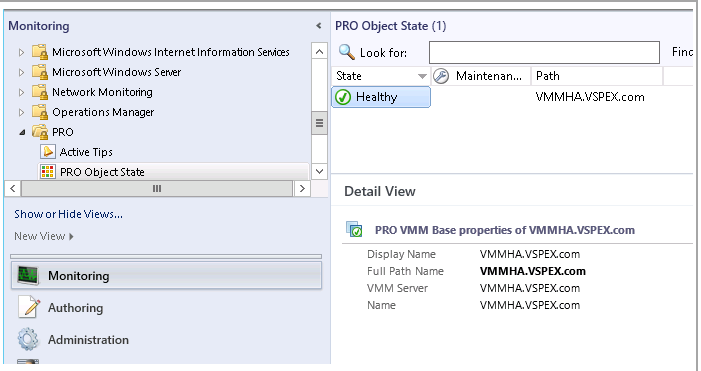
In the **Configure connection to SQL Server Analysis Services (SSAS)** dialog, provide the following information.
Select the **Enable SSAS** check box. Provide the following information on the text boxes provided:

- **SSAS server** – *Specify the Operations Manager database server instance.*
- **SSAS Instance** – *Specify the SSAS instance name created earlier.*
- **Port** – *Specify the port number assigned earlier*

In the **Provide credentials with administrative rights on the SSAS instance**, select **the Enter a user name and password** option and provide the supplied credentials for the Operations Manager Data Reader account.
Click **OK** to save these settings.



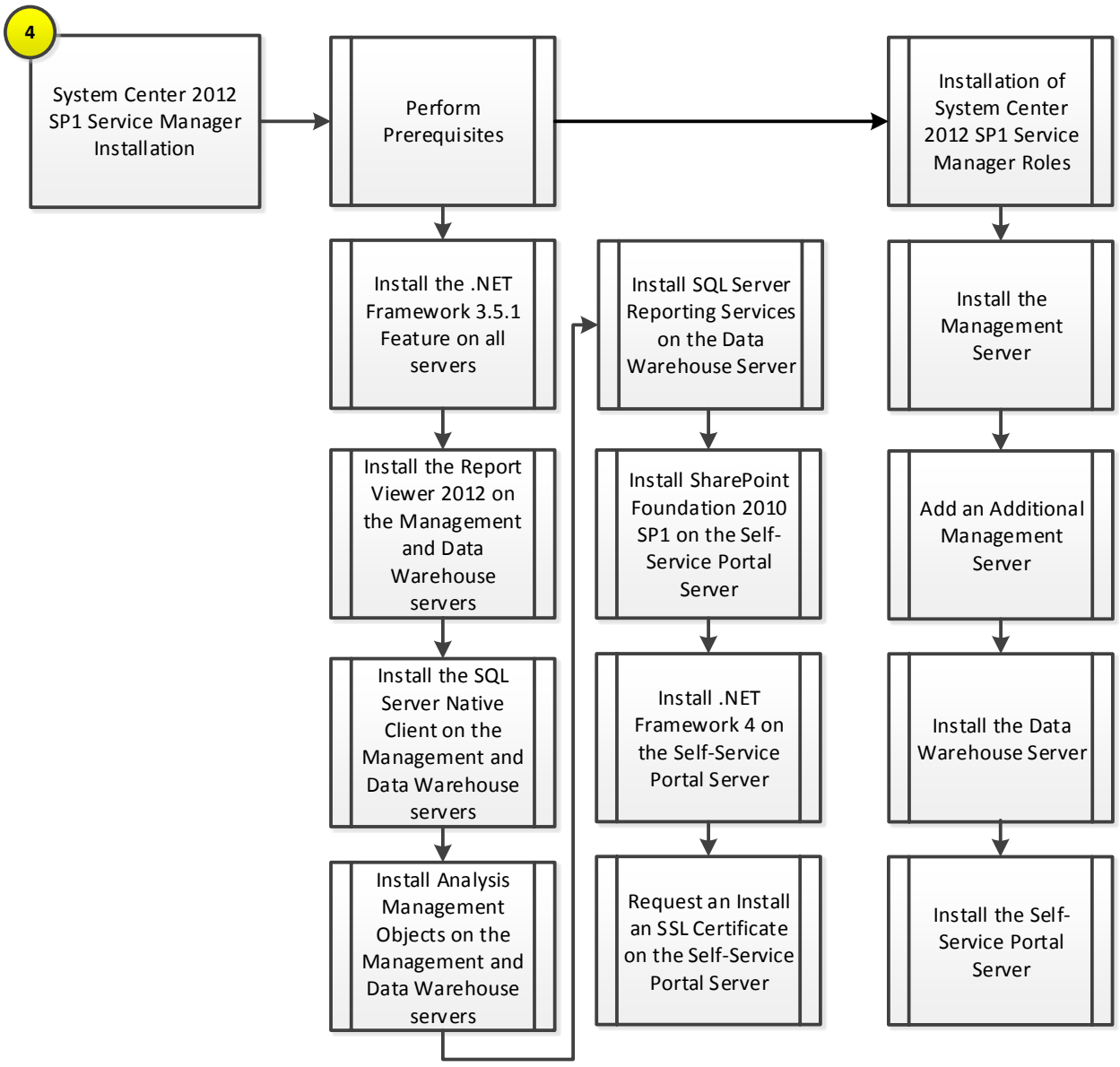
On the **Operations Manager** console, go to **Monitoring** workspace, navigate to the **PRO** node and select **PRO Object State**. Verify the VMM server is listed with a health state other than "*Not Monitored.*"



11 System Center Service Manager

The Service Manager installation process is comprised of the following high-level steps:

Table 30 Service Manager Installation Process



11.1 Overview

This section provides a high-level walkthrough on deploying Service Manager into the Fast Track fabric management architecture. The following assumptions are made:

Management Server

- A base virtual machine running Windows Server 2012 has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with dedicated Service Manager instances that has been established in previous steps for Service Manager.
    - Service Manager database – instance for Service Manager management database.

- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed- http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409.
- The Microsoft SQL Server 2012 Analysis Management Objects is installed - http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409.

Data Warehouse Server

- A base virtual machine running Windows Server 2012 has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with dedicated instance that has been established in previous steps for Service Manager.
  - SCSMAS – instance for SQL Server 2012 Analysis Services and SQL Server Reporting Services databases.
  - SCSMDW – instance for Service Manager Data Warehouse databases.
- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed - http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409.
- The Microsoft SQL Server 2012 Analysis Management Objects are installed- http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409.
- The Microsoft SQL Server 2012 Reporting Services (split configuration) is installed.
- The Microsoft SQL Server 2012 Management tools are installed.

Self-Service Portal Server

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with a database instance that has been established in previous steps for Service Manager.
  - SCDB – shared instance for Self Service Portal SharePoint Farm databases.
- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed - http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409.
- The Microsoft SQL Server 2012 Analysis Management Objects is installed - http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409.
- SharePoint Foundation 2010 Service Pack 1 is installed.
- The .NET Framework 4 Redistributable is installed.

11.2 Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following accounts have been created:

Table 31 Prerequisite Accounts for Service Manager

User Name	Purpose	Permissions
<DOMAIN>\ FT-SCSM-SVC	SCSM Services Account	Add the account to the local Administrators group on the all SCSM servers. Must be a local admin on all SQL nodes.
<DOMAIN>\ FT-SCSM-WF	SCSM Workflow Account	Must have permissions to send e-mail and must have a mailbox on the SMTP server (required for the E-mail Incident feature). Must be member of Users local security group on all SCSM servers. Must be made a member of the Service Manager Administrators user role in order for e-mail Must be a local admin on all SQL nodes.
<DOMAIN>\ FT-SCSM-SSRS	SCSM Reporting Account	Must be a local admin on all SQL nodes.
<DOMAIN>\ FT-SCSM-OMCI	SCSM Operations Manager CI Connector Account	Must be a member of the Users local security group on all SCSM servers. Must be an Operations Manager Operator.
<DOMAIN>\ FT-SCSM-ADCI	SCSM Active Directory CI Connector Account	Must be a member of the Users local security group on the Service Manager Management server. Must have permissions to bind to the domain controller that the connector will read data from. Needs generic read rights on the objects that are being synchronized into the Service Manager database from Active Directory.

User Name	Purpose	Permissions
<DOMAIN>\ FT-SCSM-OMAlert	SCSM Operations Manager Alert Connector Account	Must be a member of the Users local security group on the Service Manager Management server. Must be a member of FT-SCSM-Admins
DOMAIN>\ FT-SCSM-VMMCI	Virtual Machine Manager CI Connector Account	Member of the VMM Admin domain group. The account must also be in the Service Manager Advanced Operator role
DOMAIN>\ FT-SCSM-OCI	Orchestrator CI Connector	Member of SCO Operators (Users) domain group. The account must also be in the Service Manager Advanced Operator role
<DOMAIN>\ FT-SM-OLAP	SM Analysis Services Account	Must be a local admin on all SQL nodes.

Groups

Verify that the following security groups have been created for Service Manager:

Table 32 Prerequisite Security Groups

Security Group Name	Group Scope	Members	Member of
<DOMAIN>\ FT-SCSM-ADMINS	Global	DOMAIN\ FT-SCSM-SVC	Must be added to the Service Manager Administrators user role and added to the Operations Manager Administrators role in Operations Manager and a member of the Administrators group on each SQL Server.

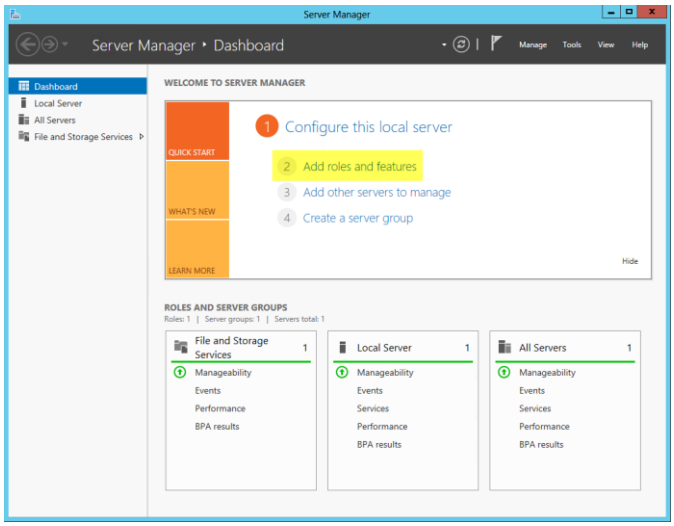
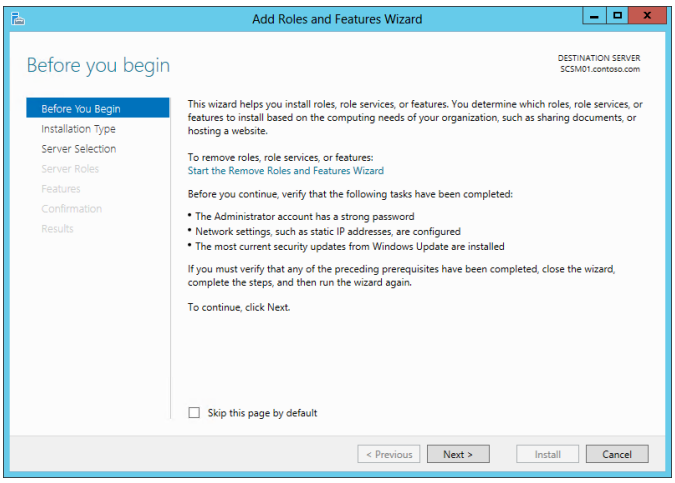
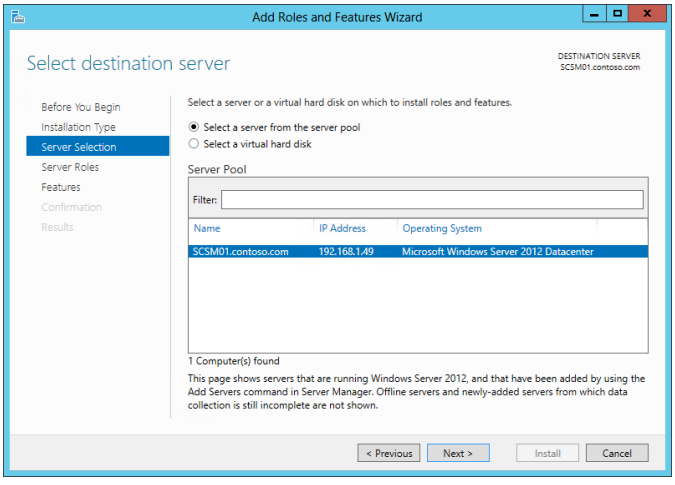
Required Networks

VMaccess

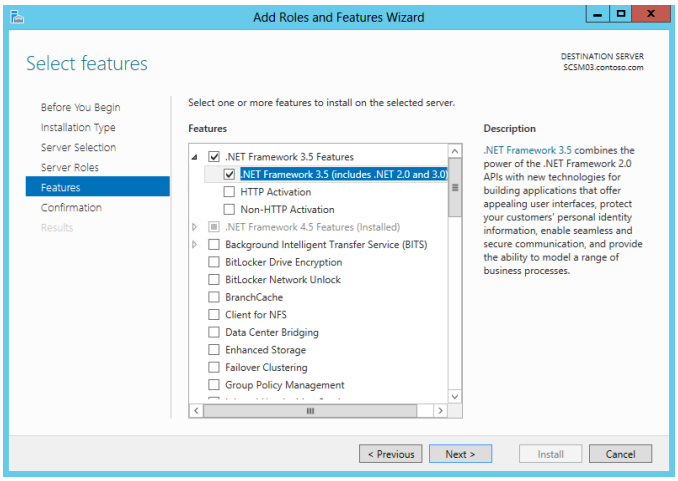
Add the .NET Framework 3.5 Feature on all Server Manager Servers

The Service Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. If you did not include this installation in your sysprepped image, follow the provided steps to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on the **Service Manager management server and data warehouse** virtual machines.

Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.	
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.	
In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next - for** this installation, click the **Features** menu option to continue.	

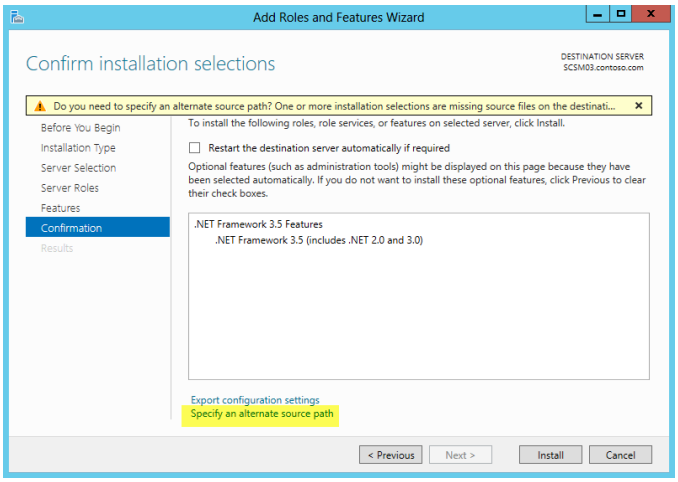
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear.
Click **Next** to continue.



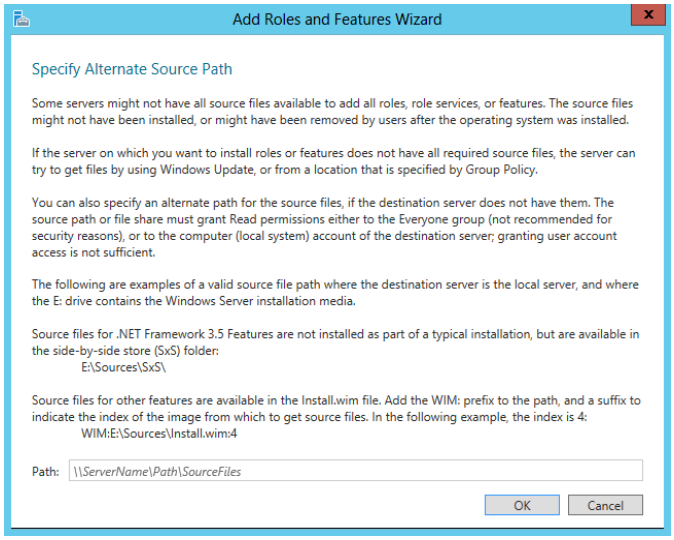
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. Once exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.

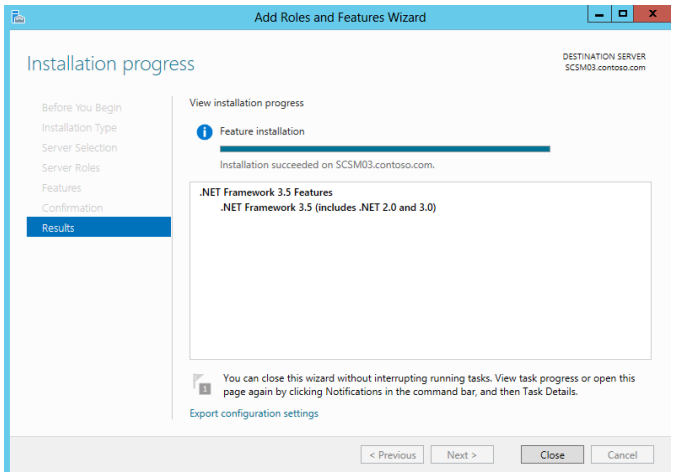
Note: If the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.



For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location be specified for the installation.

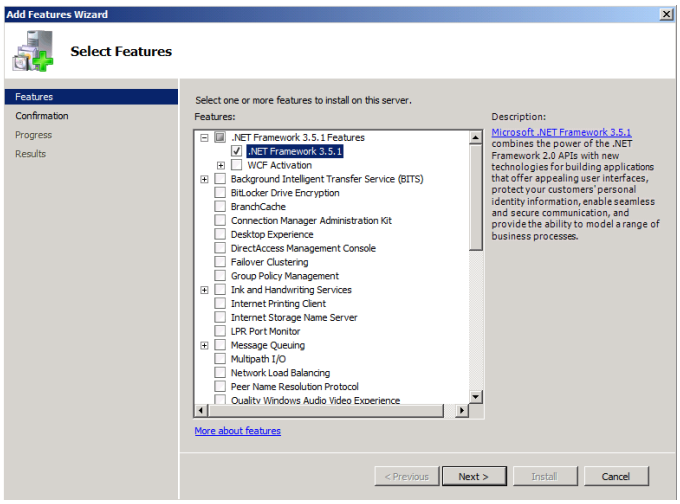


The **Installation Progress** dialog will show the progress of the feature installation.
Click **Close** when the installation process completes.

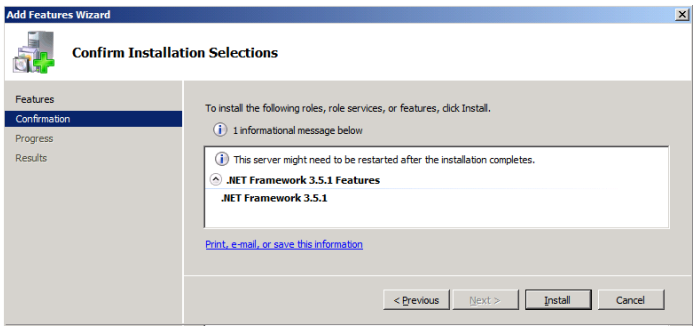


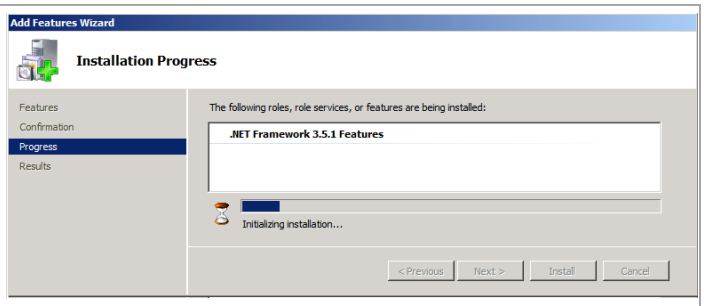
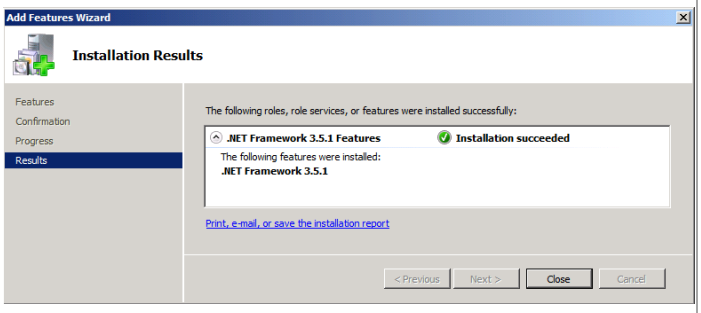
- Perform the following steps on the **Service Manager Self-Service Portal** virtual machine running Windows Server 2008 R2.

To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features,** and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.



In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.

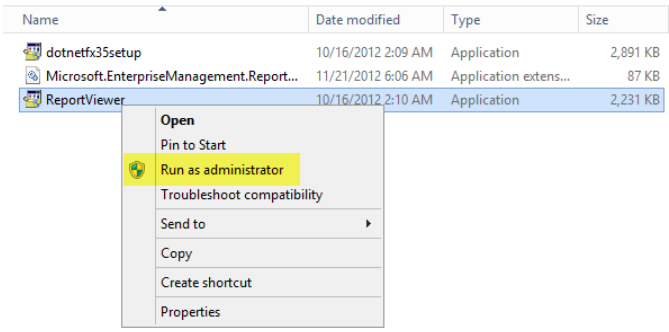


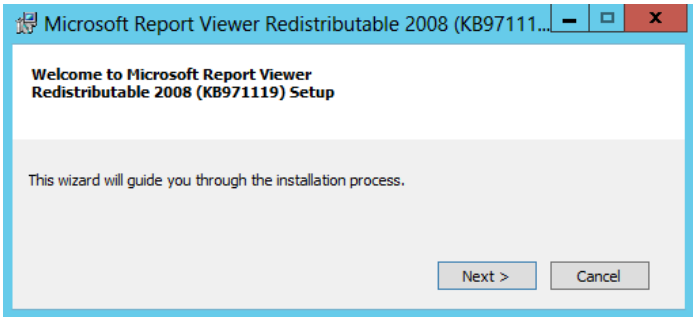
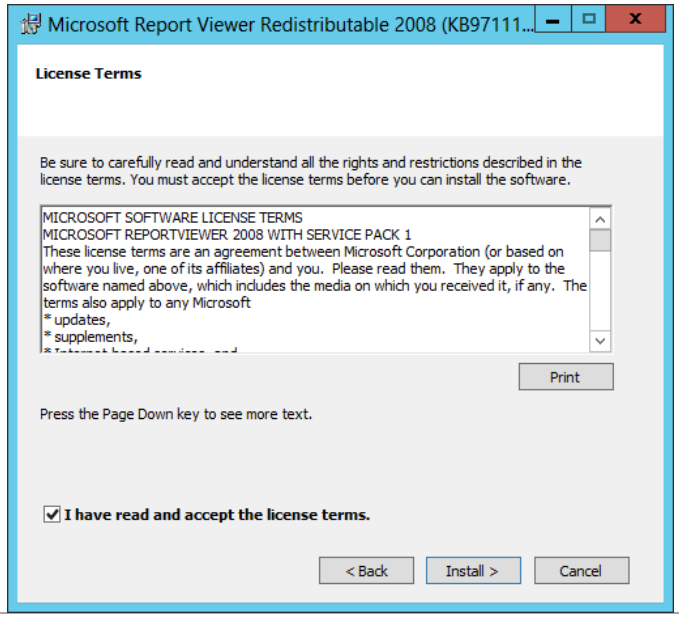
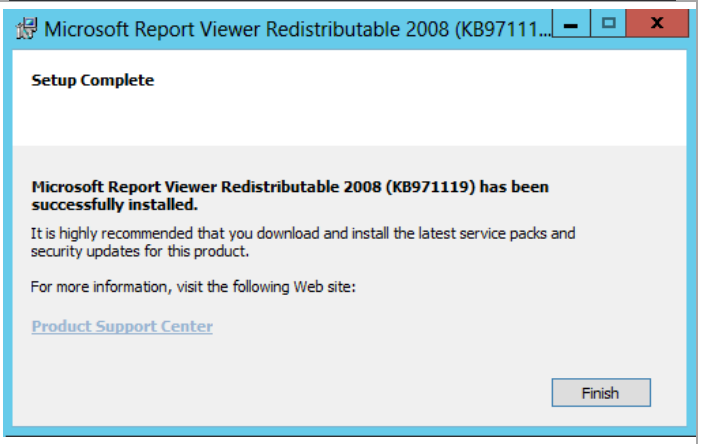
The **Installation Progress** dialog will show the progress of the feature install.	
When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. Once verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.	

Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers

The Server Manager management and Data Warehouse server installations also require the Microsoft Report Viewer 2008 SP1 Redistributable be installed prior to installation. The following steps are provided to help install the Microsoft Report Viewer 2008 SP1 Redistributable.

▶ Perform the following steps on the **Server Manager management and Data Warehouse server** virtual machines.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup. **Note:** Report Viewer can be found in the prerequisites folder of the Service Manager 2012 SP1 installation media or it can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=3203	

The setup wizard will appear. Click **Next** to continue.	
Within the **License Terms** dialog, select the **I have read and accept the license terms** check box. Click **Install** to begin the installation.	
When completed, click **Finish** to exit the installation.	

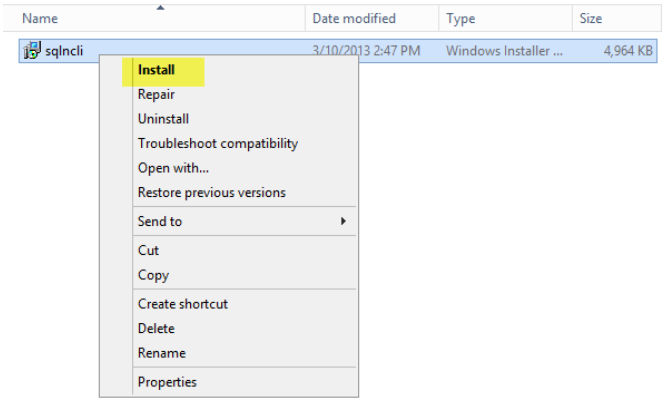
Install SQL Server 2012 Native Client on the on the Management and Data Warehouse Servers

The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 Native Client be installed prior to installation. Follow the provided steps to install the SQL Server 2012 Native Client.

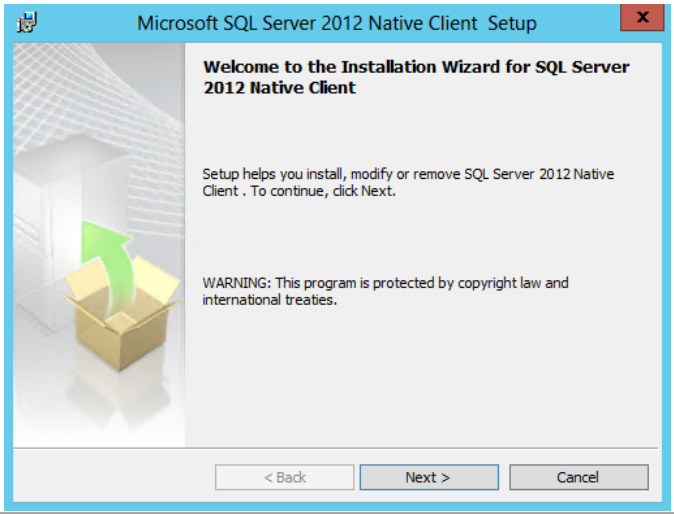
▶ Perform the following steps on the **Server Manager management and Data Warehouse server** virtual machines.

From the installation media source, right-click **SQLNCLI.MSI** and select **Install** from the context menu to begin setup.

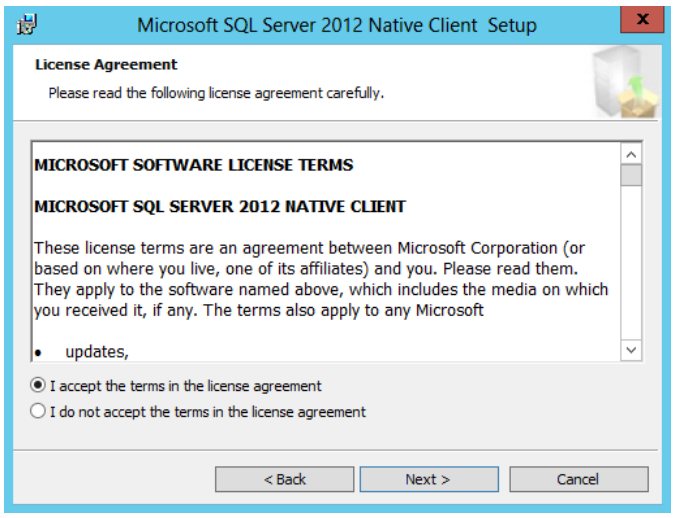
Note: The SQL Server 2012 SP1 Native Client installer, **1033\x64\sqlncli.msi,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580 .

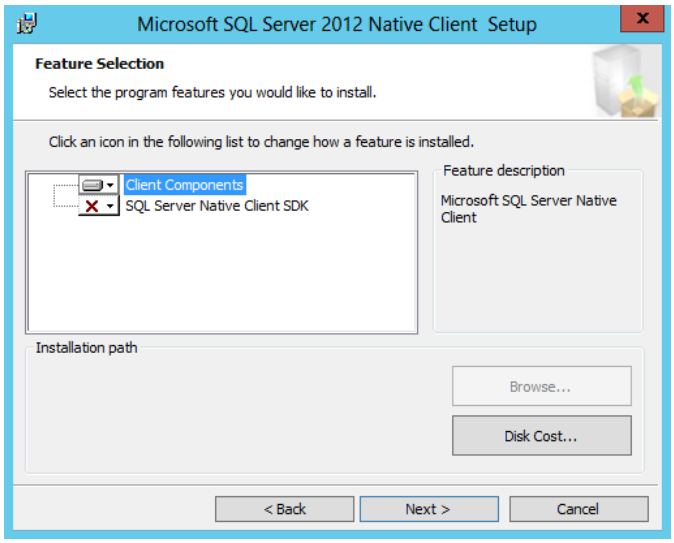
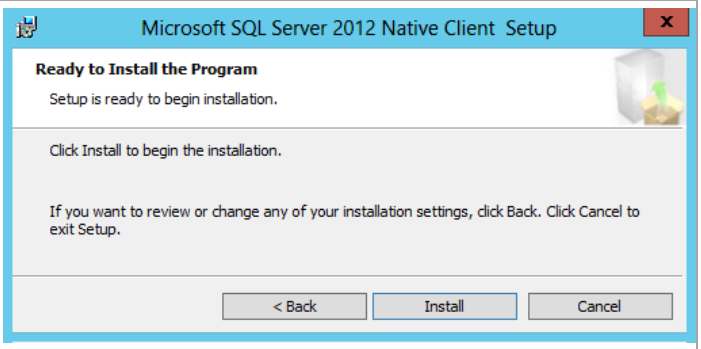
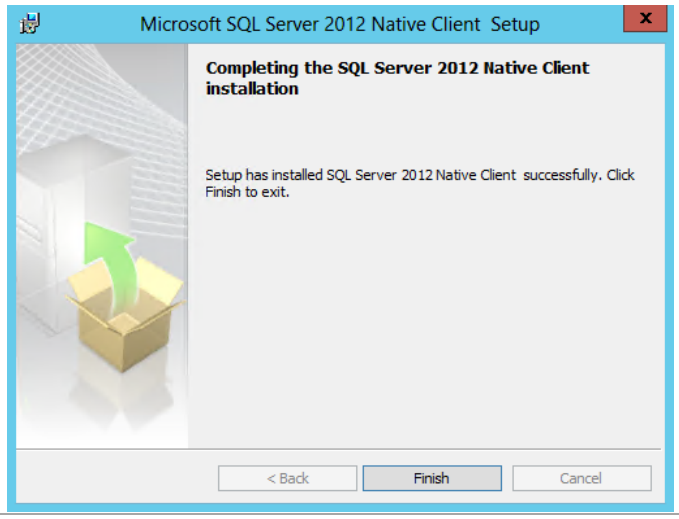


The setup wizard will appear.
Click **Next** to continue.



Within the **License Terms** dialog, select the **I accept the terms in the license agreement** check box.
Click **Next** to continue.



In the **Feature Selection** dialog, verify that the **Client Components** feature is selected for installation. Click **Next** to continue.	
In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
When completed, click **Finish** to exit the installation.	

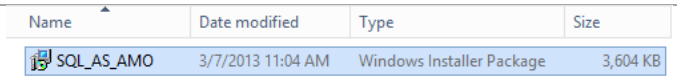
Install SQL Server 2012 SP1 Analysis Management Objects

The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 SP1 Analysis Management Object be installed prior to installation. Follow the provided steps to install the SQL Server 2012 SP1 Analysis Management Objects.

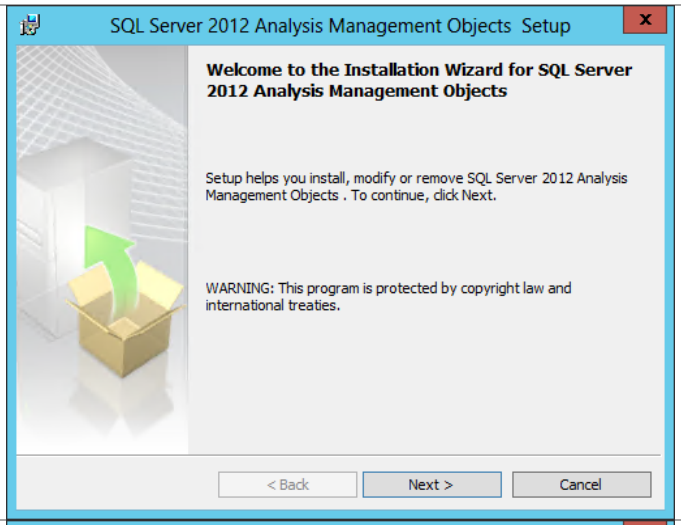
▶ Perform the following steps on the **Server Manager management and Data Warehouse server** virtual machines.

From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.

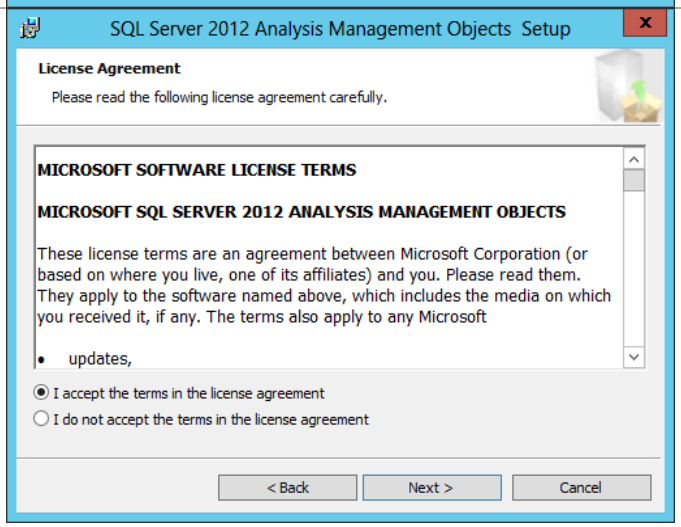
Note: The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580.

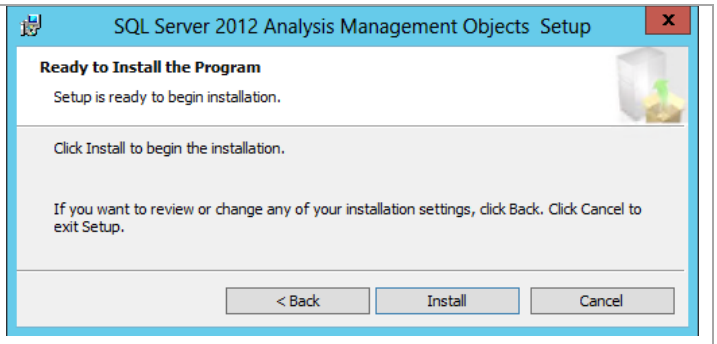
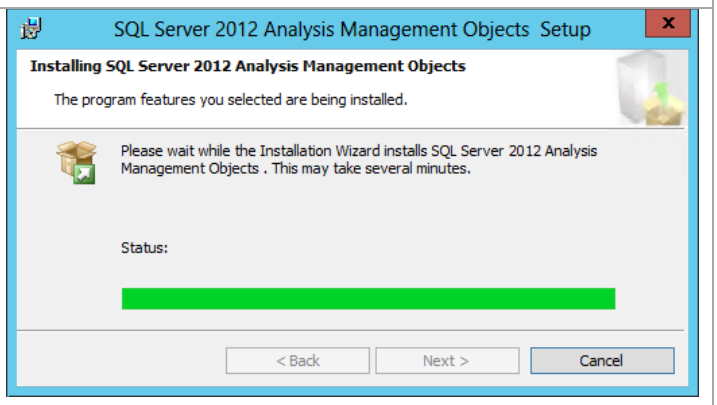
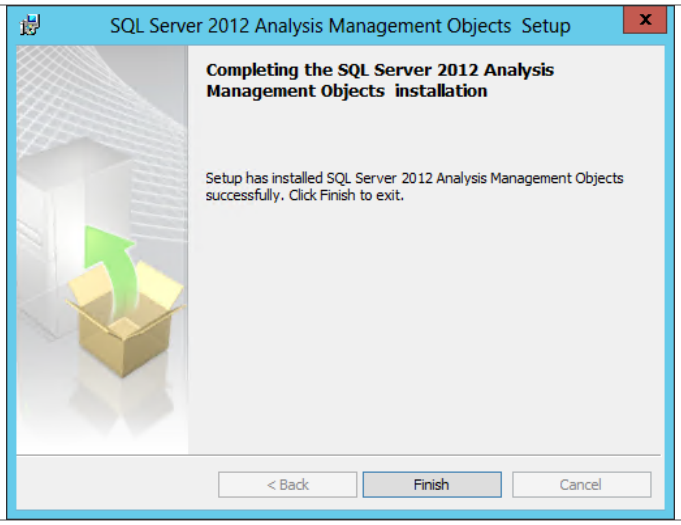


The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.

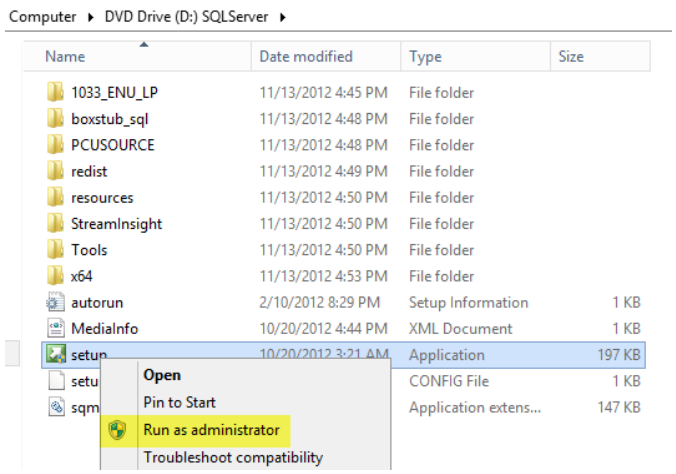
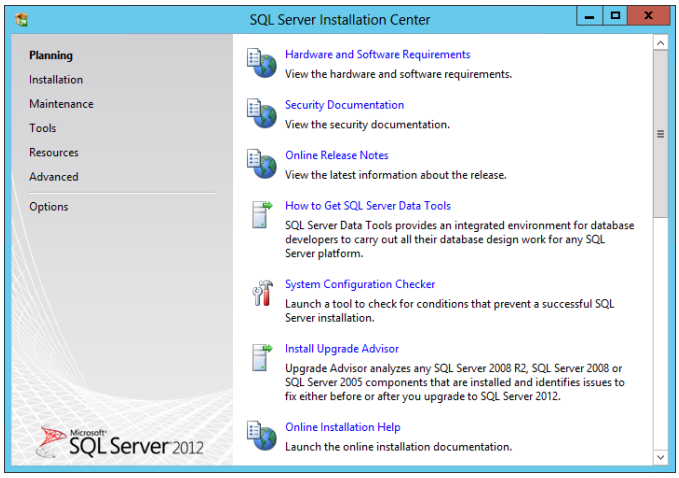
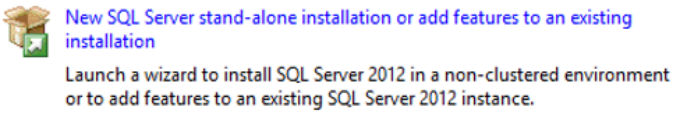
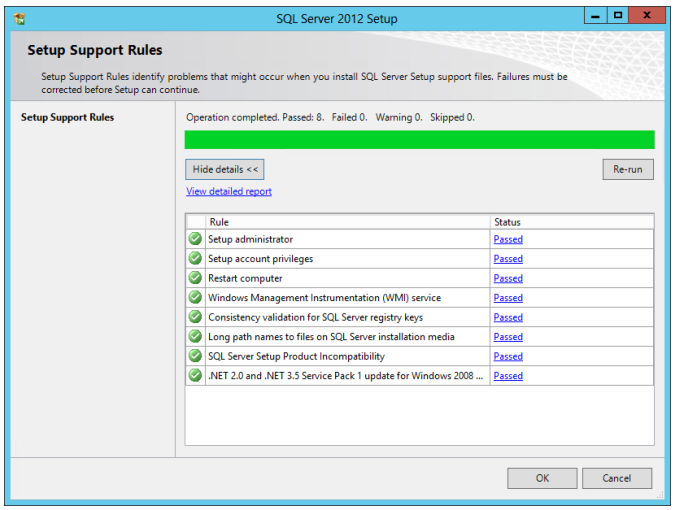


In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
The installation process may take several minutes to complete. The progress is displayed on the status dialog.	
In the **Completing the SQL Server 2012 Analysis Management Objects** installation dialog, click **Finish** to exit the installation.	

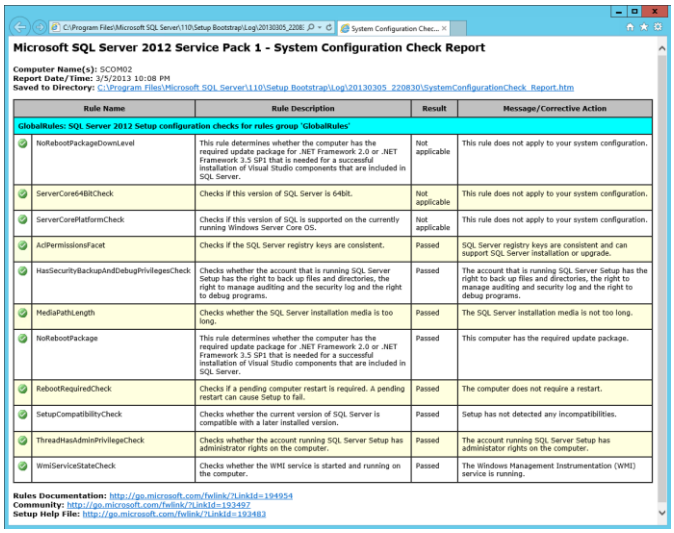
Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

The Service Manager Data Warehouse installation requires SQL Server Reporting Services to be installed to support the Service Manager reporting features. Follow the provided steps to install SQL Server Reporting Services.

▶ Perform the following steps on the **Service Manager Data Warehouse** virtual machine.

From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The **SQL Server Installation Center** will appear. Select the **Installation** menu option.	
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.	
The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.	

If the **View detailed report** link is selected, the following report is available.



Microsoft SQL Server 2012 Service Pack 1 - System Configuration Check Report

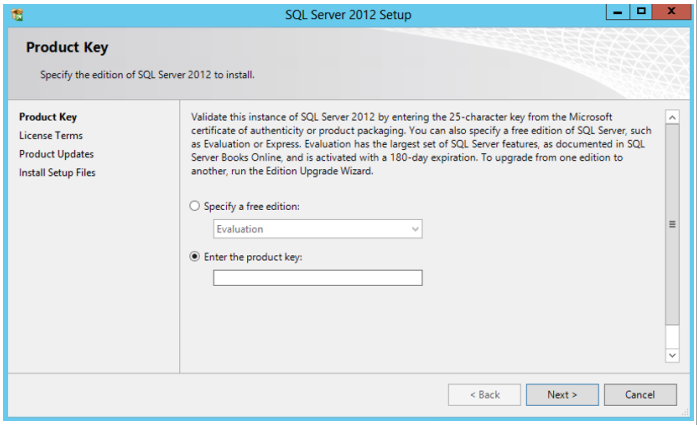
Computer Name(s): SCOM02
Report Date/Time: 3/5/2013 10:08 PM
Saved to Directory: C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap\Log\20130305_220830\SystemConfigurationCheck_Report.htm

Rule Name	Rule Description	Result	Message/Corrective Action
GlobalRules: SQL Server 2012 Setup configuration checks for rules group 'GlobalRules'			
NoRebootPackageDownLevel	This rule determines whether the computer has the required update package for .NET Framework 2.0 or .NET Framework 3.5 SP1 that is needed for a successful installation of Visual Studio components that are included in SQL Server.	Not applicable	This rule does not apply to your system configuration.
ServerCore64BitCheck	Checks if this version of SQL Server is 64bit.	Not applicable	This rule does not apply to your system configuration.
ServerCorePlatformCheck	Checks if this version of SQL is supported on the currently running Windows Server Core OS.	Not applicable	This rule does not apply to your system configuration.
AclPermissionsFacet	Checks if the SQL Server registry keys are consistent.	Passed	SQL Server registry keys are consistent and can support SQL Server installation or upgrade.
HasSecurityBackupAndDebugPrivilegesCheck	Checks whether the account that is running SQL Server Setup has the right to back up files and directories, the right to manage auditing and the security log and the right to debug programs.	Passed	The account that is running SQL Server Setup has the right to back up files and directories, the right to manage auditing and security log and the right to debug programs.
MediaPathLength	Checks whether the SQL Server installation media is too long.	Passed	The SQL Server installation media is not too long.
NoRebootPackage	This rule determines whether the computer has the required update package for .NET Framework 2.0 or .NET Framework 3.5 SP1 that is needed for a successful installation of Visual Studio components that are included in SQL Server.	Passed	This computer has the required update package.
RebootRequiredCheck	Checks if a pending computer restart is required. A pending restart can cause Setup to fail.	Passed	The computer does not require a restart.
SetupCompatibilityCheck	Checks whether the current version of SQL Server is compatible with a later installed version.	Passed	Setup has not detected any incompatibilities.
ThreadHasAdminPrivilegeCheck	Checks whether the account running SQL Server Setup has administrator rights on the computer.	Passed	The account running SQL Server Setup has administator rights on the computer.
WmiServiceStateCheck	Checks whether the WMI service is started and running on the computer.	Passed	The Windows Management Instrumentation (WMI) service is running.

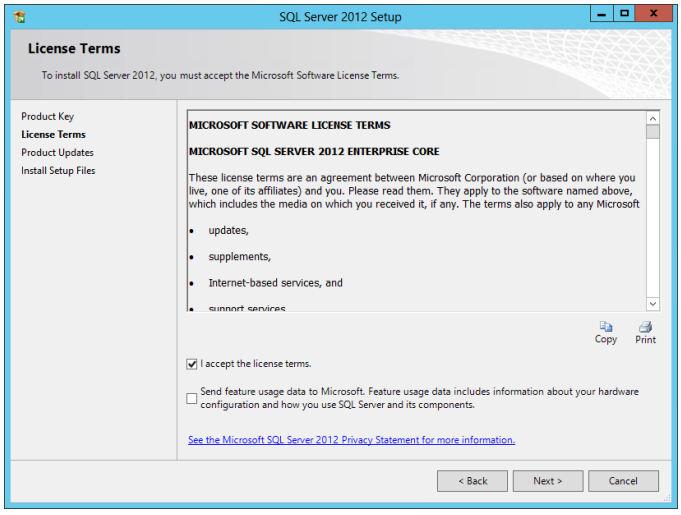
Rules Documentation: http://go.microsoft.com/fwlink/?LinkId=194954
Community: http://go.microsoft.com/fwlink/?LinkId=193497
Setup Help File: http://go.microsoft.com/fwlink/?LinkId=193483

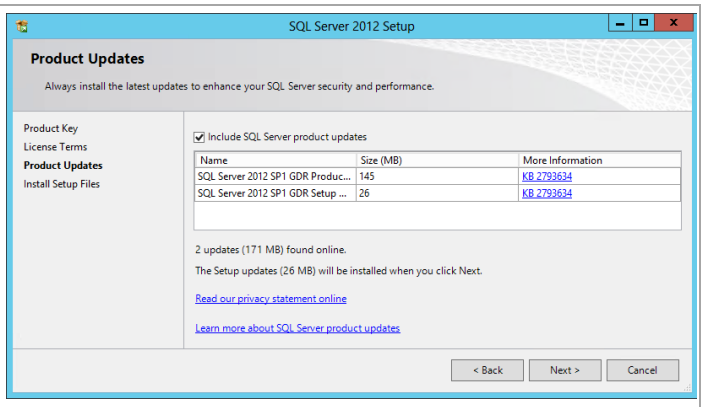
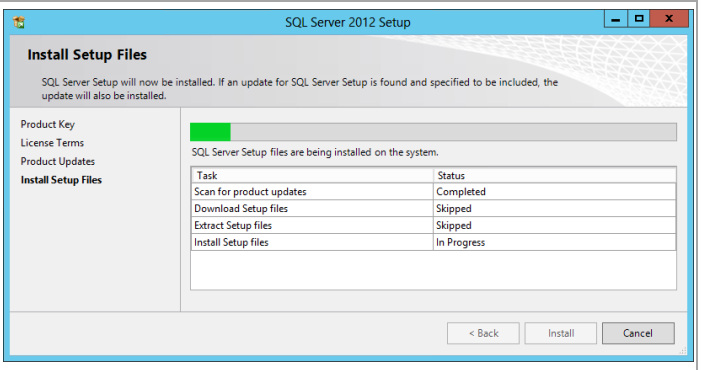
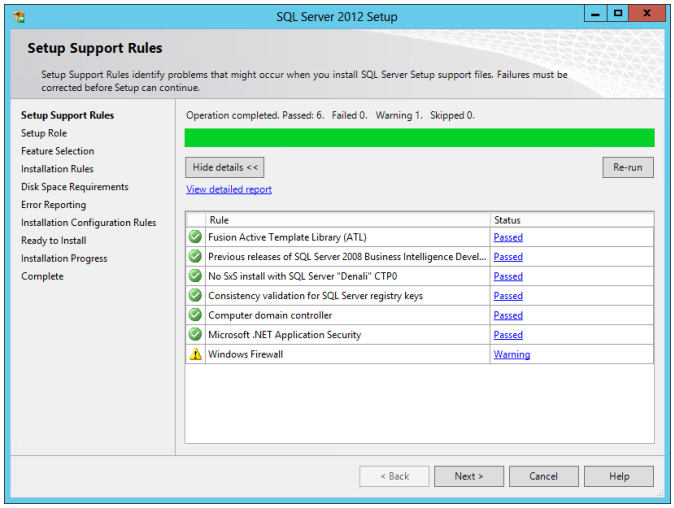
In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

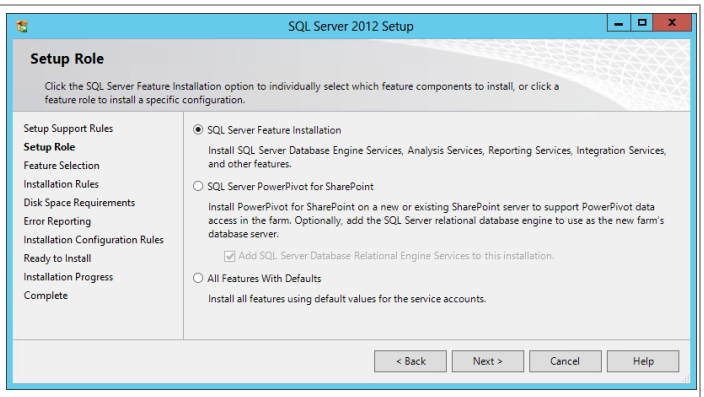
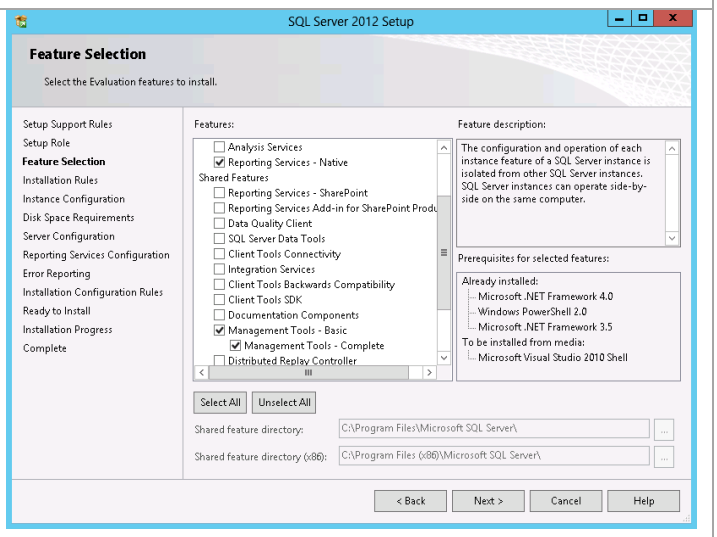
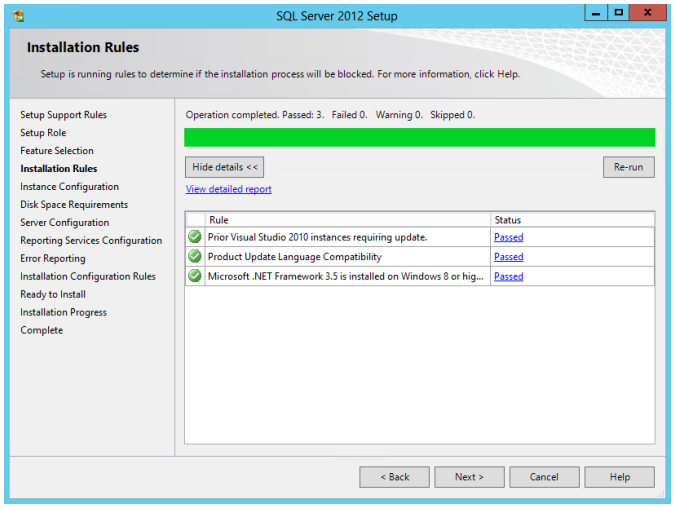
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.

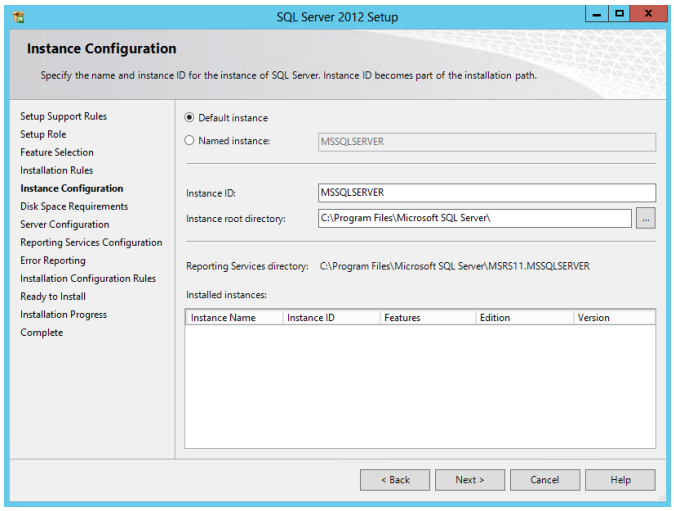


In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.	
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.	
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment. Click **Next** to continue.	

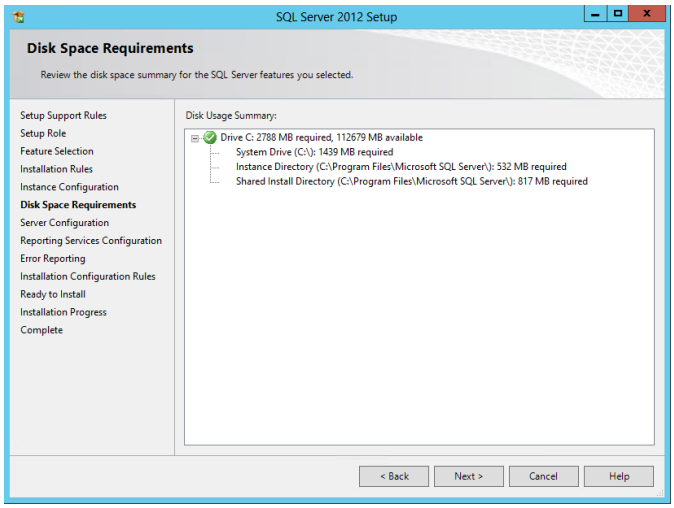
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.	
In the **Feature Selection** dialog, select **Reporting Services - Native, Management Tools – Basic,** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.	
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

In the **Instance Configuration** dialog, select the **Default instance** option and accept the default options for **Instance ID** and **Instance root directory** values.
Click **Next** to continue.

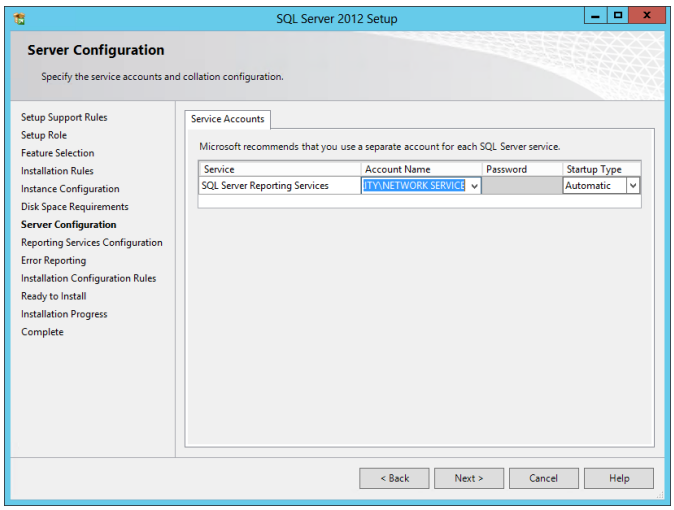
Note: A post-installation configuration process will occur to configure the reporting server database within the Service Manager Data Warehouse SQL Server instance.

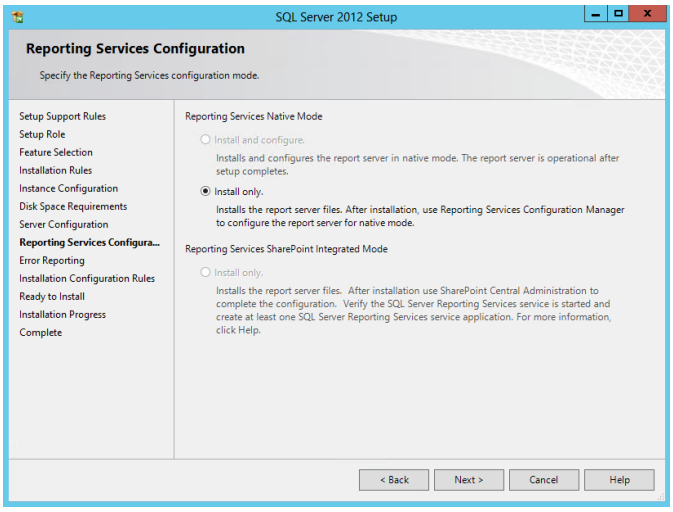
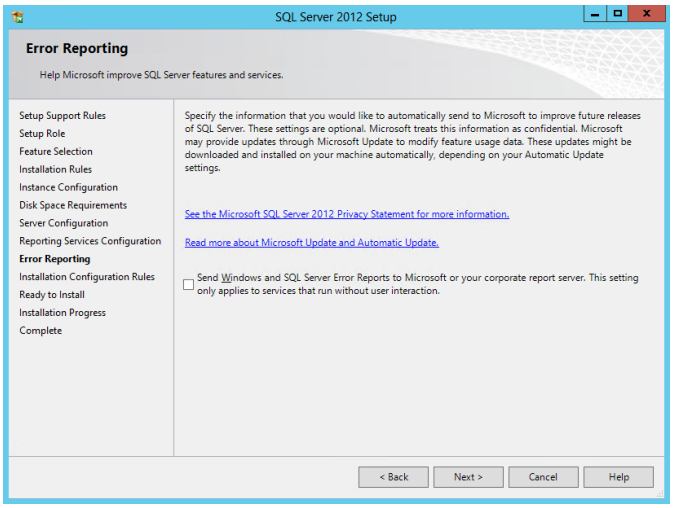
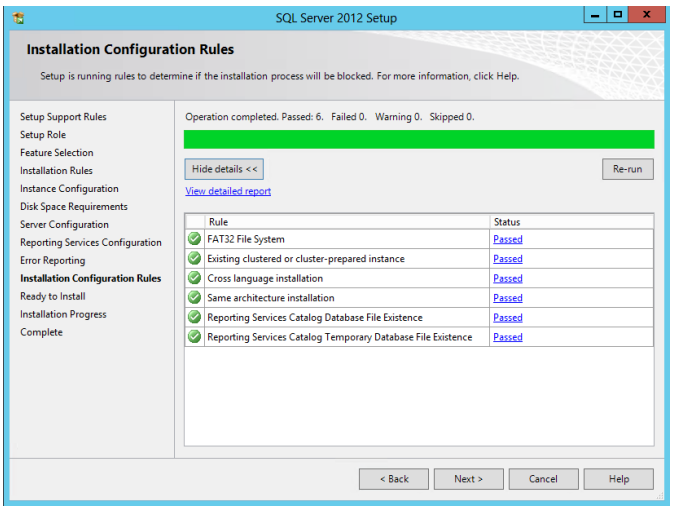


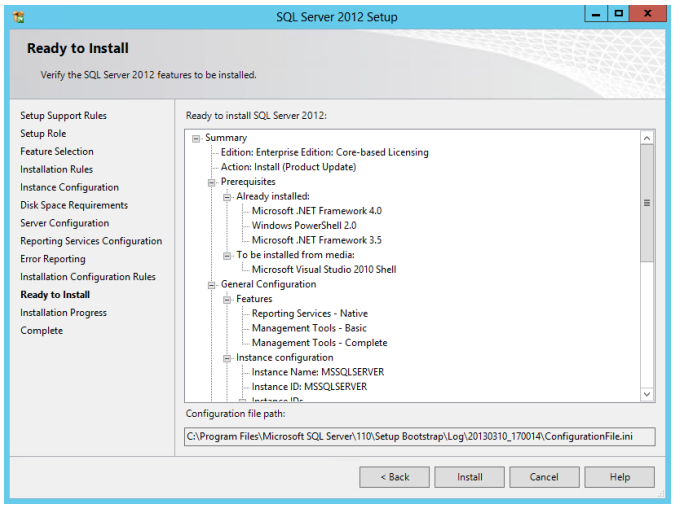
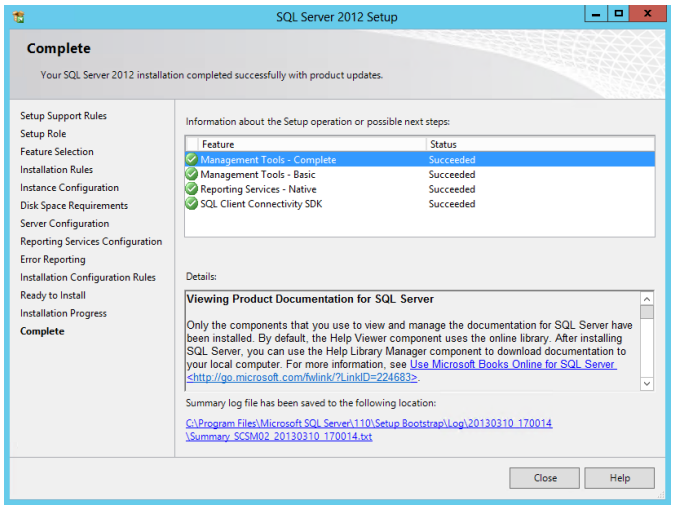
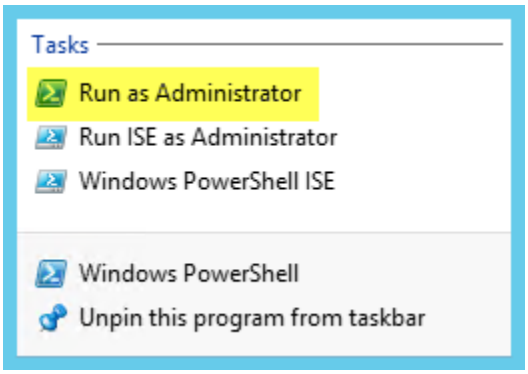
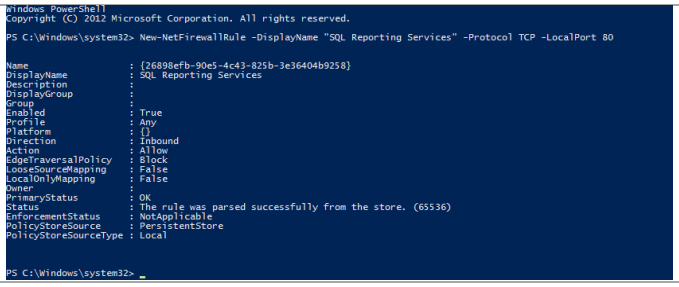
In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.

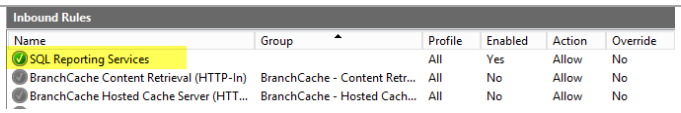
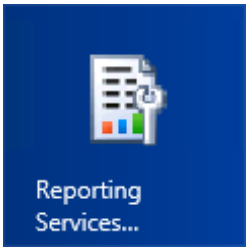
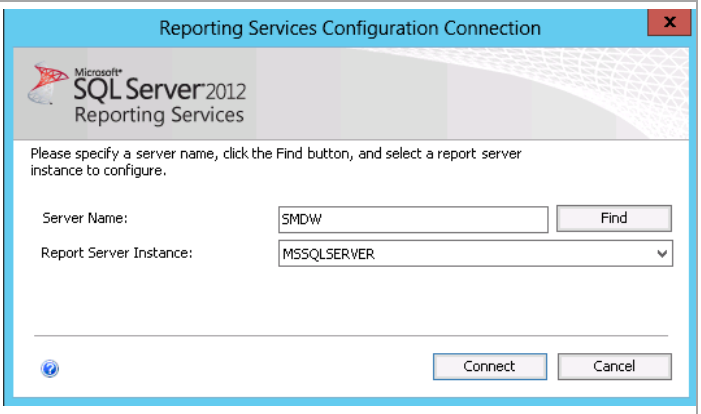
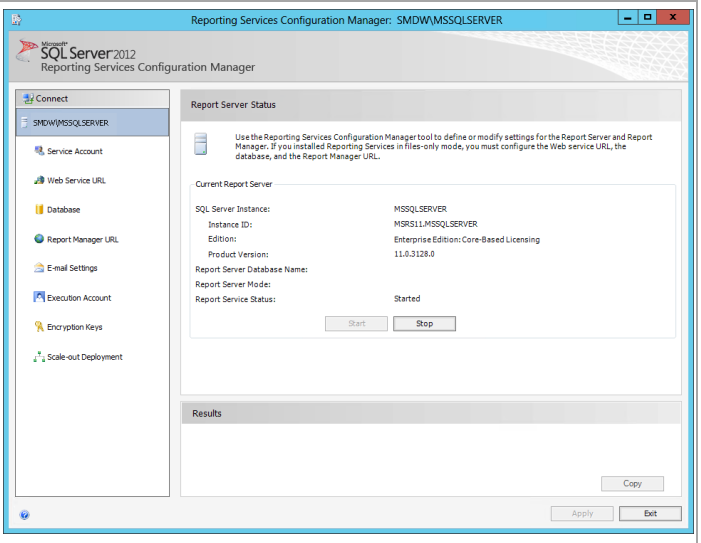


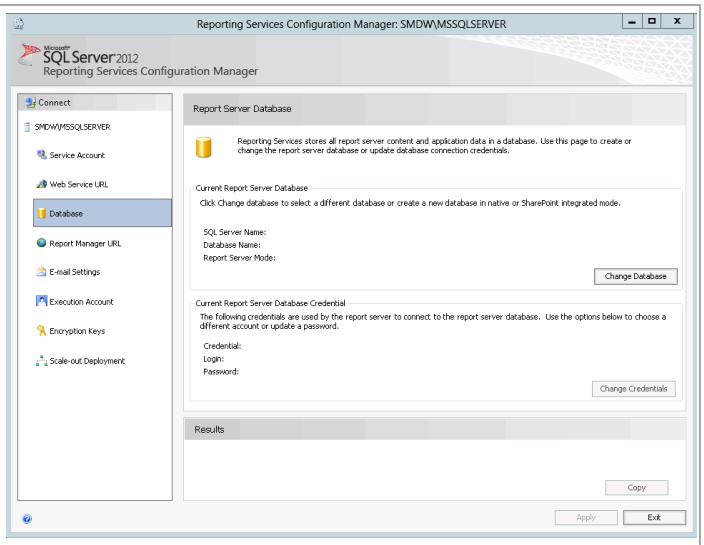
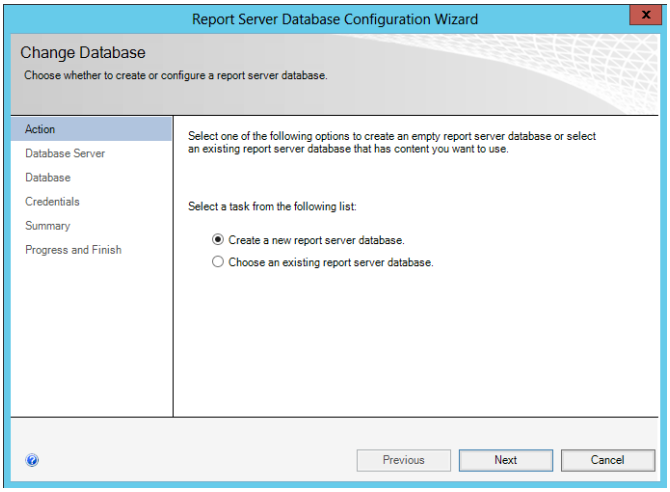
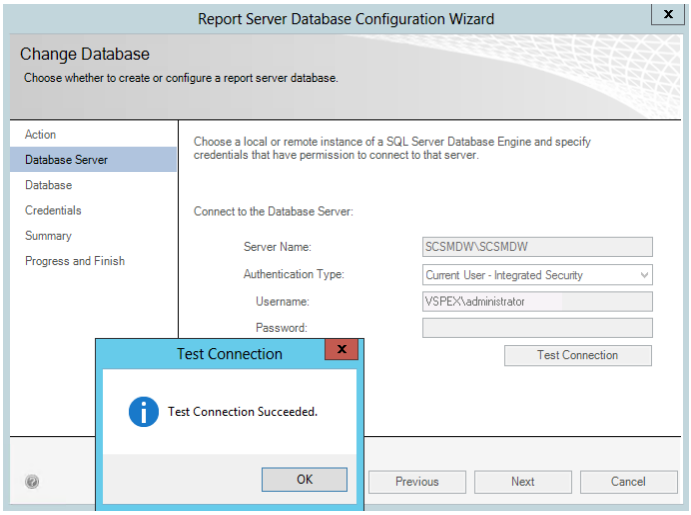
In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NT AUTHORITY\NETWORK SERVICE** account for the SQL Server Reporting Services service.
Click **Next** to continue.

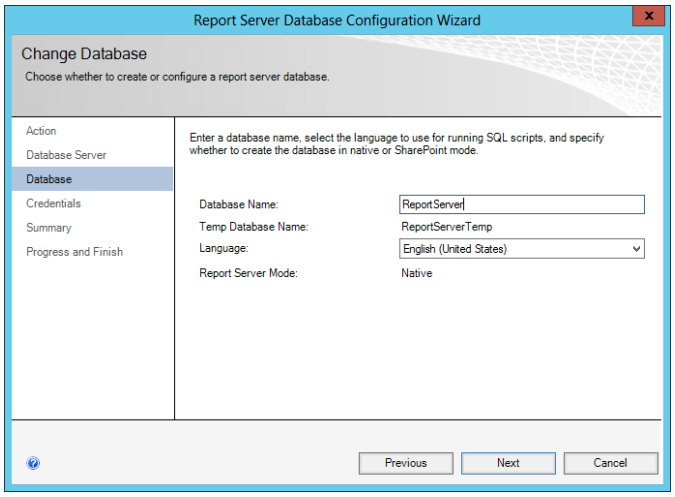
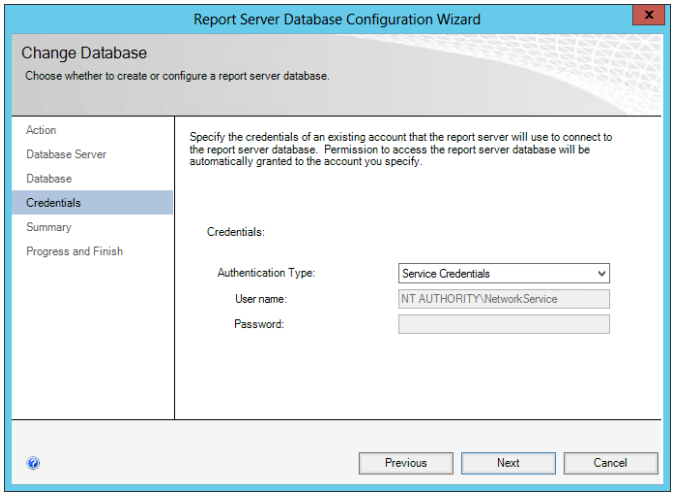
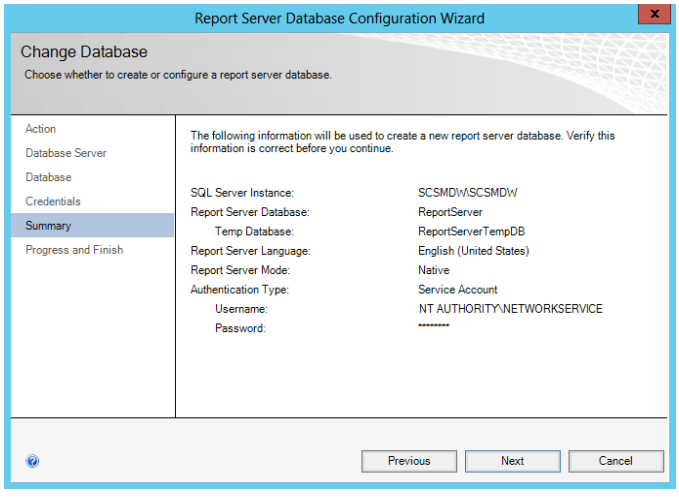


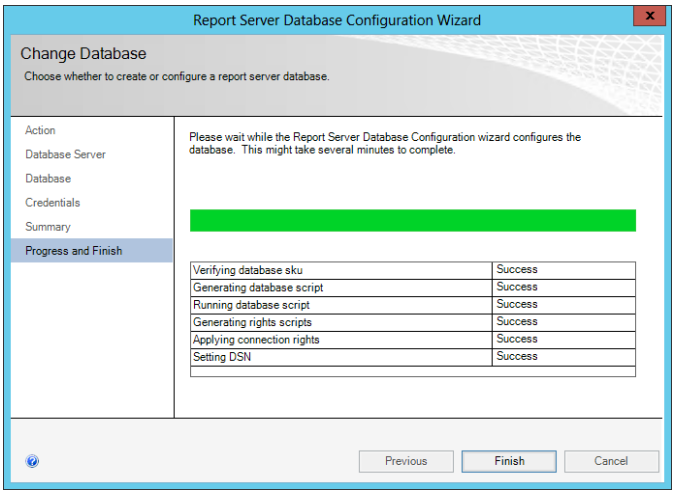
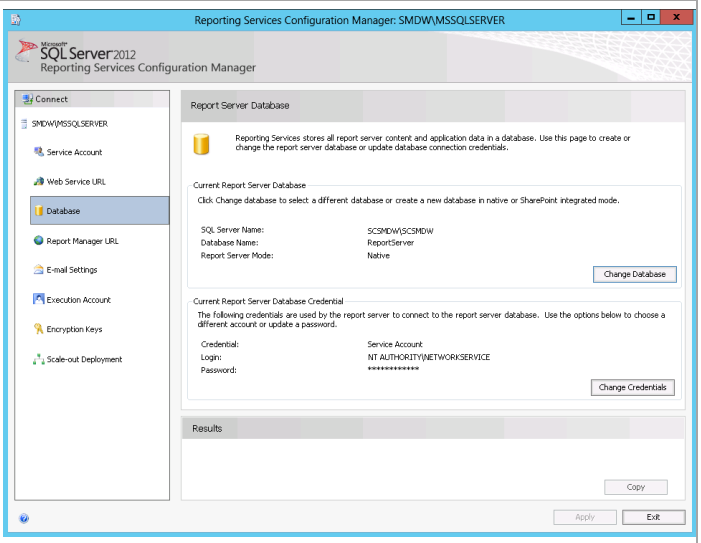
In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.	
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.	
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.	

In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.	
When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.	
By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled. Open an administrative session of PowerShell.	
Execute the following command to create the needed Firewall Rules: `New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80` Adjust the display names and ports based on organizational requirements.	

Open the **Windows Firewall with Advanced Security** MMC console to verify the results. Once verified, close the MMC console.	
When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start** screen, navigate and select the **Reporting Services Configuration Manager** tile.	
The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Service Manager server. In the **Report Server Instance** text box, use the default **MSSQLSERVER** drop-down menu value. Click **Connect**.	
The **Reporting Services Configuration Manager** tool will appear.	

In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.	
The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.	
In the **Database Server** section, specify the following values: • **Server Name** – *specify the name of the SQL Server Cluster SCSMDW Instance CNO and the database instance created for the Service Manager Data Warehouse installation.* • **Authentication Type** – *specify* ***Current User – Integrated Security*** *from the drop-down menu.* Click the **Test Connection** button to verify the credentials and database connectivity. Once verified, click **Next** to continue.	

In the **Database** section, specify the following values: • **Database Name** – *accept the default value of ReportServer.* • **Language** – *specify the desired language option from the drop-down menu.* • **Report Server Mode** – *select the **Native Mode** option.* Click **Next** to continue.	
In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.	
In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.	

The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.	
In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.	

In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer** in the provided text box.

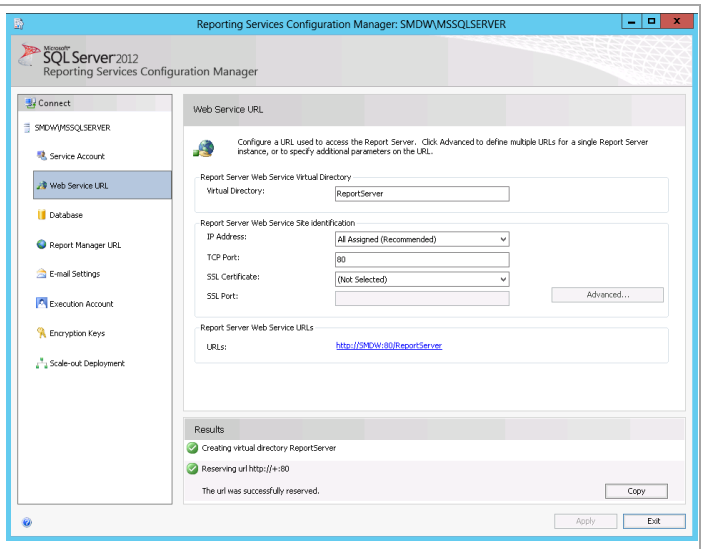
- In the **Report Server Web Service Site Identification** section, set the following values**:**

    - **IP Address** – *set the **All Assigned** drop-down menu value.*

    - **TCP Port** – *specify the desired TCP Port (default 80).*

    - **SSL Certificate** – *select the available certificate or choose the default of (Not Selected).*

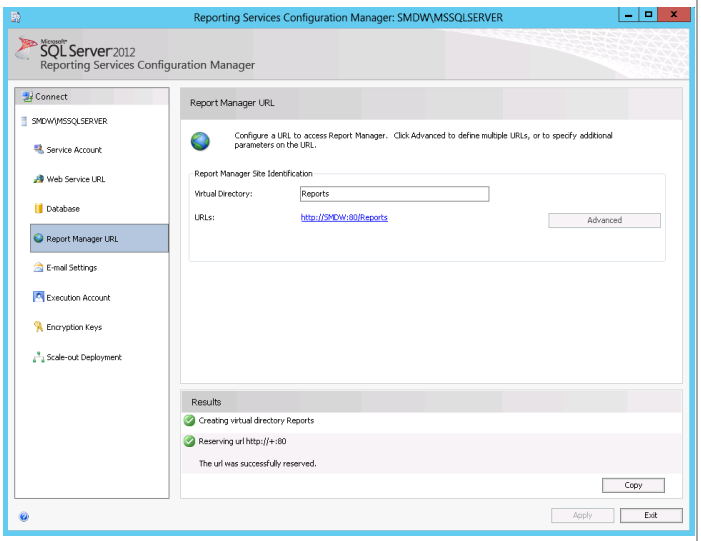
Click the **Apply** button to save the settings and create the Web Service URL.



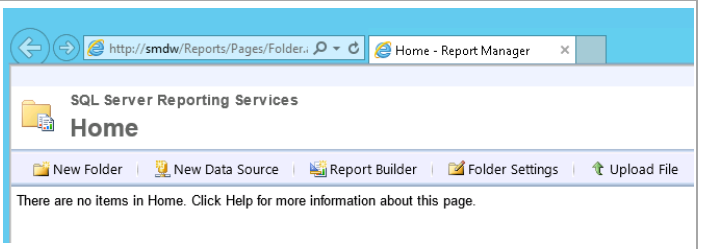
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

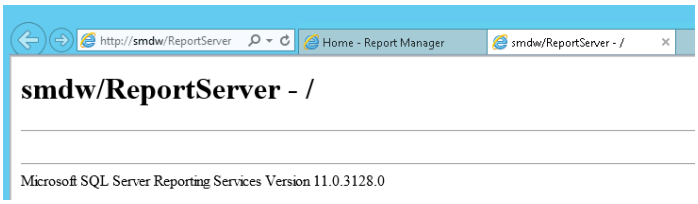
- In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports** (default) in the provided text box.

Click the **Apply** button to save the settings and create the Report Manager URL.



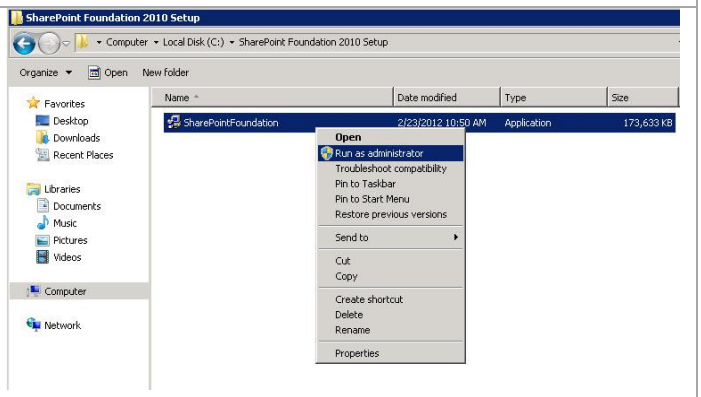
Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



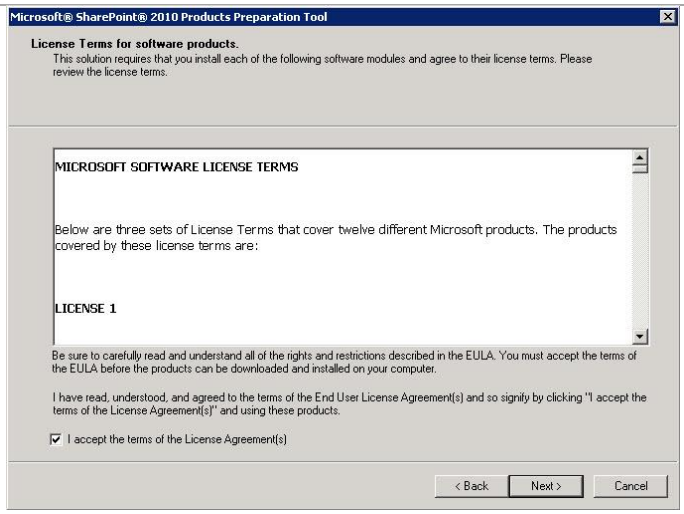
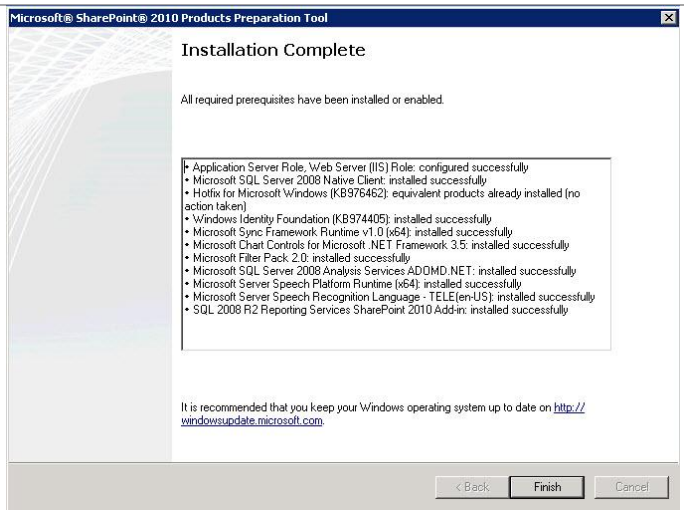
Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly. **Note:** In order to test the URL directory from the Service Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.	
Close the Reporting Server Configuration Manager.	

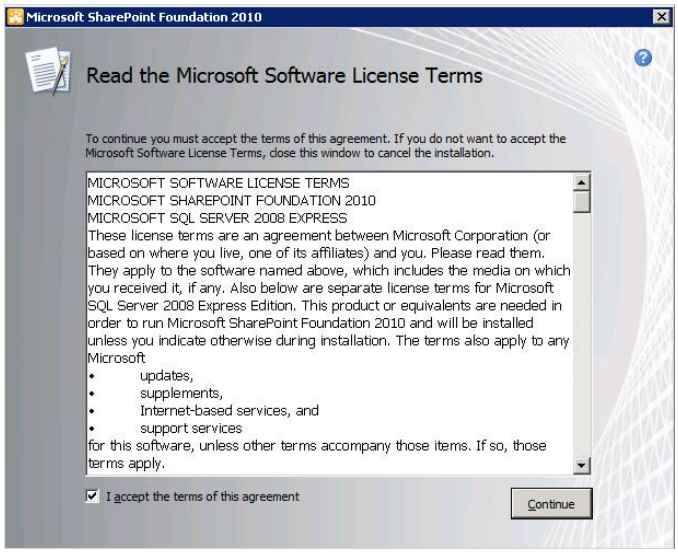
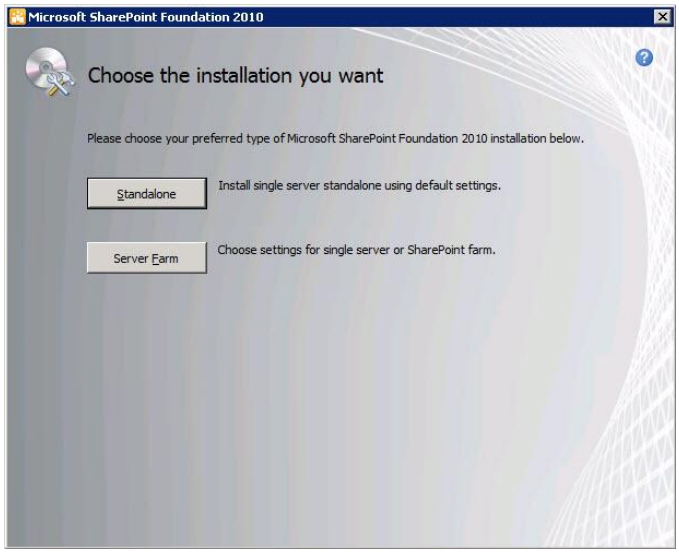
Install SharePoint Foundation 2010 Service Pack 1 on the Self-Service Portal Server

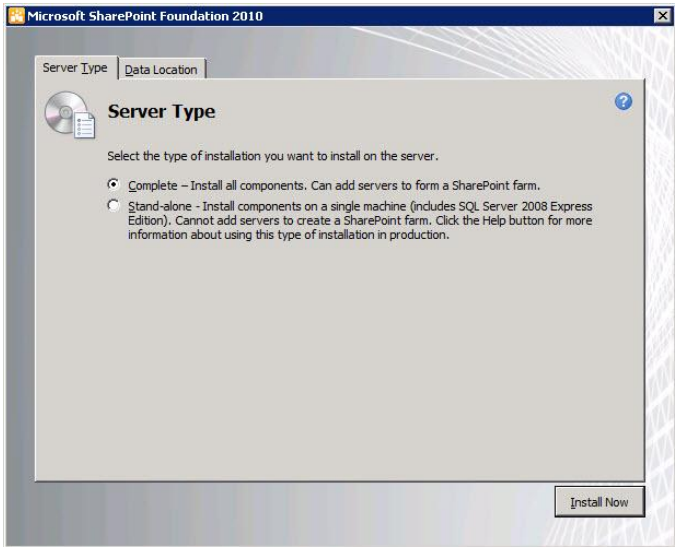
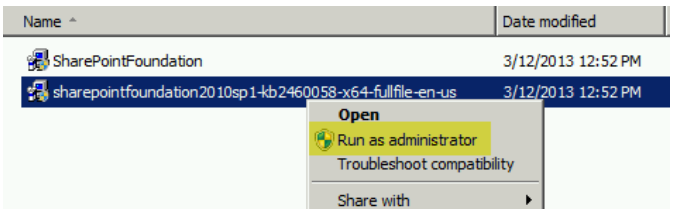
SharePoint Foundation 2010 SP1 must be installed to allow for configuration of SharePoint with the SQL Server 2012 installation. The following steps must to be completed in order to install SharePoint Foundation 2010 SP1 on the Service Manager self-service portal server only.

▶ Perform the following steps on the **Service Manager self-service portal** virtual machine.
Log on to Service Manager self-service portal server (**NOT** a Service Manager management server or the Data Warehouse server). Locate the SharePoint Foundation 2010 installation file. Right-click **SharePointFoundation.exe** and select **Run as administrator** from the context menu to begin setup.[15] 
The **SharePoint Foundation 2010** setup dialog will appear. In the **Install** section, select **Install software prerequisites**. 

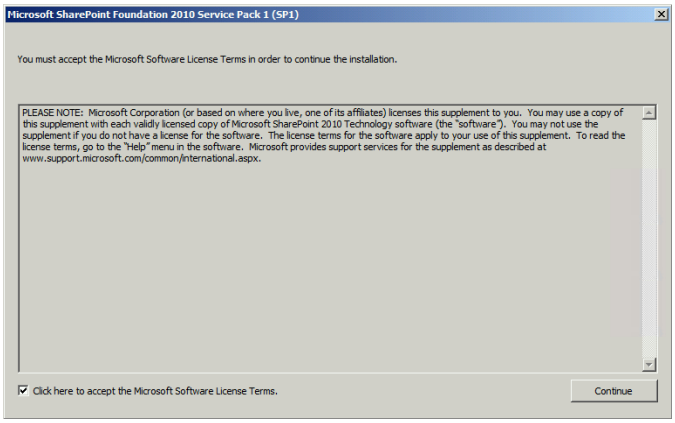
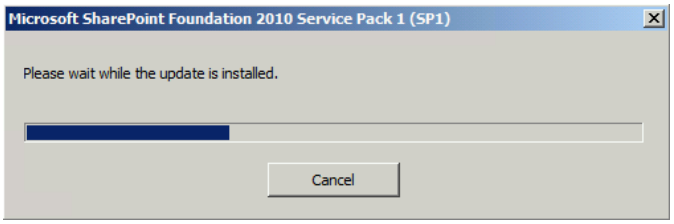
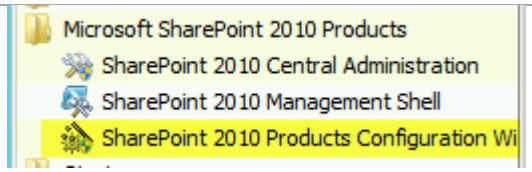
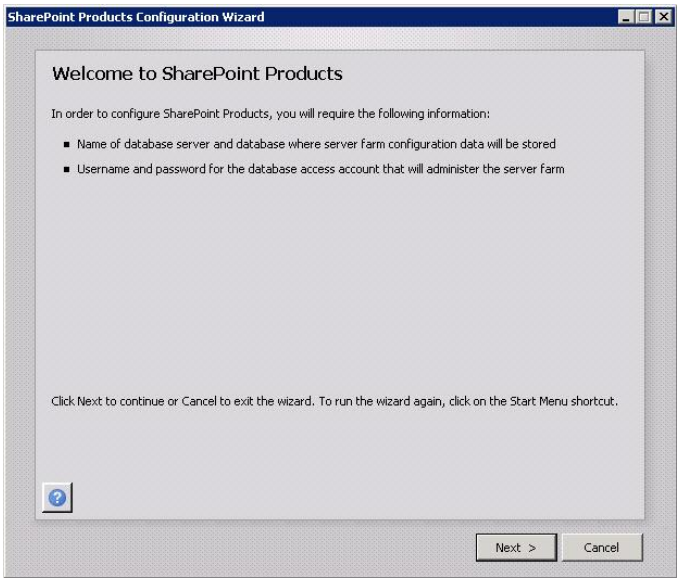
15 Microsoft SharePoint Foundation 2010 - http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5970.

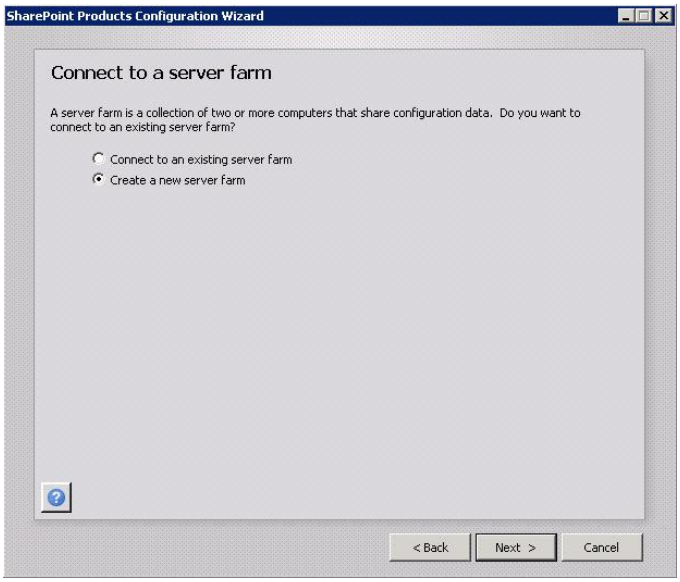
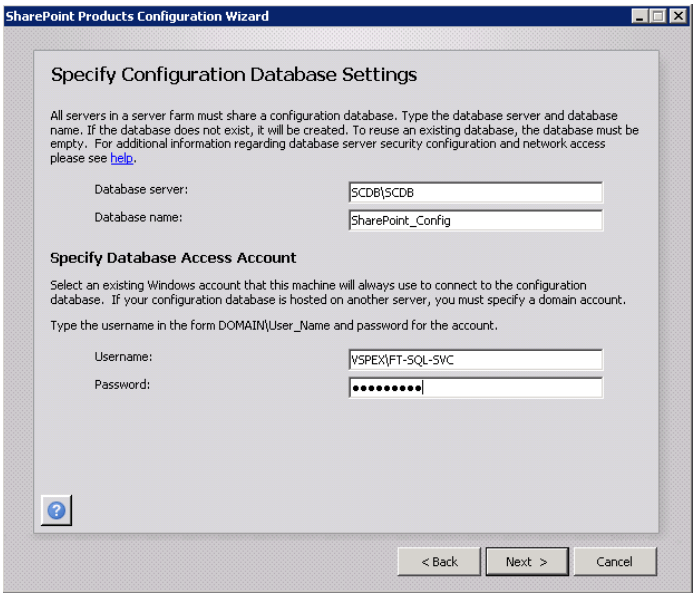
The **Microsoft SharePoint 2010 Products Preparation Tool** will open. Click **Next** to continue.	
In the **License Terms for software products** dialog, verify that the **I accept the terms of the License Agreement** installation option check box is selected and click **Next** to continue.	
After the prerequisites install, the **Installation Complete** dialog will appear. Click **Finish** to complete the installation then **restart** the system.	

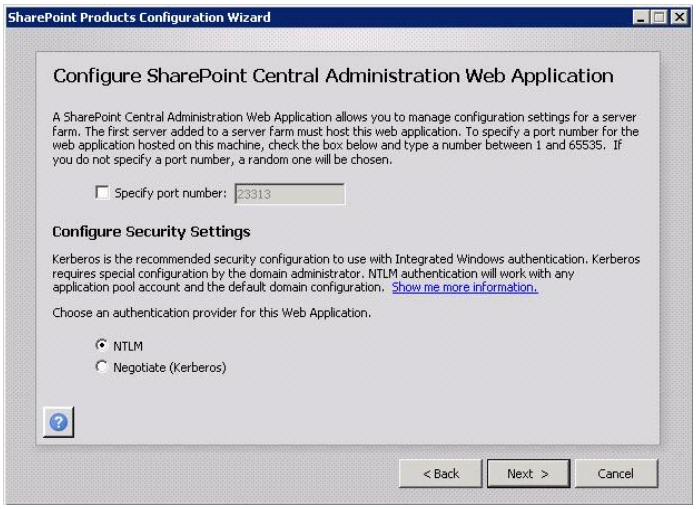
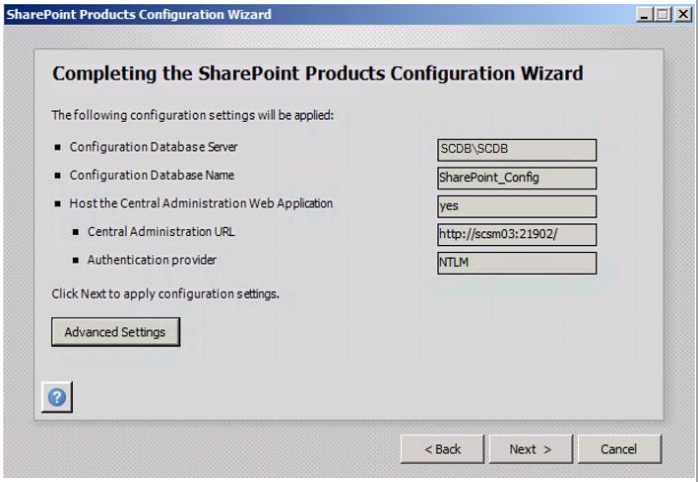
After the system restart, log back on with an account with administrative privileges. Re-launch the SharePoint Foundation 2010 installation. In the **SharePoint Foundation 2010** setup dialog, navigate to the **Install** section and select **Install SharePoint Foundation**.	
In the **Read the Microsoft Software License Terms** dialog, verify that the **I accept the terms of this Agreement installation** option check box is selected and click **Continue**.	
In the **Choose the installation you want** dialog, click the **Server Farm** button.	

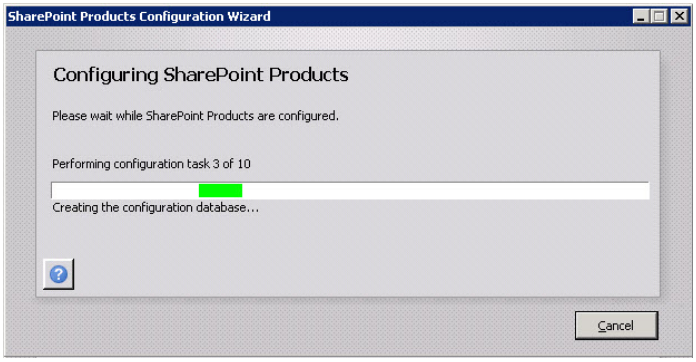
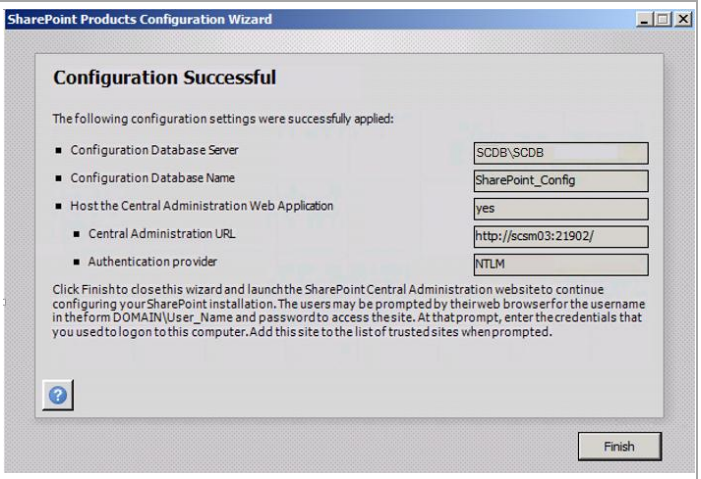
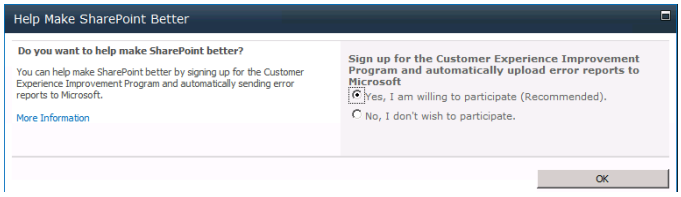
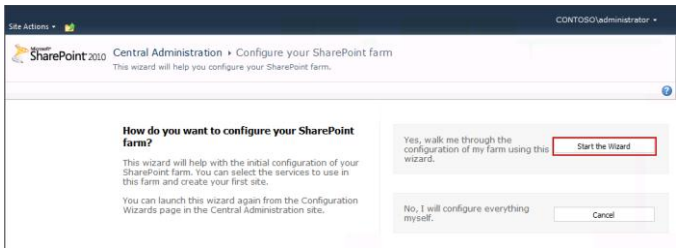
In the **Server Type** dialog, select the **Complete** option and click **Install Now**.	
After installation, the **Run Configuration Wizard** dialog will appear. Verify that the **Run the SharePoint Products Configuration Wizard now** check box is <u>not selected</u> and click **Close**. **Note:** SharePoint Foundation Server 2010 Service Pack 1 must be installed prior to the configuration wizard being run.	
Service Pack 1 <u>must</u> be applied to SharePoint Foundation server after this installation.[16] Locate the Service Pack 1 for SharePoint Foundation 2010 installation file, right-click the installation file and select **Run as administrator** from the context menu to begin the Service Pack setup.	

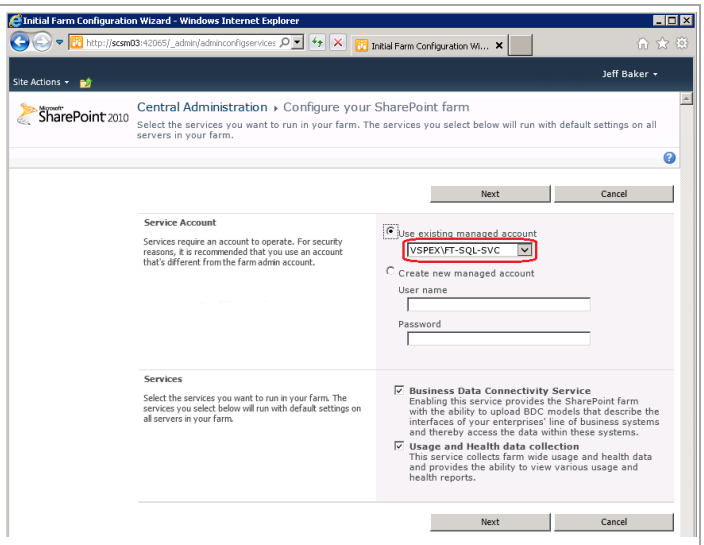
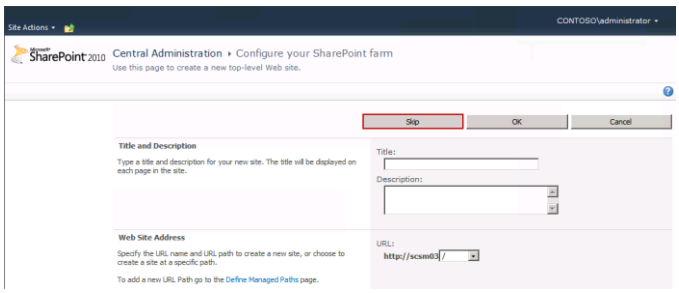
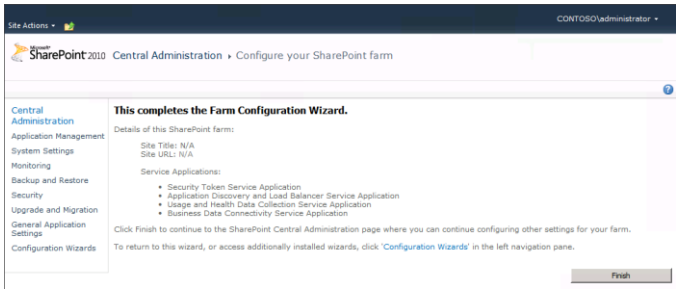
[16] Microsoft SharePoint Foundation 2010 SP1 - http://www.microsoft.com/download/en/details.aspx?id=26640.

The **Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1**) wizard will appear. Verify that the **Click here to accept the Microsoft Software License Terms** installation option check box is selected and click **Continue**.	
The installation will continue without interaction until it completes. When prompted, click **OK** to complete the installation. You must restart the system after the service pack installation.	
From the **Start** menu, expand the **Microsoft SharePoint 2010 Products** program folder and select **SharePoint 2010 Products Configuration Wizard**.	
The **SharePoint Products Configuration Wizard** will appear. Click **Next** to continue with the wizard.	

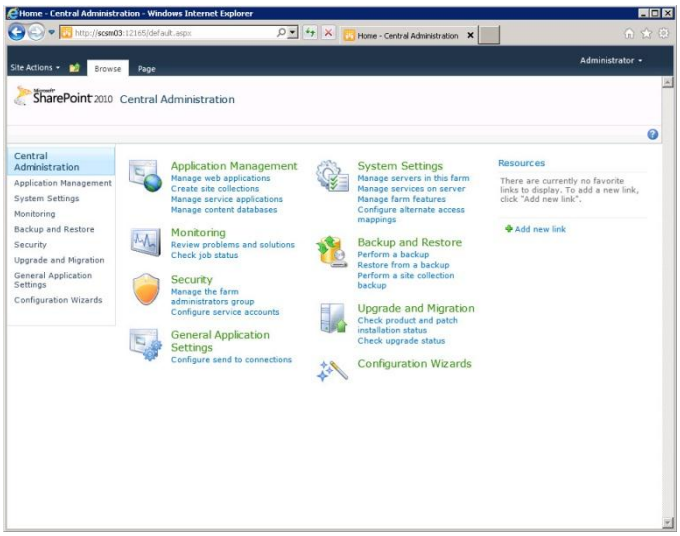
A dialog will appear that states that some services require restart as part of the installation. Click **Yes** to perform the services restart.	
The **Connect to a server farm** dialog will appear. Select the **Create a new server farm** option and click **Next** to continue.	
In the **Specify Configuration Database Settings** dialog, specify the following information in the provided text boxes: • **Database server** – *specify the name of the SQL Server CNO and the database instance created for the Service Manager installation.* • **Database name** – *specify the name of the SharePoint database. In most cases the default value of SharePoint_Config should be used.* In the **Specify Database Access Account** section, specify the Username (<DOMAIN>\<USERNAME>) and associated password for the Service Manager Service Account. Once complete, click **Next** to continue.	

In the **Specify Farm Security Settings** dialog, enter a unique passphrase in the **Passphrase** text box. Re-type the passphrase in the **Confirm passphrase** text box and click **Next** to continue.	
In the **Configure SharePoint Central Administration Web Application** dialog specify a TCP port by selecting the **Specify port number** check box and providing a port number in the supplied text box. In the **Configure Security Settings** section, select the **NTLM** option. When completed, click **Next** to continue.	
The **Completing the SharePoint Products Configuration Wizard** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Next** to continue.	

The wizard will display the progress while performing the SharePoint configuration.	
When successful, the **Configuration Successful** dialog will appear. Click **Finish** to complete the configuration of SharePoint Foundation 2010 Service Pack 1.	
When prompted in the **Help Make SharePoint Better** page, select the appropriate option based on your organization's policies and click **OK** to save this setting.	
In the **Central Administration - Configure your SharePoint farm** page, click the **Start the Wizard** button to begin the SharePoint configuration.	

In the **Service Account** section, select the **Use existing managed account** and select the Service Manager Service Account from the drop-down menu. In the **Services** section, select the **Business Data Connectivity Services** and **Usage and Health data collection** check boxes. Click **Next** to continue.	
In the Web Site configuration page, click the **Skip** button to continue without configuring these settings.	
The SharePoint farm configuration is now complete. Click the **Finish** button to exit.	

The **SharePoint Central Administration** portal will open. Verify that SharePoint is operating properly by launching the Central Administration portal prior to proceeding to the Service Manager self-service portal installation.



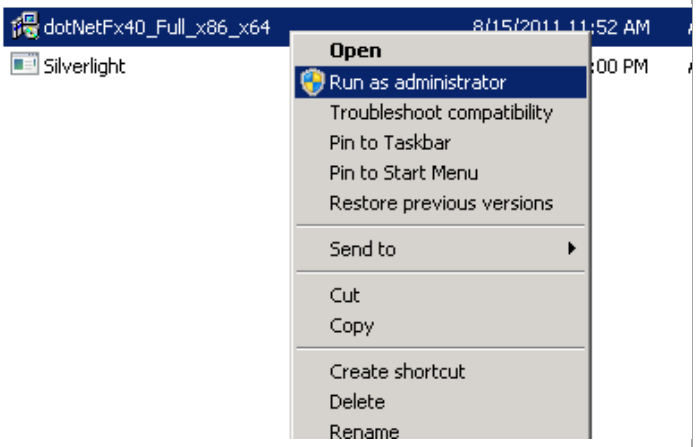
Install .NET Framework 4 on the Self-Service Portal Server

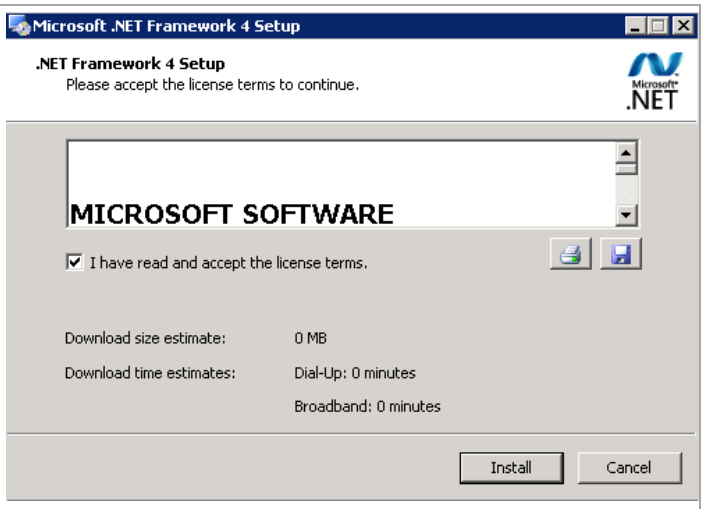
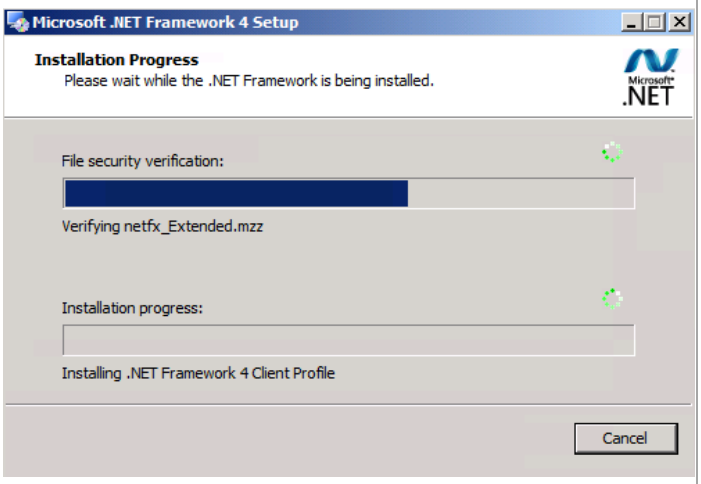
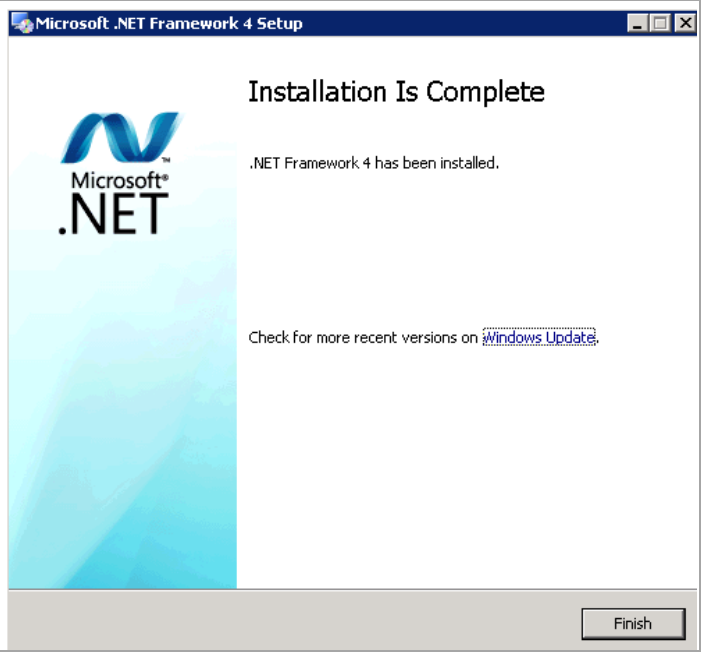
Additionally, the Service Manager self-service portal installation also requires the .NET Framework 4 package to be installed prior to installation. Follow the provided steps to install the .NET Framework 4 on the self-service portal.

Note: If you have applied all the latest patches, including optional patches, .NET Framework 4.0 will already be installed.

▶ Perform the following steps on the **Service Manager self-service portal** virtual machine.

From the installation media source, right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** from the context menu to begin setup.



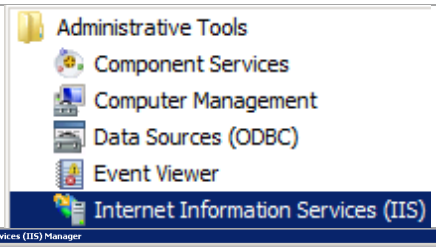
Within the **Microsoft .NET Framework 4 Setup** dialog, select the **I have read and accept the license terms** check box and click **Install** to begin the installation.	
The installation progress will be displayed in the setup wizard.	
When completed, click **Finish** to exit the installation.	

Request and Install an SSL Certificate on the Self-Service Portal Server

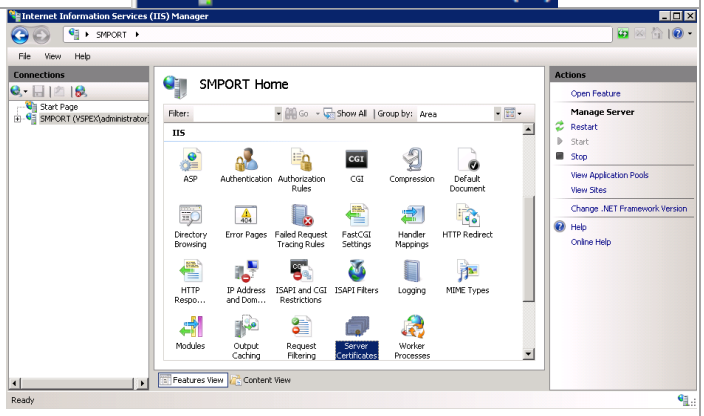
Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website. If the self-service portal is to be installed without SSL this section can be skipped. There are several ways to request an SSL Certificate. One method, through the IIS Manager console, is outlined below if you are using a third party certificate service.

▶ Perform the following steps on the **Service Manager self-service portal** virtual machine.

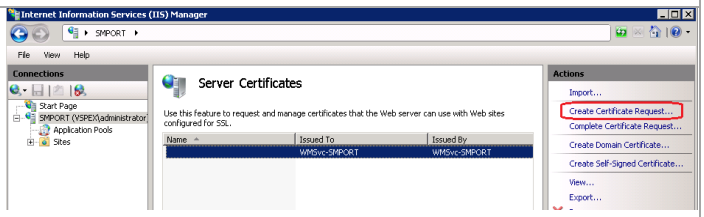
Log on to the Service Manager virtual machine with a user with local admin rights. From the Start Menu select **Administrative Tools** then select **Internet Information Services (IIS) Manager.**



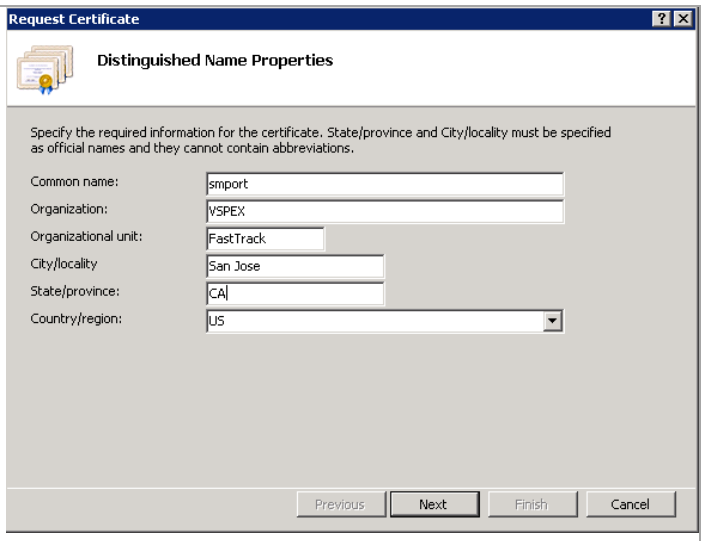
In the **Internet Information Services (IIS) Manager** console, select the server node and in the IIS section, double-click **Server Certificates**.



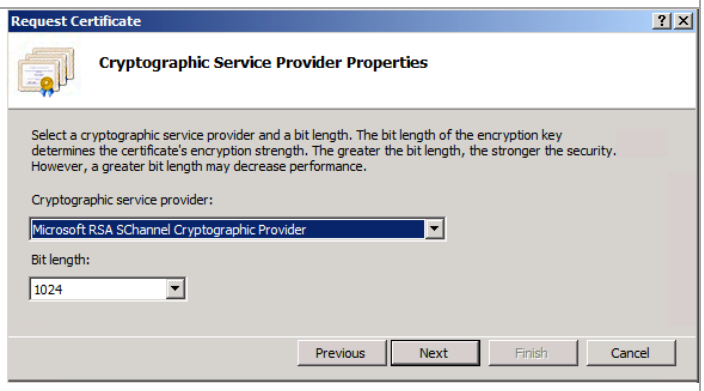
The **Server Certificates** pane will expand. Under actions, click **Create Certificate Request...**



The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name that the server will be accessed in the web browser. Click **Next** to continue.

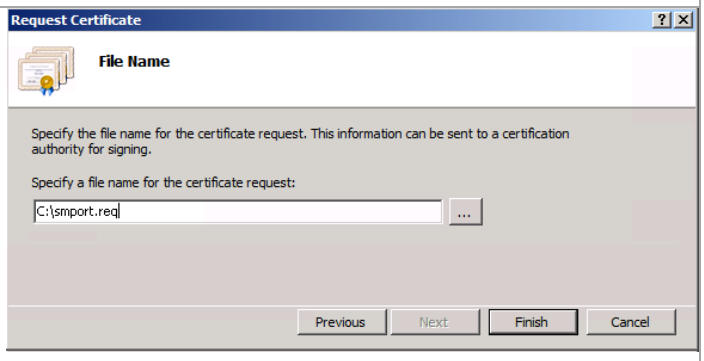


In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing certification authority (CA). In most cases, selecting the default CSP and default bit length is satisfactory.
Click **Next** to continue.

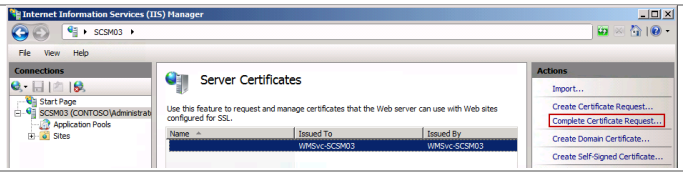


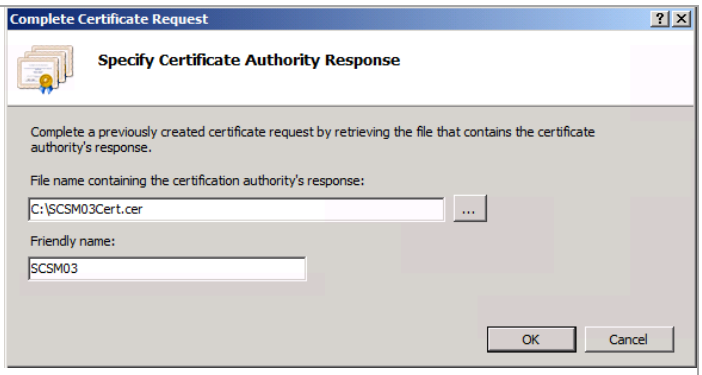
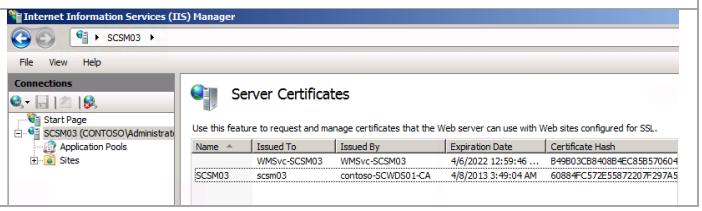
In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

When completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.



After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** once again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Click **OK** to complete the operation.	
In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.	

Configuration of Service Manager Environmental Prerequisites

The following steps must to be completed in order to install the Service Manager roles correctly.

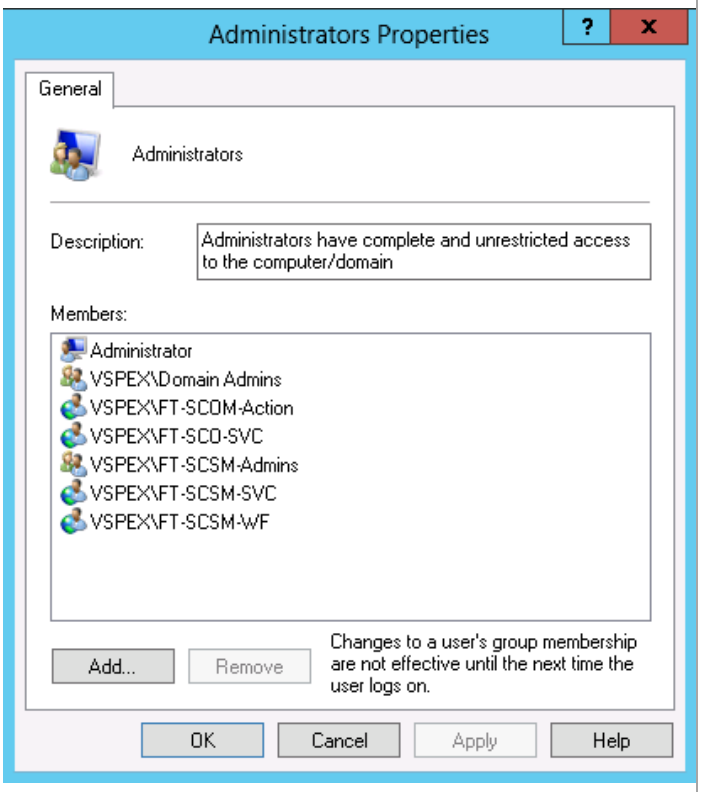
▶ Perform the following steps on **all Service Manager Servers** virtual machines.

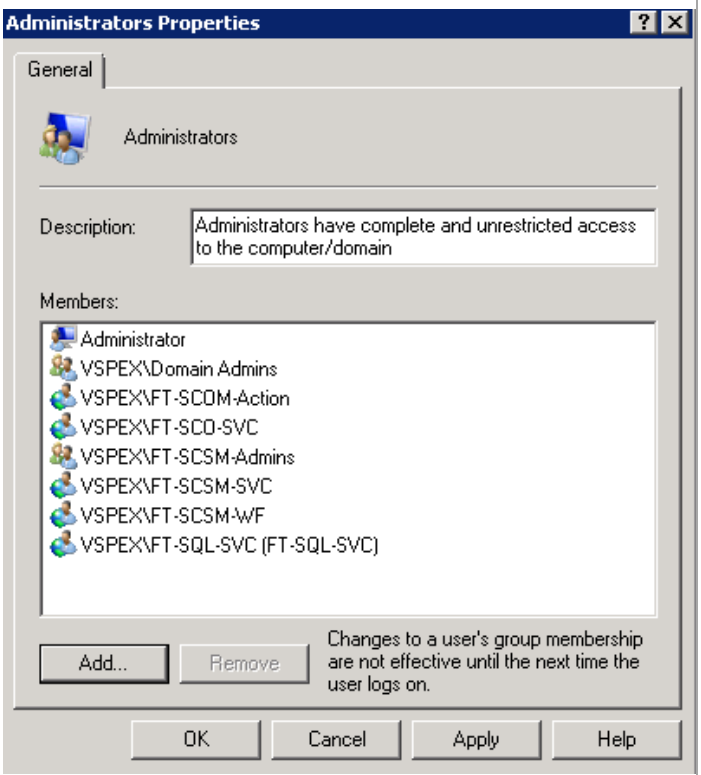
Log on to each Service Manager virtual machine with a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on each Service Manager virtual machine:

- Operations Manager action account.
- Service Manager workflow account.
- Service Manager service account.
- Service Manager Admins group.
- Orchestrator service account.

On the self-service portal server, also add the following accounts:

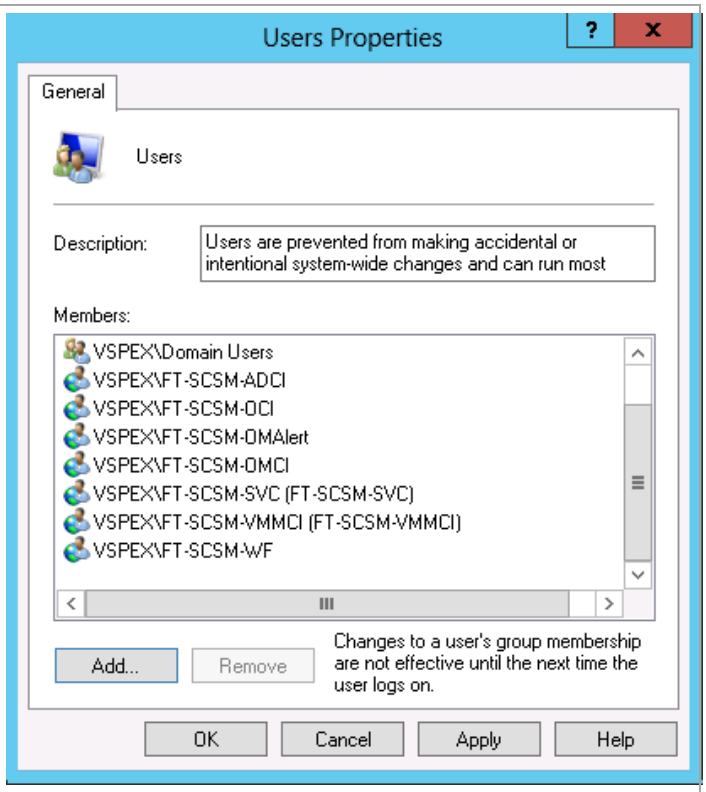
- SQL service account





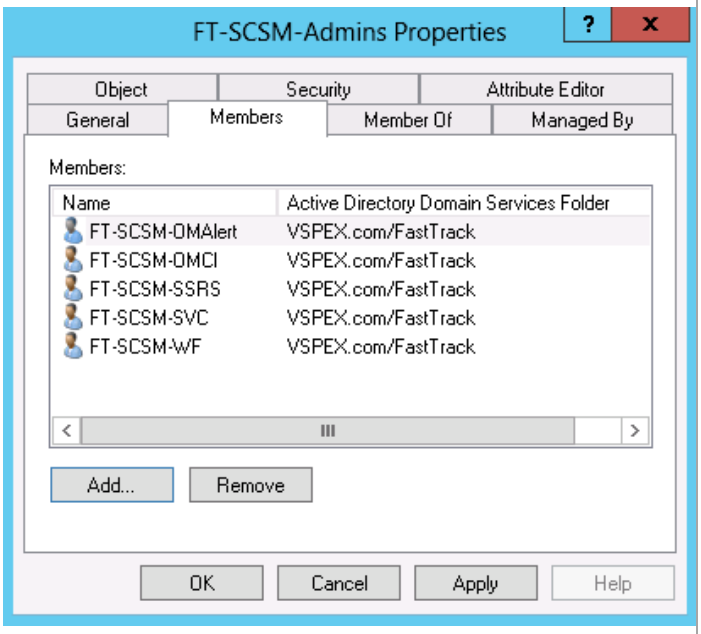
Verify that the following accounts and/or groups are members of the Local Users group on each Service Manager virtual machine:

- Service Manager Active Directory CI connection account.
- Service Manager Orchestrator CI connection account.
- Service Manager Operations Manager alert connection account.
- Service Manager Operations Manager CI connection account.
- Service Manager service account.
- Service Manager users group.
- Service Manager Virtual Machine Manager CI connection account.
- Service Manager workflow account.

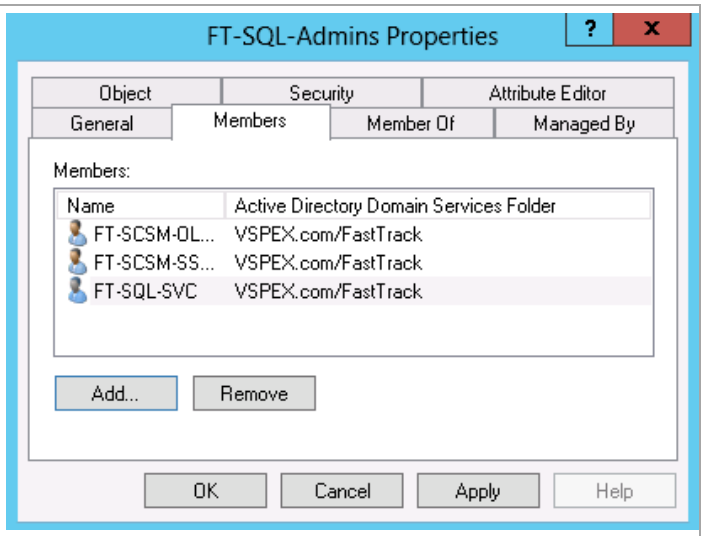


▶ Perform the following step on an **Active Directory Domain Controller** in the target environment.

In the domain where Service Manager will be installed, verify that the SM Operations Manager alert connectors and the Service Manager service accounts are members of the SM Admins group created earlier.

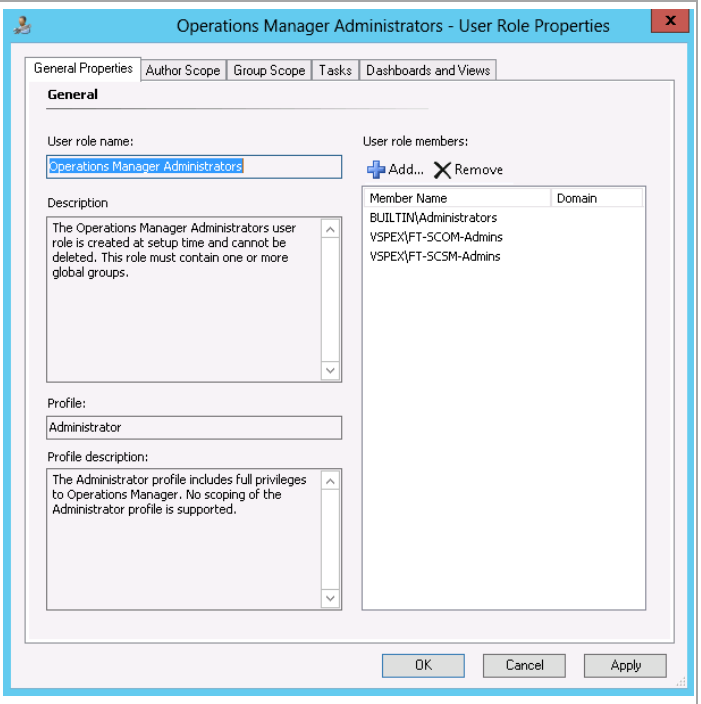


In the domain where Service Manager will be installed, verify that the SM OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group created earlier.

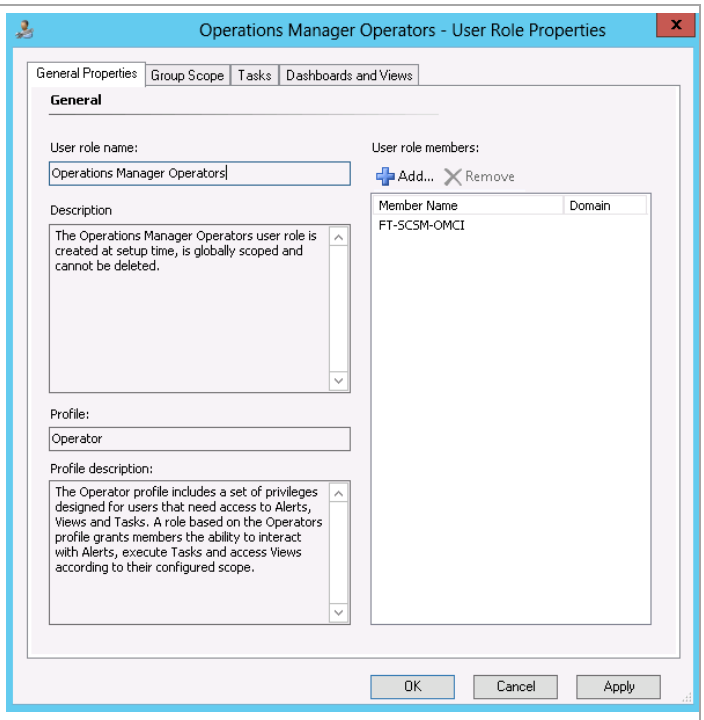


▶ Perform the following steps on the **Operations Manager** virtual machine.

Log on to the Operations Manager server as an Administrator. In the **Operations Manager console**, navigate to Administration pane. In the **Security** node under **User Roles**, locate the **Operations Manager Administrators** role and add the **SCSM Admins** group to the role.
Click **OK** to save the changes.



While still in the **Security** node under **User Roles**, locate the **Operations Manager Operators** role and add the **SCSM OMCI** user to the role.
Click **OK** to save the changes.



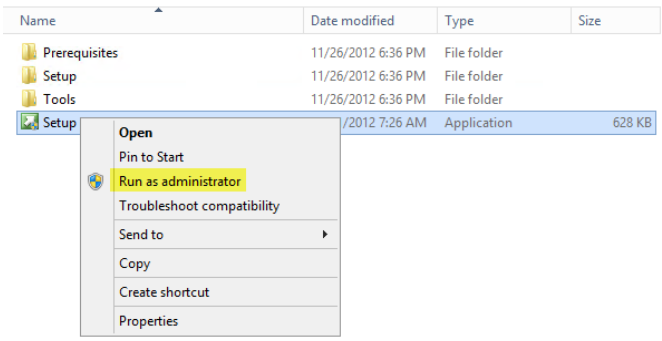
11.3 Installation

Installation – Management Server

The following steps must to be completed in order to install the Service Manager Management Server role.

▶ Perform the following steps on the **first Service Manager management server** virtual machine.

Log on to Service Manager management server (**NOT** the Service Manager Data Warehouse server or the self-service portal server).
From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



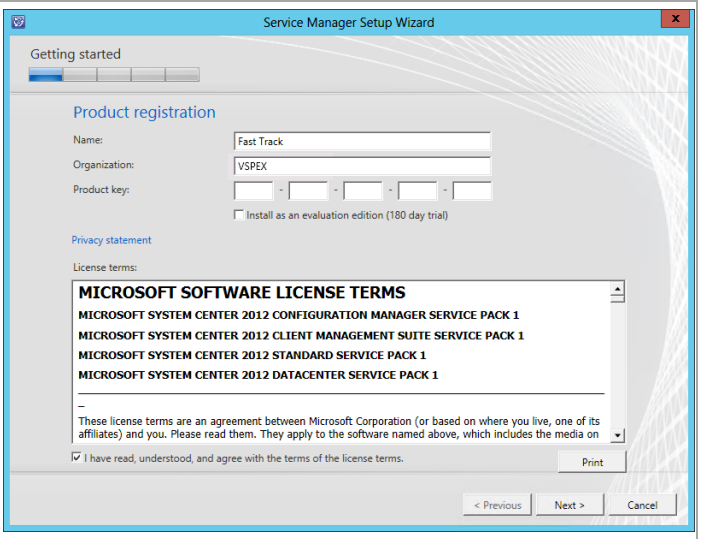
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager management server** to begin the Service Manager server installation.



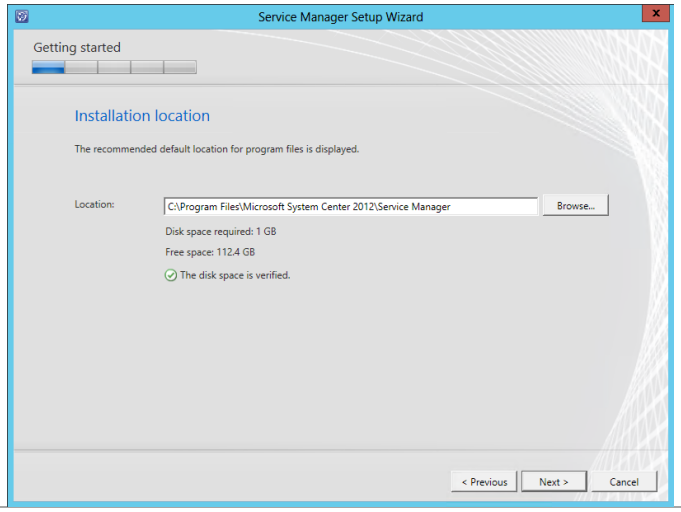
In the **Product registration** dialog, provide the following information in the provided text boxes:

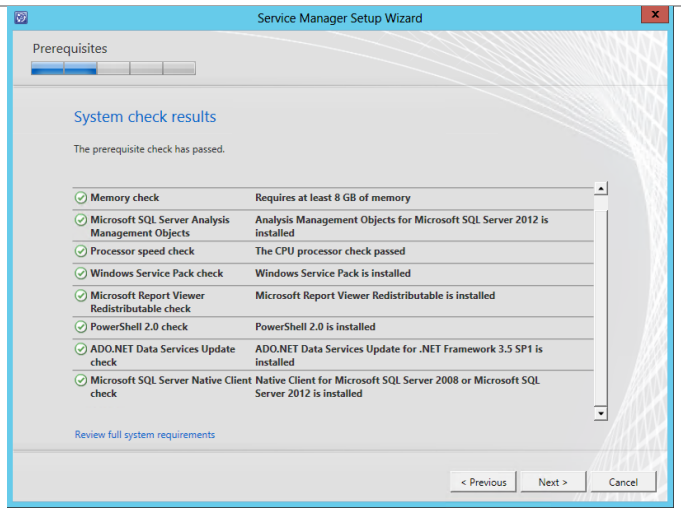
- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** – *specify the name of the licensed organization*.
- **Product key** – *provide a valid product key for installation of Service Manager. If no key is provided, select the* ***Install as an evaluation edition (180-day trial)*** *check box*.

In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. Once all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation.
Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.	

In the **Configure the Service Manager database** dialog, specify the following information in the provided text boxes:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation.*

- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation.*

Select the **Create a new database** option and specify the following information in the provided text boxes:

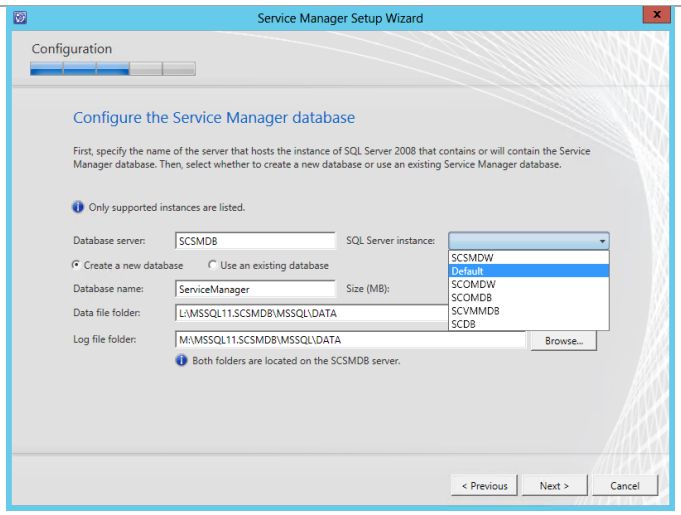
- **Database name** – *specify the name of the Service Manager database. In most cases the default value of ServiceManager should be used.*

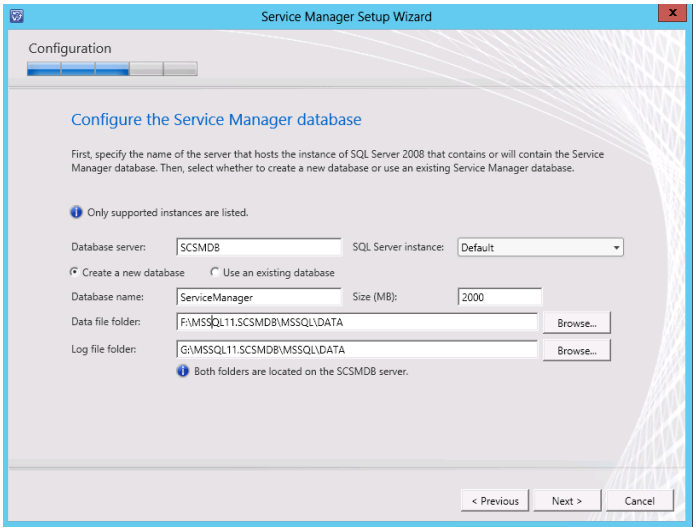
- **Size (MB)** – *specify the initial database size[17]. The default value can be used for Fast Track validation.*

- **Data file folder** – *specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager database. This should be cross-checked with the worksheet identified earlier.*

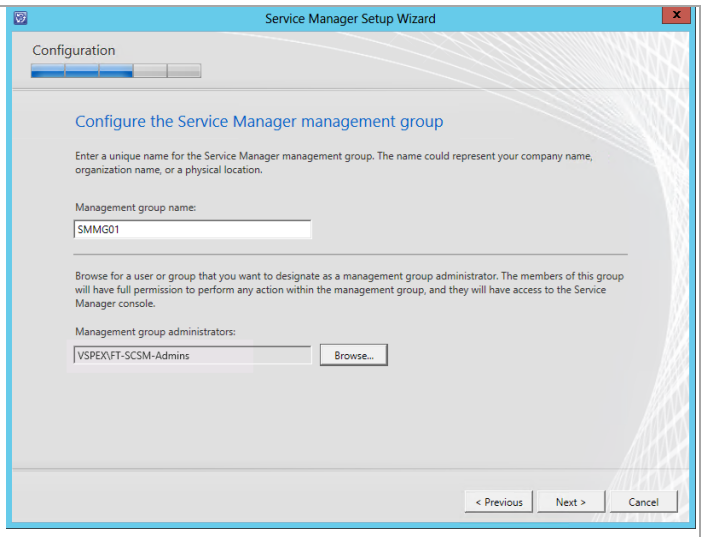
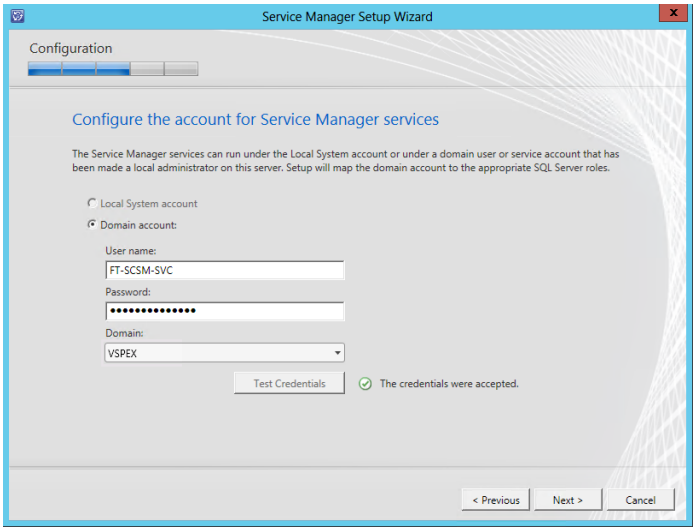
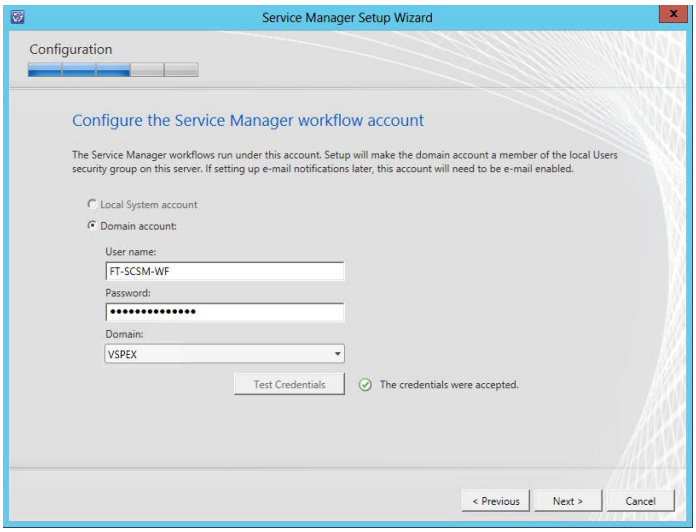
- **Log file folder** – *specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager database. This should be cross-checked with the worksheet identified earlier.*

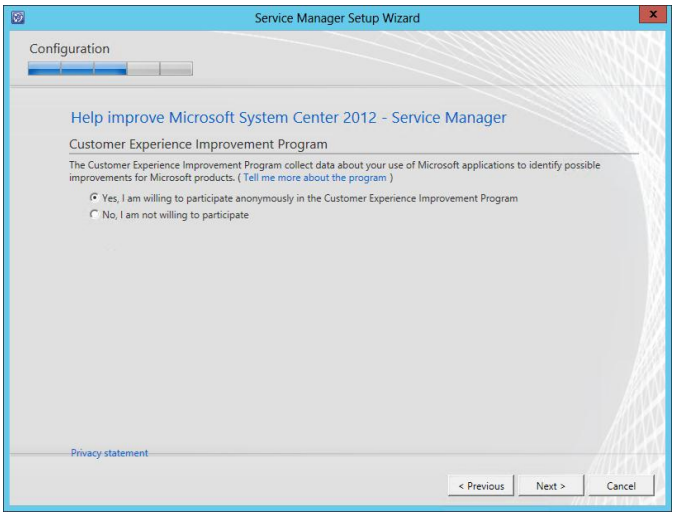
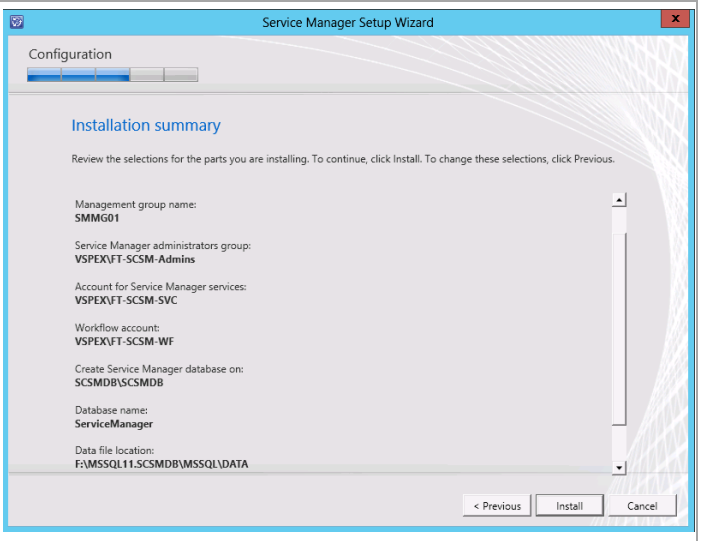
Click **Next** to continue.

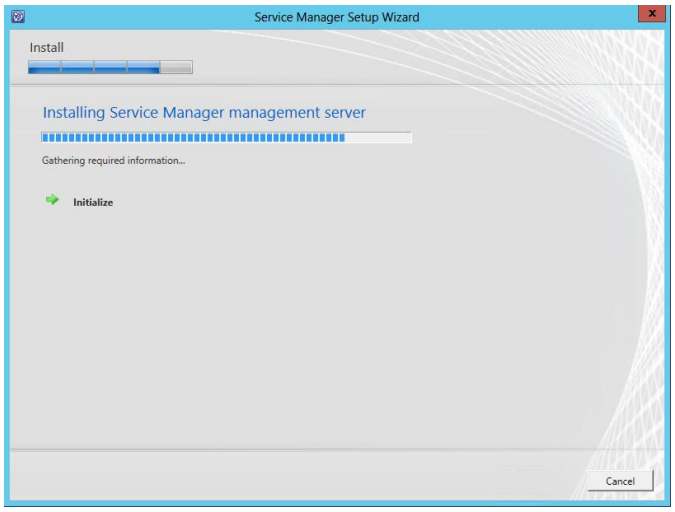
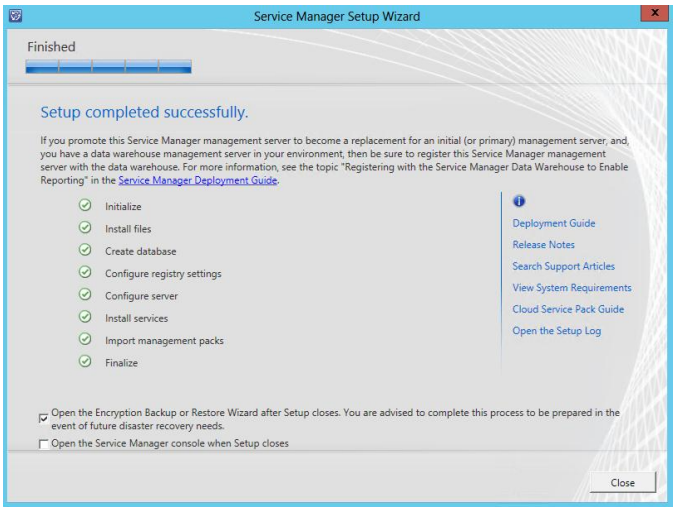


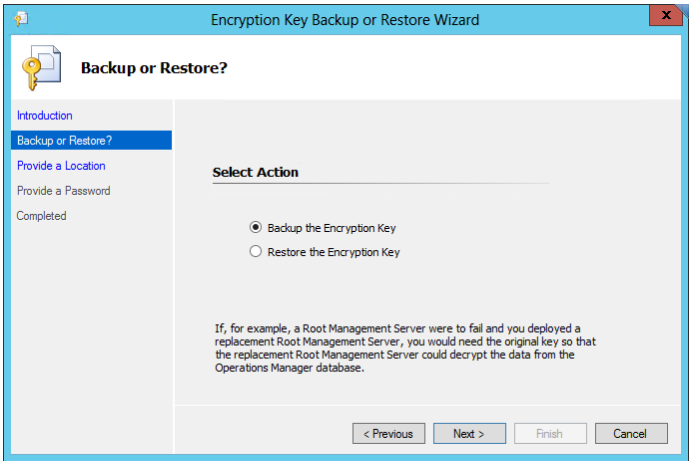
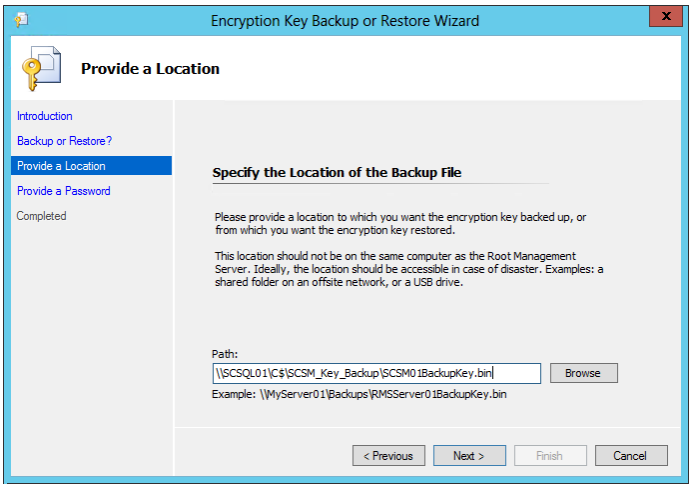
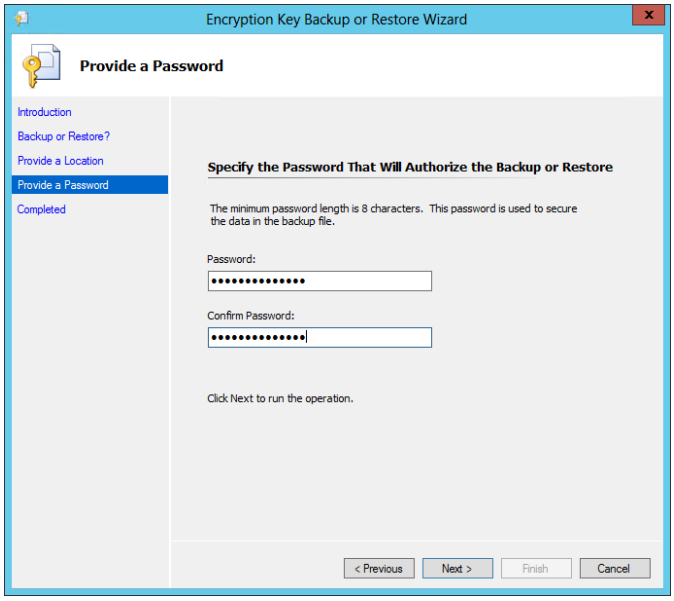


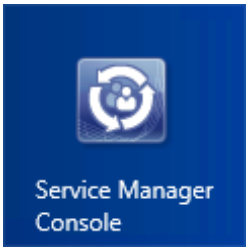
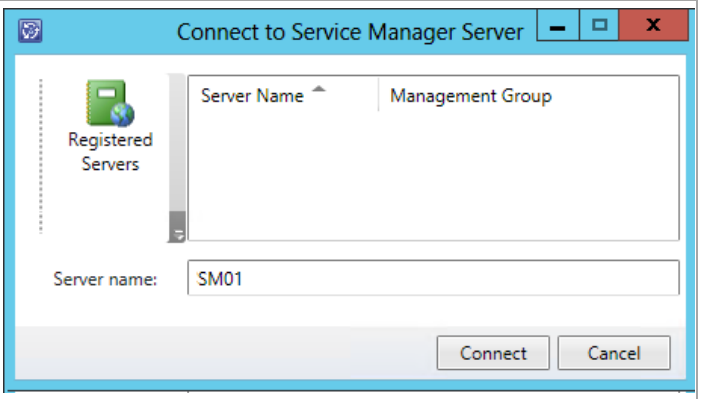
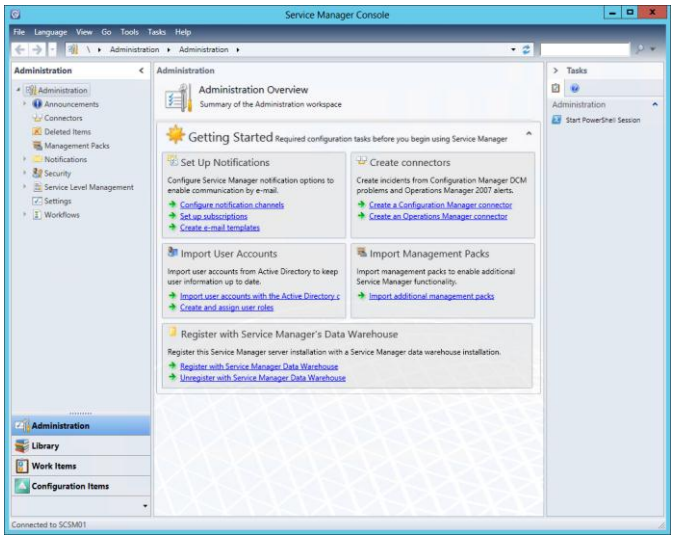
[17] Planning for Performance and Scalability in System Center 2012 - Service Manager - http://technet.microsoft.com/en-us/library/hh495684.aspx contains a link to the Service Manager job aids and provides general guidance for database sizing

In the **Configure the Service Manager management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager Data Warehouse and Operations Manager installations. Specify the Service Manager Administrators group in the **Management group administrators** object picker section. Click **Next** to continue.	
In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.	
In the **Configure the account for Service Manager workflow account** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. Once successful, click **Next** to continue.	

In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

The wizard will display the progress while installing features.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Once all steps show successful installation, ensure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to launch the wizard after setup. Click **Close** to complete the installation.	
When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.	

In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.	
In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** text box and object picker. The directory for the backup location must exist. Click **Next** to continue.	
In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.	

When complete, click **Finish** to exit the wizard.	
When installed, verify that the Service Manager management server installed properly by opening the console. From the **Start** screen, click the **Service Manager Console** tile.	
In the **Connect to Service Manager Server** dialog, specify the Service Manager management server name in the **Server name** text box and click **Connect** to start the console.	
The Service Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.	

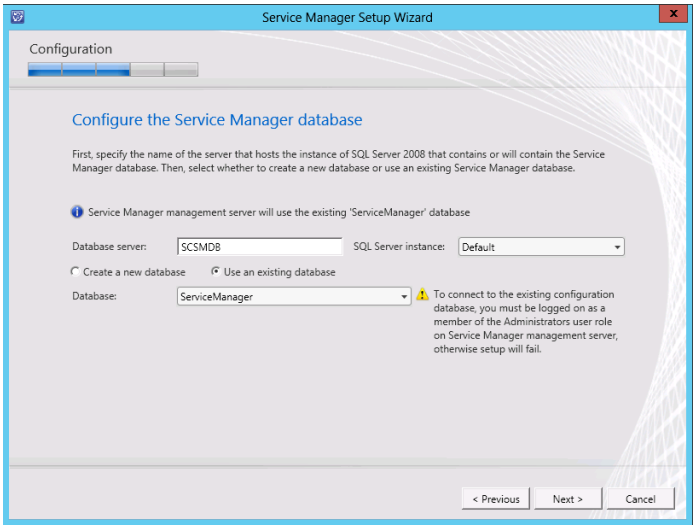
Installation – Second Management Server

The following steps must to be completed in order to install the Service Manager Management Server role. The process is the same as the installation on the first machine except for the following changes.

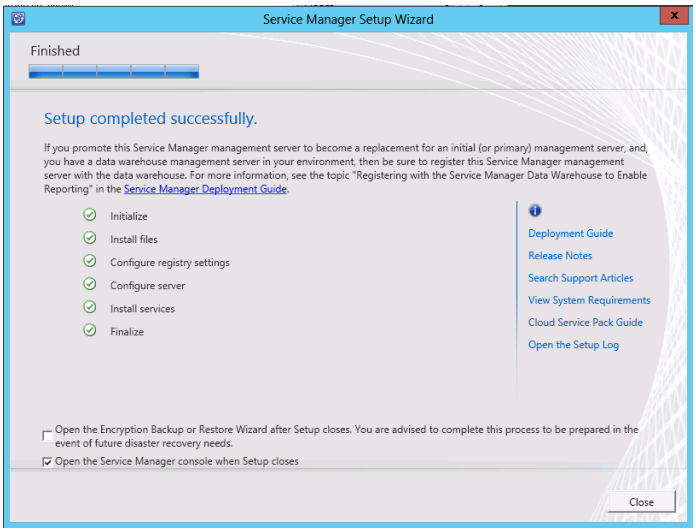
▶ Perform the following steps on the **second Service Manager management server** virtual machine.

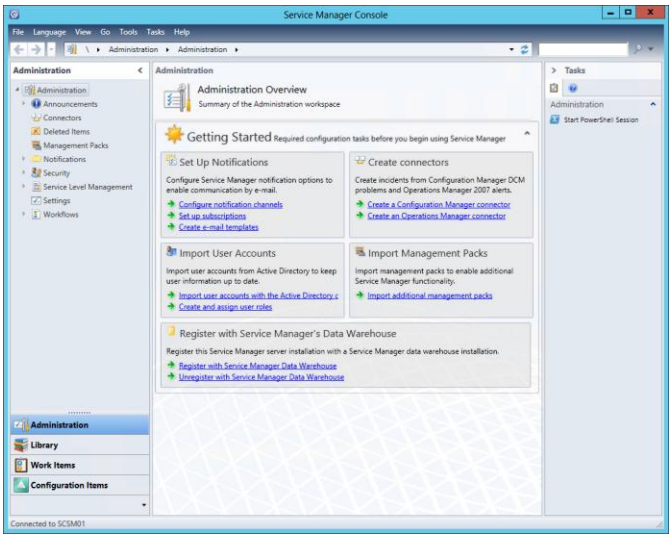
In the **Configure the Service Manager database** dialog, you will request to **Use an existing database** and will select the ServiceManager database.
Click **Next** to continue.

Note: You will see a slightly different set of subsequent screens because you are connecting into an existing environment instead of creating a new environment.



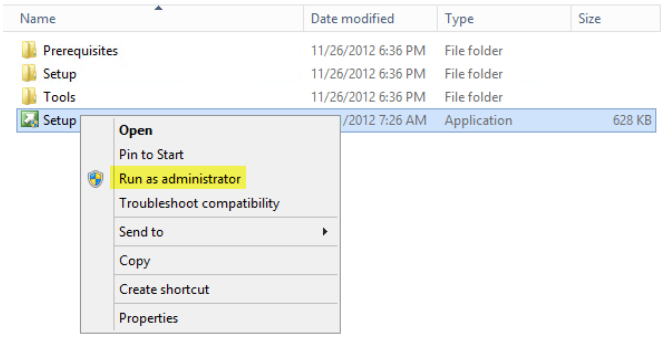
When the installation is complete, it is not necessary to back up the encryption key again. Clear that checkbox and check the box to open the Service Manager console.
Click **Close** to continue.



The Service Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.	

Installation – Data Warehouse Server

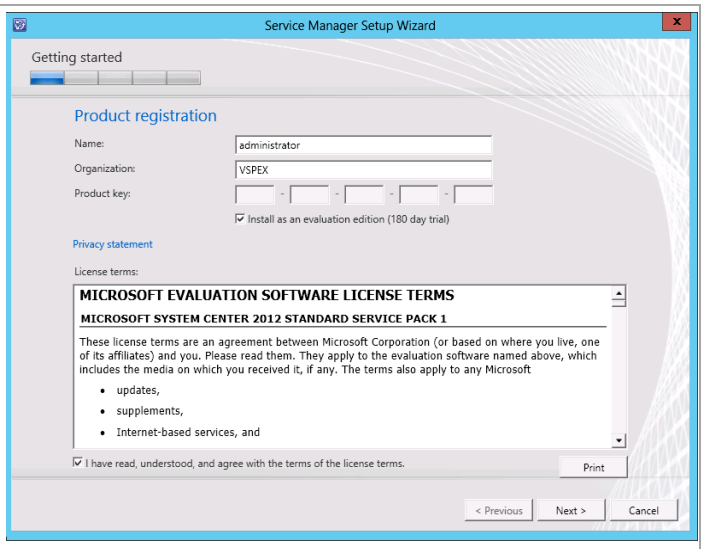
The following steps must to be completed in order to install the Service Manager Data Warehouse server role.

▶ Perform the following steps on the **Service Manager Data Warehouse server** virtual machine.	
Log on to Service Manager Data Warehouse server (**NOT** the Service Manager management server or the self-service portal server). From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager data warehouse management server** to begin the Service Manager server installation.	

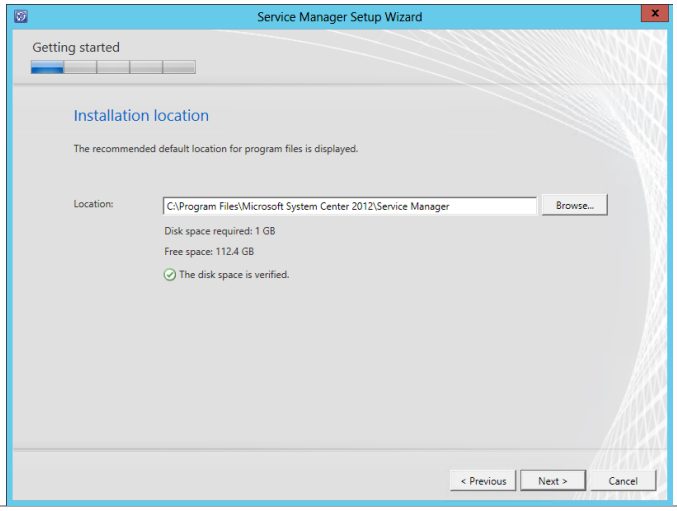
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** - *specify the name of the licensed organization*.
- **Product key** – *provide a valid product key for installation of Service Manager. If no key is provided, select the* ***Install as an evaluation edition (180-day trial)*** *check box*.

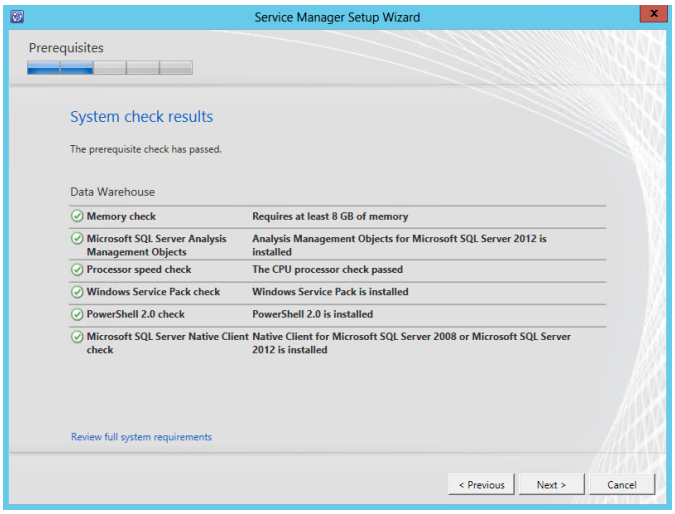
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. Once all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.

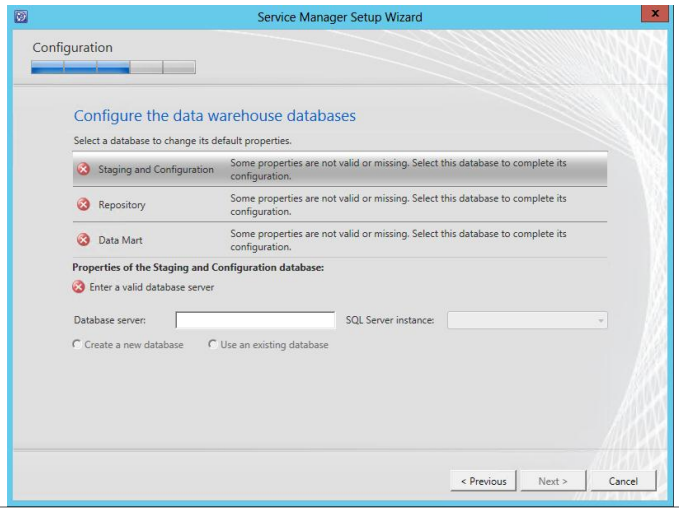


The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog.
When verified, click **Next** to continue.



When the **Configure the data warehouse databases** dialog launches each subcategory will appear with an error message until each of the following sections are configured:

- **Staging and Configuration**
- **Repository**
- **Data Mart**



In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.*

- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse.*

Select the **Create a new database** option and specify the following information in the provided text boxes:

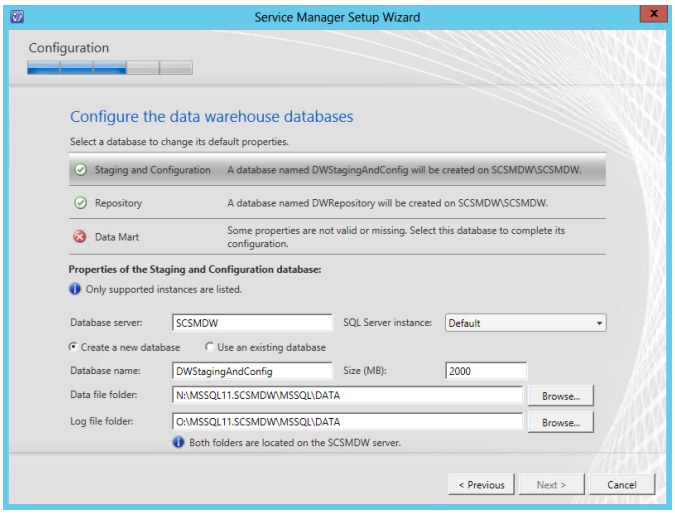
- **Database name** – *specify the name of the SM Data Warehouse database. In most cases the default value of DWStagingAndConfig should be used should be used for the Staging and Configuration section and DWRepository should be used for the Repository section.*

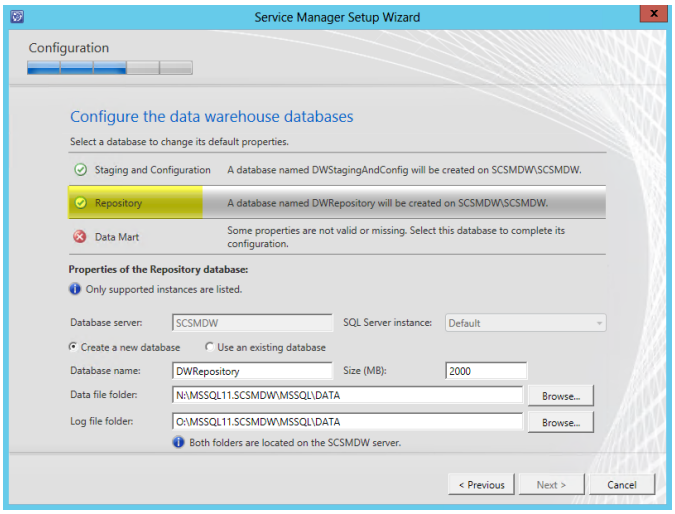
- **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*

- **Data file folder** – *specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. Set the correct value on the Staging and Configuration section as well as the Repository section.*

- **Log file folder** – *specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. Set the correct value on the Staging and Configuration section as well as the Repository section*

Click **Data Mart** to continue.





In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).*

- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).*

Select the **Create a new database** option and specify the following information in the provided text boxes:

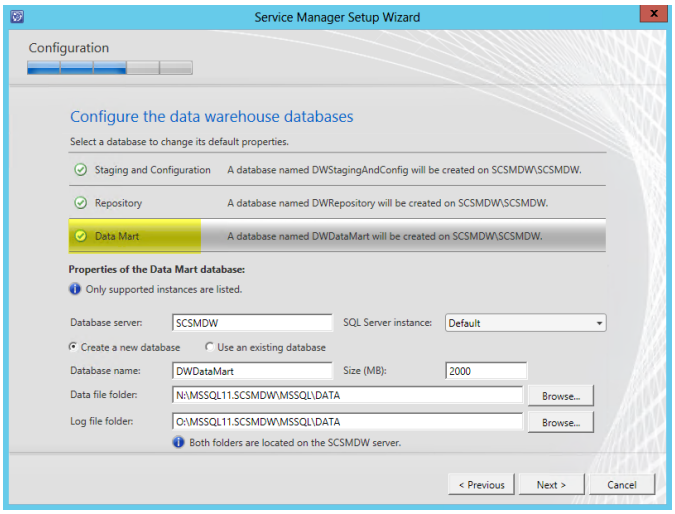
- **Database name** – *specify the name of the Service Manager Data Warehouse database. In most cases the default value of DWDataMart should be used.*

- **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*

- **Data file folder** – *specify the same drive letter associated above for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

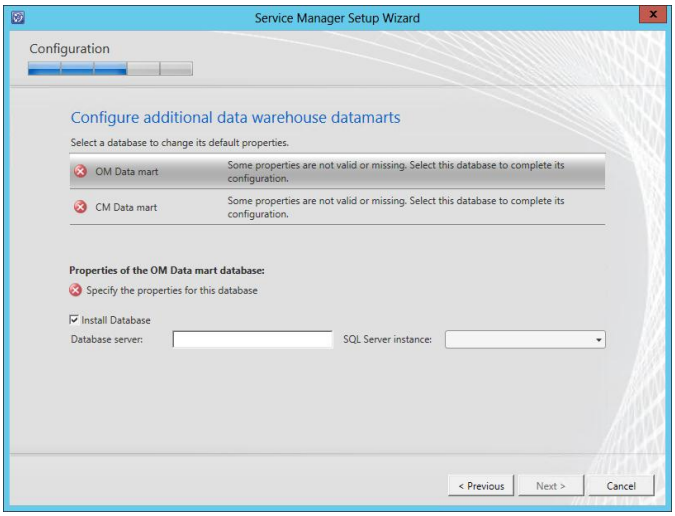
- **Log file folder** – *Specify the same drive letter associated above for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

Click **Next** to continue.



When the **Configure additional data warehouse datamarts** dialog launches, each subcategory will appear with an error message until each of the following sections are configured:

- **OM Data mart.**
- **CM Data mart.**



In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **OM Data Mart** section:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*

- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*

Select the **Create a new database** option and specify the following information in the provided text boxes:

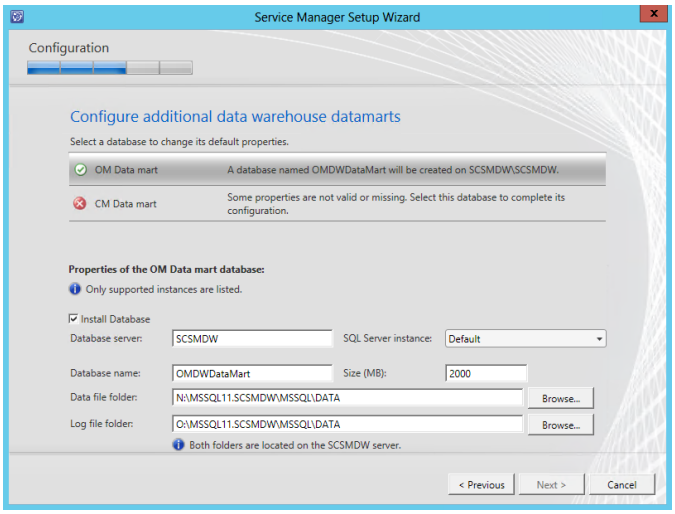
- **Database name** – *specify the name of the Service Manager OM Data mart database. In most cases the default value of OMDWDataMart should be used.*

- **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*

- **Data file folder** – *specify the same drive letter associated above for the database data files for the Service Manager OM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

- **Log file folder** – *specify the same drive letter associated above for the database log files for the Service Manager OM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

Click **CM Data mart** to continue.



In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **CM Data Mart** section:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*

- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*

Select the **Create a new database** option and specify the following information in the provided text boxes:

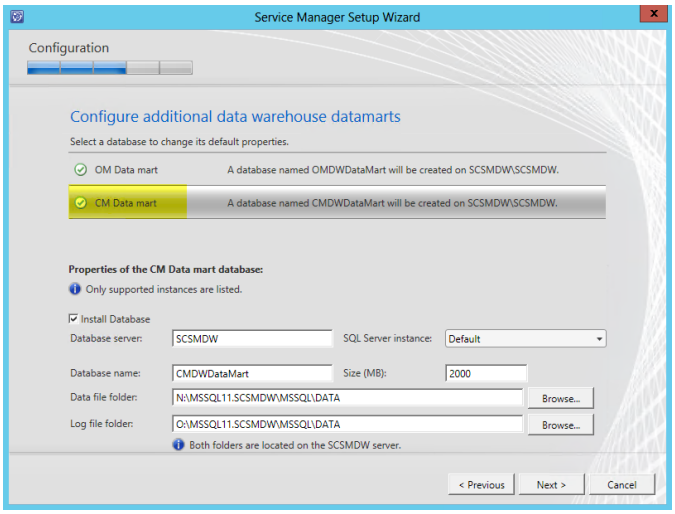
- **Database name** – *specify the name of the Service Manager CM Data mart database. In most cases the default value of CMDWDataMart should be used.*

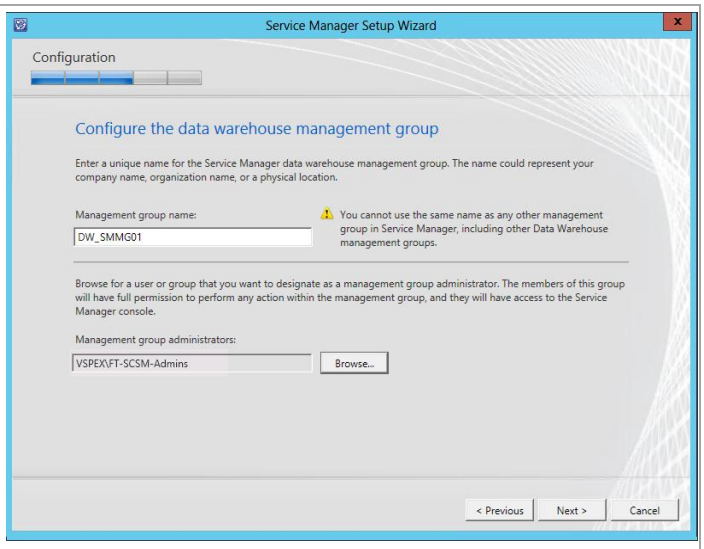
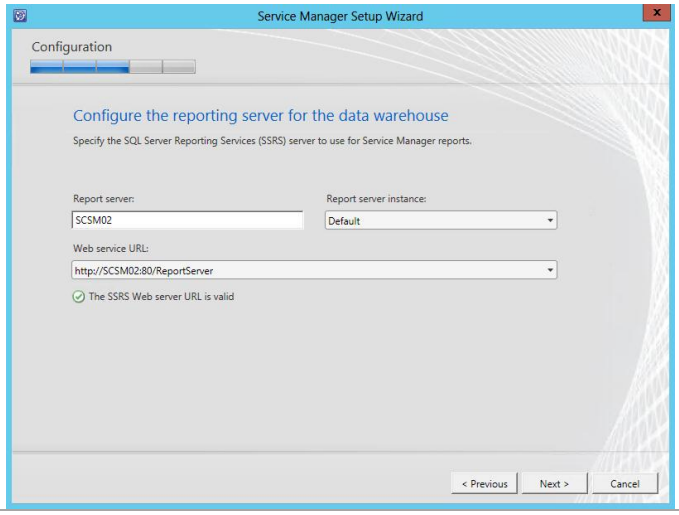
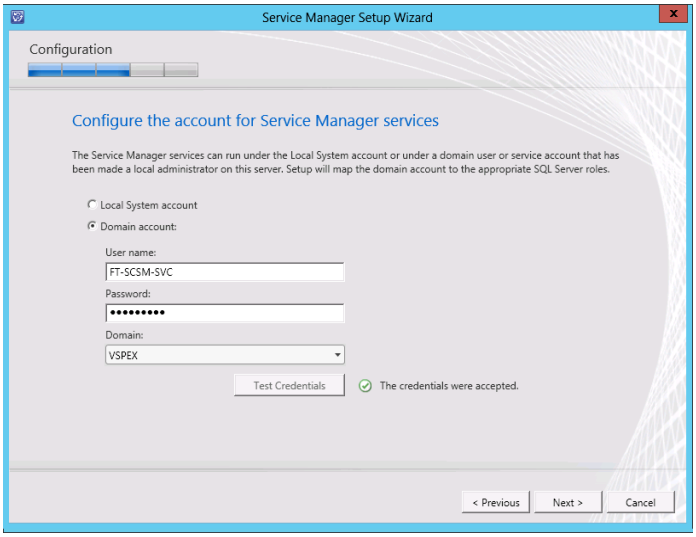
- **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*

- **Data file folder** – *specify the same drive letter associated above for the database data files for the Service Manager CM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

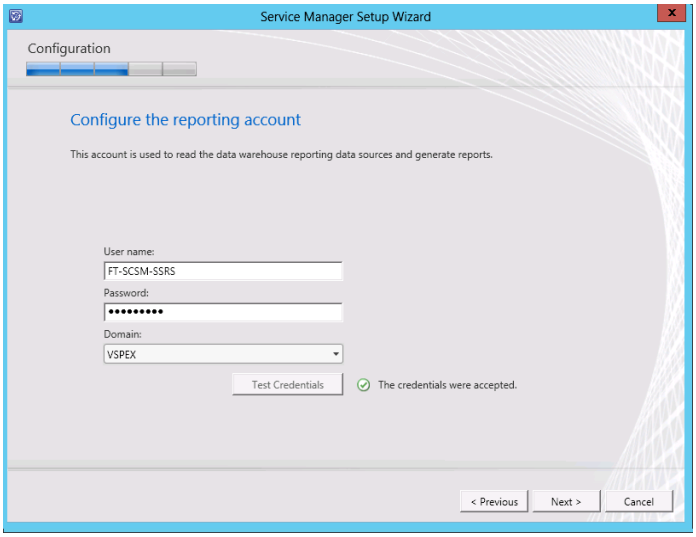
- **Log file folder** – *specify the same drive letter associated above for the database log files for the Service Manager CM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

Click **Next** to continue.



In the **Configure the data warehouse management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager management server and Service Manager Operations Manager installations. Specify the SM Administrators group in the **Management group administrators** object picker section. Click **Next** to continue.	
In the **Configure the reporting server for the data warehouse** dialog, specify the Data Warehouse server in the **Report server** text box. In the **Report server instance** drop-down menu, select **Default**. In the **Web service URL** drop-down menu, select the default reporting server URL. Click **Next** to continue.	
In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.	

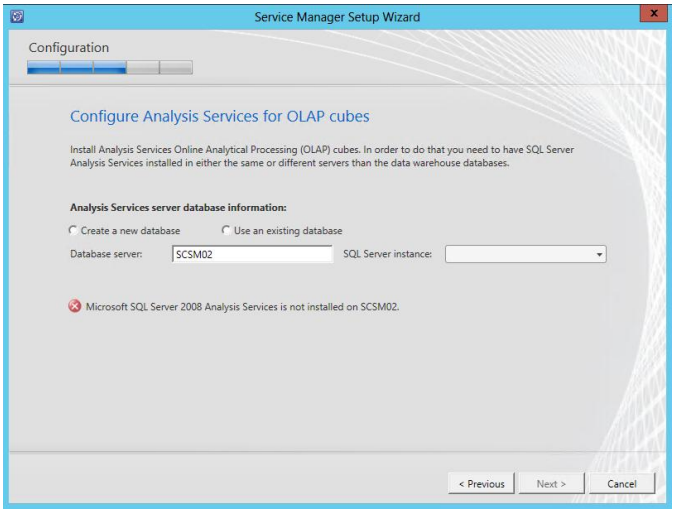
In the **Configure the reporting account** dialog, specify the SCSM SQL Server Reporting Services Account in the **User name** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
Before proceeding, click the **Test Credentials** button to verify the credentials provided.
When successful, click **Next** to continue.

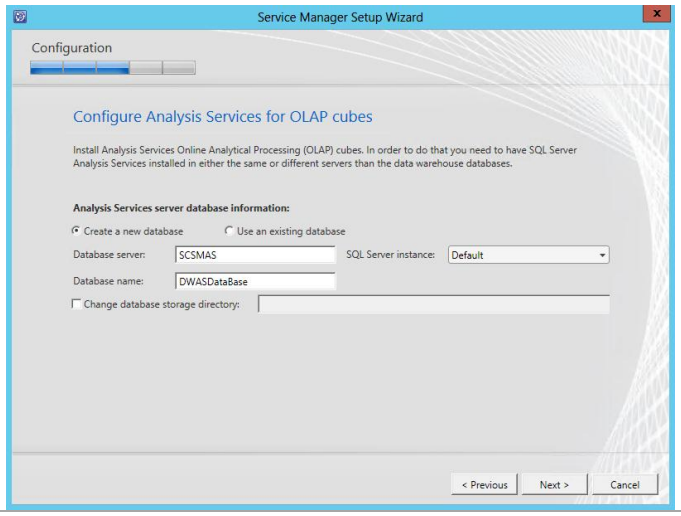


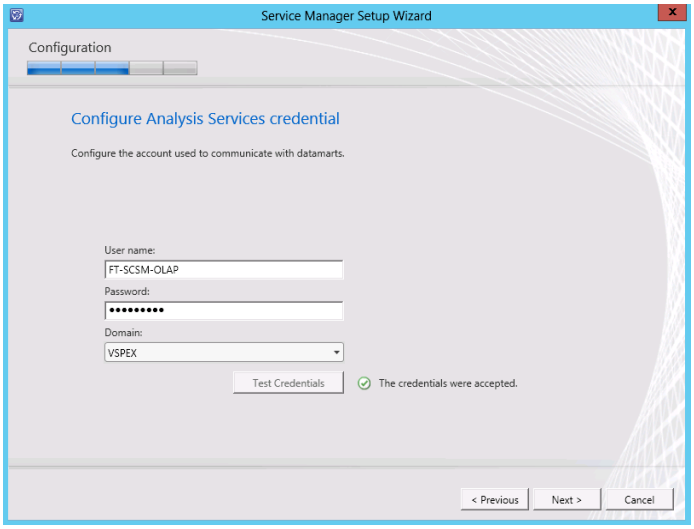
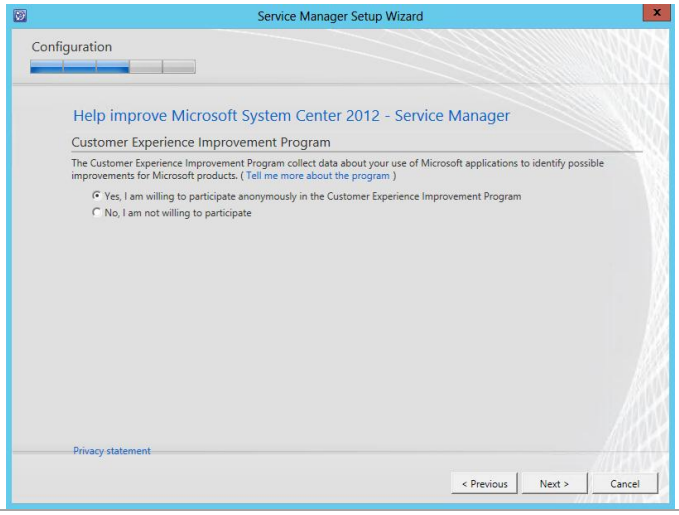
In the **Configure Analysis Services for OLAP cubes** dialog, select the **Create a new database** option and specify the following information in the provided text boxes:

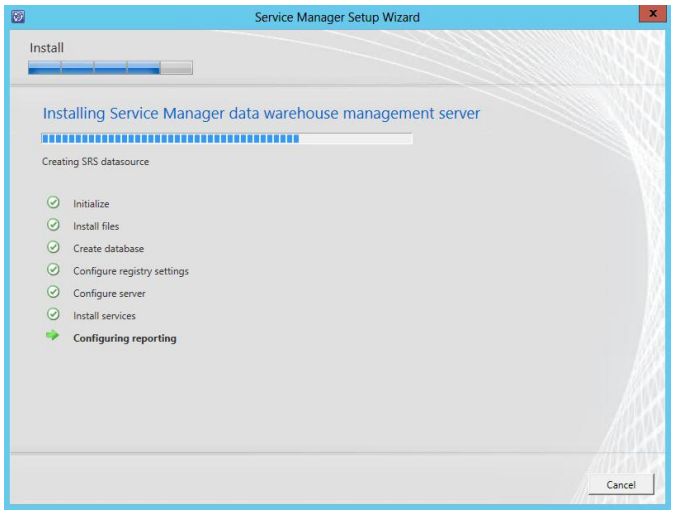
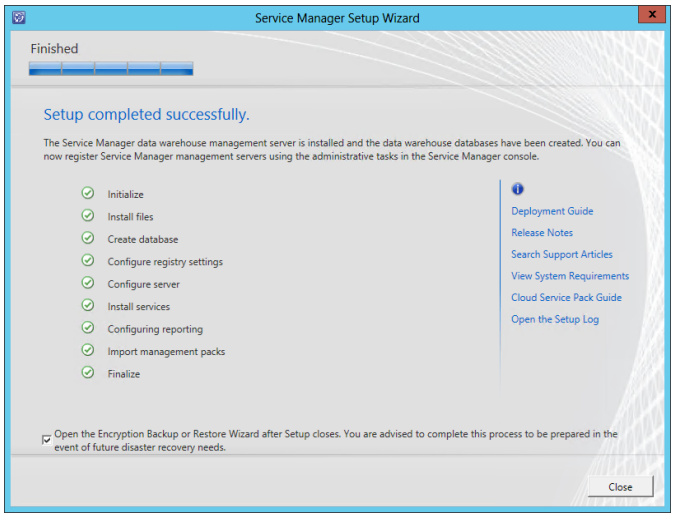
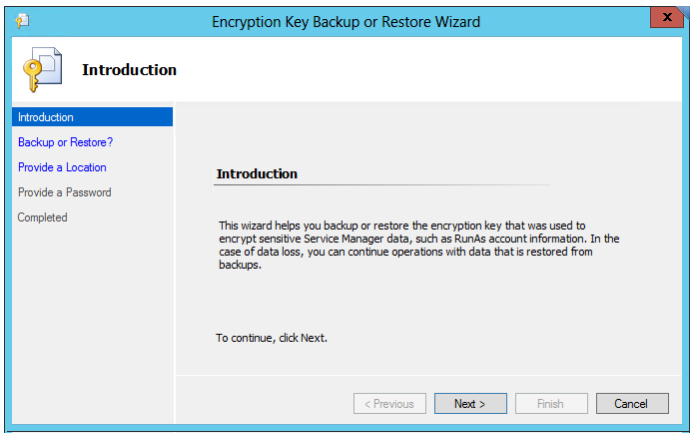
- **Database server** – *specify the name of the SQL Server cluster CNO created for the Service Manager installation SQL Server Analysis Services.*
- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation SQL Server Analysis Services.*
- **Database name** – *specify the name of the SQL Server Analysis Services database. In most cases the default value of DWASDataBase should be used.*

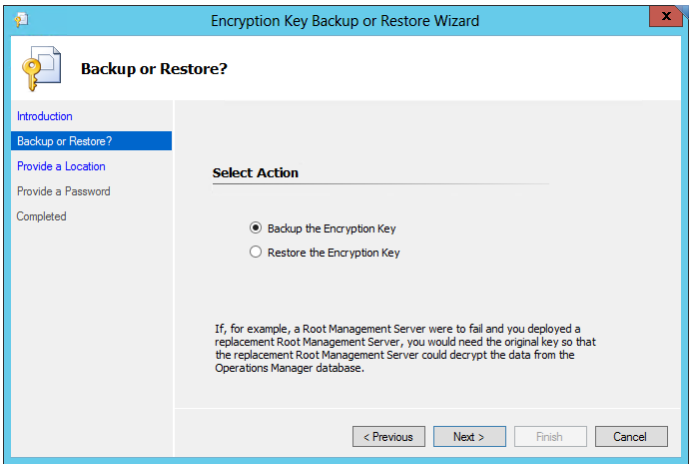
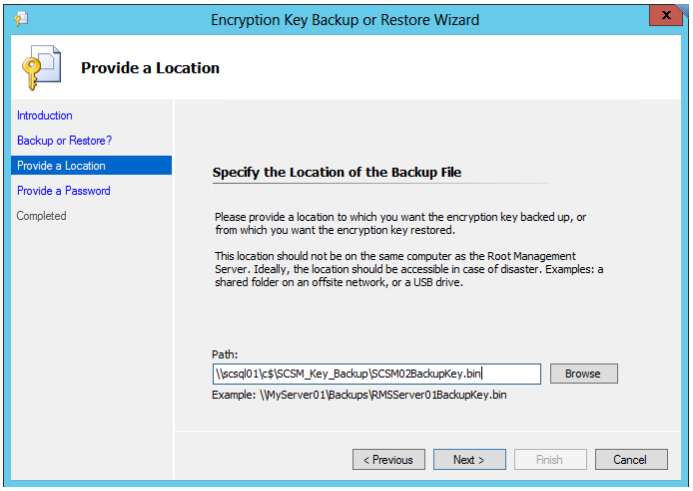
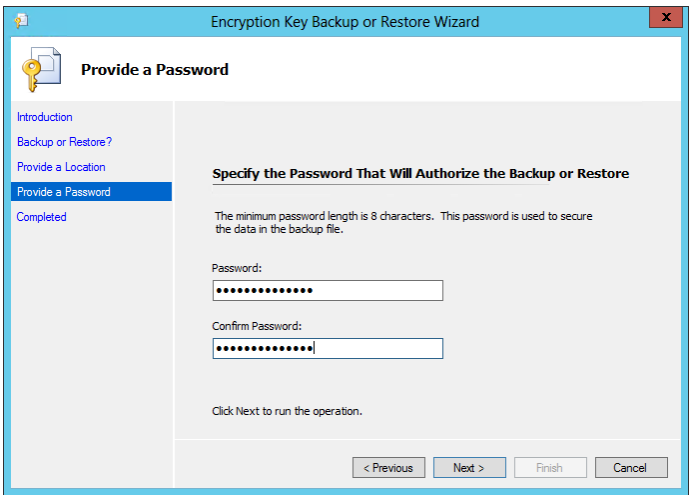
Confirm that the **Change database storage directory** check box is clear and click **Next** to continue.





In the **Configure Analysis Services Credential** dialog, specify the SM OLAP Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.	
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.	
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.	

The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue. The wizard will display the progress while installing features.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Ensure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to launch the wizard after setup. Click **Close** to complete the installation.	
When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.	

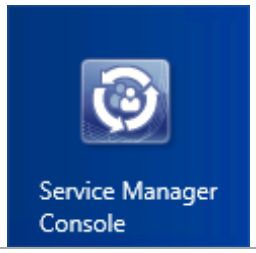
In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.	
In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** text box and object picker. Click **Next** to continue.	
In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.	

When complete, click **Finish** to exit the wizard.



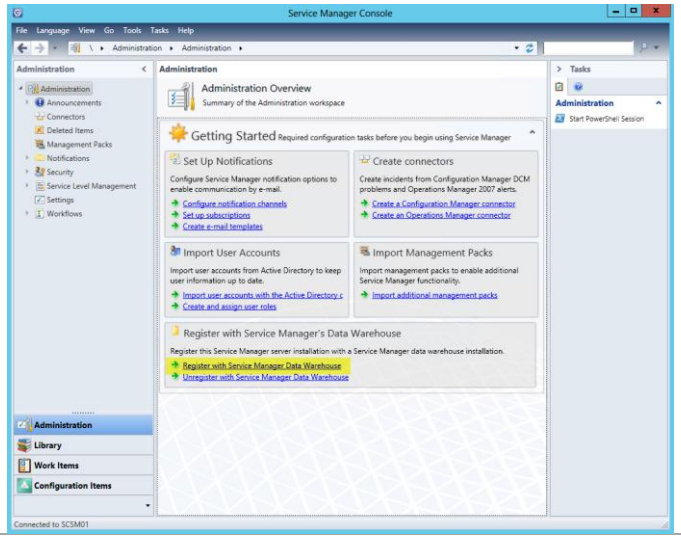
▶ Perform the following steps on the **Service Manager management server** virtual machine to register the Service Manager Data Warehouse and enable reporting in the Service Manager instance.

Logon to the Service Manager management server using an account with administrator permissions. From the Windows **Start** screen, select the **Service Manager Console** tile.

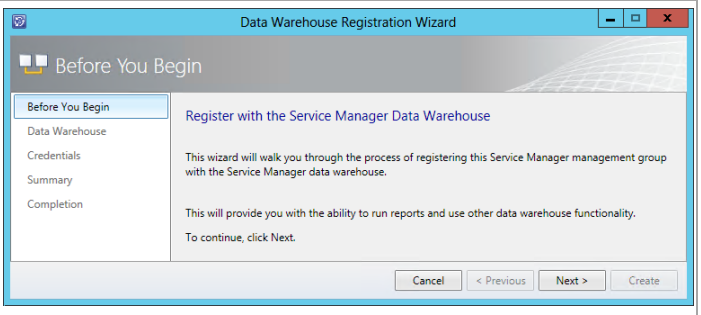


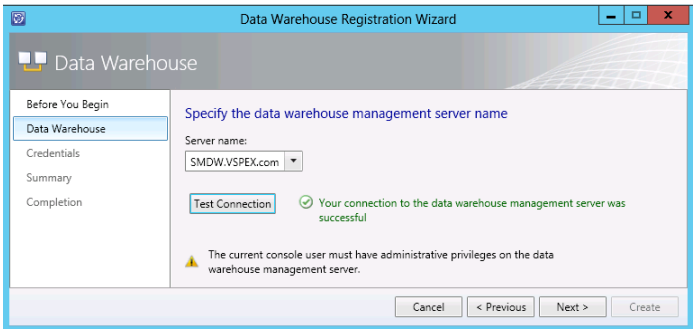
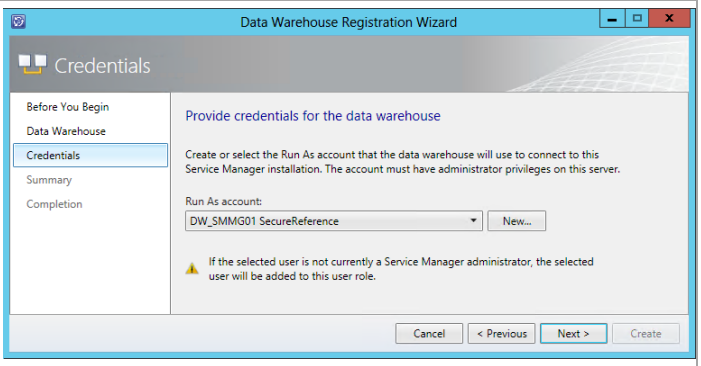
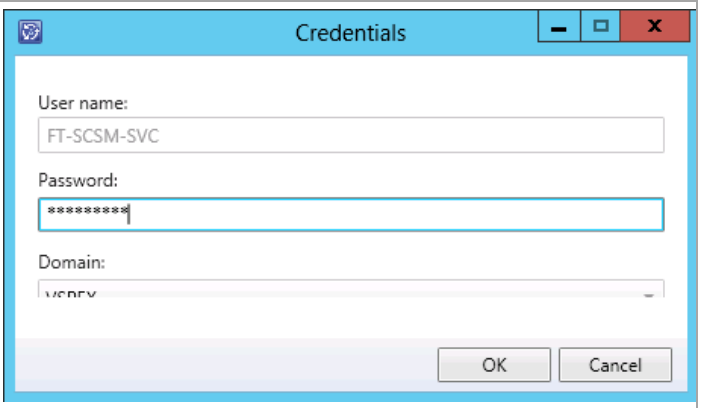
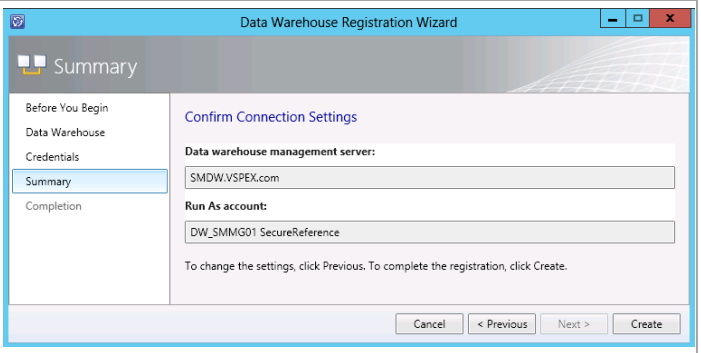
Within the Service Manager Console, select the Administration node and navigate to the Register with Service Manager's Data Warehouse section. Click the Register with Service manager Data Warehouse link to enable reporting.

Note: If the console was open from the previous installation, close it and re-open the console.

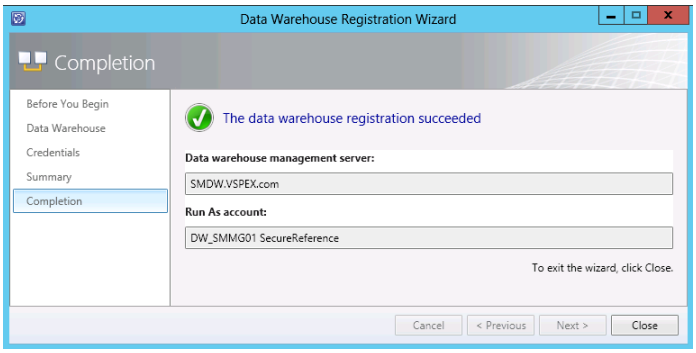


The **Data Warehouse Registration Wizard** will launch.
Click **Next** to begin registration.

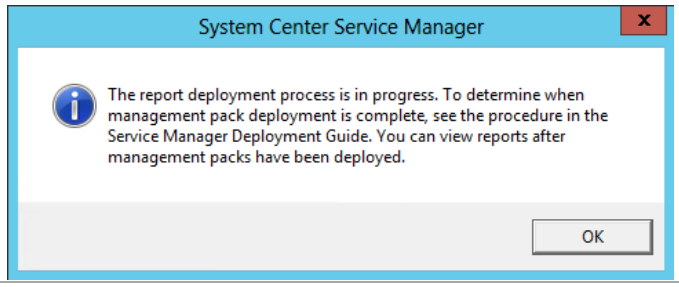


In the **Specify the data warehouse management server name** dialog, specify the Service Manager Data Warehouse server FQDN in the **Server name** drop-down menu. When selected, click the **Test Connection** button to validate connectivity between the Service Manager management and Data Warehouse servers. Click **Next** to continue.	
In the **Provide credentials for the data warehouse** dialog. Click **Next** to use the current SM and DW service account as the **Run As account** for the Data Warehouse connection.	
A **Credentials** dialog will appear and prompt you for the password for the SM service account. Once provided, click **OK** to continue.	
The **Summary** dialog will appear. Review the information that was provided earlier and click **Create** to begin the registration process.	

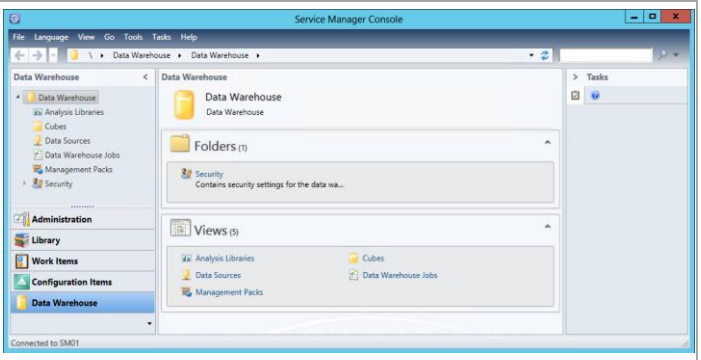
The **Completion** dialog will show the successful registration of the Data Warehouse.
Click **Close** to exit the wizard.



Note: The Data Warehouse registration process can take several hours for the registration process to complete. During this time several management packs are imported into the Data Warehouse server and several Data Warehouse jobs run.

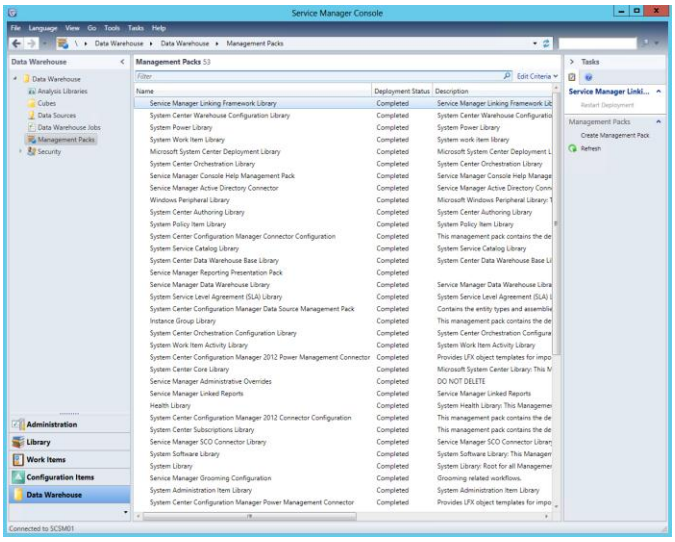


After a few minutes the **Data Warehouse** button will be added to the **Service Manager Console**.



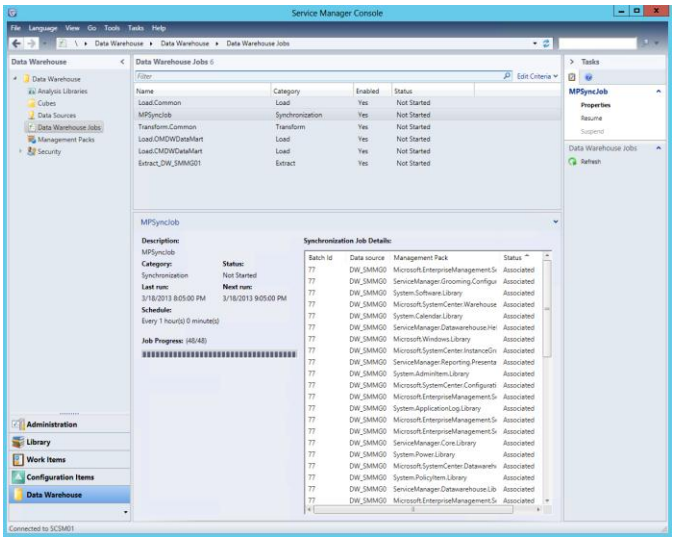
Note: This deployment and association process can take up to two hours to complete.

The status of the management pack imports can be checked by selecting **Management Packs** in the **Data Warehouse** pane.
Deployment is complete when all listed management packs show a deployment status of **Completed.**



Note: This deployment and association process can take up to two hours to complete.

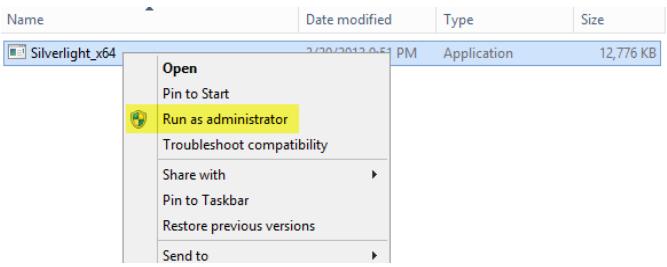
In the **Data Warehouse** pane, select **Data Warehouse Jobs**.
In the **Data Warehouse Jobs** pane, click **MPSyncJob**.
In the **MPSyncJob** details pane, in the **Synchronization Job Details** list, scroll to the right to view the **Status** column, and then click **Status** to alphabetically sort the status column.
Scroll through the **Status** list. The management pack deployment process is complete when the status for all of the management packs is **Associated** or **Imported**. Confirm that there is no status of either **Pending Association** or **Failed** in the status list. In the **Data Warehouse Jobs** pane, the status of the **MPSyncJob** will have changed from **Running** to **Not Started** when the registration process is complete.



Install the Silverlight Runtime

▶ Perform the following steps on the **System Center Service Manager self-service portal** virtual machine.

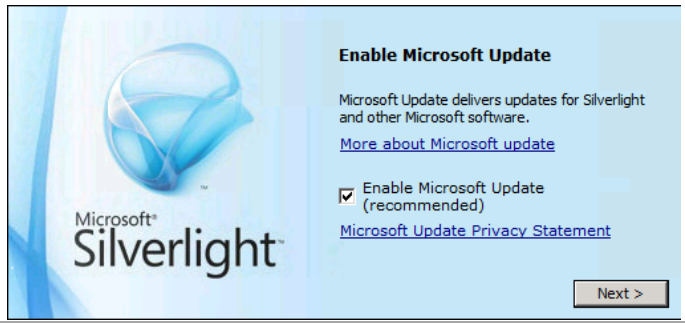
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.

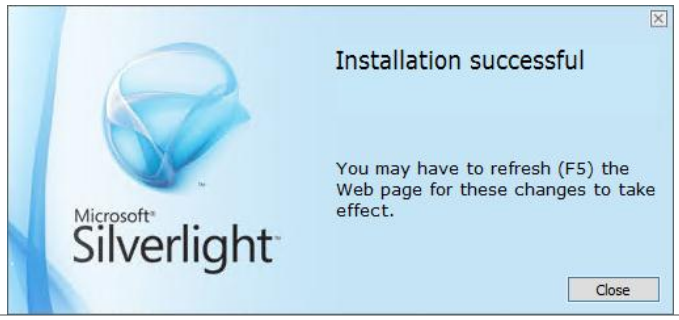


In the **Install Silverlight** dialog, click **Install** now.



In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.

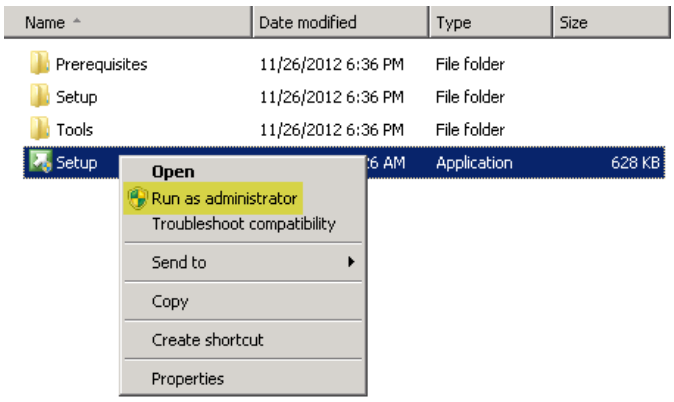
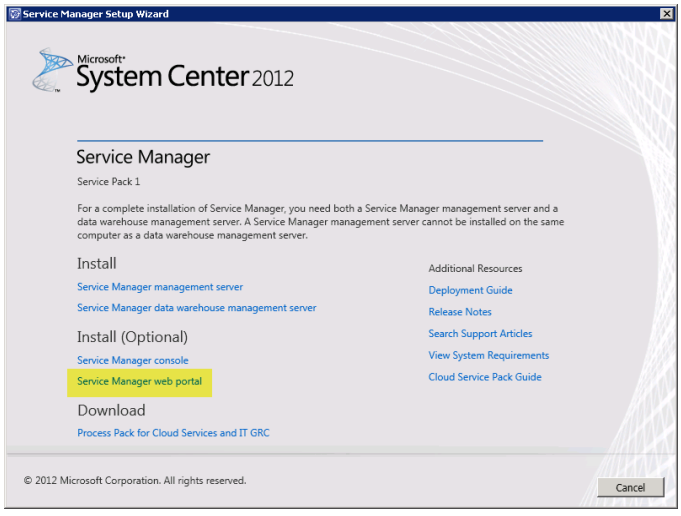


In the **Installation Successful** dialog, click **Close** to exit the installation.	

Installation – Self-Service Portal Server

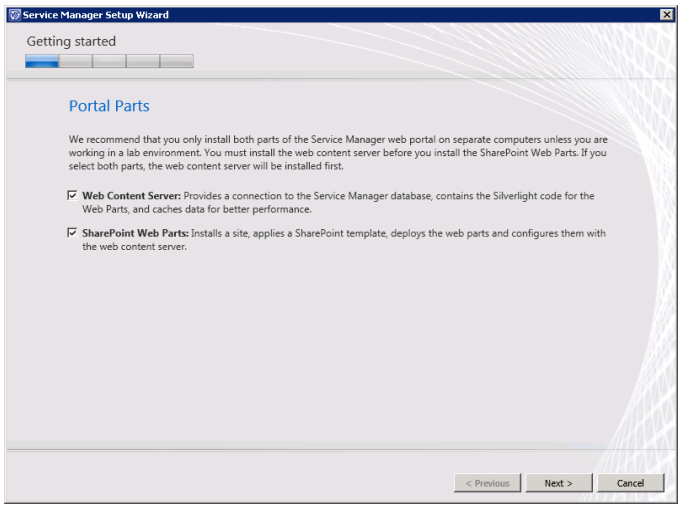
The following steps must to be completed in order to install the Service Manager Self-Service Portal server role.

▶ Perform the following steps on the **System Center Service Manager self-service portal** virtual machine.

Log on to Service Manager self-service portal server (**NOT** the Service Manager management server or the Data Warehouse server). From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager web portal** to begin the Service Manager self-service portal server installation.	

The Service Manager Setup Wizard will open. In the Portal Parts dialog, select the Web Content Server and SharePoint Web Parts check boxes and click Next to continue.

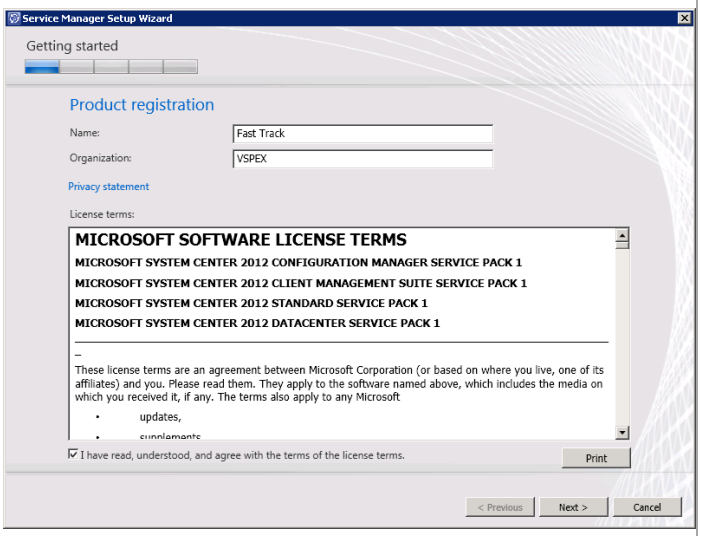
Note: The warning about installing both Portal Parts on a single server can be safely ignored. The setup wizard assumes that the SharePoint Farm is using a local SQL Server installation whereas the Fast Track design uses a dedicated SQL Server instance for the SharePoint farm drastically reducing the load on the SharePoint Web Parts installation.



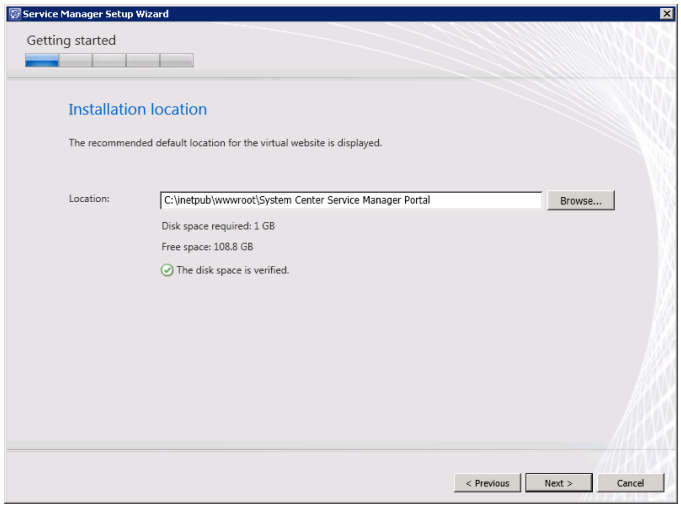
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** – *specify the name of the licensed organization*.

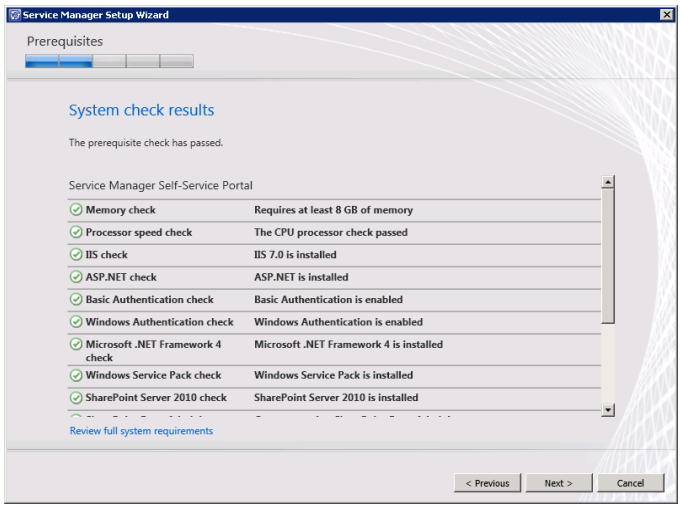
In the License terms section, select **I have read, understood, and agree with the terms of the license terms** check box. Once all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of *C:\inetpub\wwwroot\System Center Service Manager Portal* for the installation.
Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.

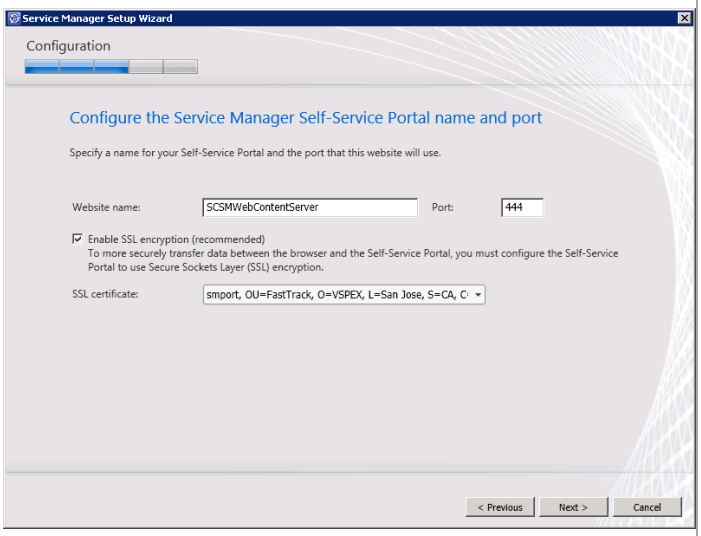


In the **Configure the Service Manager Self-Service Portal name and port** dialog, specify the following information in the provided text boxes:

- **Website name** – *specify the name of the website used for the self-service portal. In most cases, the default name of SCSMWebContentServer should be used.*

- **Port** – *specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases this value should be changed to **444**.*

In addition, select the appropriate Server Authentication certificate from the **SSL certificate** drop-down menu. The certificate CN field must match the name of the server.
Click **Next** to continue.



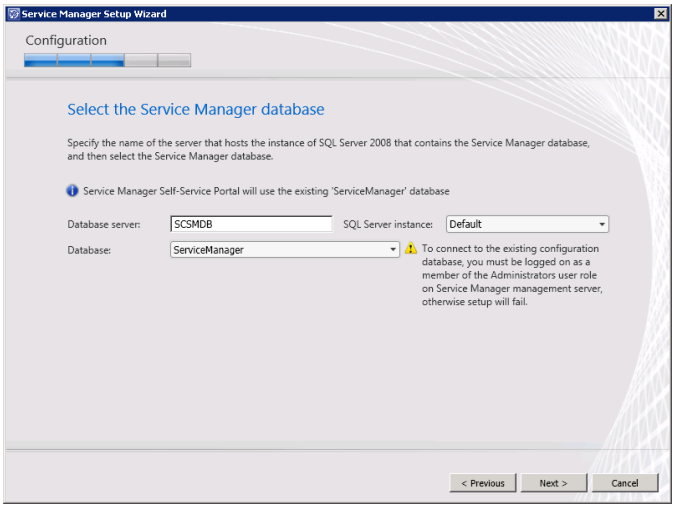
In the **Select the Service Manager database** dialog, specify the following information in the provided text boxes:

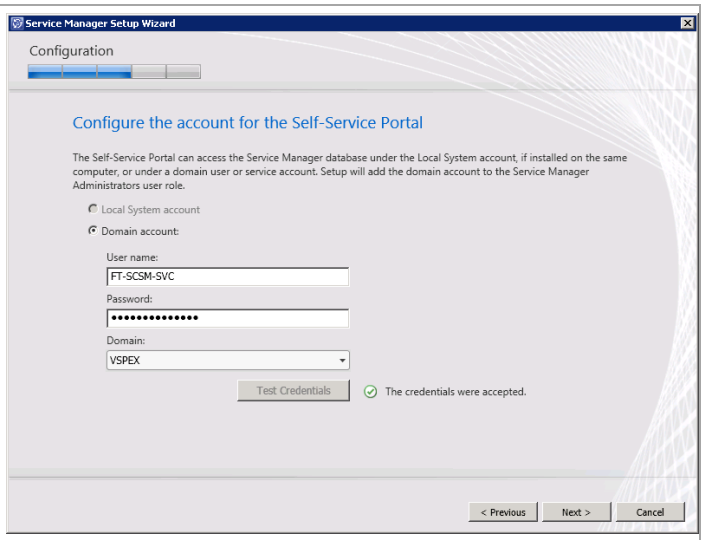
- **Database server** – *specify the name of the SQL Server cluster CNO created for the Service Manager management server.*

- **SQL Server instance** – *specify the SQL Server database instance created for the Service Manager management server.*

- **Database** – *specify the name of the Service Manager database configured earlier. In most cases the default value of ServiceManager should be used.*

Click **Next** to continue.

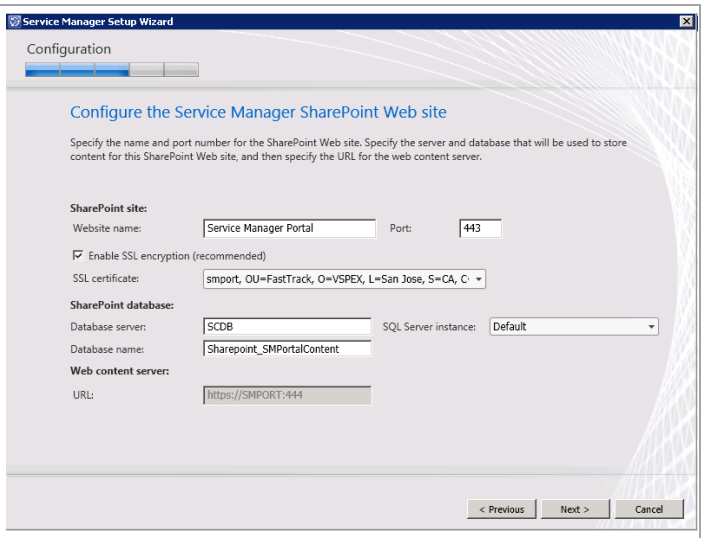


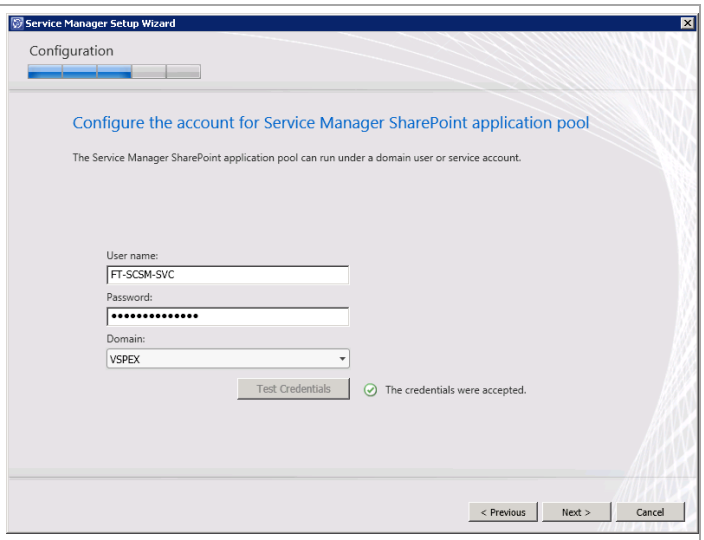
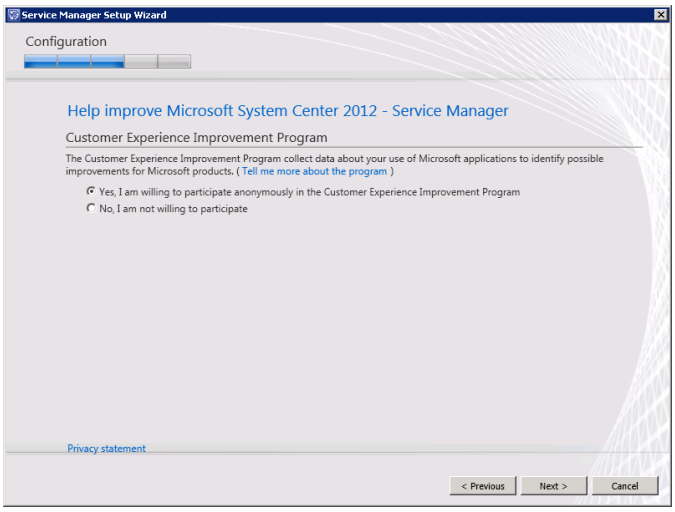
In the **Configure the account for the Self-Service Portal** dialog, verify that the **Domain account** option is selected and specify the SM Service Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.	

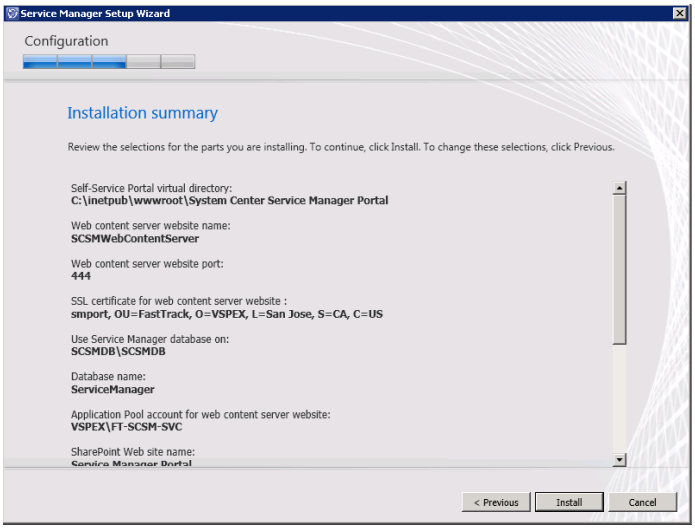
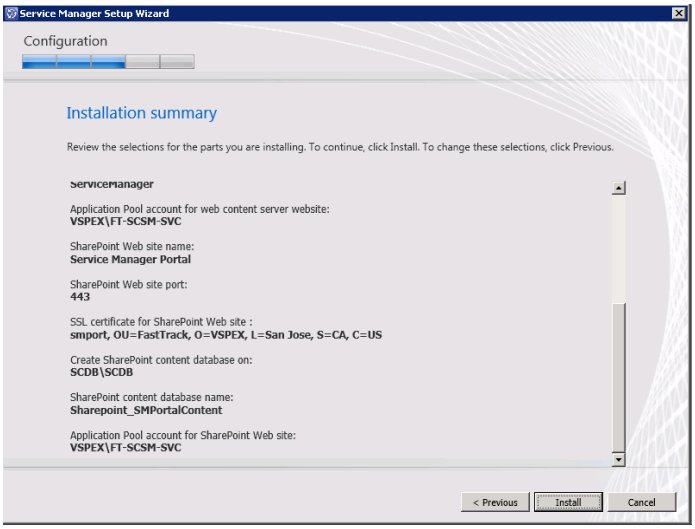
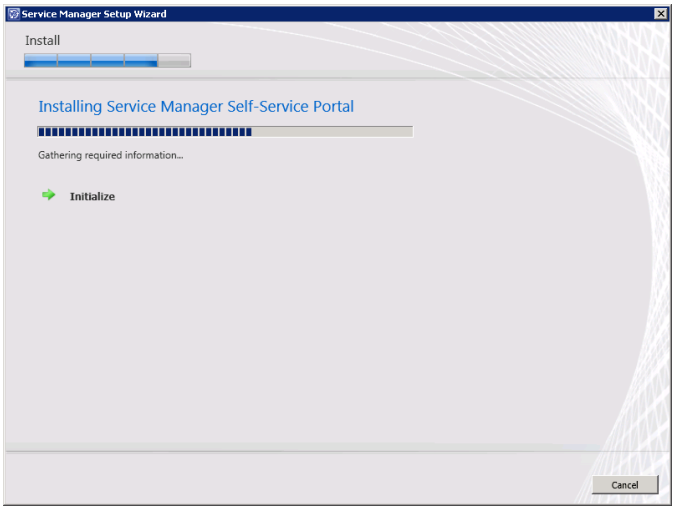
In the **Configure the Service Manager SharePoint Web site** dialog, provide the following information:

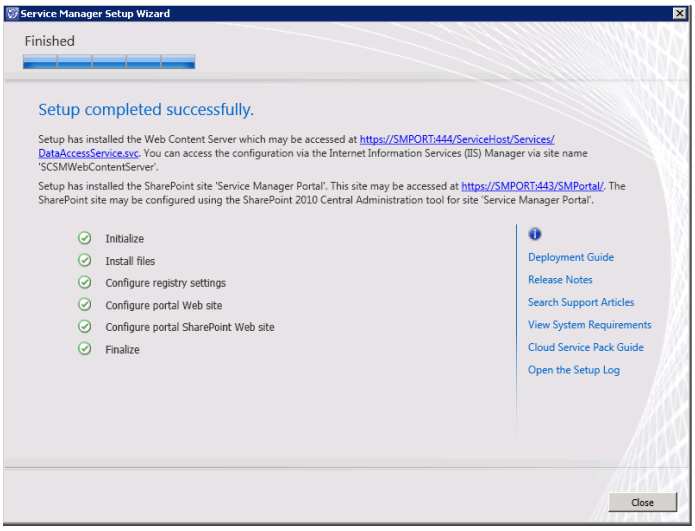
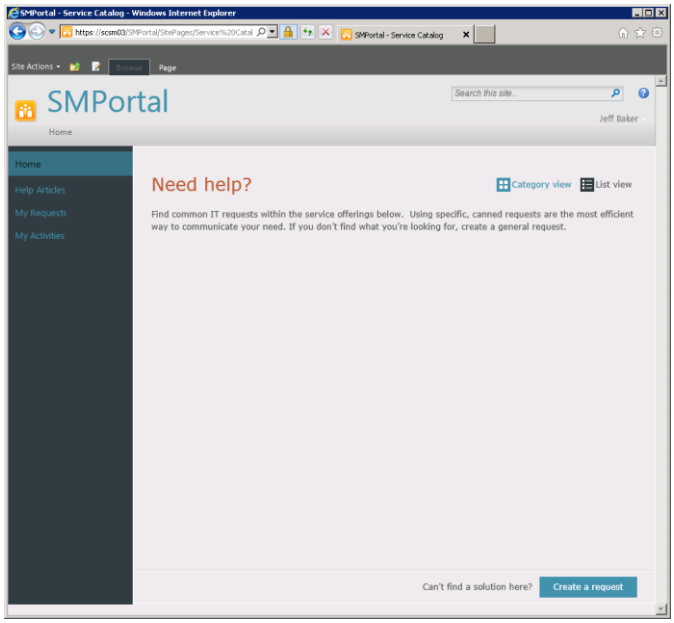
- In the **SharePoint site** section, specify the following information in the provided text boxes:
    - **Website name** – *specify the name of the website used for the self-service portal. In most cases, the default name of Service Manager Portal should be used.*
    - **Port** – *specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases the default value of **443** should be kept.*
- Select the appropriate server authentication certificate from the **SSL certificate** drop-down menu. This will be the same certificate used for the content server in the previous step.
- In the SharePoint database section, specify the following information in the provided text boxes:
    - **Database server** – *specify the name of the SQL Server cluster network name created for the Service Manager installation SharePoint Farm.*
    - **SQL Server instance** – *specify the SQL Server database instance created for the Service Manager installation SharePoint Farm.*
    - **Database server** – *specify the database name for the portal. In most cases, the default value of SharePoint_SMPortalContent will be used.*

Click **Next** to continue.



In the **Configure the account for Service Manager SharePoint application pool** dialog, specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.	
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.	
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.	

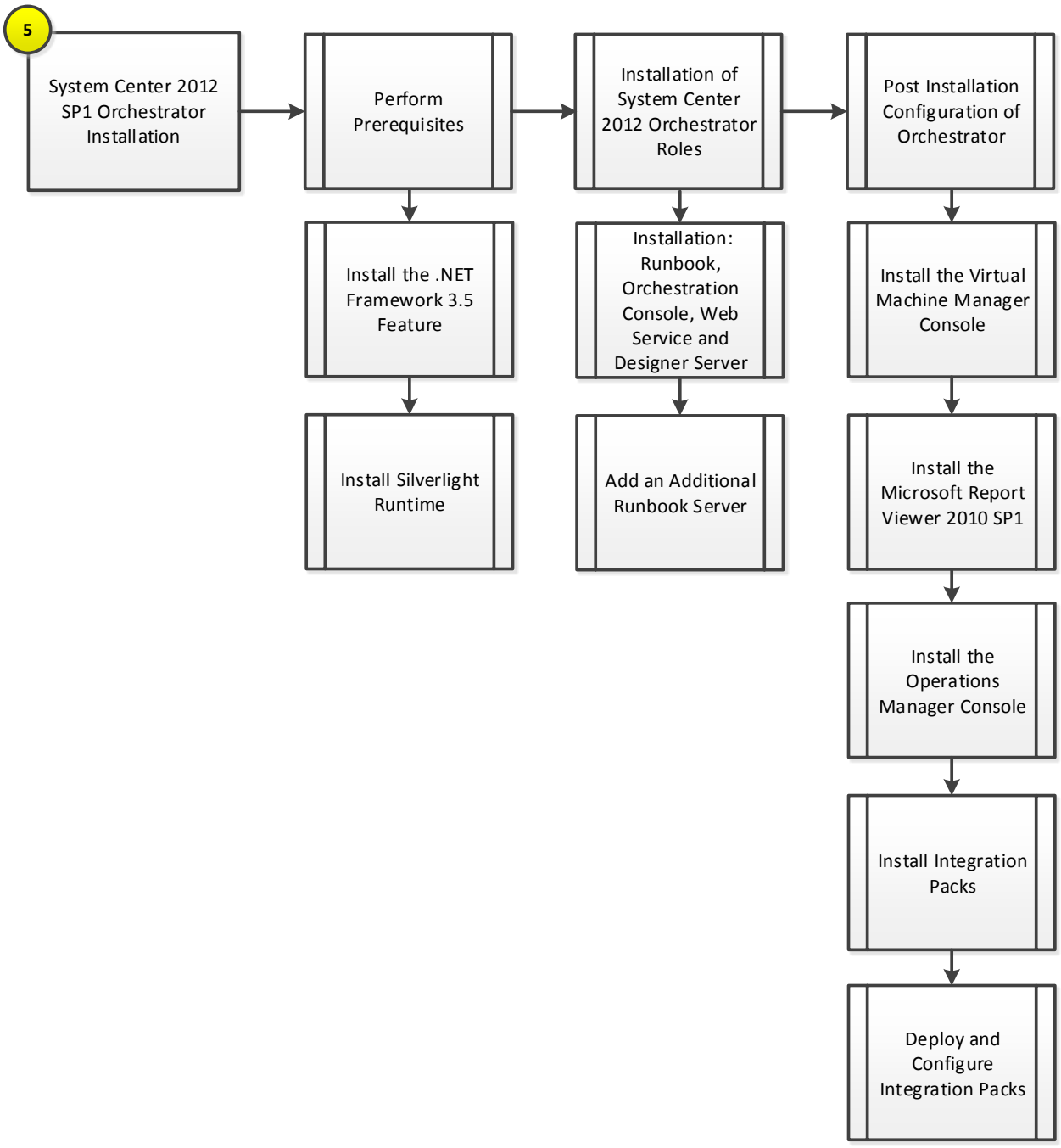
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	 
The wizard will display the progress while installing features.	

When completed, the **Service Manger Setup Wizard** will display the **Setup completed successfully** dialog. Click **Close** to finish the installation. Note the SMPortal link provided in the dialog.	
From Microsoft Internet Explorer®, open the Service Manager self-service portal at https://<servername>/SMPortal. Verify that the page loads completely and that all sections display as expected.	

12 System Center Orchestrator

The Orchestrator installation process is comprised of the following high-level steps:

Figure 13 Orchestrator Installation Process



12.1 Overview

This section provides the setup procedure for Orchestrator into the Fast Track fabric management architecture. The following assumptions are made:

- Base virtual machines running Windows Server 2012 have been provisioned.
- A multi-node, SQL Server 2012 cluster with dedicated instance has been established in previous steps for Orchestrator.

- The .NET Framework 3.5 Feature is installed.

12.2 Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created for Orchestrator:

Table 33 Prerequisite Accounts

User Name	Purpose	Permissions
<DOMAIN>\FT-SCO-SVC	Orchestrator Service Account	This account will need: • Full admin permissions on all target systems to be managed. • Logon As a Service rights (User Rights) on the Orchestrator VM • *Sysadmin* on the SQL server, or dbo rights to the Orchestrator database after its created This account will need to be a member in the following groups: • FT-SCVMM-Admins

Groups

Verify that the following security groups have been created for Orchestrator:

Table 34 Prerequisite Security Groups

Security Group Name	Group Scope	Members	Member of
<DOMAIN>\FT-SCO-Operators	Global		
<DOMAIN>\FT-SCO-Admins	Global	<DOMAIN>\FT-SCO-SVC	Local Administrators Target Active Directory domain BUILTIN\Distributed COM Users

Required Networks

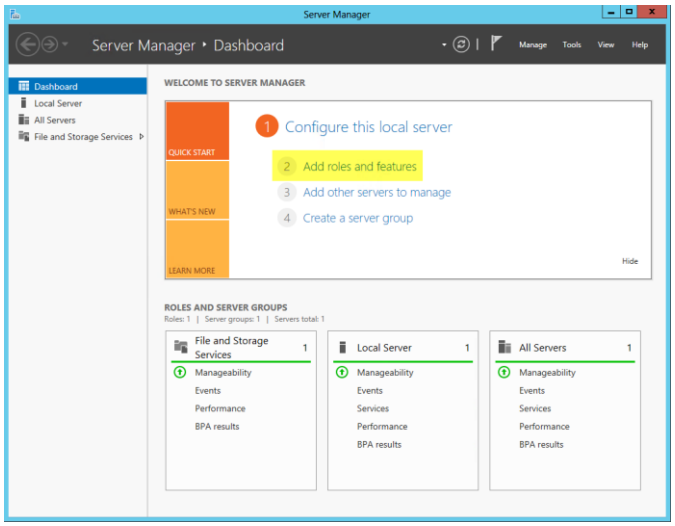
VMaccess

Add the .NET Framework 3.5 Feature

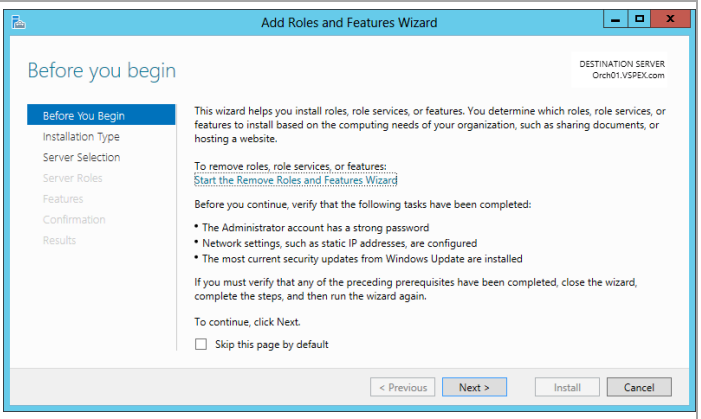
The Orchestrator installation requires the .NET Framework 3.5 Feature be enabled to support installation. If you did not include this in your sysprepped image, follow the provided steps to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on <u>all</u> **Operations Manager** virtual machines.

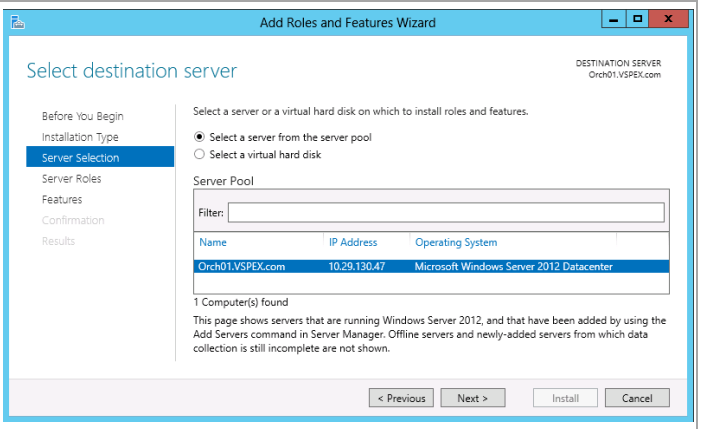
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



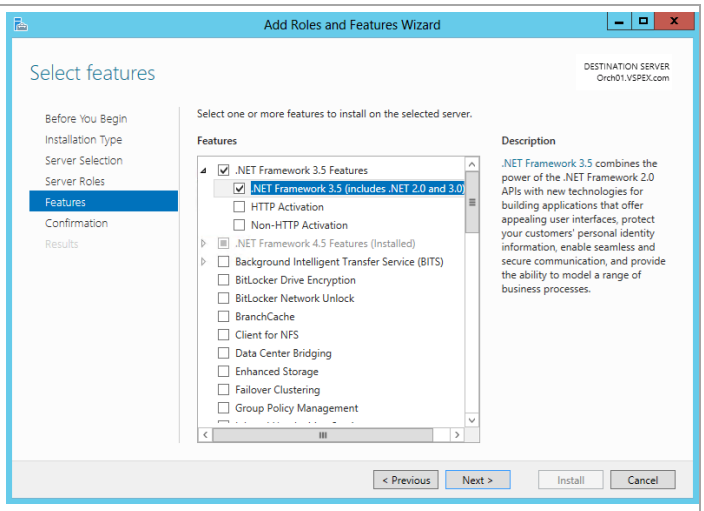
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next - for** this installation, click the **Features** menu option to continue.



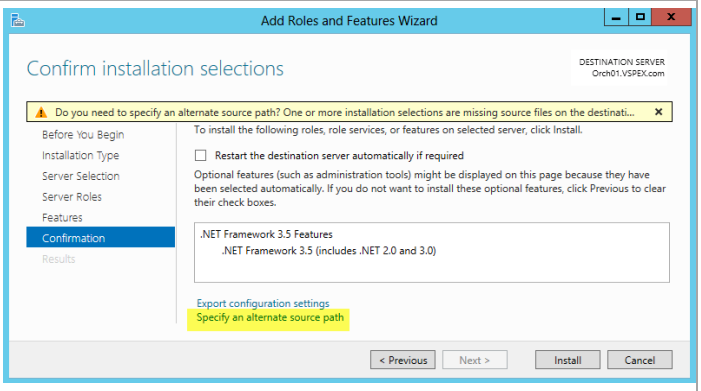
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



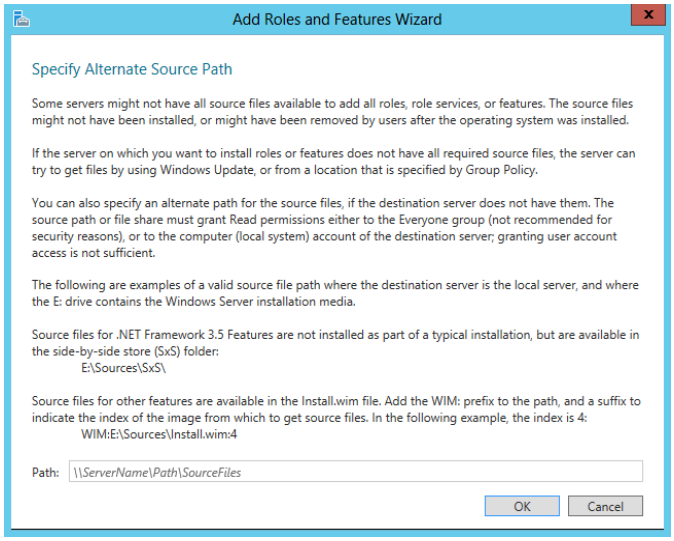
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

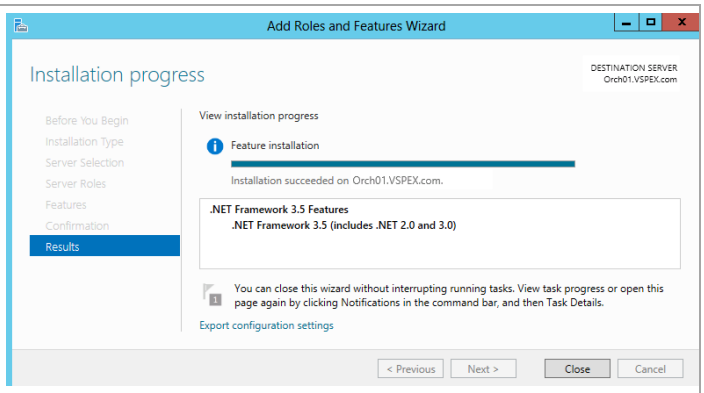
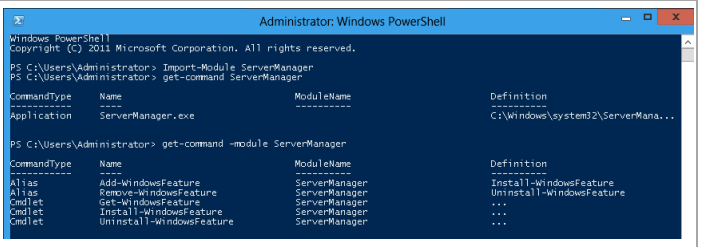
Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. Once exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.

Note: If the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.

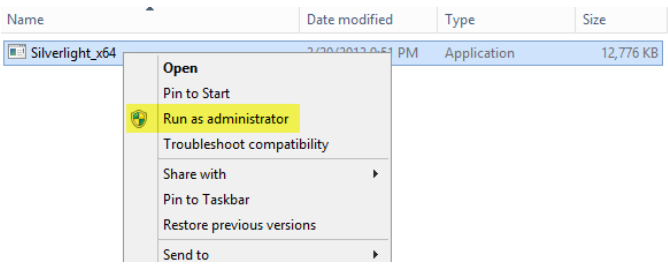


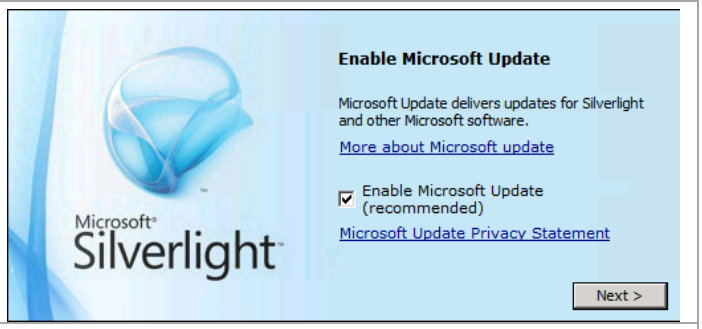
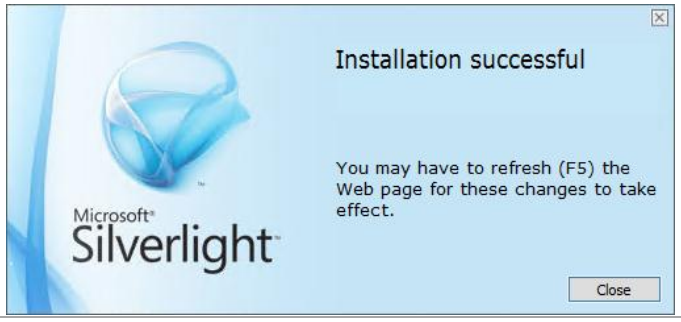
For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location be specified for the installation.



The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.	
Note that while the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.	

Install the Silverlight Runtime

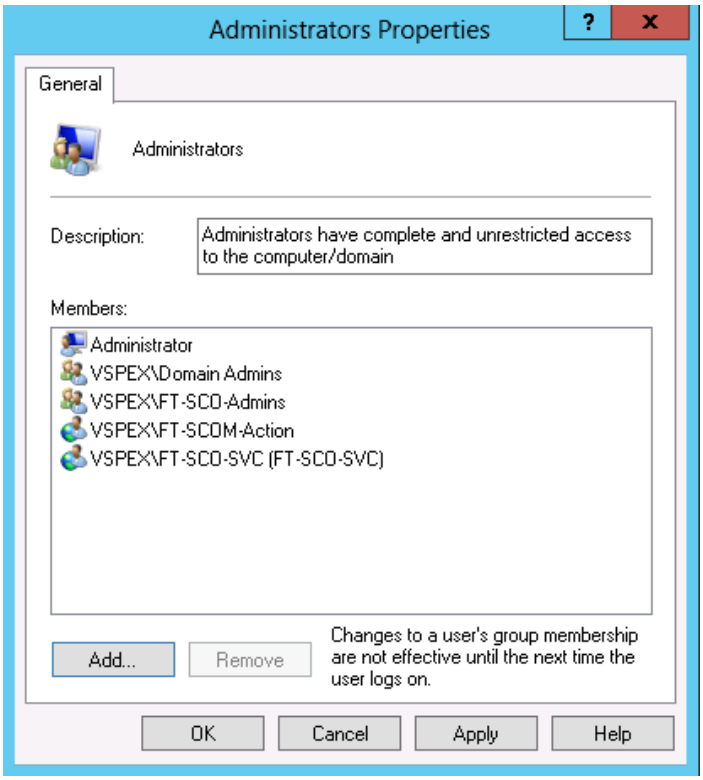
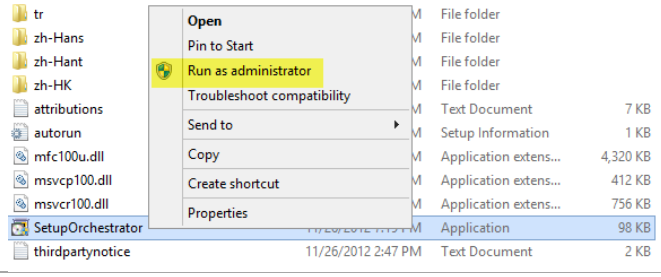
▶ Perform the following steps on the **Orchestrator** virtual machine.	
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.	
In the Install Silverlight dialog, click Install now.	

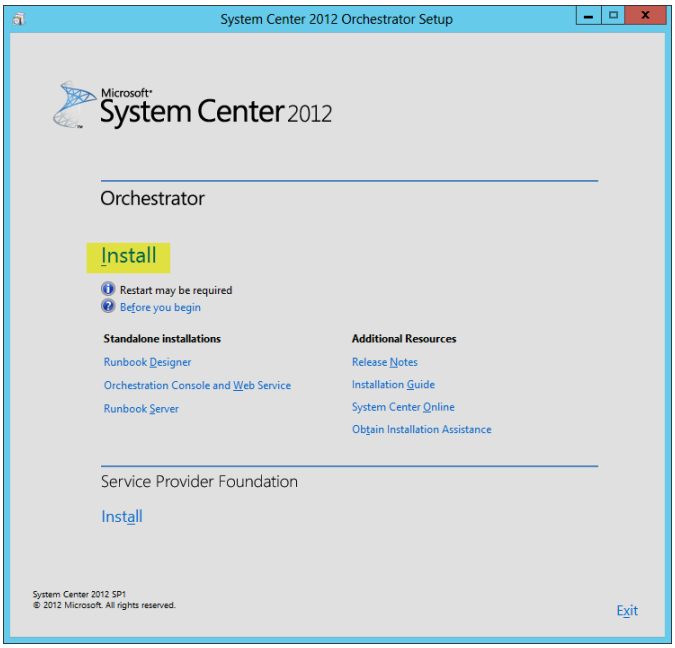
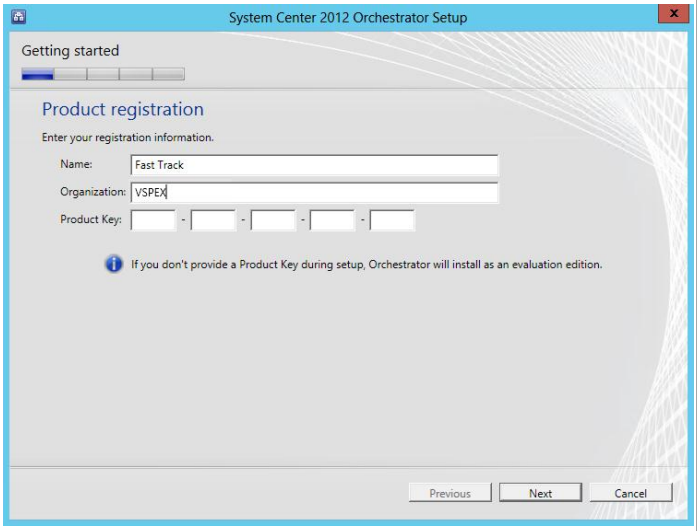
In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.	
In the **Installation Successful** dialog, click **Close** to exit the installation.	

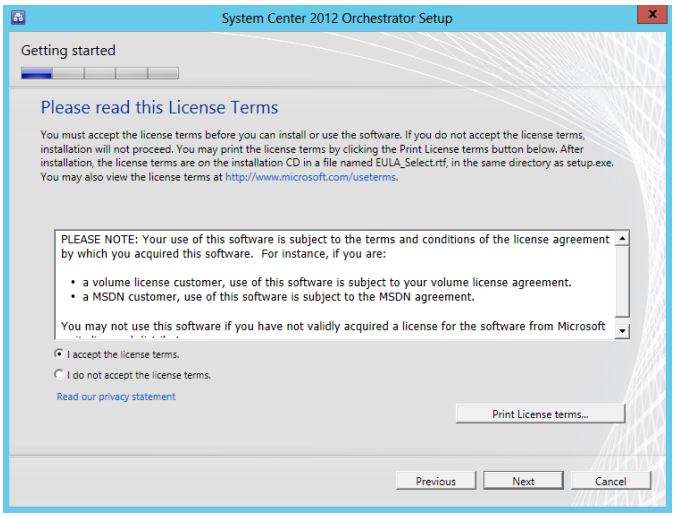
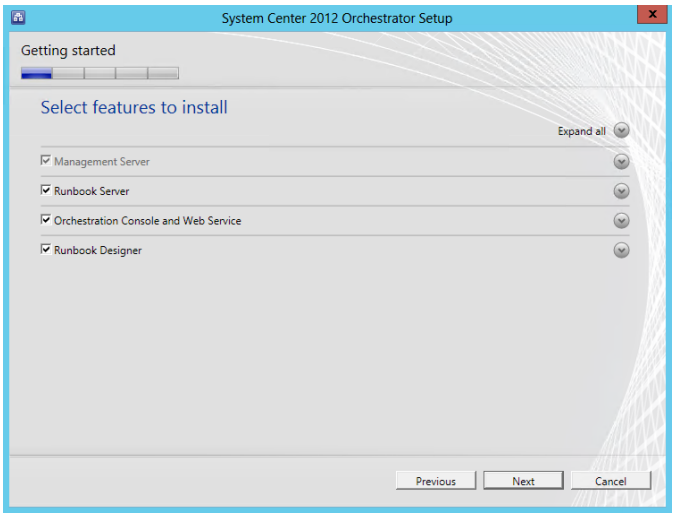
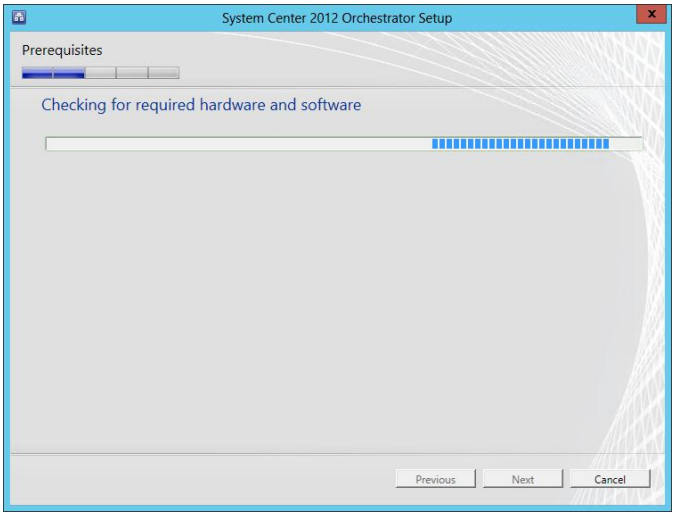
12.3 Installation – Orchestrator Runbook, Web Service, and Designer Server

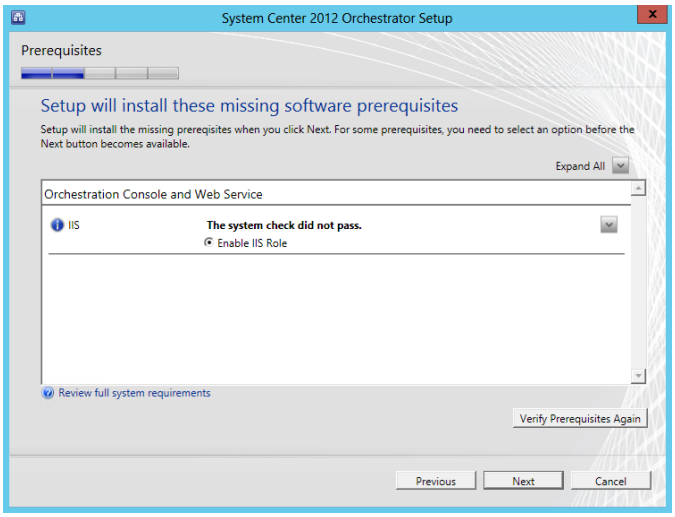
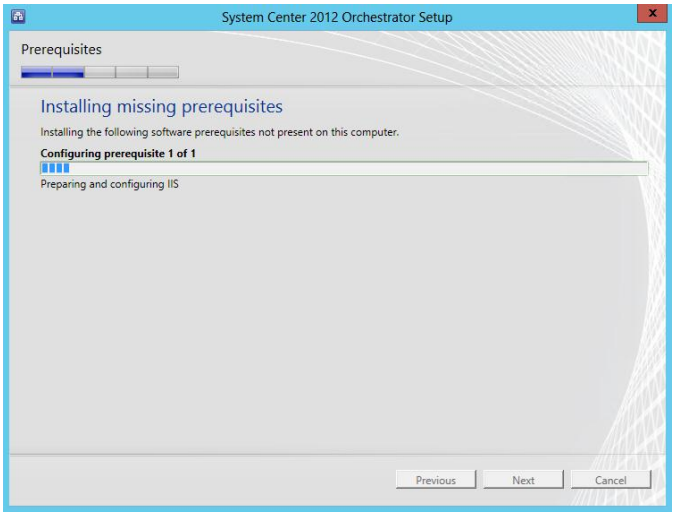
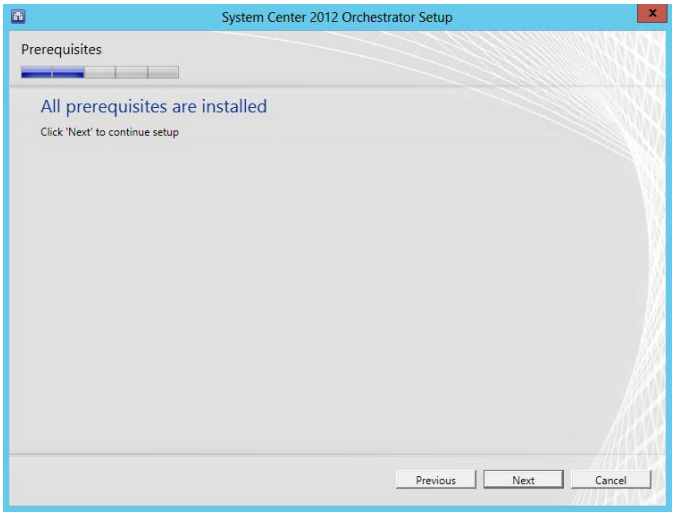
The following steps needs to be completed in order to install the first Orchestrator Runbook Server component.

▶ Perform the following steps on the **Orchestrator** virtual machine.

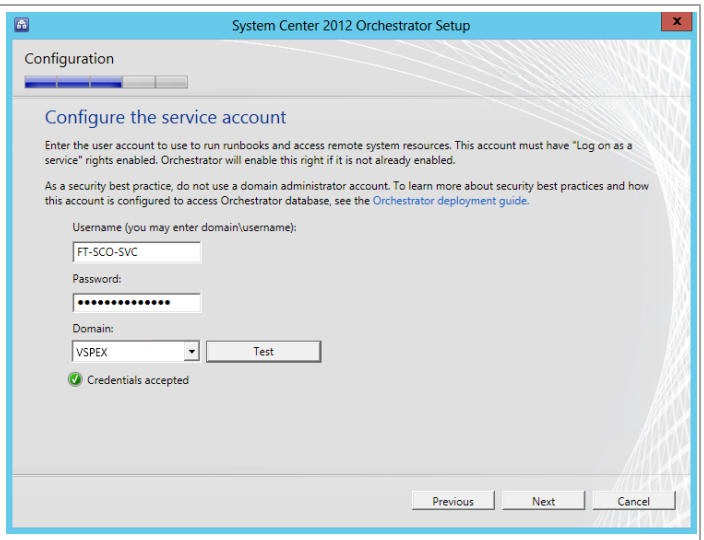
Log on to the Orchestrator virtual machine with a user with local admin rights. Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine: • Orchestrator service account. • Orchestrator Admins group. • Operations Manager action account.	
Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.	

The Orchestrator installation wizard will begin. At the splash page, click **Install** to begin the Orchestrator server installation.	
In the **Product registration information** dialog, provide the following information in the provided text boxes: • **Name** – *specify the name of the primary user or responsible party within your organization*. • **Organization** – *specify the name of the licensed organization*. • **Product Key** – *provide a valid product key for installation of Orchestrator. If no key is provided, Orchestrator will be installed in evaluation mode*. Click **Next** to continue.	

In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option check box is selected and click **Next** to continue.	
In the **Select Features to install** dialog, select the **Management Server** (default selected), **Runbook server, Orchestration console and web service,** and **Runbook Designer** check boxes and click **Next** to continue.	
The **Checking for required hardware and software** dialog will appear to verify the installation prerequisites. When validation completes, click **Next** to continue.	

The Orchestrator setup will identify any prerequisite software required for the installation to complete. The **Setup will install these missing software prerequisites** dialog will attempt to perform the installation of missing prerequisites. When completed, click **Next** to continue.	 
When the installation of the missing prerequisites is completed, click **Next** to continue.	

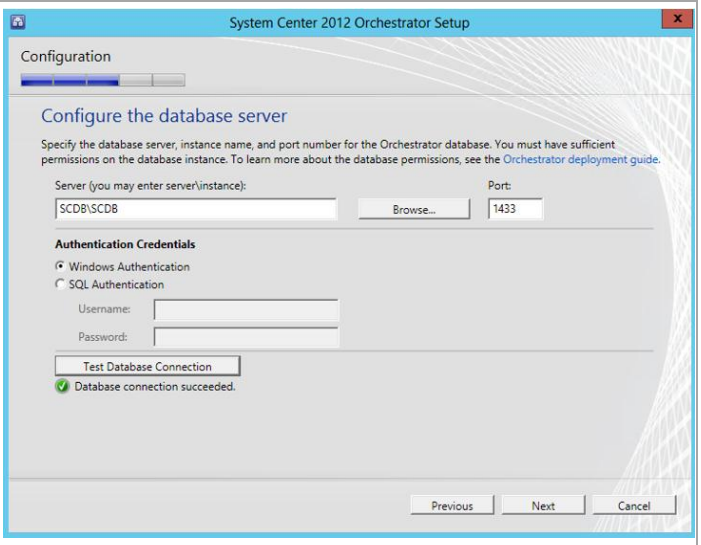
In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
Before proceeding, click the **Test** button to verify the credentials provided.
When successful, click **Next** to continue.



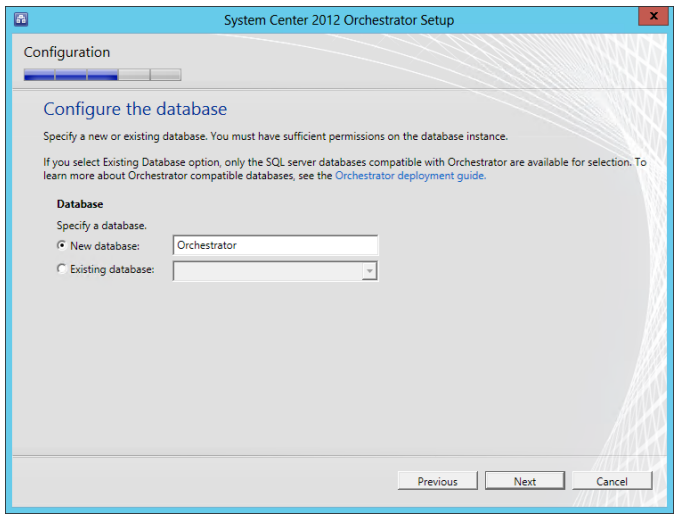
In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
- **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*

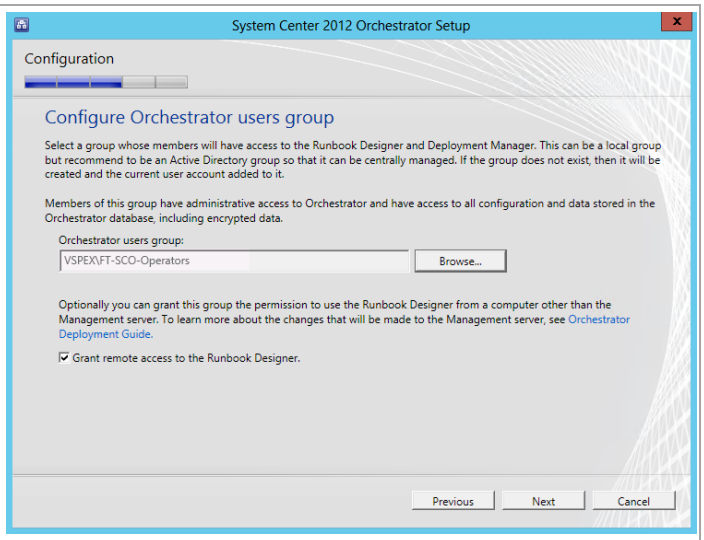
In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.
When successful, click **Next** to continue.



In the **Configure the database** dialog in the **Database** section, select the **New Database** option. Specify the default database name of *Orchestrator*.
Click **Next** to continue.



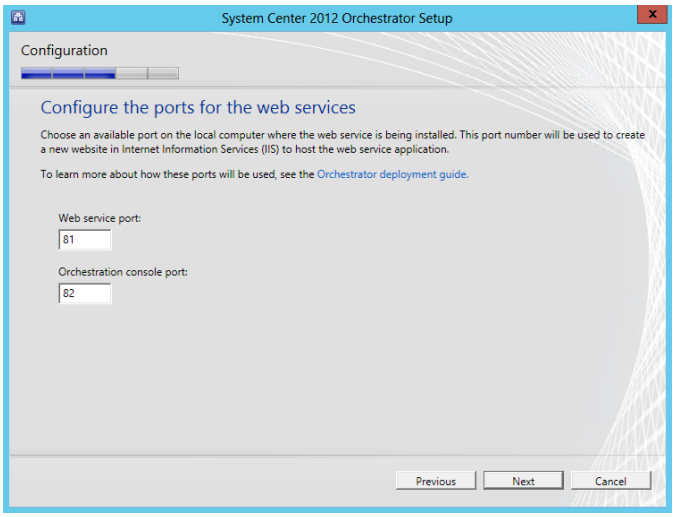
In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse…** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.
Verify that that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



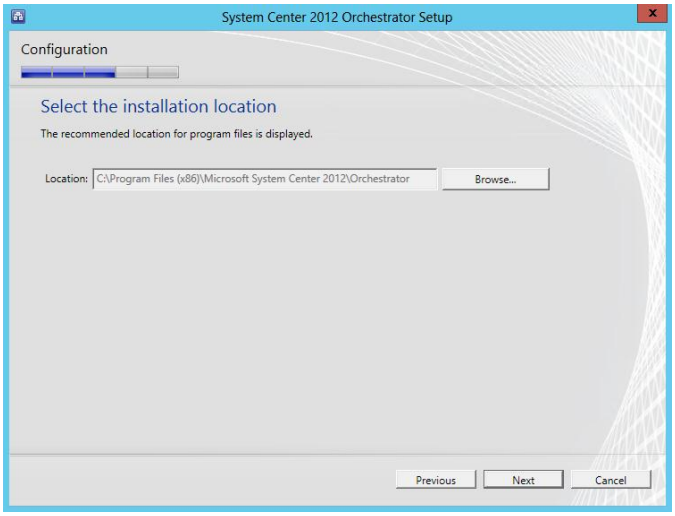
In the **Configure the ports for the web services** dialog, provide the following information in the provided text boxes:

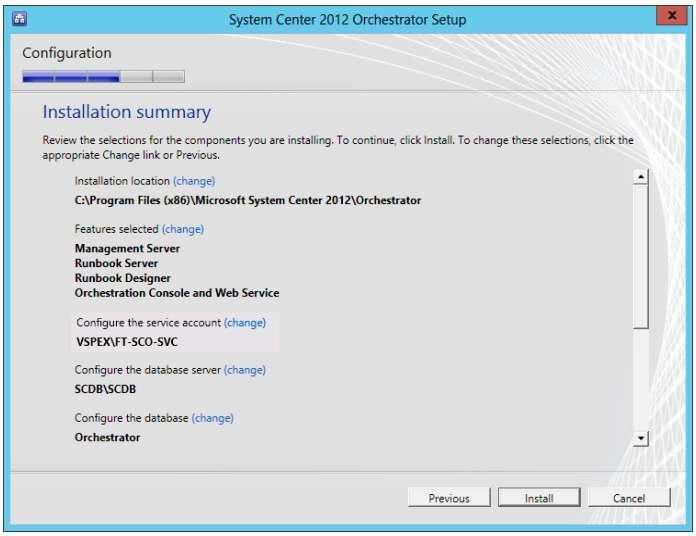
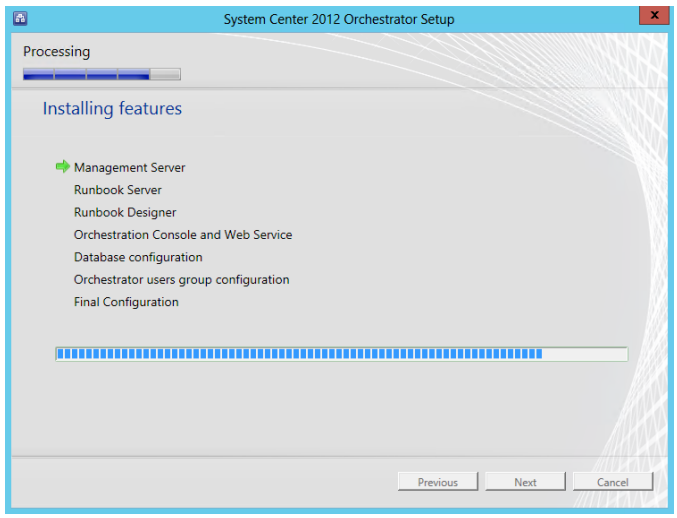
- **Web service port** – *specify the TCP port used for the Orchestrator Web Service. The default value of 81 is recommended.*
- **Orchestration console port** – *specify the TCP port used for the Orchestrator console port. The default value of 82 is recommended.*

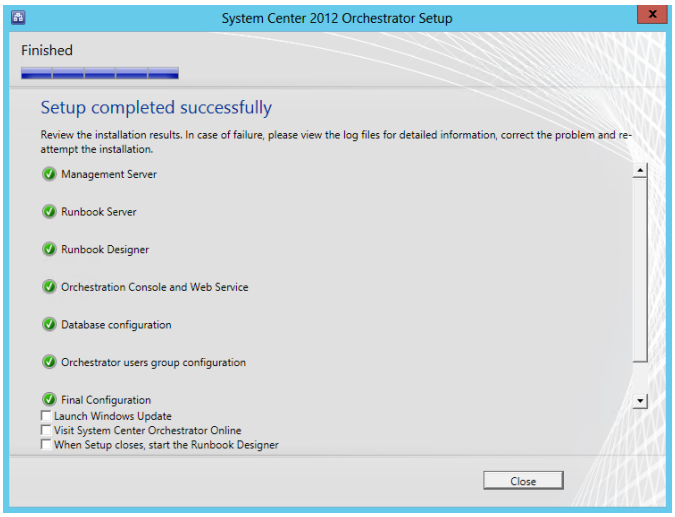
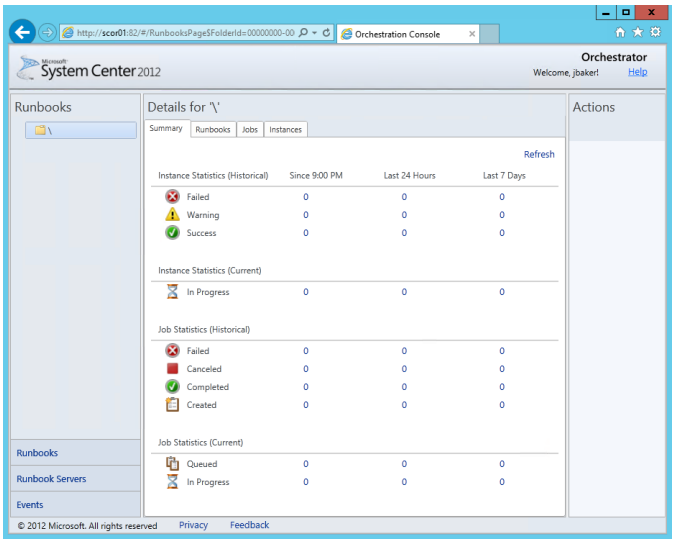
When successful, click **Next** to continue.

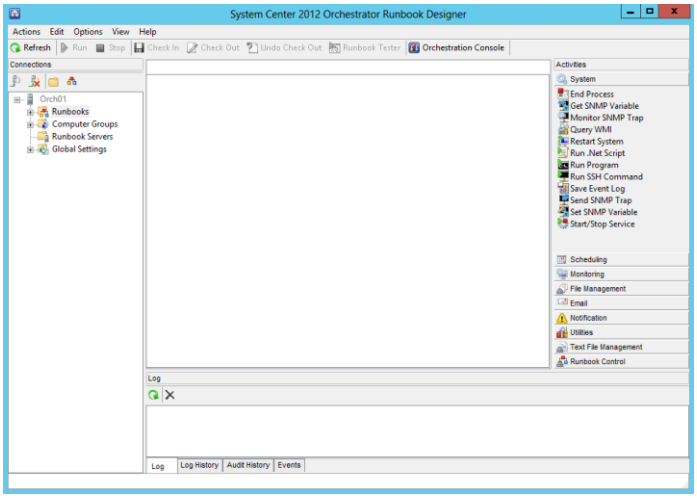
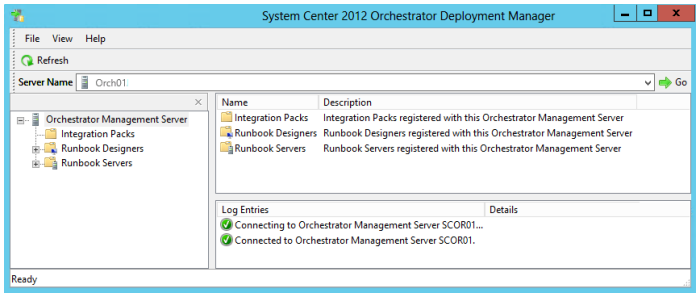
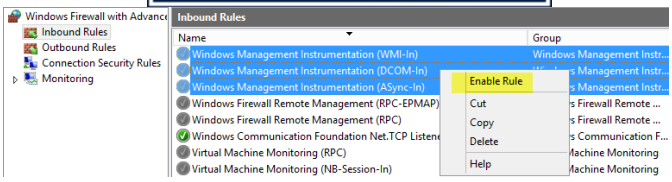


In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation.
Click **Next** to continue.



The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. These include: • **Customer Experience Improvement Program (CEIP)** • **Error Reporting** Select the appropriate option based on your organization's policies and click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
In the **Installing features** dialog, the installation will proceed and show progress.	

The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.	
When installed, verify that the Orchestrator roles installed properly by opening the consoles. From the **Start** screen, then select the **Orchestration Console** tile. **Note:** In order to run the Orchestration Console on the Orchestrator server, Internet Explorer Enhanced Security must be disabled or configured to function with the console.	
Validate that the **Orchestration console** performs properly in Internet Explorer.	
From the **Start Menu**, then select the **Runbook Designer** tile.	

Launch the **Runbook Designer** console and verify that it performs properly.	
From the **Start Menu**, then select the **Deployment Manager** tile.	
Launch the **Deployment Manager** console and verify that it performs properly.	
From the Start Screen, click on the Windows Firewall tile. Configure Windows Firewall for the first Orchestrator Runbook Server.[18] If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall: • Windows Management Instrumentation (WMI-In). • Windows Management Instrumentation (DCOM-In). • Windows Management Instrumentation (ASync-In). Right-click each rule and select **Enable Rule** from the context menu.	 

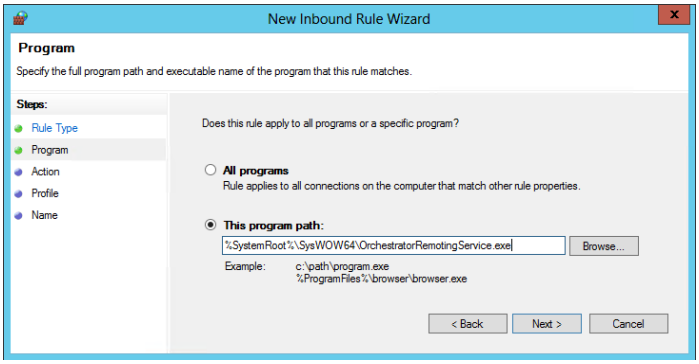
[18] Orchestrator guidance is provided by the following TechNet resources: Using Windows Firewall with Orchestrator - http://technet.microsoft.com/en-us/library/hh912321.aspx and TCP Port Requirements http://technet.microsoft.com/en-us/library/hh420382.aspx.

Alternatively, the following PowerShell commands can be executed to create the firewall rules:

```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
```

```
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
PS C:\Windows\system32>
```

In Windows Firewall create a new Program rule using the following program path:
%SystemRoot%\SysWOW64\orchestratorRemotingService.exe
Name the rule **SCO – Orchestrator Remoting Service (x64)**.



Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO – Orchestrator Remoting Service (x64)" -Program C:\Windows\SysWOW64\OrchestratorRemotingService.exe
```

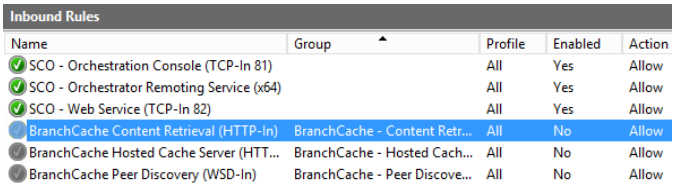
```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "SCO – Orchestrator Remoting Service (x64)" -Program
%SystemRoot%\SysWOW64\OrchestratorRemotingService.exe

Name                  : {abd2120c-7c27-4e12-be18-d30ec87fb805}
DisplayName           : SCO – Orchestrator Remoting Service (x64)
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```

Since the first server runs the Orchestration console and web service, two additional ports (TCP 81 and 82) must be opened on the Windows Firewall as well. Create two additional firewall port rules named **SCO – Orchestration Console (TCP 81)** and **SCO – Web Service (TCP 82)** for each port and enable them.
Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO – Orchestration Console (TCP-In 81)"
New-NetFirewallRule -DisplayName "SCO – Web Service (TCP-In 82)"
```




```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "SCO – Web Service (TCP-In 82)"

Name                  : {b71b0a5b-d013-4372-8519-beafe3afb6a8}
DisplayName           : SCO – Web Service (TCP-In 82)
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```

Restart the Orchestrator server.

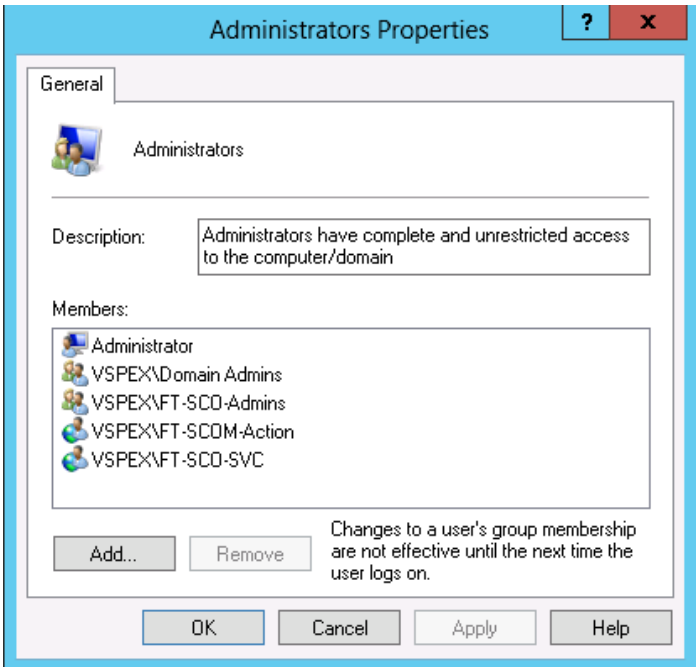
12.4 Install an Additional Orchestrator Runbook Server

The following steps needs to be completed in order to install an additional Orchestrator Runbook Server.

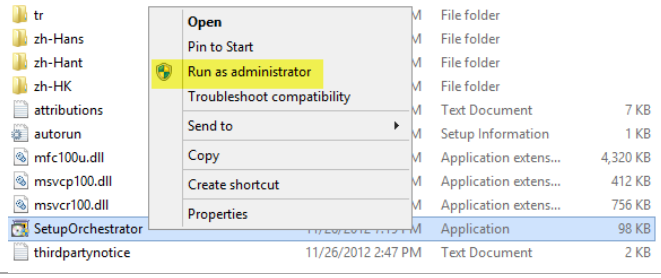
▶ Perform the following steps on the **second Orchestrator Runbook Server** virtual machine.

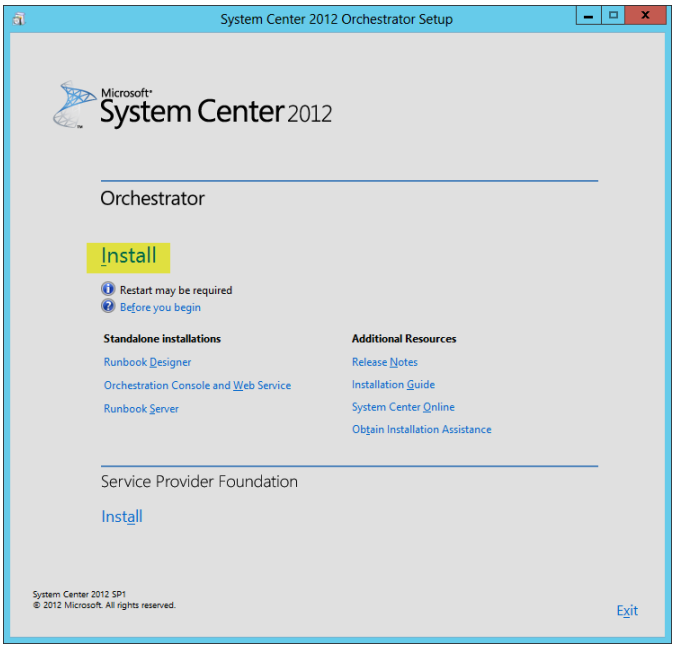
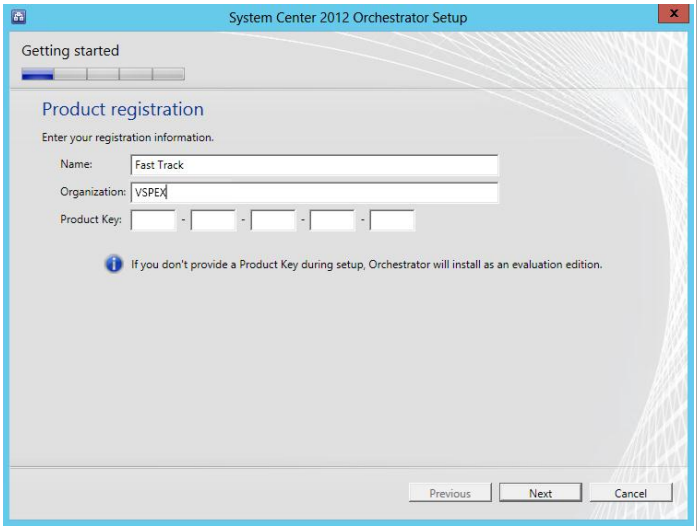
Log on to the Orchestrator virtual machine with a user with local admin rights.
Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:

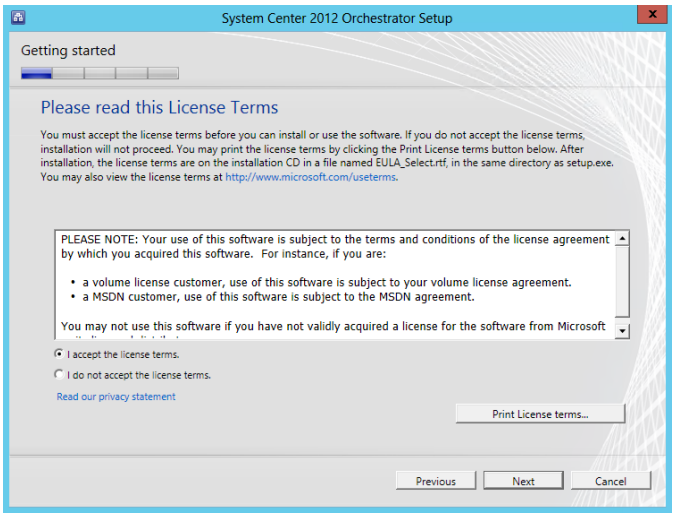
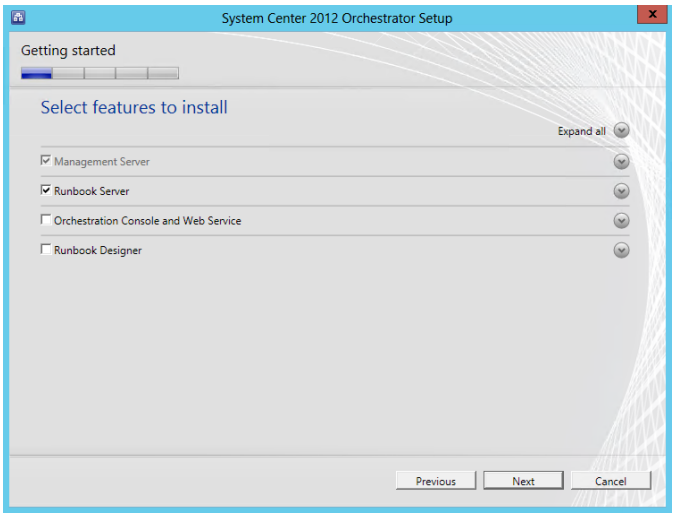
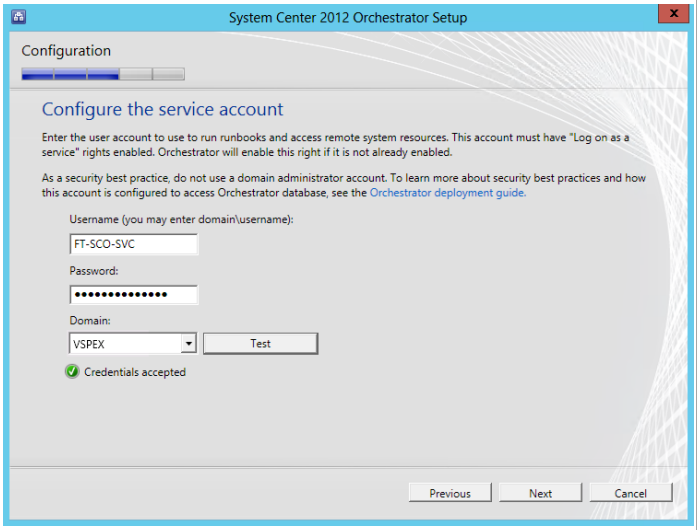
- Orchestrator service account.
- Orchestrator Admins group.
- Operations Manager action account.



Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



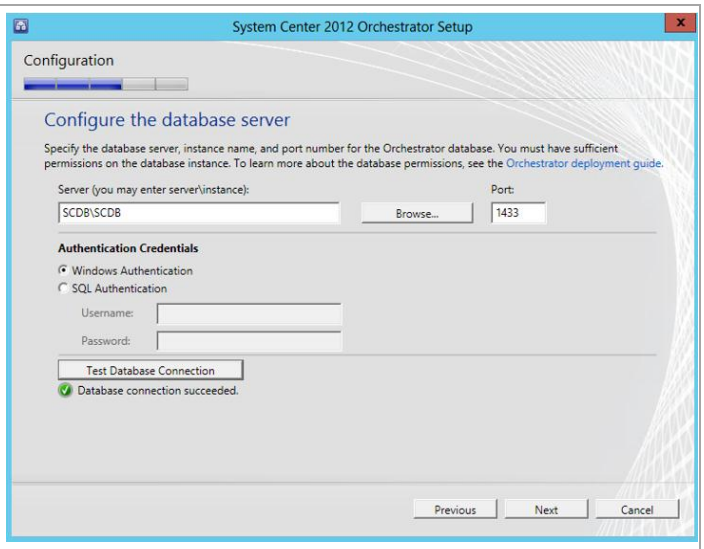
The Orchestrator installation wizard will begin. At the splash page, click **Install** begin the Orchestrator server installation.	
In the **Product registration information** dialog, enter the following information in the provided text boxes: • **Name** – *specify the name of the primary user or responsible party within your organization*. • **Organization** – *specify the name of the licensed organization*. • **Product key** – *provide a valid product key for installation of Orchestrator. If no key is provided, Orchestrator will be installed in evaluation mode*. Click **Next** to continue.	

In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option check box is selected and click **Next** to continue.	
In the **Select Features to install** dialog, select the **Management Server** (default selected) and **Runbook server** check boxes and click **Next** to continue.	
In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test** button to verify the credentials provided. When successful, click **Next** to continue.	

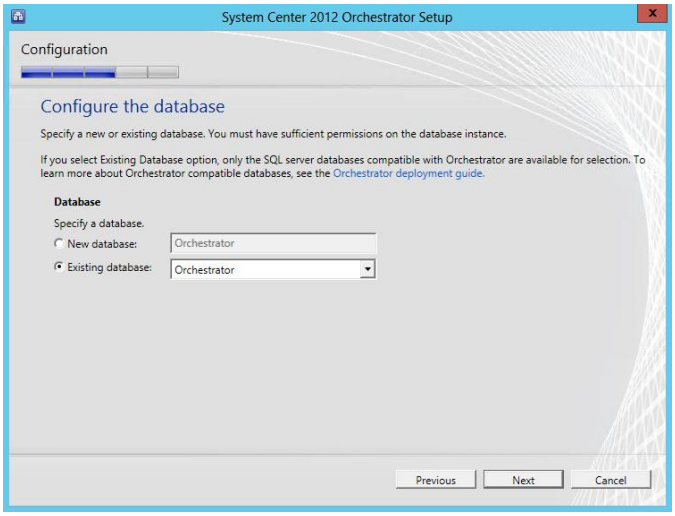
In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
- **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*

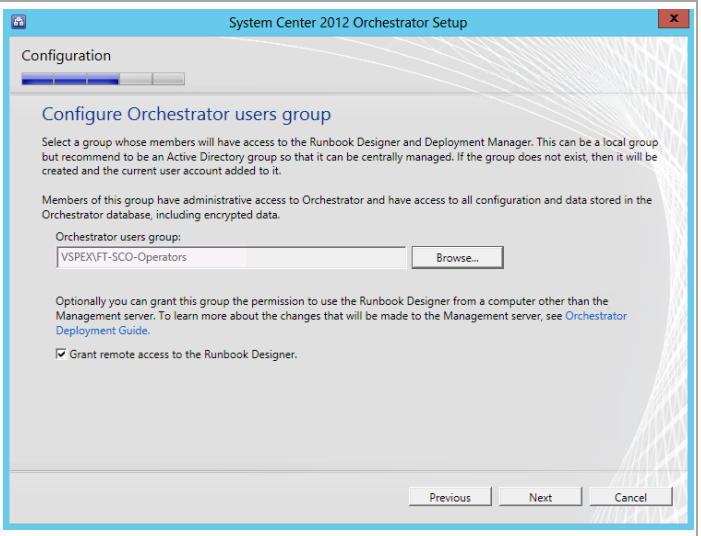
In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.
When successful, click **Next** to continue.

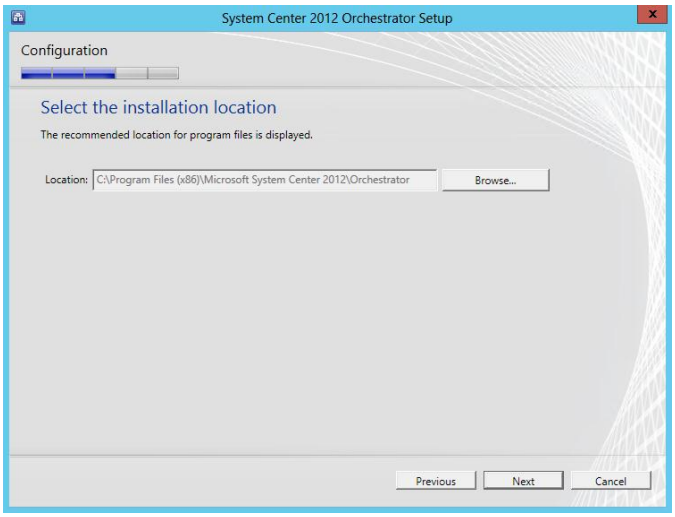


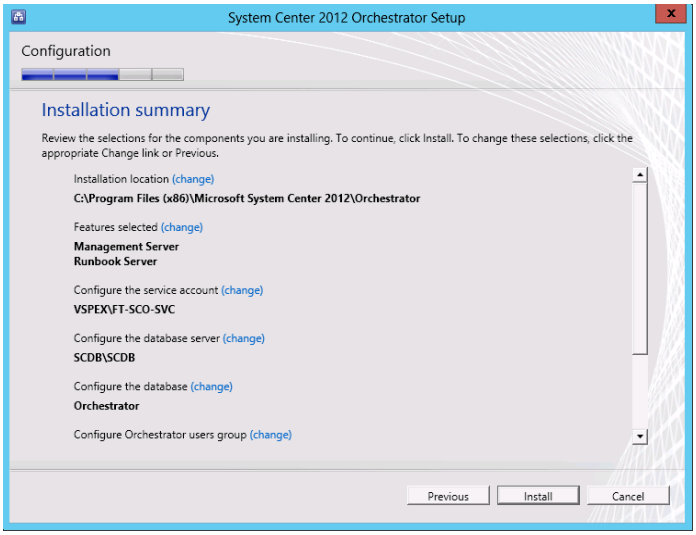
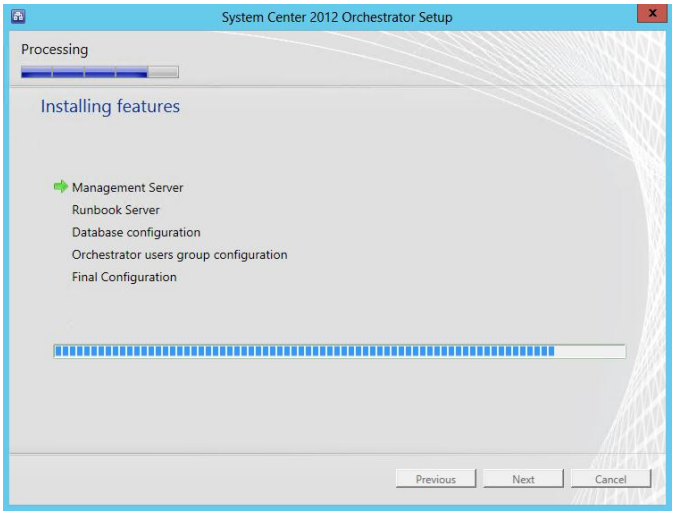
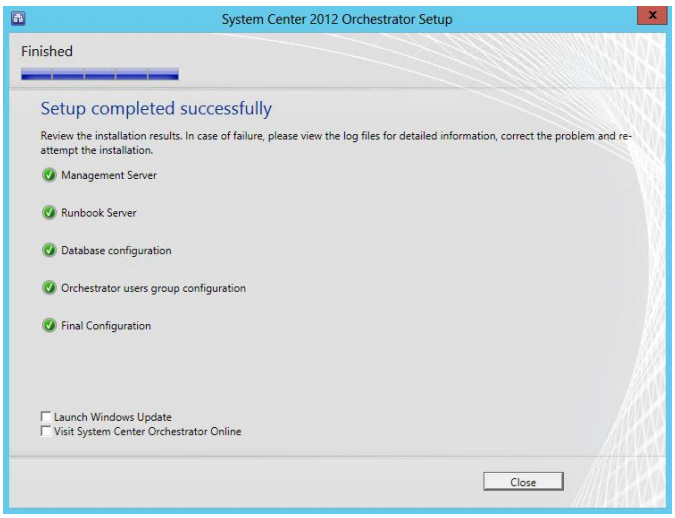
In the **Configure the database** dialog in the **Database** section, select the **Existing Database** option. Select the default database name of *Orchestrator* from the drop-down menu.
Click **Next** to continue.



In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse…** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.
Verify that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.	
Depending on the current configuration of the server the Microsoft Updates Dialog may appear. The **Microsoft Update** dialog provides options for participating in automatic updates for Orchestrator. Select the appropriate option based on your organization's policies and click **Next** to continue.	
The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. This includes: • **Customer Experience Improvement Program (CEIP)** • **Error Reporting** Select the appropriate option based on your organization's policies and click **Next** to continue.	

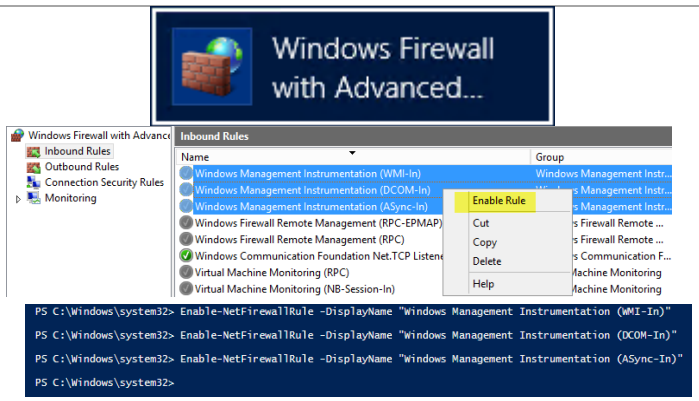
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
In the **Installing features** dialog, the installation will proceed and show progress.	
The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.	

Configure Windows Firewall for the second Orchestrator Runbook Server.[19]
If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:

- Windows Management Instrumentation (WMI-In).
- Windows Management Instrumentation (DCOM-In).
- Windows Management Instrumentation (ASync-In).

Right-click each rule and select **Enable Rule** from the context menu.
Alternatively, the following PowerShell commands can be executed:

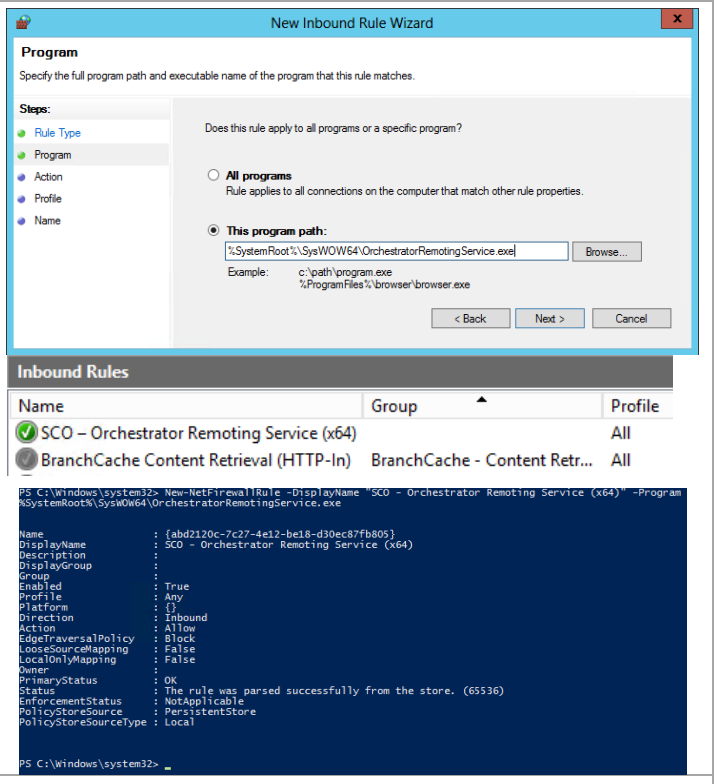
```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
```



[19] Orchestrator guidance is provided from the following TechNet resources: Using Windows Firewall with Orchestrator - http://technet.microsoft.com/en-us/library/hh912321.aspx and TCP Port Requirements http://technet.microsoft.com/en-us/library/hh420382.aspx.

In Windows Firewall create a new Program rule using the following program path: %SystemRoot%\SysWOW64\orchestratorRemotingService.exe
Name the rule **SCO – Orchestrator Remoting Service (x64)**.
Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO – Orchestrator Remoting Service (x64)" -Program C:\Windows\SysWOW64\OrchestratorRemotingService.exe
```



Restart the Orchestrator server.

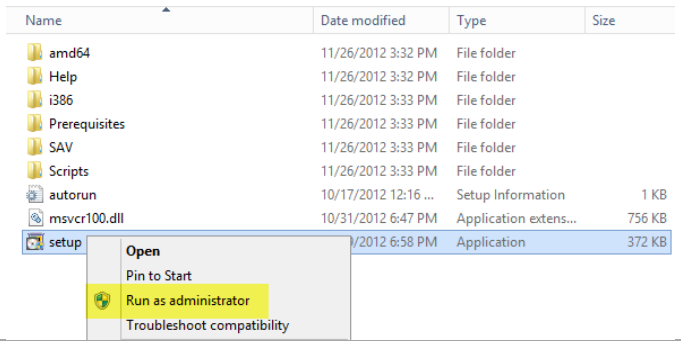
12.5 Post-Installation Tasks

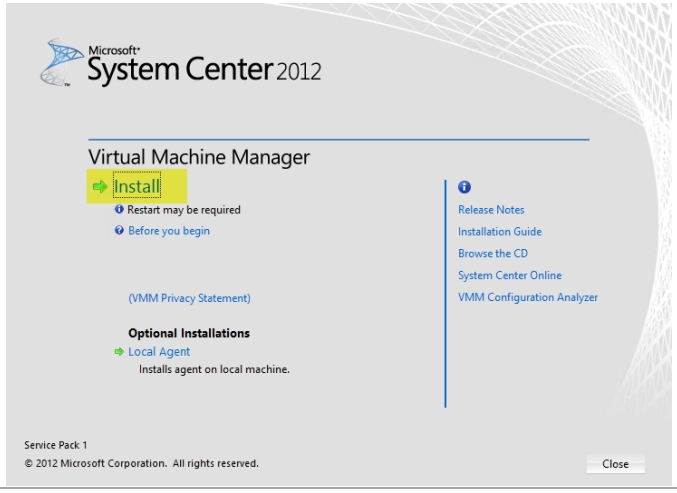
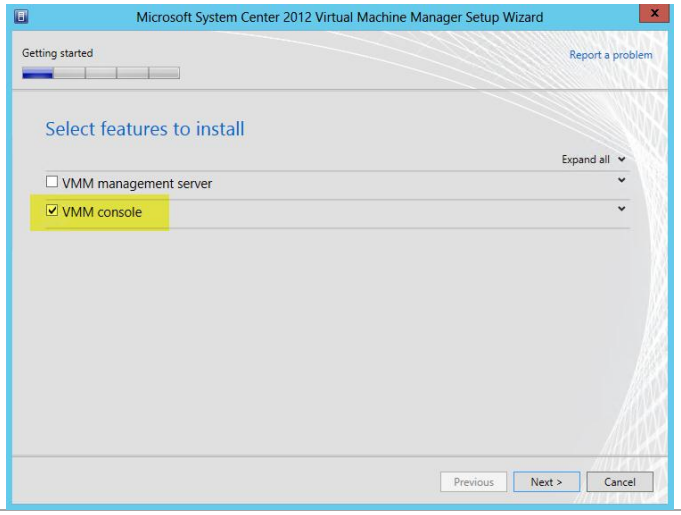
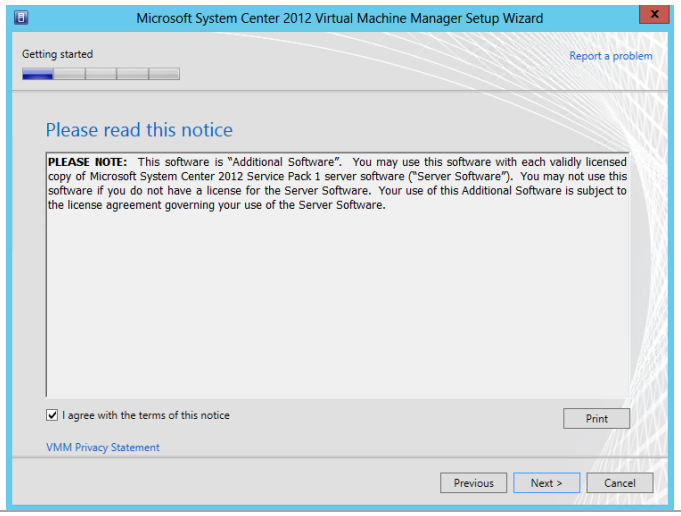
When the installation is complete, the installation and configuration of Orchestrator Integration Packs on the target runbook servers.

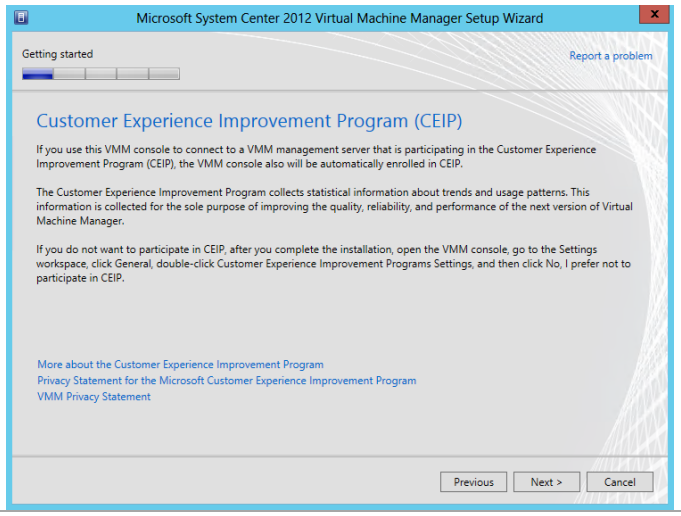
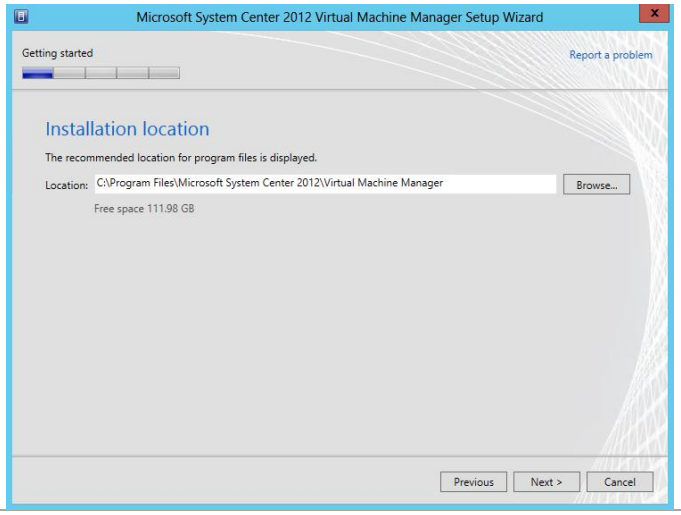
Install the Virtual Machine Manager Console

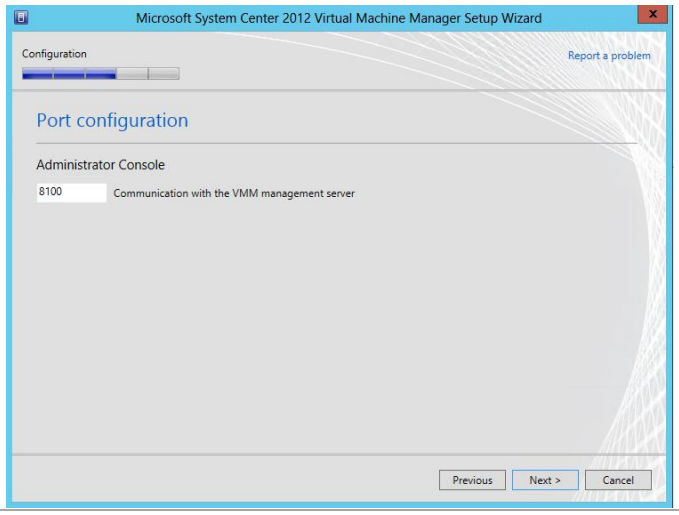
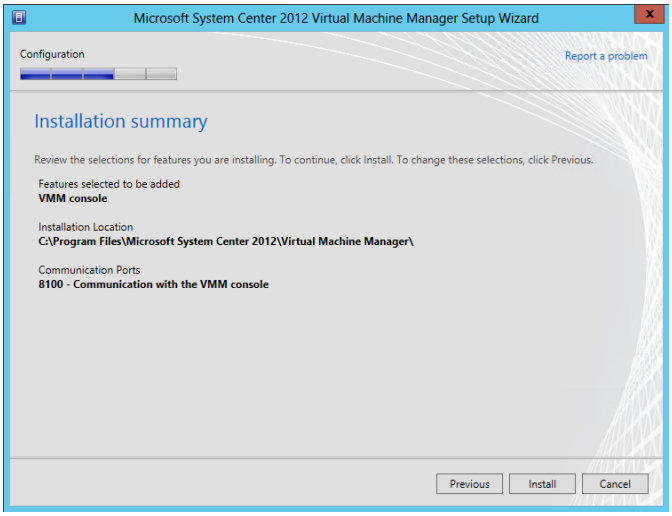
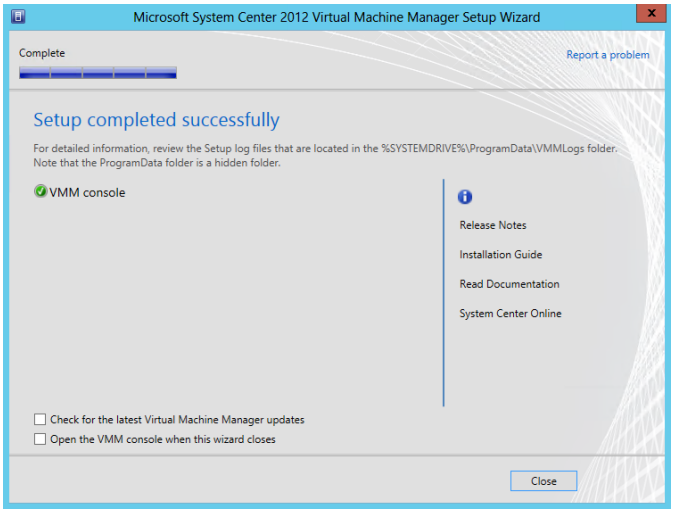
▶ Perform the following steps on the **Orchestrator** virtual machines.

Log on to the Orchestrator server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.	
In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.	
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.	

In the **Customer Experience Improvement Program** dialog, click **Next** to continue.	
Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.	

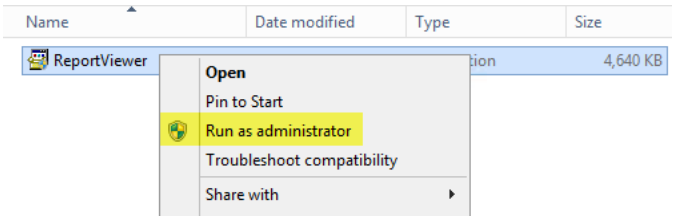
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

Install the Microsoft Report Viewer 2010 SP1

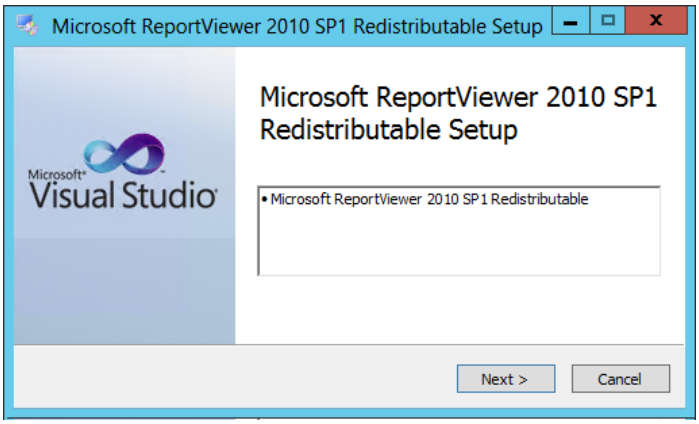
Additionally, inside Orchestrator the Operations Manager console is required, but this also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation. Follow the provided steps to install the SP1 package.

▶ Perform the following steps on both **Orchestrator** virtual machines.

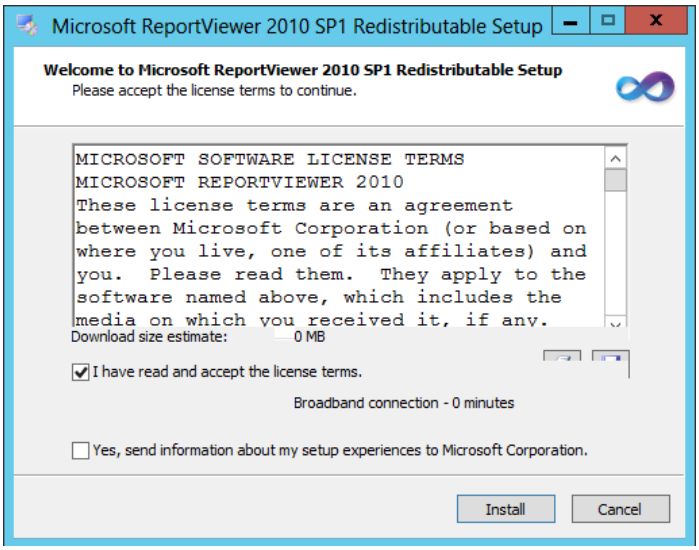
From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



Within the Microsoft ReportViewer 2010 SP1 Redistributable Setup dialog, select Next to begin the installation.

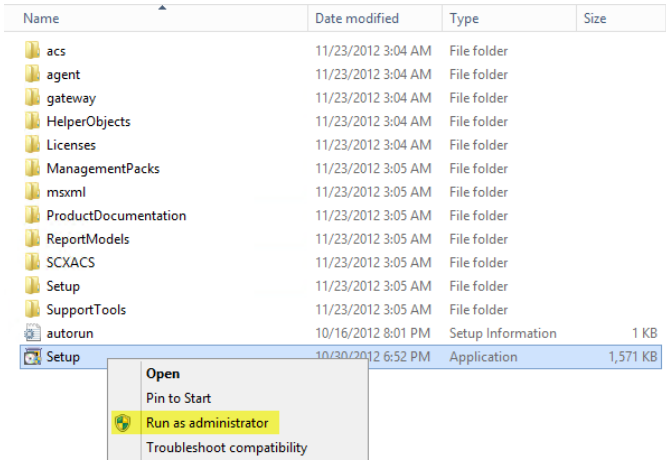


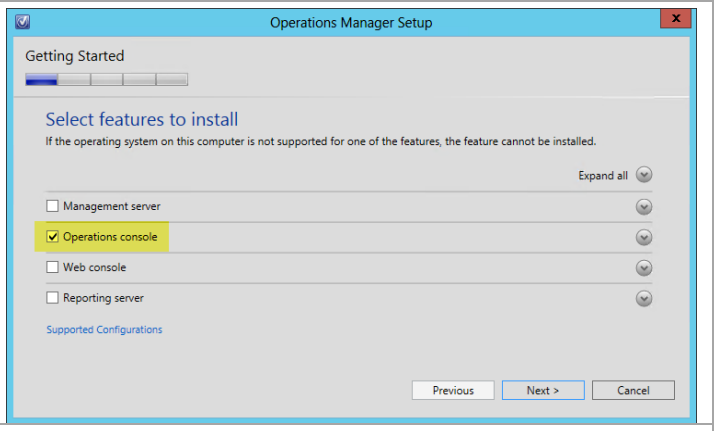
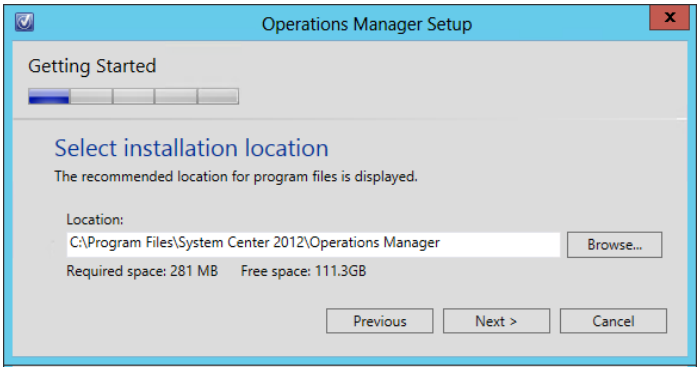
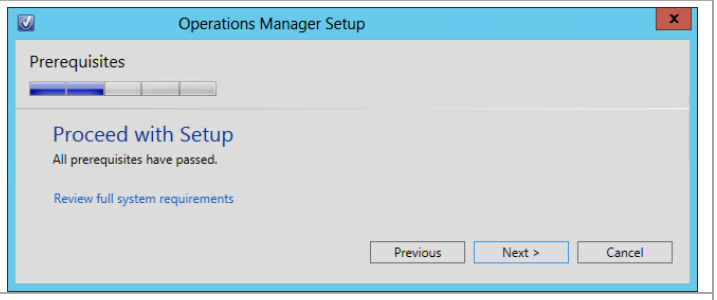
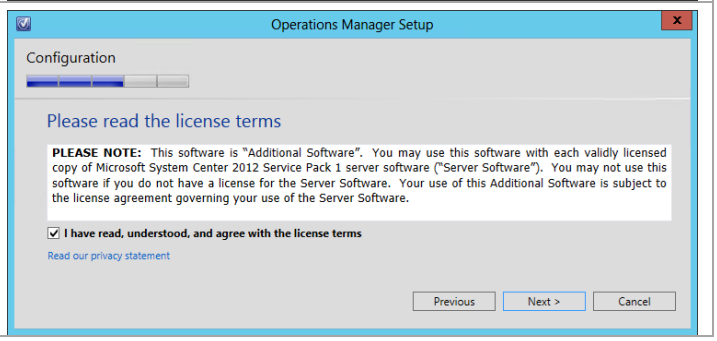
Select **I have read and accept the license terms** check box and click Install.

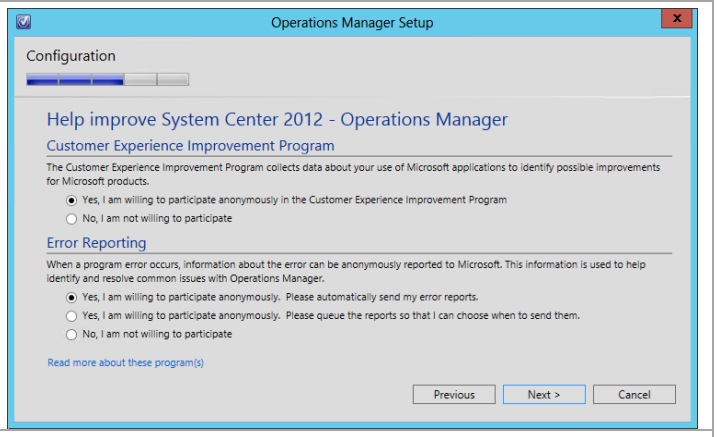
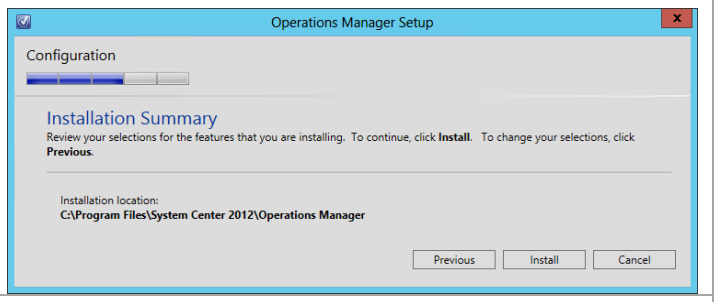
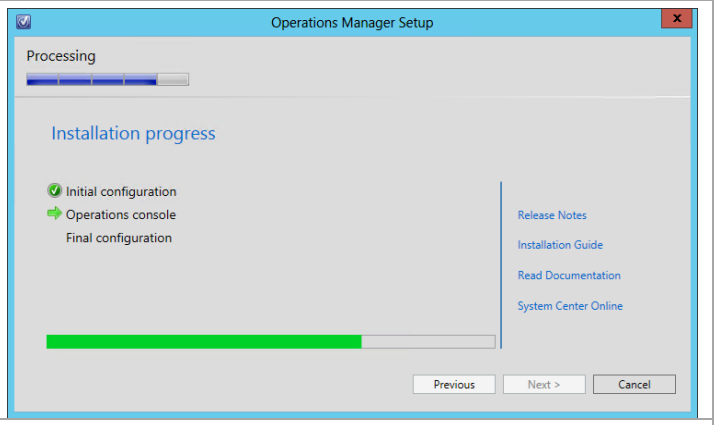
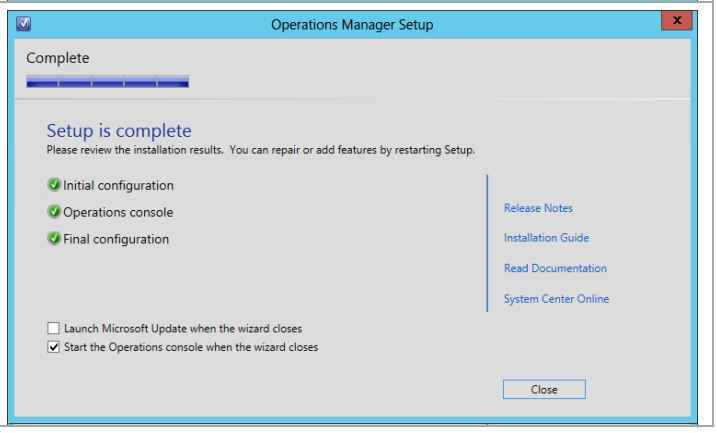


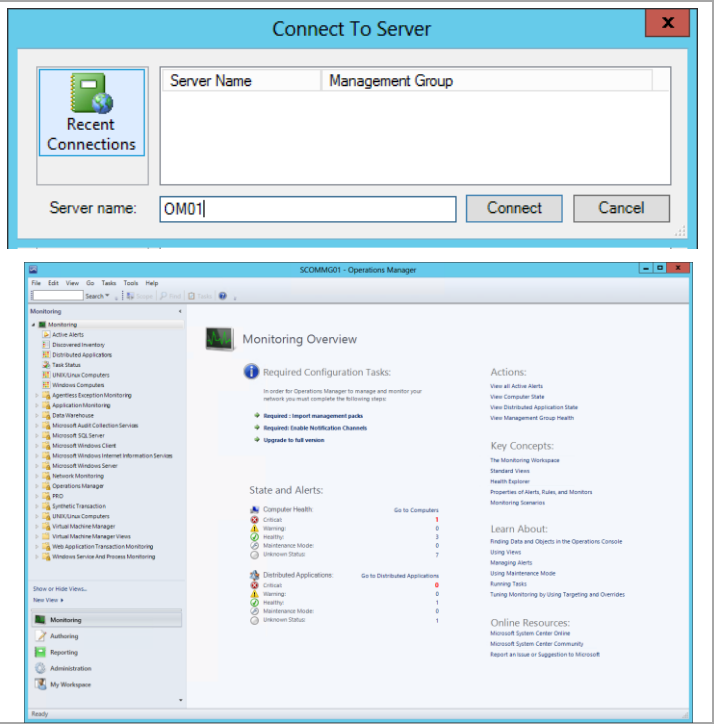
The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.	

Install the Operations Manager Console

▶ Perform the following steps on both of the **Orchestrator** virtual machines.	
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.	

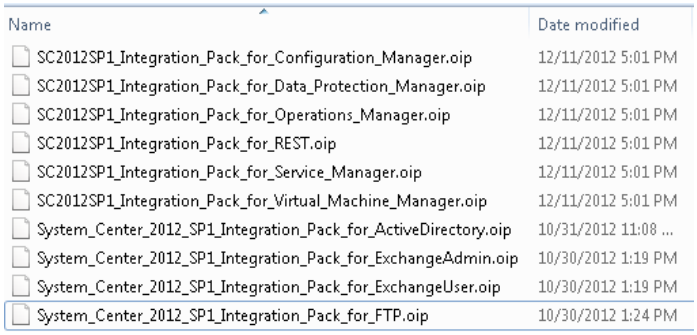
In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.	
The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.	
In the **Please read the license terms** dialog, verify that the I have read, understood and agree with the terms of the license agreement installation option check box is selected and click **Next** to continue.	

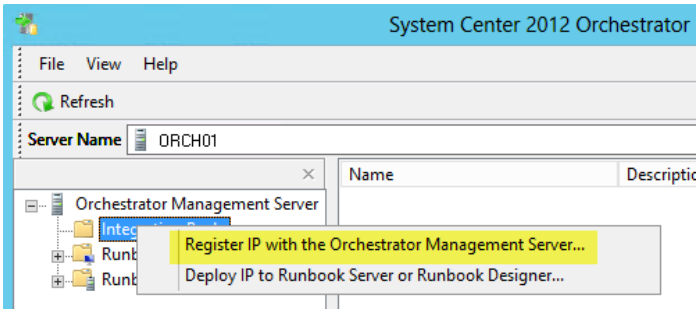
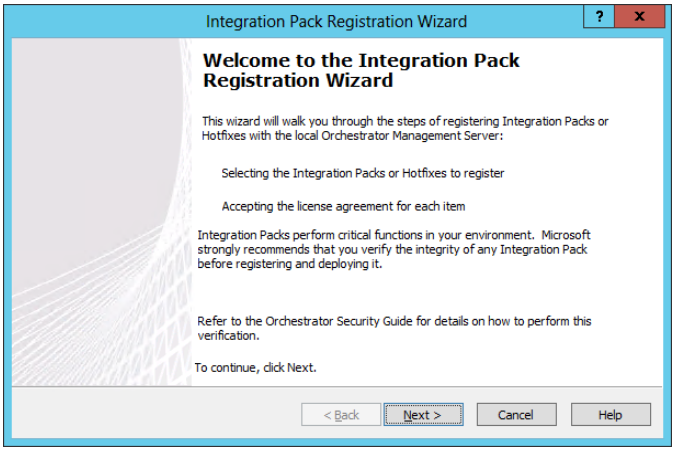
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include: • **Customer Experience Improvement Program (CEIP)** • **Error Reporting** Select the appropriate option based on your organization's policies and click **Next** to continue.	
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
The installation progress will be displayed during the installation.	
When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.	

When completed, the Operations Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.	

Install Integration Packs

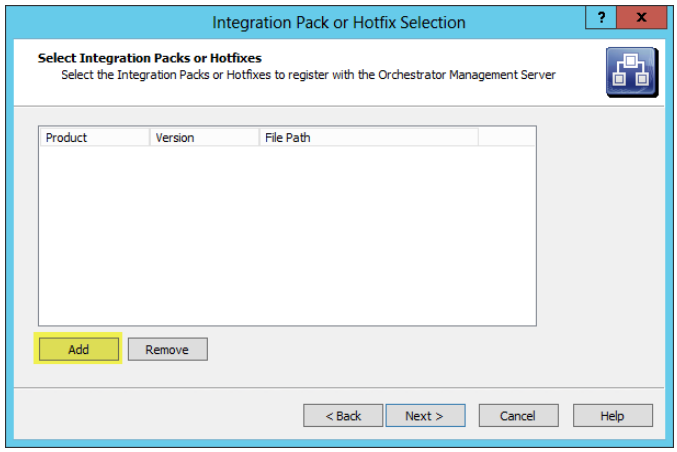
The following steps needs to be completed in order to install the Orchestrator Integration Packs.

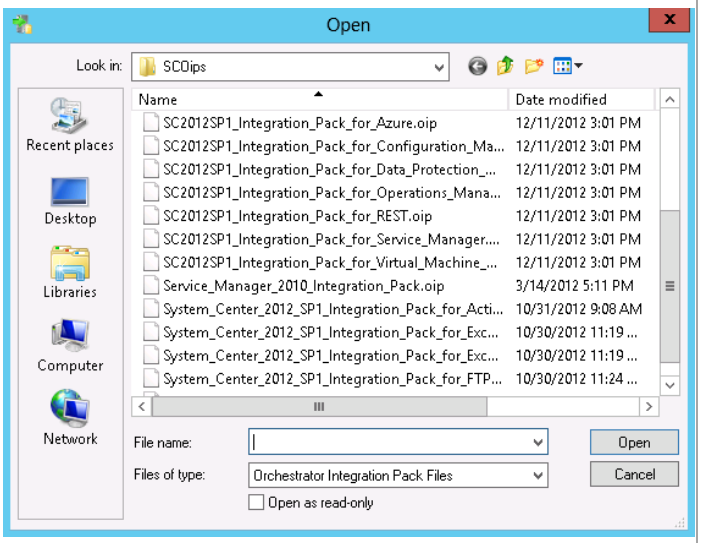
▶ Perform the following steps on the **Orchestrator Runbook Server** virtual machine.	
Download the System Center 2012 SP1 Integration Packs from http://www.microsoft.com/en-us/download/details.aspx?id=34611, and expand them to a single location so the Orchestrator Integration Pack files are expanded.	
From the **Start** screen, click the **Deployment Manager** tile.	

In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Register IP with the Orchestrator Management Server…** option from the context menu.	
The **Integration Pack Registration Wizard** will appear. Click **Next** to continue.	

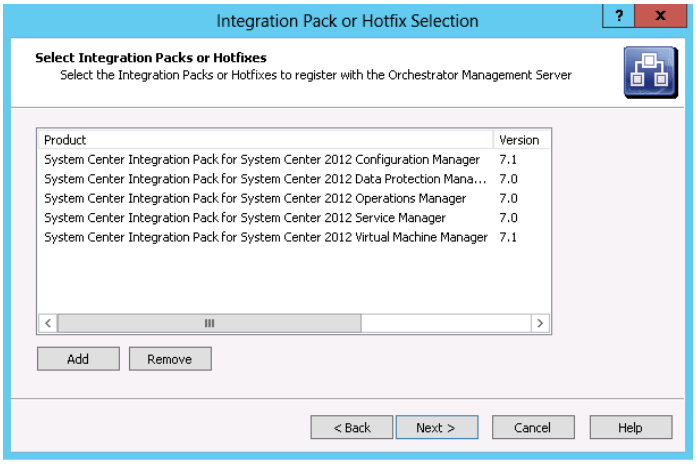
In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the expanded integration packs folder created earlier and select the following integration packs and click **Open**:

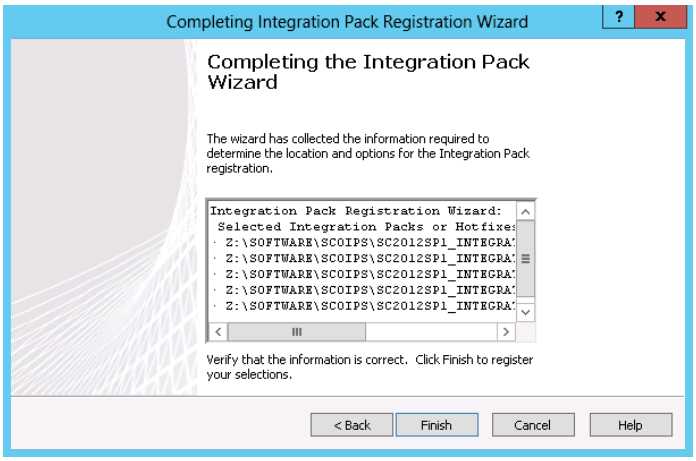
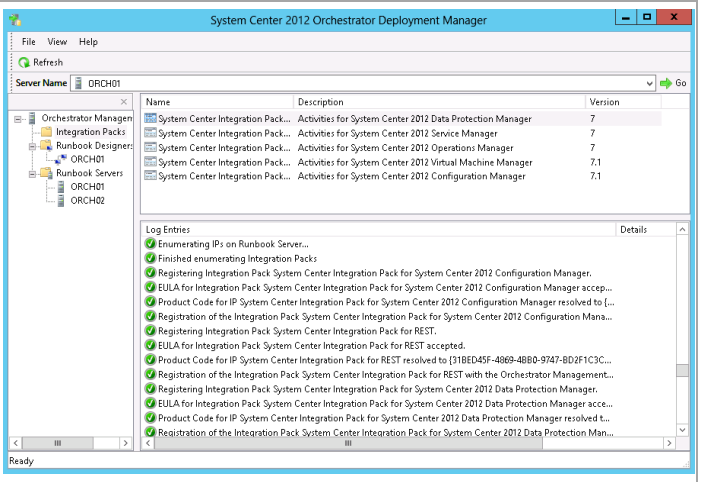
- System Center 2012 Configuration Manager.
- System Center 2012 Data Protection Manager.
- System Center 2012 Operations Manager.
- System Center 2012 Service Manager.
- System Center 2012 Virtual Machine Manager.





When all integration packs are selected, click **Next** to continue.

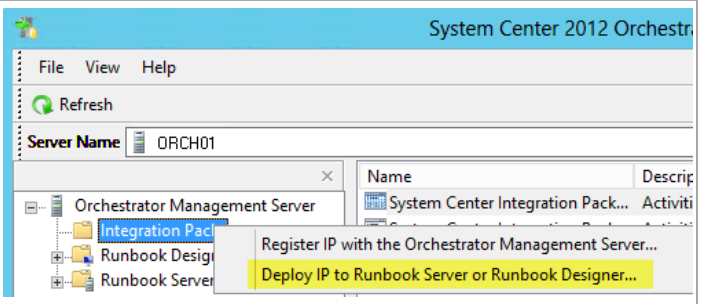
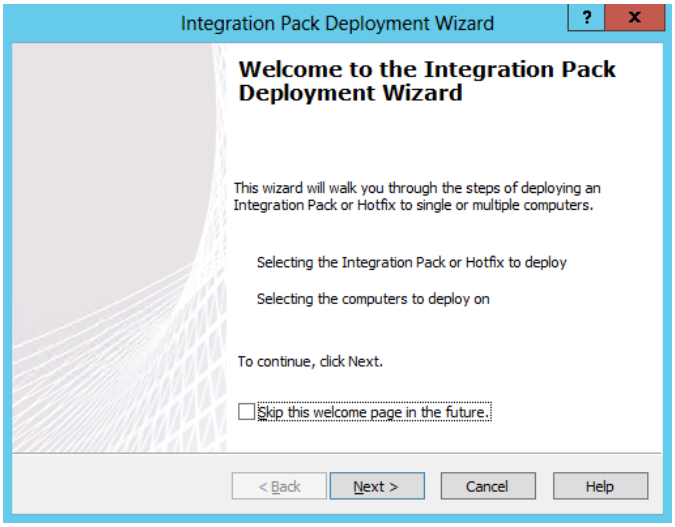


The **Completing the Integration Pack Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.	
During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.	
When complete, each integration pack will be displayed in the Deployment Manager interface.	

Deploy Integration Packs

The following steps needs to be completed in order to deploy the Orchestrator Integration Packs.

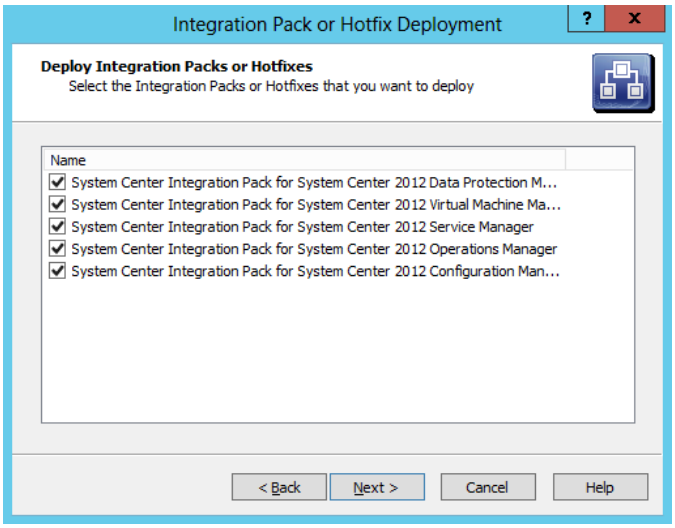
▶ Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

From the **Start** screen, click the **Deployment Manager** tile.	
In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer…** option from the context menu.	
The **Integration Pack Deployment Wizard** will appear. Click **Next** to continue.	

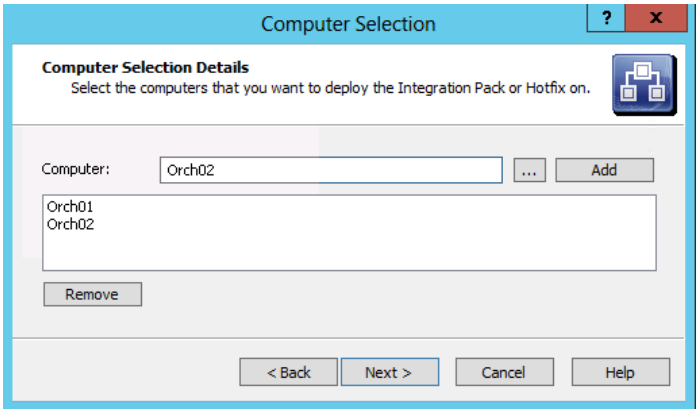
In the **Deploy Integration Packs or Hotfixes** dialog, select the check boxes integration packs folder created earlier and select the following integration packs:

- System Center 2012 Configuration Manager.
- System Center 2012 Data Protection Manager.
- System Center 2012 Operations Manager.
- System Center 2012 Service Manager.
- System Center 2012 Virtual Machine Manager.

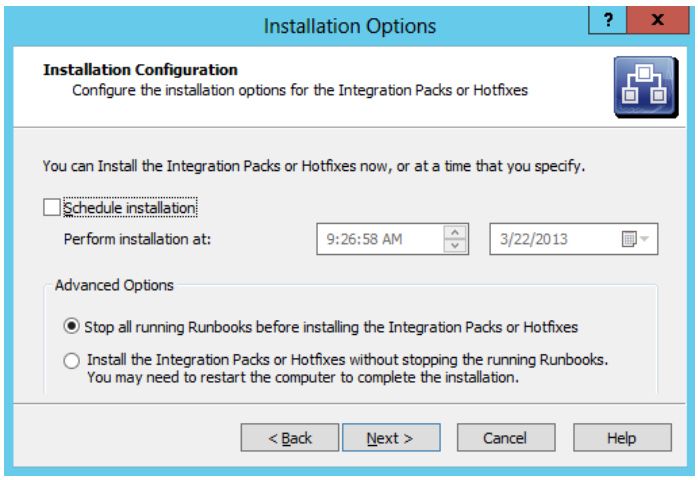
Once complete, click **Next** to continue.

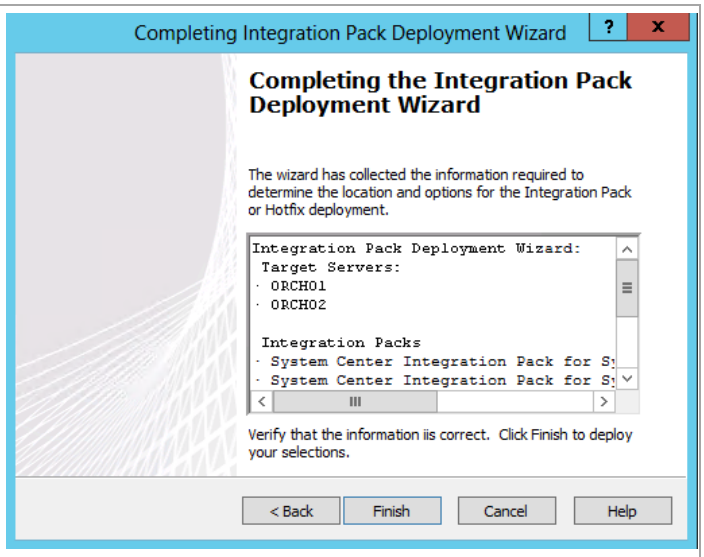
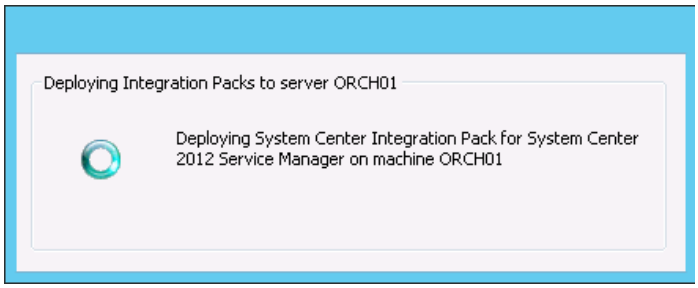


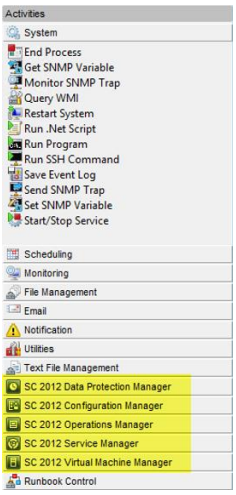
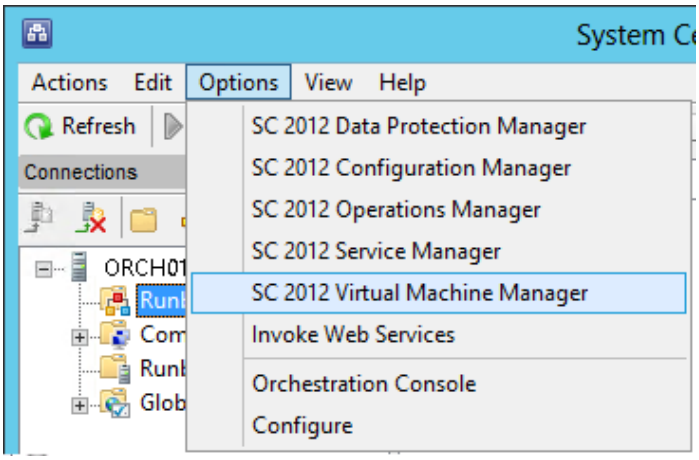
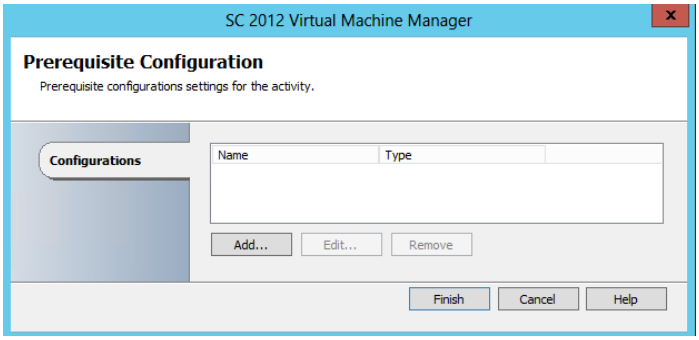
In the **Computer Selection Details**, type the name of the Orchestrator management server and click **Add**. Once added, click **Next** to continue.

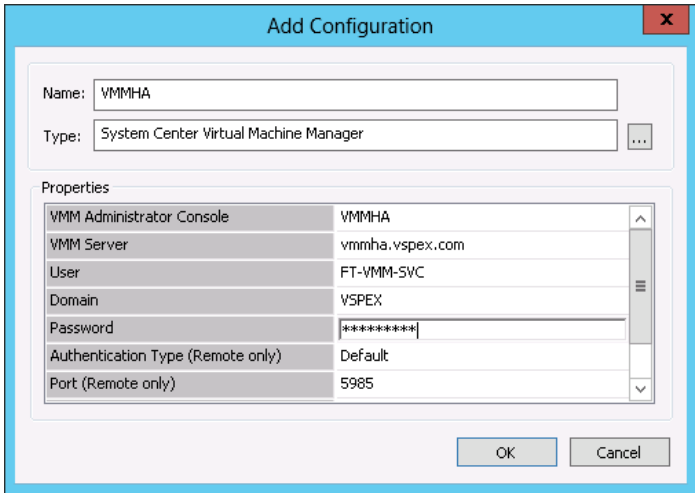
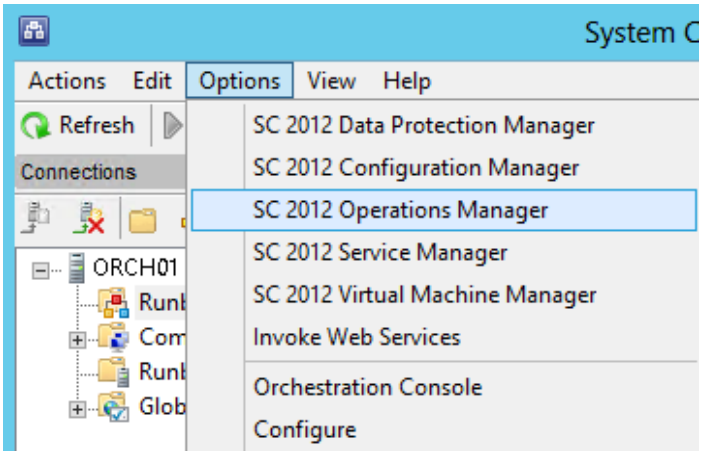
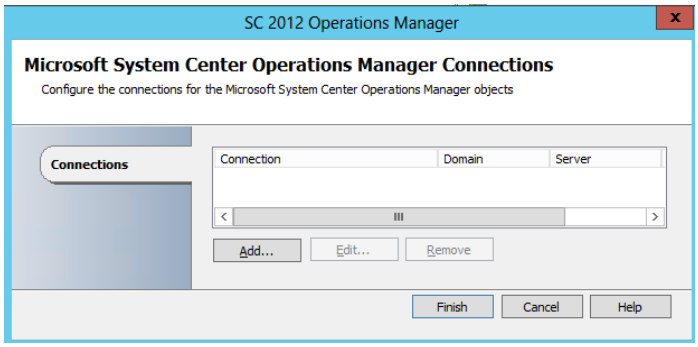


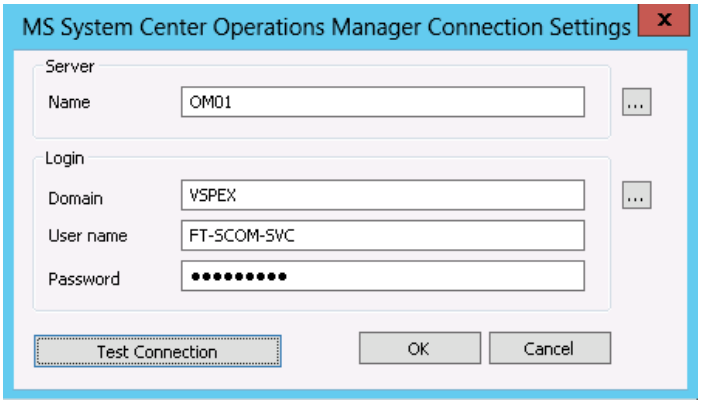
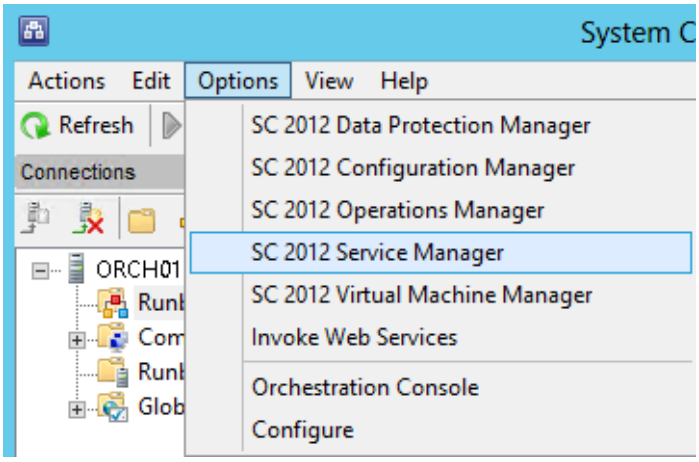
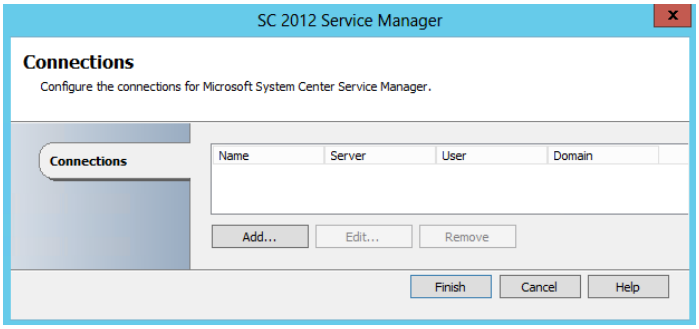
In the Installation Configuration dialog, in the Advanced Options pane select Stop all running Runbooks before installing the Integration Packs or Hotfixes option. Click Next to continue.



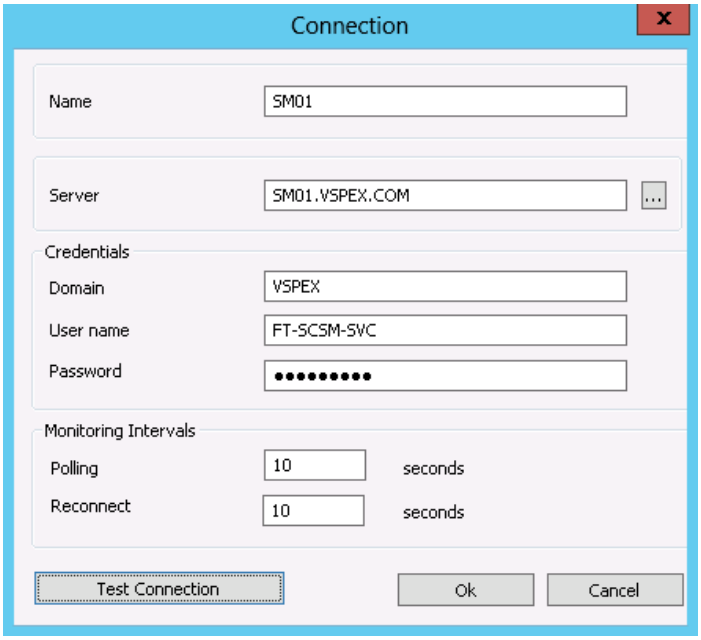
The **Completing the Integration Pack Deployment Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.	
During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.	 
From the **Start** screen, click the **Runbook Designer** tile.	

When complete, each integration pack will be displayed in the Runbook Designer interface.	
To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Virtual Machine Manager** option.	
In the Prerequisite Configuration dialog, click **Add.**	

In the **Add Configuration** dialog, fill in the required information for the Virtual Machine Manager server as shown and click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.	
While still in the Orchestrator Runbook Designer Console and go to the Options drop-down menu and select SC 2012 Operations Manager option.	
In the **Microsoft System Center Operations Manager Connections** dialog, click **Add**.	

In the **MS System Center Operations Manager Connection Settings** dialog, fill in the required information for the Operations Manager management server and click **Test Connection**[20]. Once connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes. Repeat these steps to create a secondary connection to the second Operations Manager VM.	
In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **SC 2012 Service Manager** option.	
In the **Connections** dialog, click **Add.**	

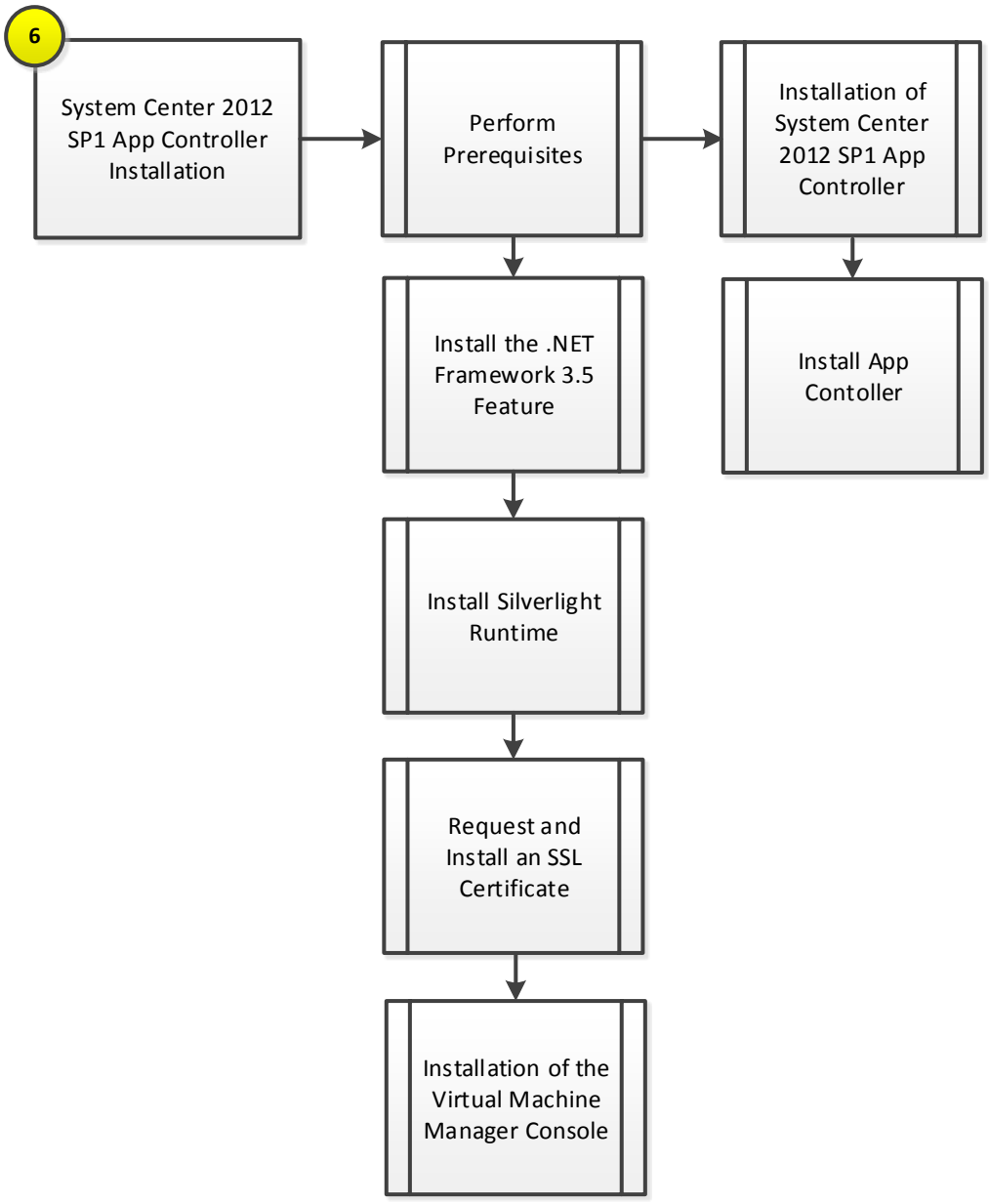
[20] The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

In the **Connection** dialog, fill in the required information for the Operations Manager management server[21] and click **Test Connection**. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes. Repeat these steps to create a secondary connection to the second Service Manager VM.	

13 System Center App Controller

The App Controller installation process is comprised of the following high-level steps:

[21] The use of the Administrator account is used as an example. Use account information that is applicable to your installation.



13.1 Overview

This section provides high-level walkthrough on how to setup App Controller. The following assumptions are made:

- A base virtual machine running Windows Server 2012 has been provisioned for App Controller.
- A SQL Server 2012 cluster with dedicated instance that has been established in previous steps for App Controller.
- The System Center Virtual Machine Manager console is installed
- The .NET Framework 3.5 Feature is installed.
- Microsoft Silverlight® Runtime is installed.

- A Trusted Server Authentication (SSL) Certificate (the CN field of the certificate must match server name) is installed.

13.2 Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created for App Controller:

Table 35 Prerequisite Accounts

User Name	Purpose	Permissions
<DOMAIN>\ FT-SCAC-SVC	App Controller Service Account	This account will need to be a member in the following groups: • FT-SCAC-Admins • FT-SCVMM-Admins

Groups

Verify that the following security groups have been created for App Controller:

Table 36 Prerequisite Security Groups

Group Name	Purpose	Members
<DOMAIN>\ FT-SCAC-Admins	App Controller Admin Group	<DOMAIN>\ FT-SCAC-Admins <DOMAIN>\ FT-SCVMM-Admins

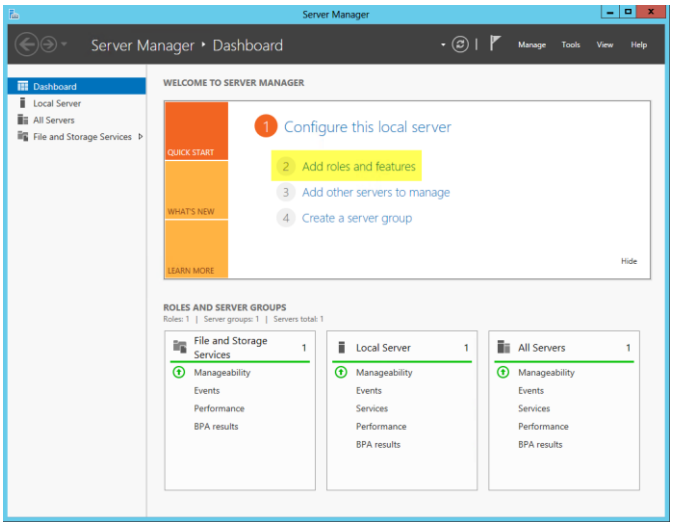
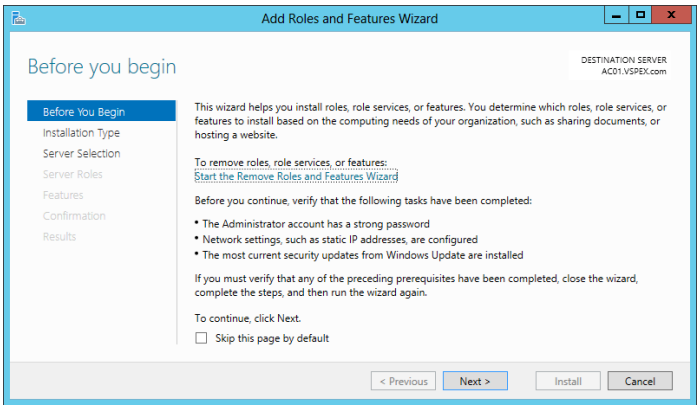
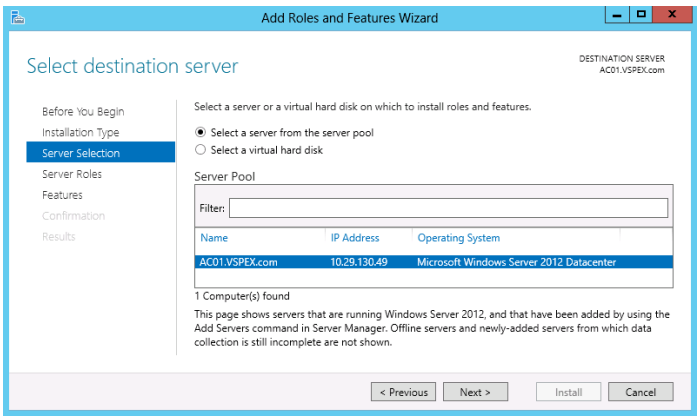
Required Networks

VMaccess

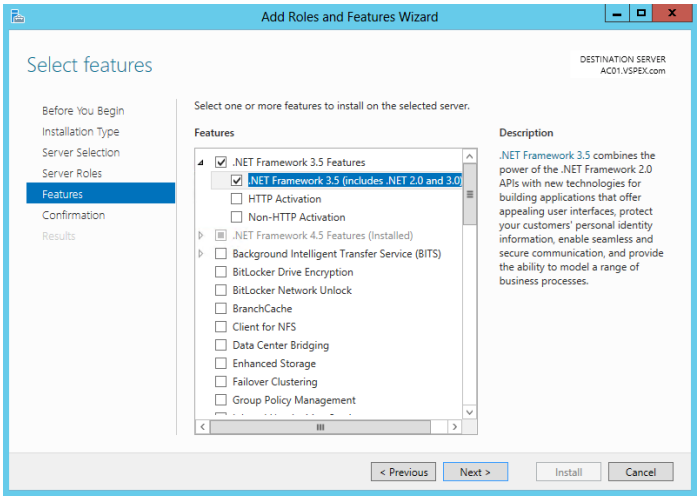
Add the .NET Framework 3.5 Feature

The Orchestrator installation requires the .NET Framework 3.5 Feature be enabled to support installation. If you did not include this in your sysprepped image, follow the provided steps to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on all **Operations Manager** virtual machines.

Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.	
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.	
In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next - for** this installation, click the **Features** menu option to continue.	

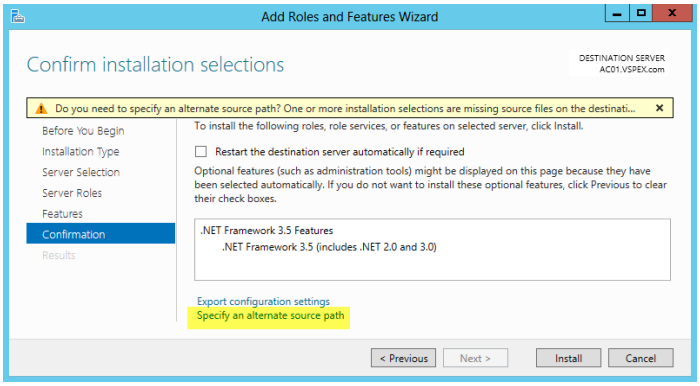
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear.
Click **Next** to continue.



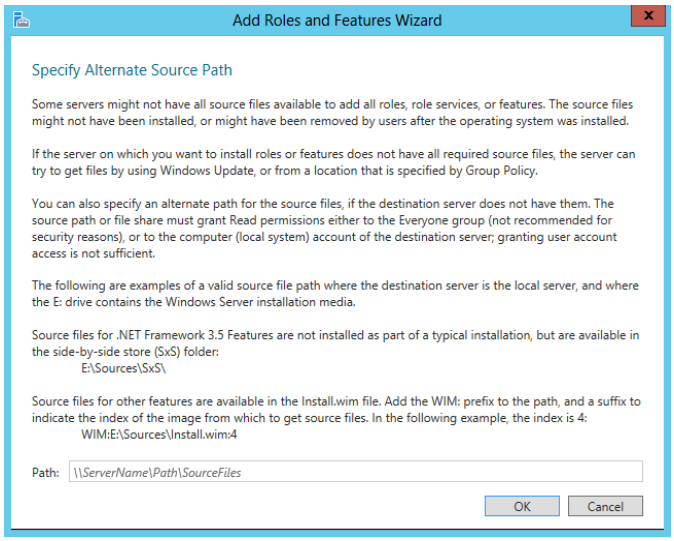
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected.
Click **Install** to begin installation.

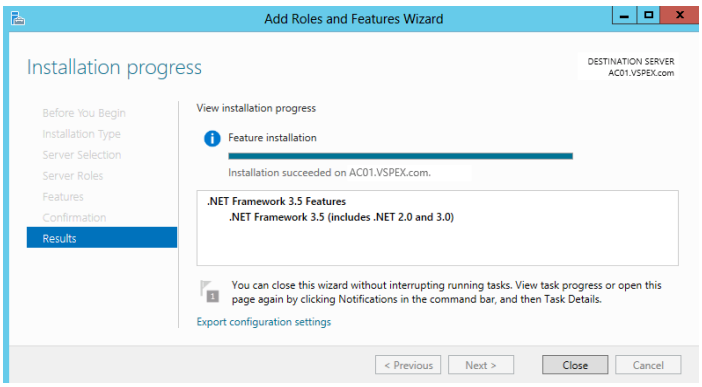
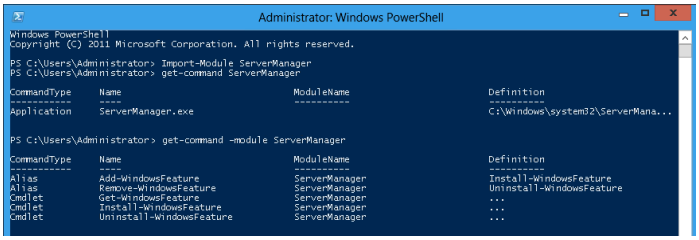
Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. Once exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.

Note: If the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.

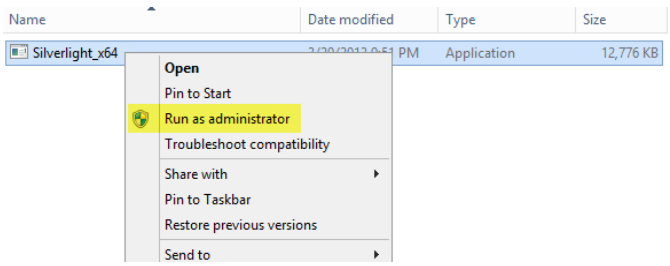


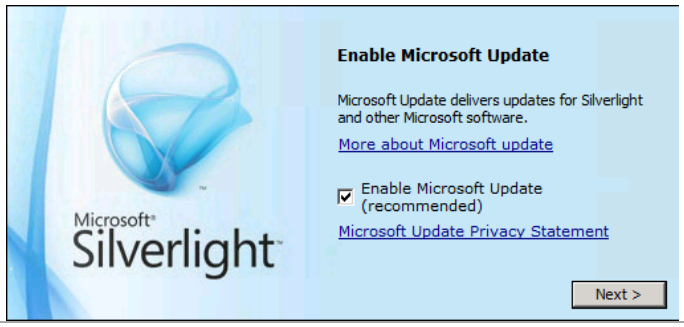
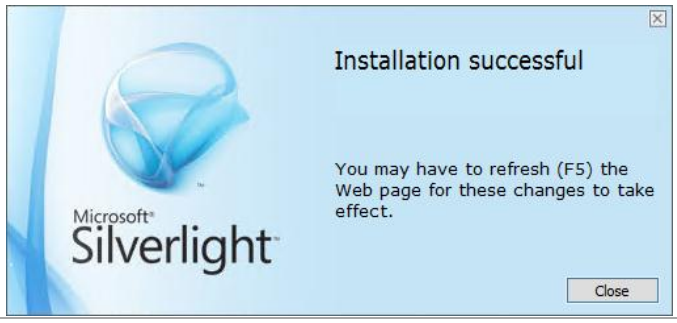
For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location can be specified for the installation.



The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.	
Note that while the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.	

Install Silverlight Runtime

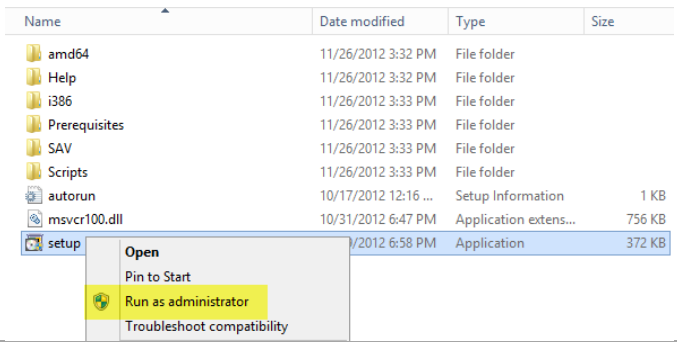
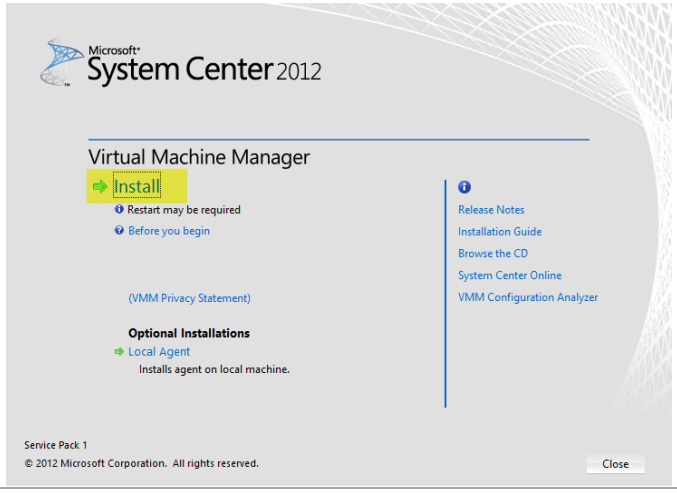
▶ Perform the following steps on the **App Controller** virtual machine.	
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.	
In the Install Silverlight dialog, click Install now.	

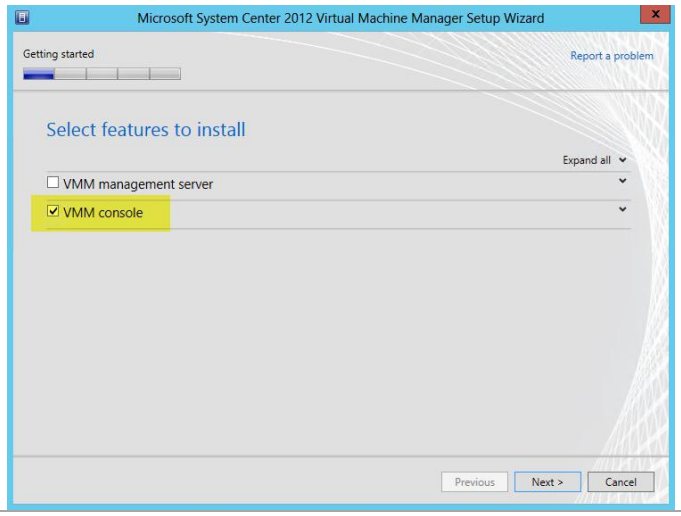
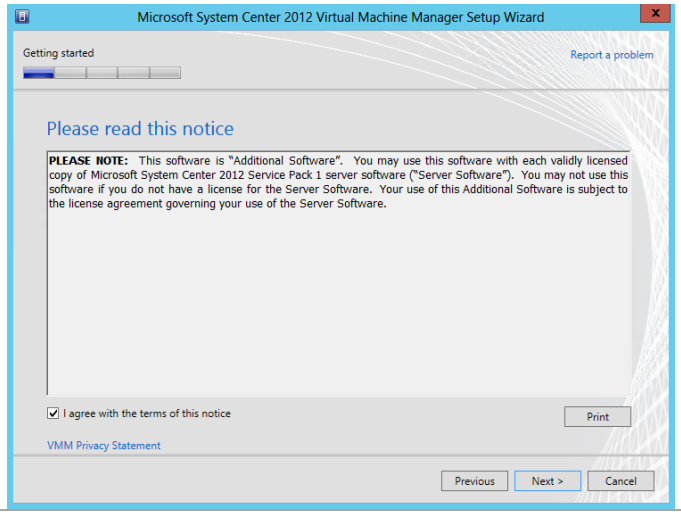
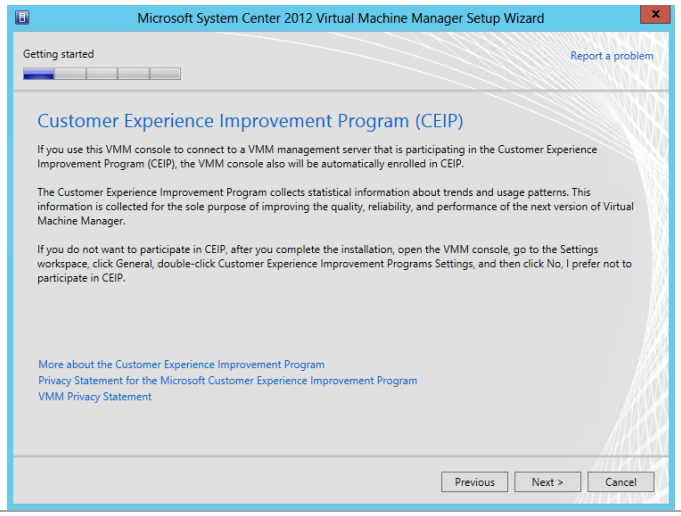
In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.	
In the **Installation Successful** dialog, click **Close** to exit the installation.	

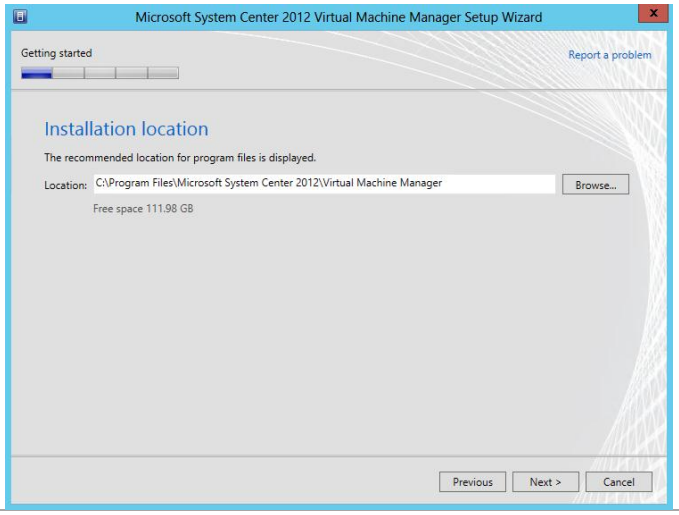
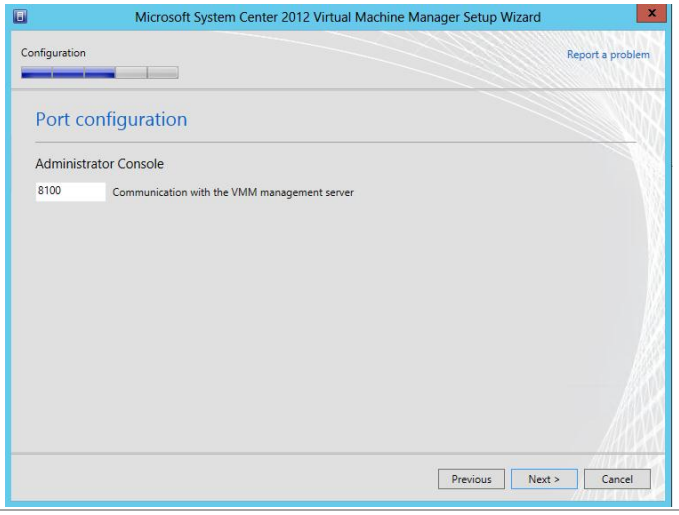
Install the Virtual Machine Manager Console

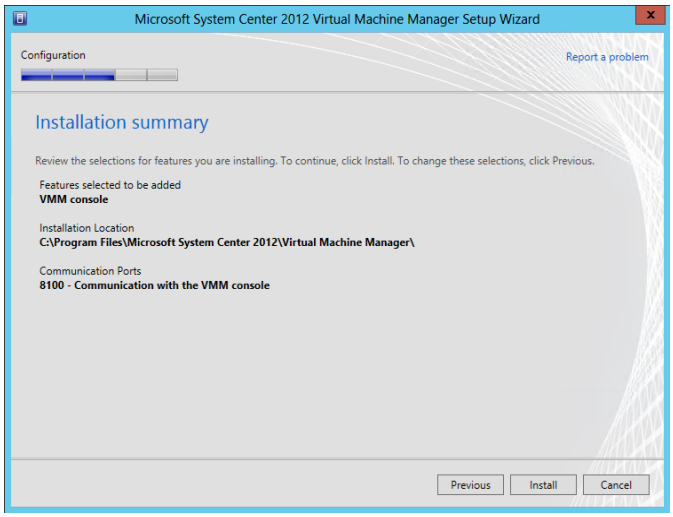
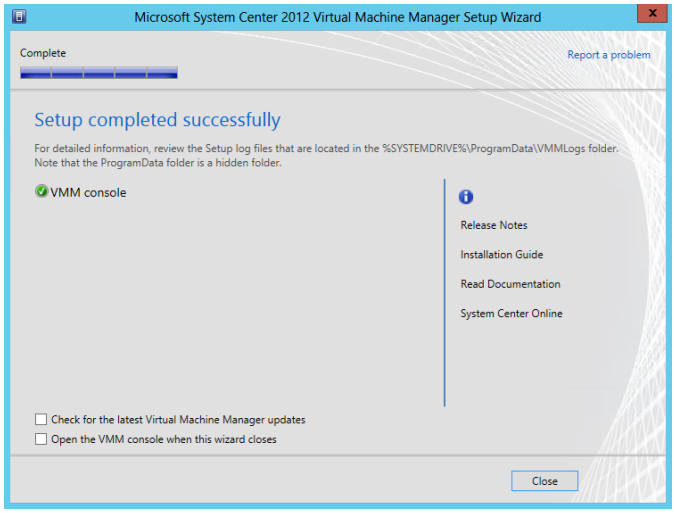
The following steps needs to be completed in order to install the Virtual Machine Manager console on the target App Controller virtual machine.

▶ Perform the following steps on the **App Controller** virtual machines.

Log on to the App Controller server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.	

In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.	
In the **Please read this license** agreement dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.	
In the Customer Experience Improvement Program dialog, click Next to continue.	

Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.	
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.	
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.	

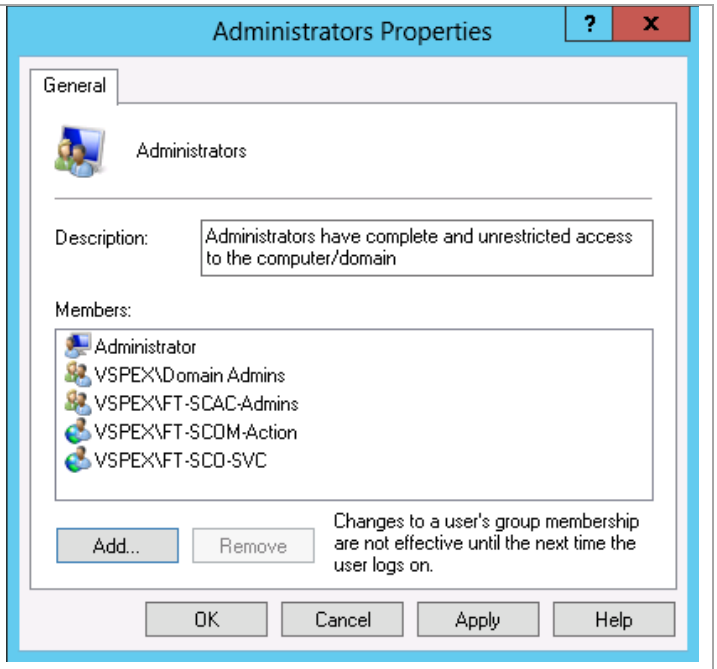
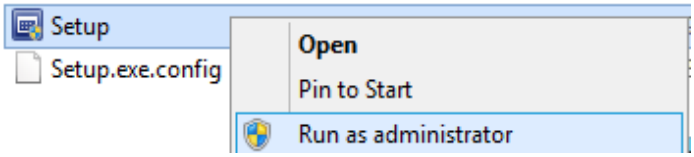
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

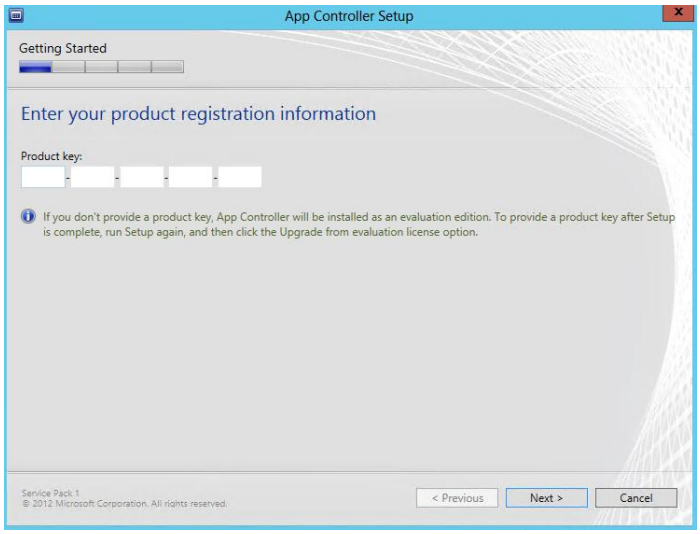
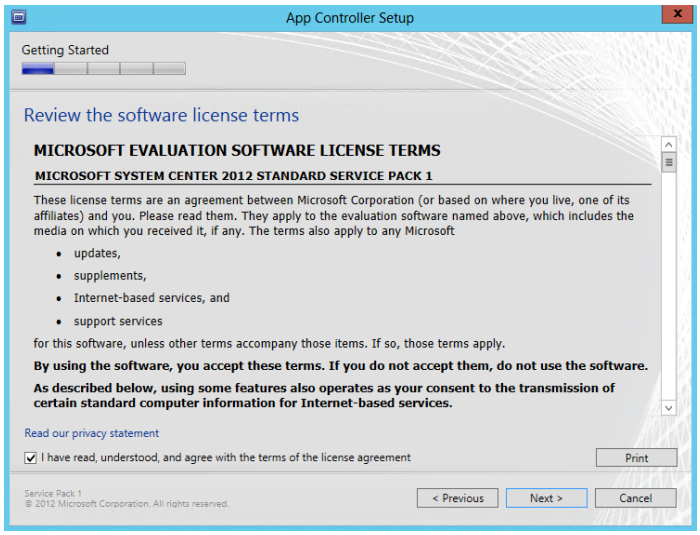
13.3 Installation

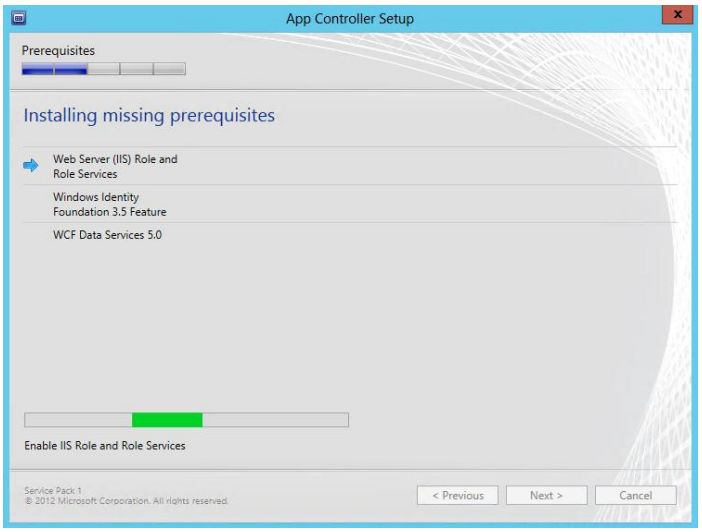
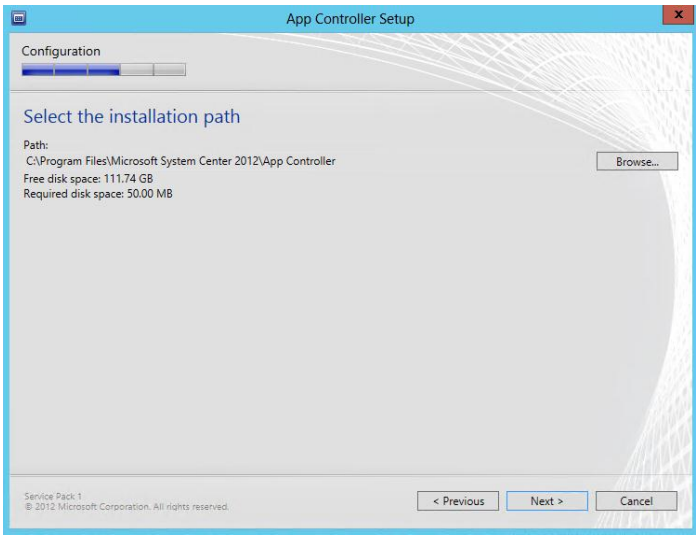
Install the App Controller Portal Server

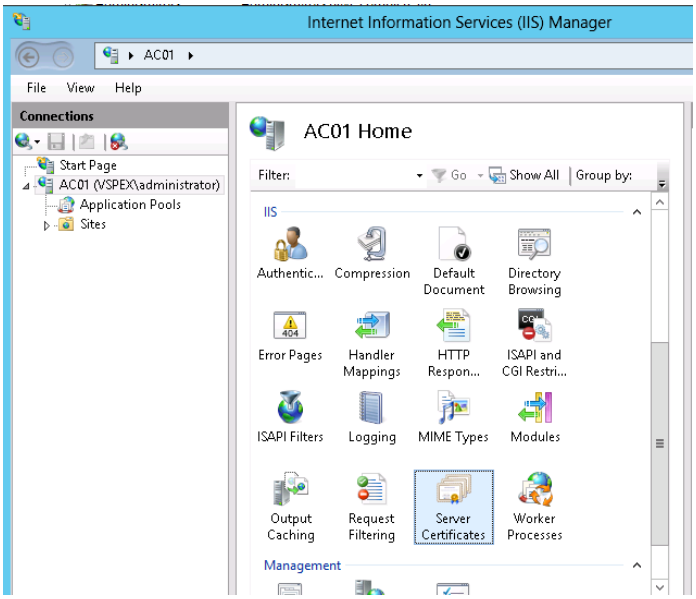
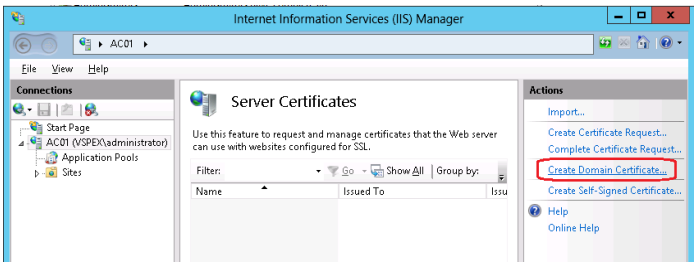
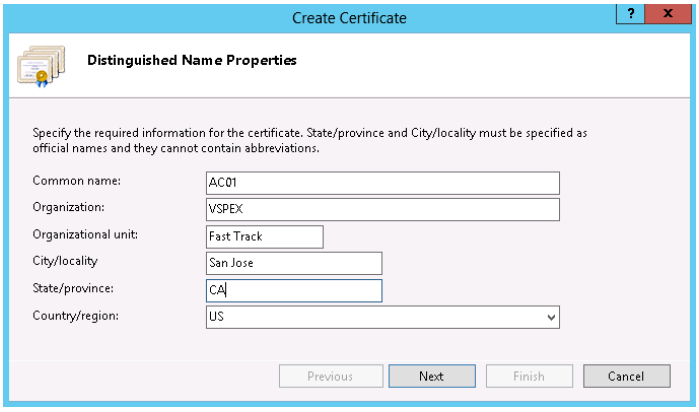
The following steps needs to be completed in order to install App Controller.

▶ Perform the following steps on the **App Controller** virtual machine.

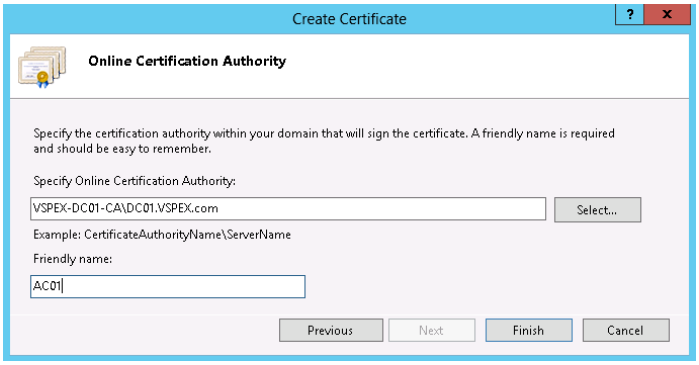
Log in to the App Controller virtual machine with a user with local admin rights. Verify the following accounts and/or groups are members of the Local Administrators group on the App Controller portal virtual machine: • Fast Track Operations Manager action account. • Fast Track App Controller service account. • Fast Track App Controller Admins group.	
Log on to System Center App controller server. From the **System Center App Controller** installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
The **App Controller Setup** wizard will begin. At the splash page, click **Install** begin the App Controller server installation.	

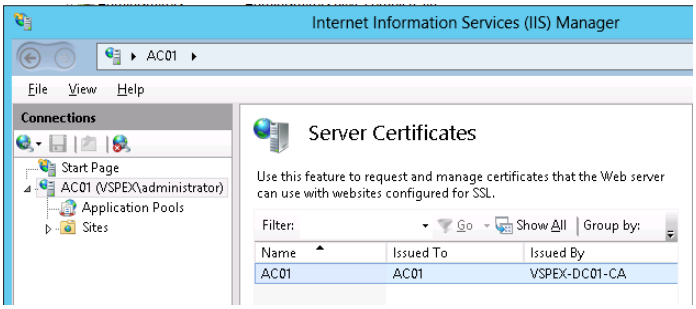
In the **Enter your product registration information** dialog, provide a valid product key for installation of Orchestrator. If no key is provided, App Controller will be installed in evaluation mode. Click **Next** to continue.	
In the **Review the software license terms** dialog, verify that the **I have read, understood and agree with the terms of this license agreement** installation option check box is selected and click **Next** to continue.	
In the **Install missing software** dialog, the wizard will detect missing roles and software and attempt installation of missing prerequisites. Click **Install** to enable missing roles and features.	

The wizard will detect missing roles and software and attempt installation of missing prerequisites. Please be patient during this process.	
In the **Select the installation path** dialog, accept the default installation location of *%ProgramFiles%\Microsoft System Center 2012\App Controller* or specify a different location by hitting the **Browse** button. After making a selection hit **Next** to continue.	
Before proceeding with the following steps, install a certificate on this system. Earlier, steps had been provided to request and install a certificate from a third party. Active Directory also has a Certificate Services component. If your organization has its own Certificate Authority and it is set up for auto-enrollment, these following steps can be followed. It happens at this point in time because IIS has now been installed on this system.	
From the Start menu, launch the **Internet Information Services Manager**.	

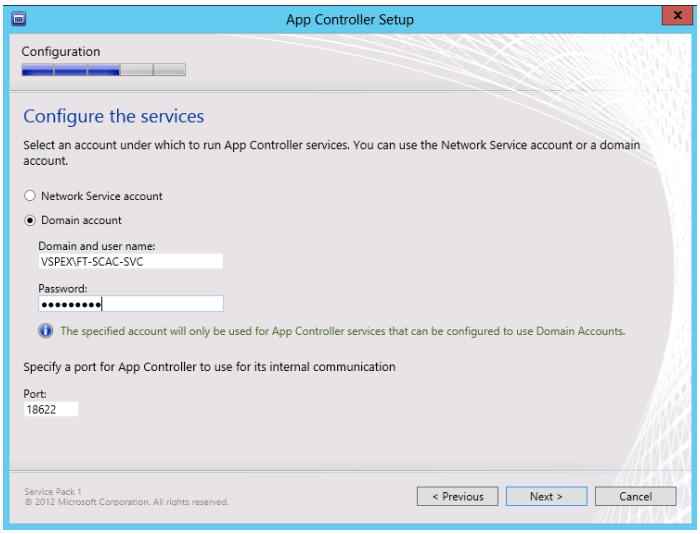
Click on the Application Controller home page in the Connections pane. From the IIS section in the middle, double-click **Server Certificates**.	
From the Actions pane, click on **Create Domain Certificate …**	
Fill in the contents of the Create Certificate window. Ensure that Common Name is the same as the name of the Applications Controller server. Click **Next** to continue.	

Click the **Select...** button to obtain a drop-down list of available certificate servers. Select the one appropriate to your environment.
Enter the name of the Application Controller server as the Friendly name.
Click **Finish** to install the certificate.
When the certificate has been installed, return to the installation of the Application Controller server software.





In the **Configure the services** dialog, verify that the **Domain account** option is selected and specify the App Controller service account in the **Domain and user name** text box. Provide the associated **Password** in the supplied text box.
In the **Port** text box, accept the default TCP port of 18622 or change the port to meet your organization's requirements. In most cases the default port selection should be kept.
When complete, click **Next** to continue.

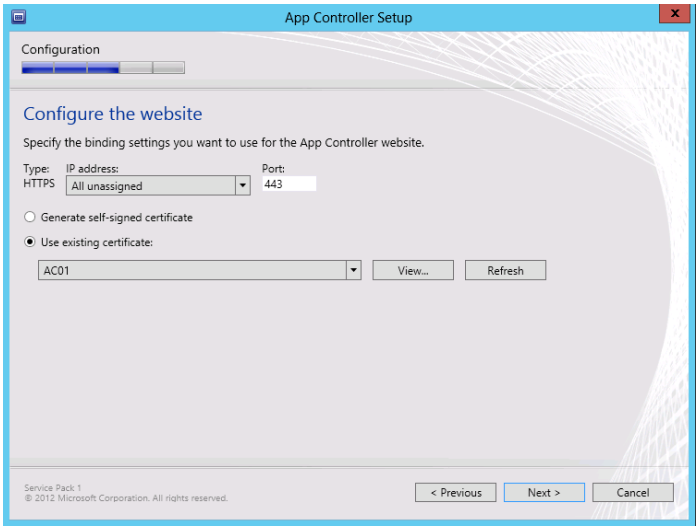


In the **Configure the website** dialog, provide the following information:

- Under Website, in **Type: HTTPS**, set the **IP address** drop-down menu to **All unassigned**. Set the **Port** value to **443**.
- Verify that the **Use existing certificate** option is selected and select the proper Server Authentication certificate that installed within the virtual machine from the drop-down menu.

When complete, click **Next** to continue.

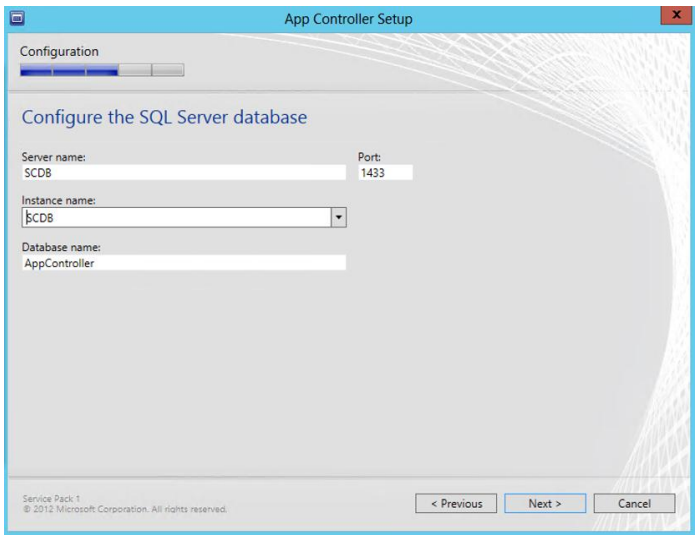
Note: While not recommended, if a Server Authentication certificate cannot be obtained and installed on the App Controller server, you may choose the **Generate self-signed certificate** option to satisfy installation requirements.

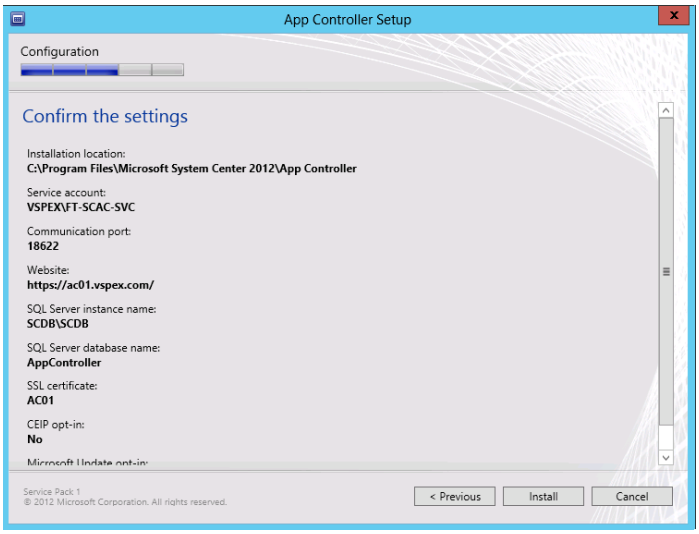
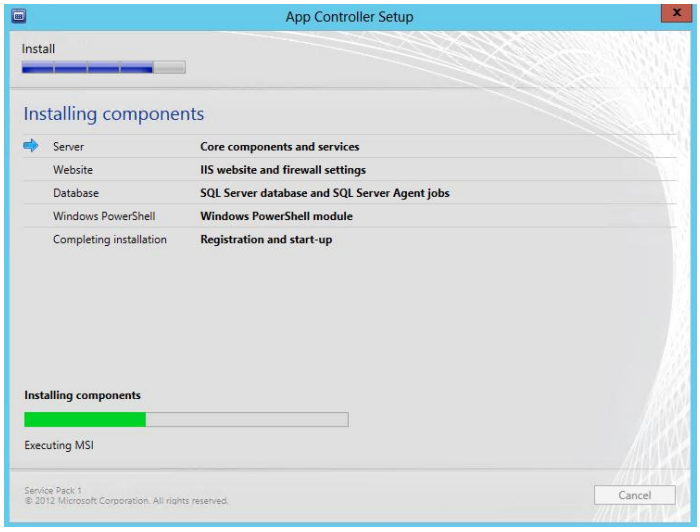


In the **Configure the SQL Server database** dialog, make the following selections install the App Controller database in the SCO instance (refer to the worksheet created earlier):

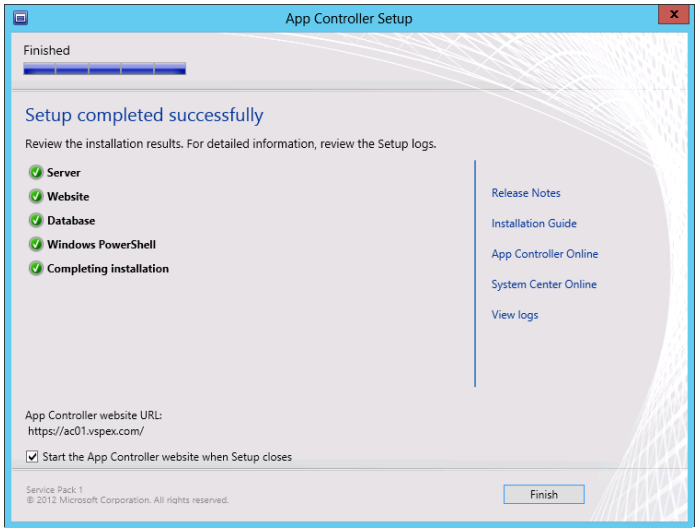
- **Server Name** – *specify the cluster network name of the SQL Server failover cluster hosting the instance.*
- **Port** – *specify the TCP port used for SQL Server connectivity. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack is deployed.*
- **Instance name** - *specify the instance name where the AppController database will be installed to (the SCDB instance).*
- **Database name** – *specify the name of the App Controller database. In most cases the default value of AppController should be used.*

Click **Next** to continue.

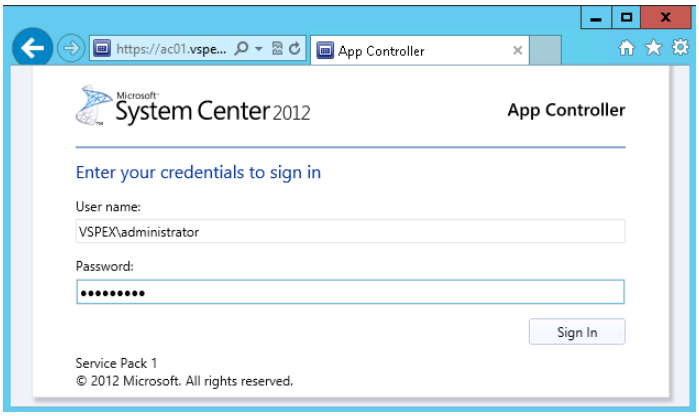


The **Help Improve App Controller for System Center 2012** dialog provides options for participating in various product feedback mechanisms. These include: • **Customer Experience Improvement Program (CEIP)** • **Microsoft Update** Select the appropriate option based on your organization's policies and click **Install** to continue.	
In the **Confirm the settings** dialog, verify the settings provided during the installation wizard and click **Install** to begin the installation.	
The required components will install and progress of the installation will be provided in the wizard.	

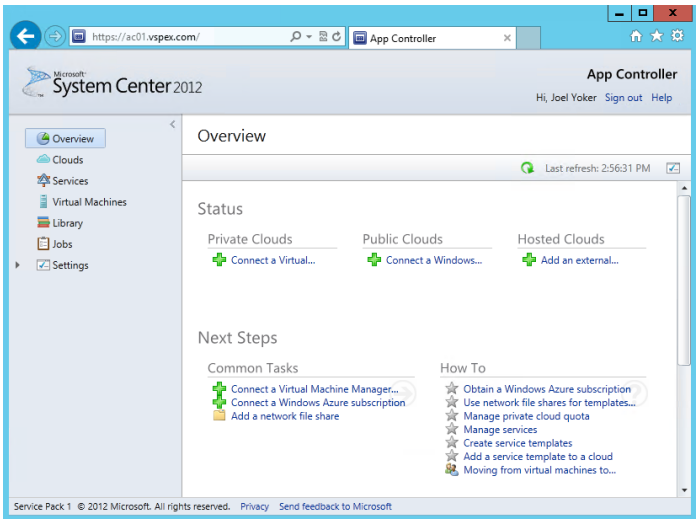
When complete, the **Setup completed successfully** dialog will appear with progress of each component. Verify that each component successfully. Note the App Controller website in the provided text box.
Verify that the **Start the App Controller website when Setup closes** check box is selected and click **Finish**.



The **System Center 2012 App Controller website** will launch. Because no users have been created in SCVMM, enter in the administrative account used to install Virtual Machine Manager (which has been assigned an admin role in SCVMM). Once complete, click **Sign in**.

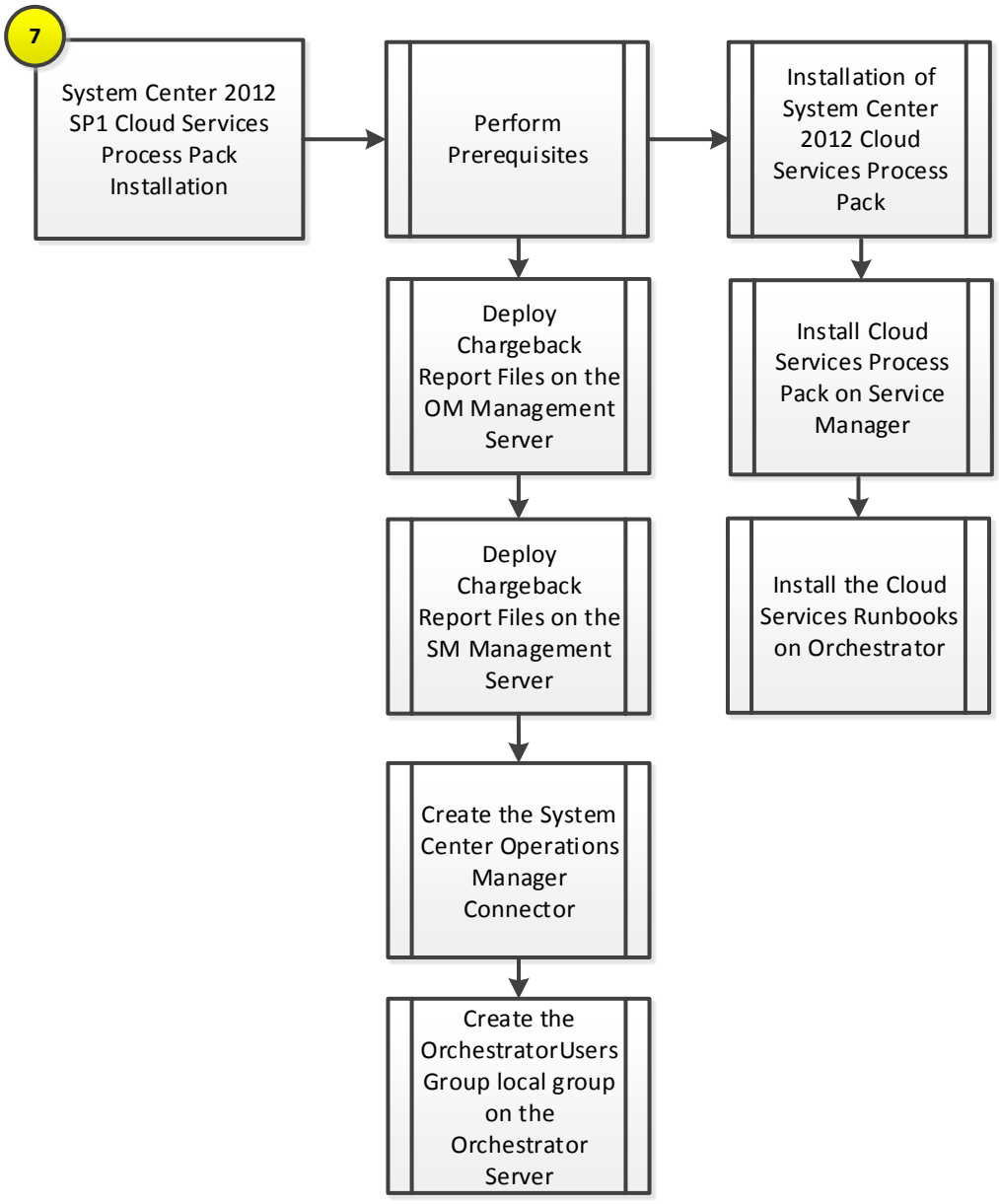


The App Controller portal will appear. After validating functionality, the App Controller installation is considered complete.



14 System Center Cloud Services Process Pack

The Cloud Services Process Pack installation process includes the following high-level steps:



14.1 Overview

This section provides the setup procedure for the Cloud Services Process Pack into the Fast Track fabric management architecture. The following assumptions are made:

- The system center integration pack for System Center 2012 – Service Manager needs to be imported into Orchestrator per previous steps.
- Operations Manager integration with Virtual Machine Manager should already be complete per previous steps.

System Center Cloud Services Process Pack is available at http://www.microsoft.com/en-us/download/details.aspx?id=36497. IT organizations considering IaaS will need to examine and adapt their existing tools, processes, workflows, and automation to meet the requirements of an effective cloud services implementation. While it is critical that the underlying components (such as self-service portal, ticketing infrastructure, notifications, workflows, and automation) integrate well

with each other and account for industry-wide recommended practices, the work involved to implement an effective cloud service can be daunting and time consuming.

System Center Cloud Services Process Pack addresses these concerns by enabling IaaS while incorporating domain expertise and recommended practices from enterprises that have successfully deployed IaaS. These recommended practices are made available out-of-the box and are evident in all aspects of the Solution.

The potential benefits offered by System Center Cloud Services Process Pack for the enterprise include:

- Deep customization and extension of the cloud services experience that is natively supported by the System Center suite of products.
- Reduced cost, effort, and time to deploy cloud services to organizations that already utilizes the System Center platform.

The potential benefits offered by System Center Cloud Services Process Pack for consumers of IT within the enterprise include:

- Standardized and well-defined processes for requesting and managing cloud services, including the ability to define projects, capacity pools, and virtual machines.
- Natively supported request, approval, and notification to help enable businesses to effectively manage their own allocated infrastructure capacity pools.

The System Center Cloud Services Process Pack offers a self-service experience to facilitate private cloud capacity requests from your business unit IT application owners and end users, including the flexibility to request additional capacity as business demands increase.

14.2 Prerequisites

The following environment prerequisites must be met before proceeding.

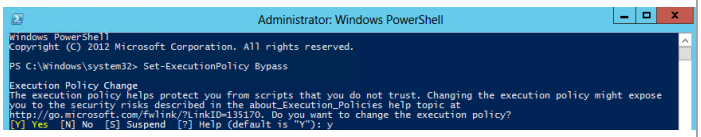
Deploy Chargeback Report Files on the Operations Manager Management Server

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

From an elevated PowerShell prompt, configure the execution policy to Bypass.

```
Set-ExecutionPolicy Bypass
```

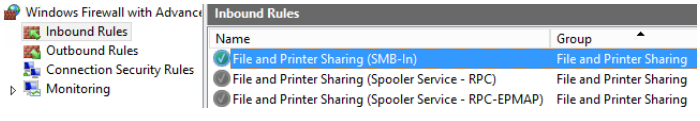
Note: When installation is complete, execution policy should be configured to a more secure level within the organization.

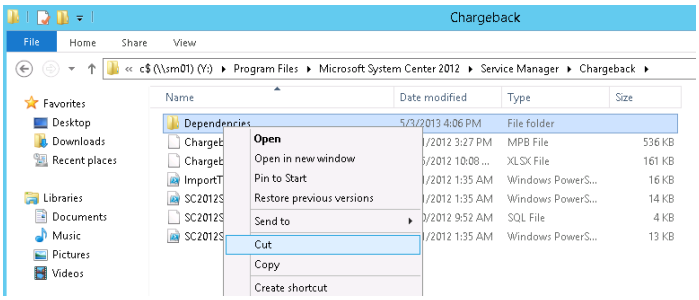
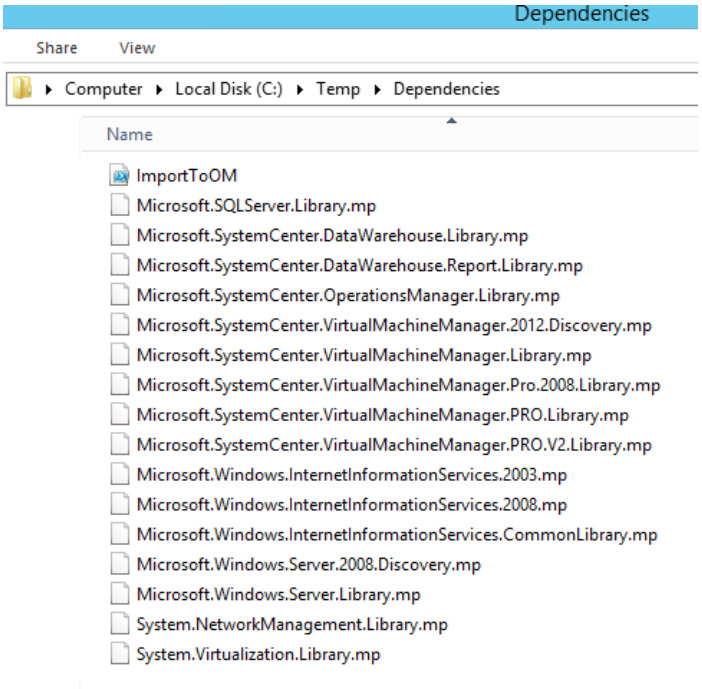
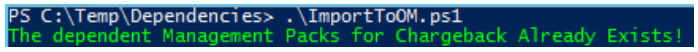


Open the **Windows Firewall with Advanced Security MMC** console.

Within the **Windows Firewall with Advanced Security MMC** console, select the **Inbound Rules** node and enable the **File and Printer Sharing (SMB-In)** rule from the action pane.

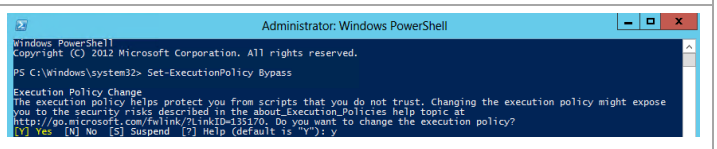


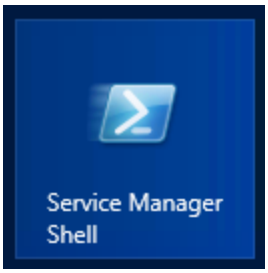
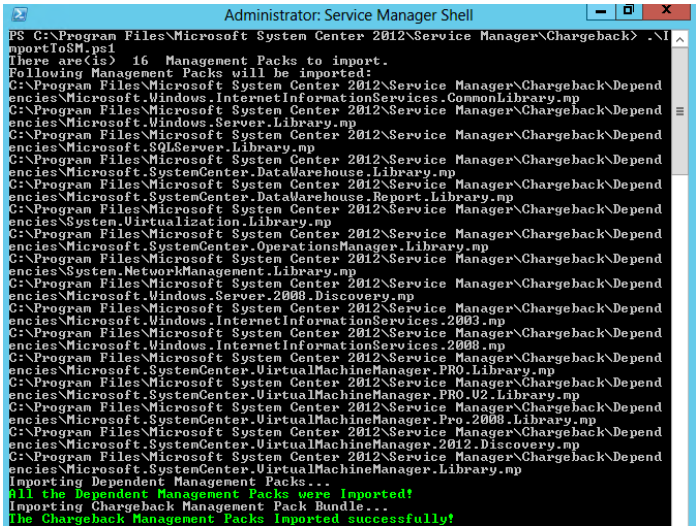


Connect to the administrative share where %ProgramFiles% resides on the Service Manager management server. Copy the **Dependencies** folder from the %ProgramFiles%\Microsoft System Center 2012\Service Manager installation folder on the remote Service Manager management server.	
Copy the **Dependencies** folder to a temporary directory on the Operations Manager management server.	
From the same elevated PowerShell session, navigate to the **Dependencies** folder which was copied locally and execute the ImportToOM.ps1 PowerShell script. In some cases the dependent management packs will already be deployed.	

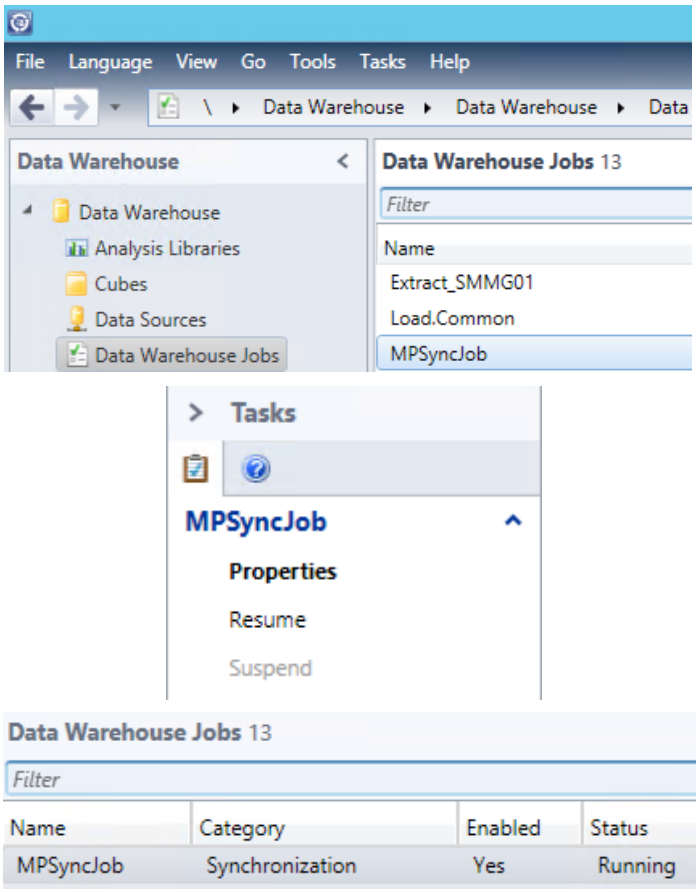
Deploy Chargeback Report Files on the Service Manager Management Server

▶ Perform the following steps on the **Service Manager management server** virtual machine.

From an elevated PowerShell prompt, configure the execution policy to Bypass. `Set-ExecutionPolicy Bypass` **Note:** When installation is complete, execution policy should be configured to a more secure level within the organization.	

From the **Start** screen, select the **Service Manager Shell** tile and run this as an administrator.	
In the elevated **Service Manager Shell** dialog, navigate to %ProgramFiles%\Microsoft System Center 2012\Service Manager\Chargeback and execute the **ImportToSM.ps1** script. Once completed, close the console.	

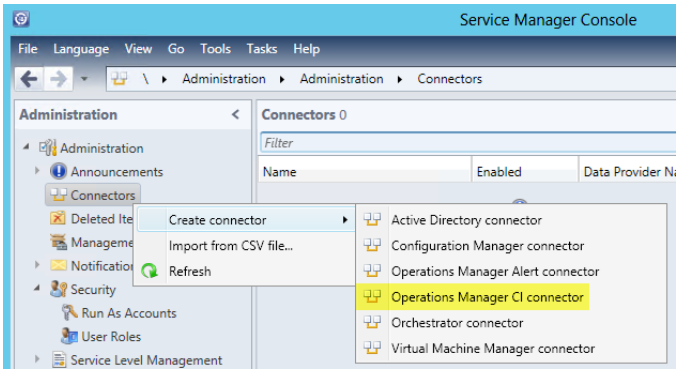
Within the **Service Manager console**, navigate to the **Data Warehouse Jobs** node and select the **MPSyncJob** data warehouse job. In the **Tasks** pane, select **Resume** to begin the synchronization task.

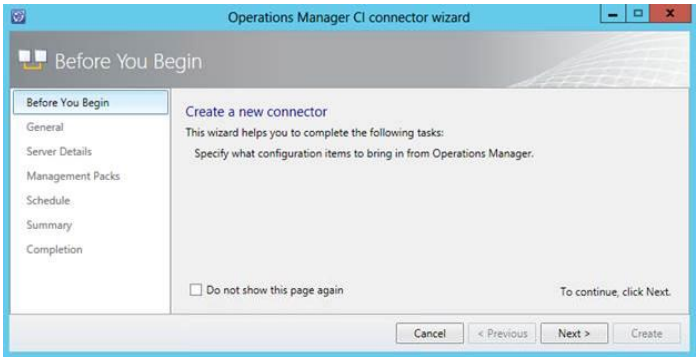
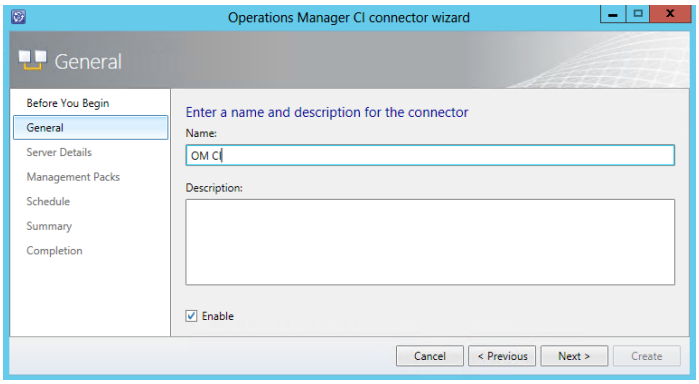
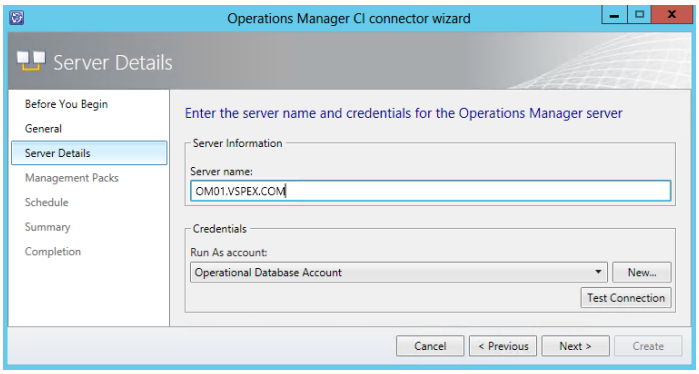


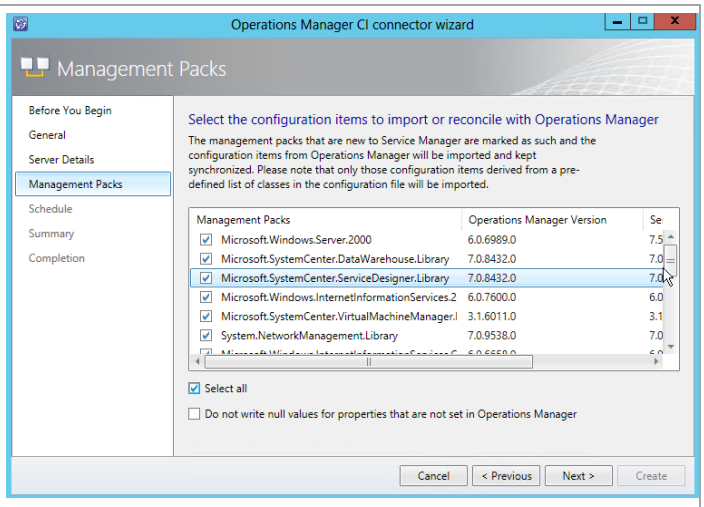
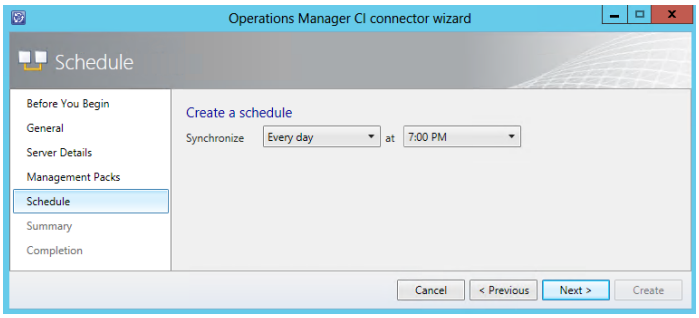
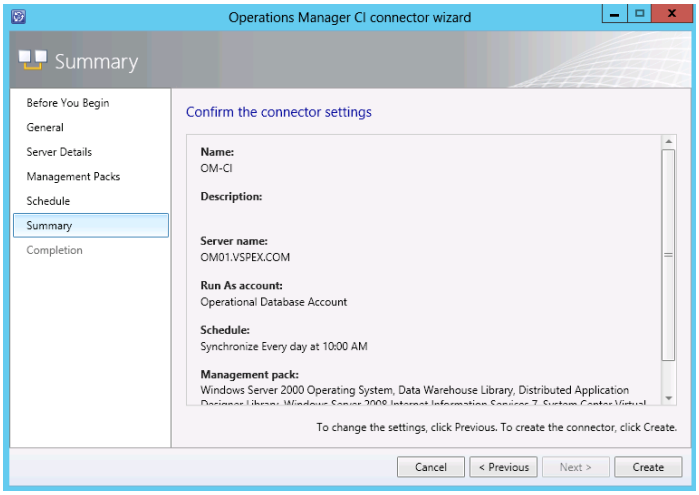
Create the System Center Operations Manager Connector

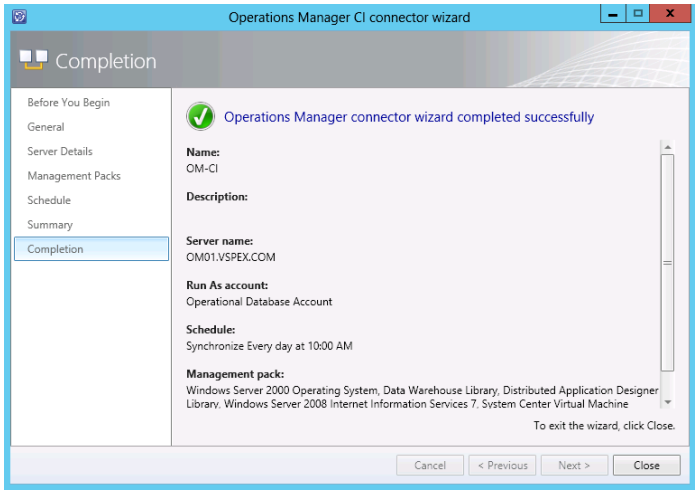
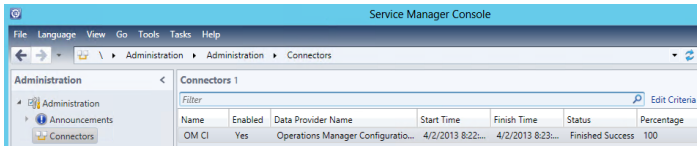
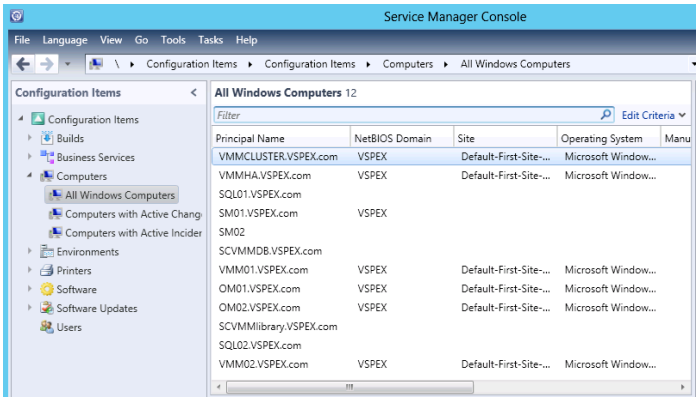
▶ Perform the following steps on the **Service Manager management server** virtual machine.

Open the **Service Manager Console**, select **Administration** from the navigation tree and navigate to the **Cloud Services** node.
In the Getting Started pane, click **Create an Operations Manager Connector**.



In the **Before you Begin** dialog, click **Next** to continue.	
The **Operations Manager CI connector** wizard will appear. In the **General** dialog, type a descriptive name for the connector in the **Name** textbox. Verify the **Enable** checkbox is selected. Click **Next** to continue.	
In the **Server Details** dialog, type the FQDN of the Operations Manager server in the **Server Name** textbox. In the **Credentials** section, click the **New…** button and create a Run As account using the **FT-SCOM-SVC** account. Click **Next** to continue.	

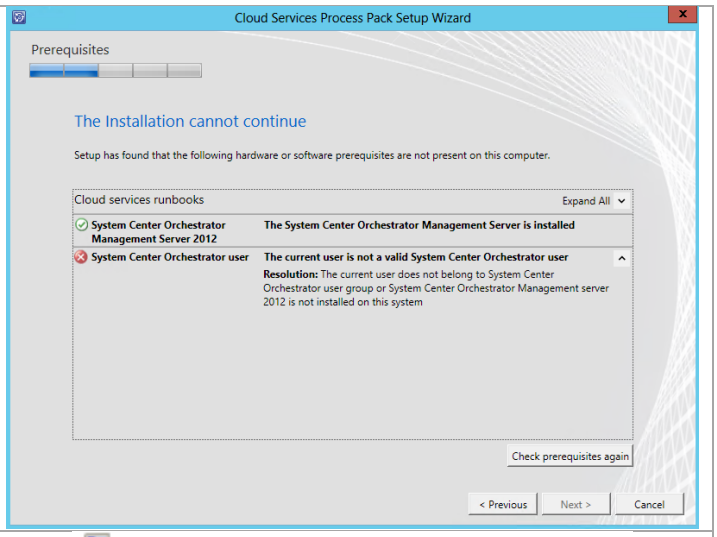
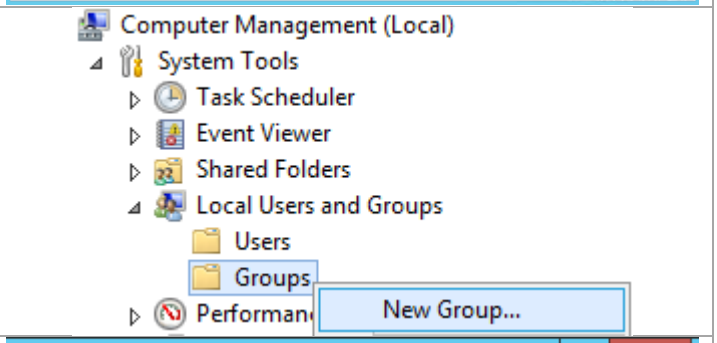
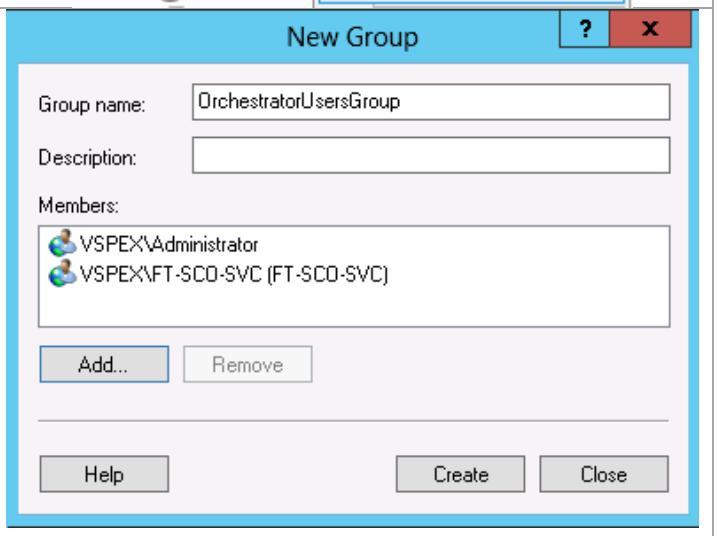
In the **Management Packs** dialog, select the **Select All** checkbox. Click **Next** to continue.	
In the **Schedule** dialog, create a schedule for the connector or leave the defaults. Click **Next** to continue.	
In the **Summary** dialog, verify the selections made and click **Create** to create the connector.	

In the **Completion** dialog, verify the process completes successfully and click **Close**.	
When created, verify the Connector has a successful run by checking that there is a time listed in the **Finish Time** column.	
In the **Service Manager console**, select the **Configuration Items** pane and navigate to the **All Windows Computers** node. Ensure that the configuration items have synchronized from the Operations Manager connector.	

Create the OrchestratorUsersGroup local group on the Orchestrator Server

Perform the following steps to avoid issues related to CSPP setup on Orchestrator.

▶ Perform the following steps on both **Orchestrator** virtual machines.

The pre-requisite checker in CSPP validates settings in Orchestrator, but during its process it verifies if the logged in user is directly a member of a local security group called "**OrchestratorUsersGroup**", regardless of how security for Orchestrator is configured. Per the recommended configuration this group was changed to a domain group, however a local group must be created with membership granted to the installation account to complete setup[22].	
To satisfy this requirement, a local group must be created on the Orchestrator servers where the runbooks will be installed. In Server Manager, navigate to the **Local Users and Groups** node, right-click **Groups** and select **New Group…** from the context menu.	
In the **New Group** dialog, provide the **Group name** of **OrchestratorUsersGroup** and ensure that the membership contains the account you are using to perform this installation. Click **Create** to complete the creation of the local group.	

14.3 Installation

Install the Cloud Services Process Pack

The following steps need to be completed in order to install the cloud Services Process Pack.

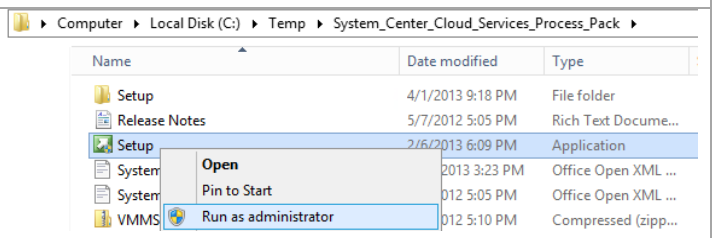
22 http://blogs.technet.com/b/orchestrator/archive/2012/05/10/faq-cloud-service-mp-pre-req-error-the-current-user-is-not-a-valid-system-center-orchestrator-user.aspx

▶ Perform the following steps on the **Service Manager management server** virtual machine.

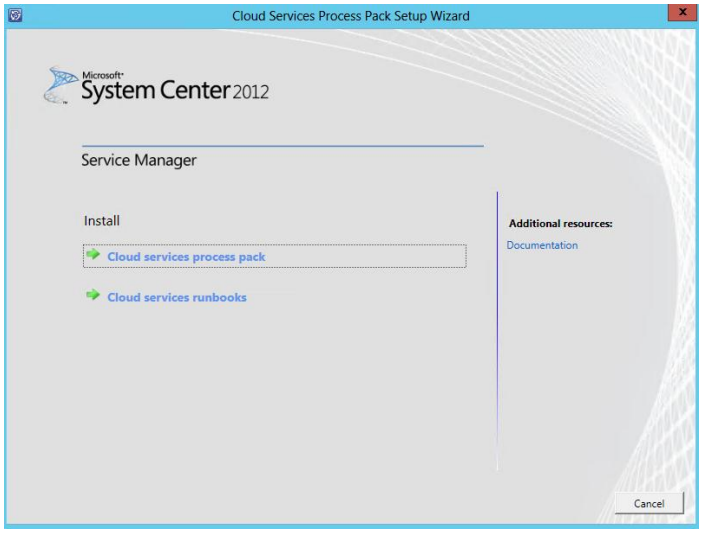
Log on to the Service Manager management server virtual machine with a user with local admin rights.
Verify the account has the following rights:

- A Service Manager administrator.
- An administrator on the server that is running Service Manager.

After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and run **Setup.exe** as an Administrator.



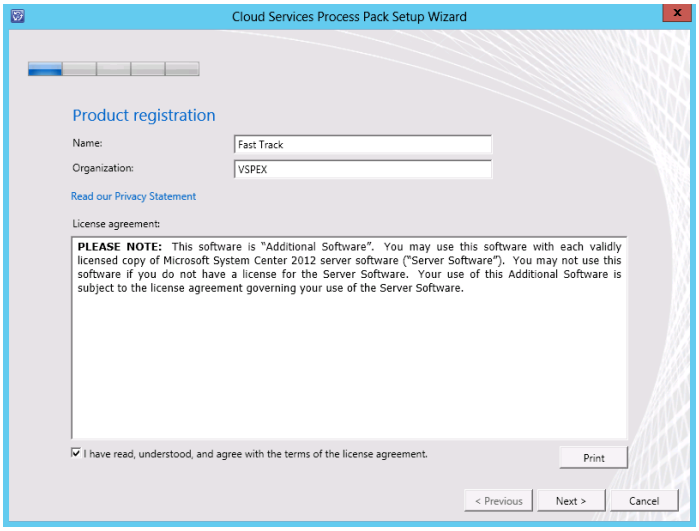
The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud services process pack.

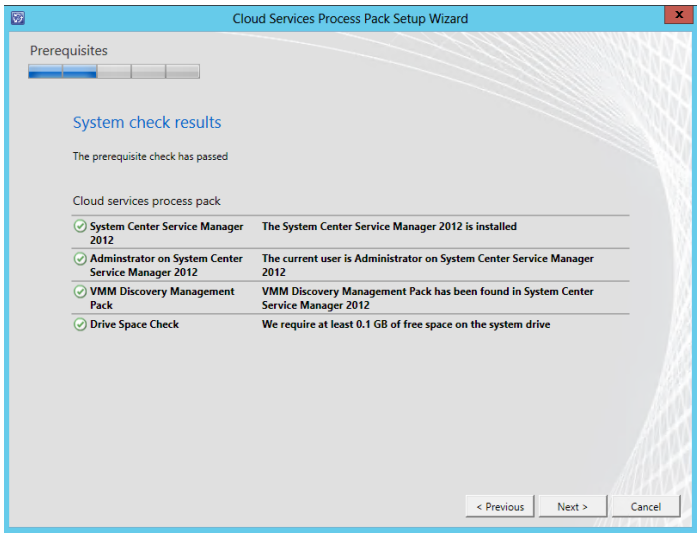
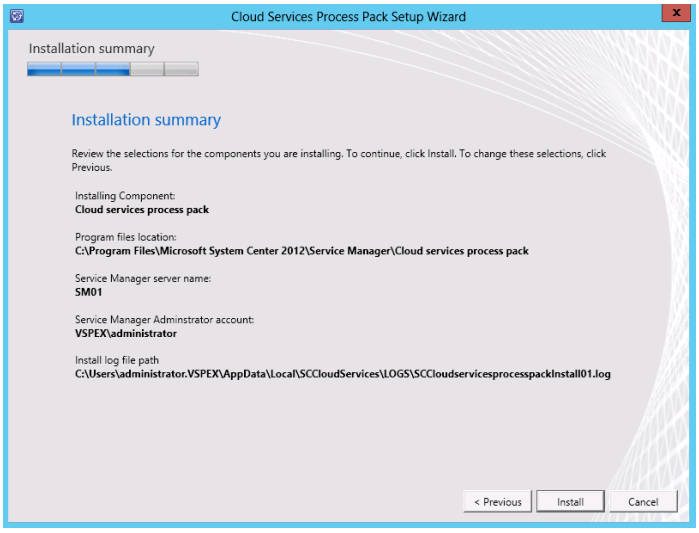
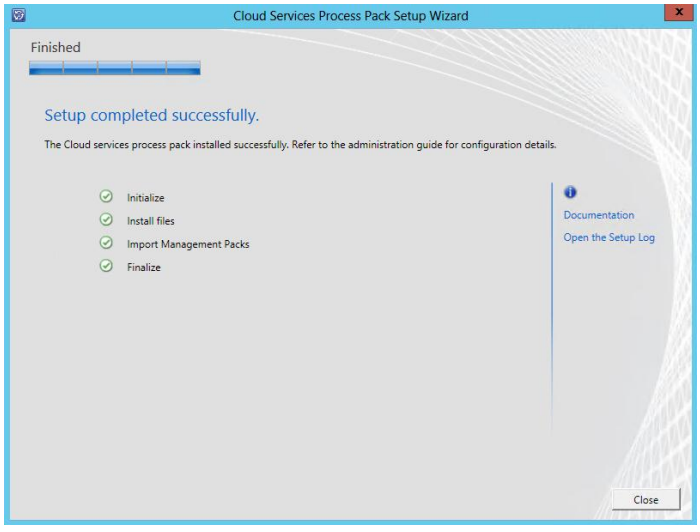


In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** - *specify the name of the licensed organization*.

Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

Install the Cloud Services Process Pack Runbooks

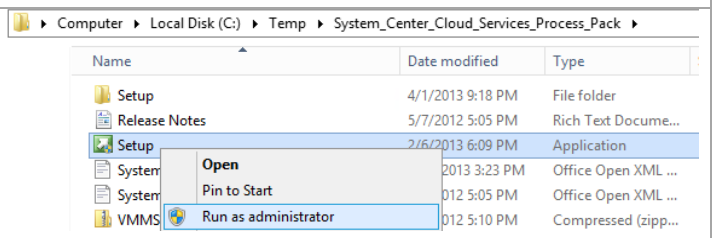
The following steps needs to be completed in order to install the Cloud Services Process Pack Orchestrator runbooks.

▶ Perform the following steps on the **Orchestrator** virtual machine.

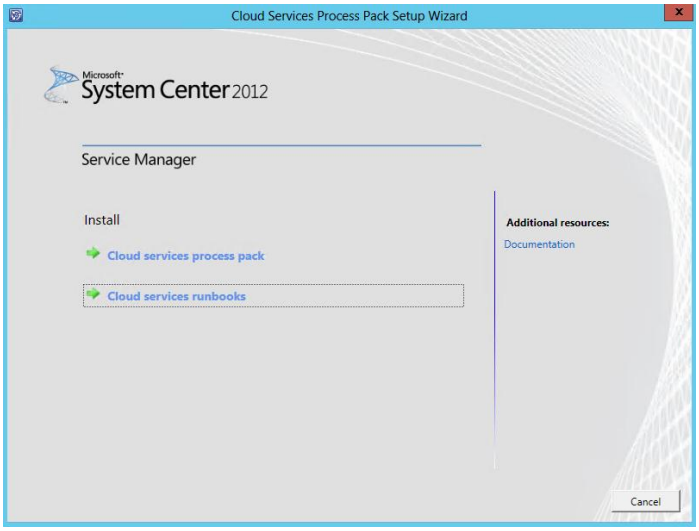
Log on to the Orchestrator management server virtual machine with a user with local admin rights.
Verify the account has the following rights:

- An administrator on the machine on which the program is installed as well as an Orchestrator administrator.
- An administrator in the Orchestrator database.
- An administrator on each SQL Server cluster node.
- An administrator on VMM.
- A member of the local OrchestratorUsersGroup created in earlier steps.

After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and click **Setup.exe** as an Administrator.



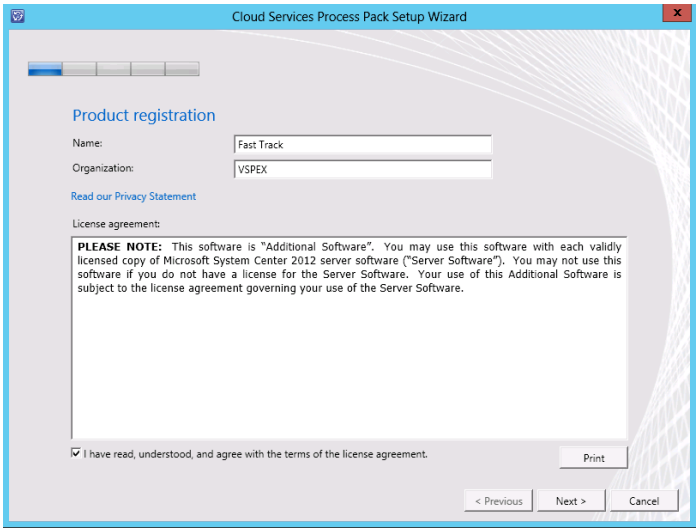
The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud services process pack.



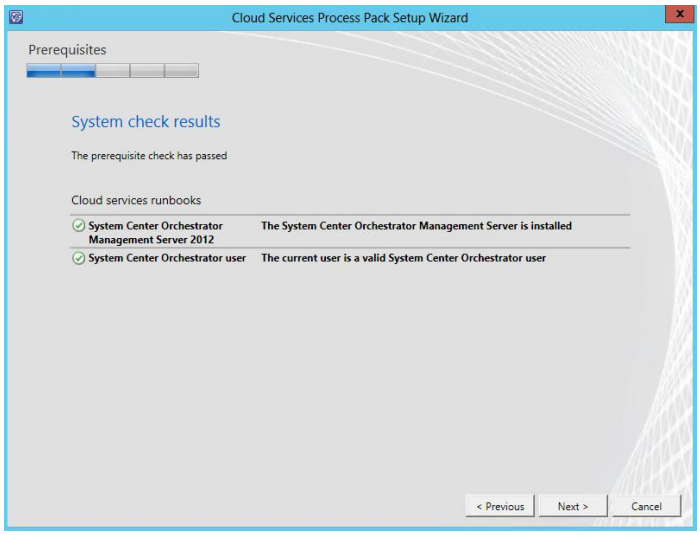
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization*.
- **Organization** - *specify the name of the licensed organization*.

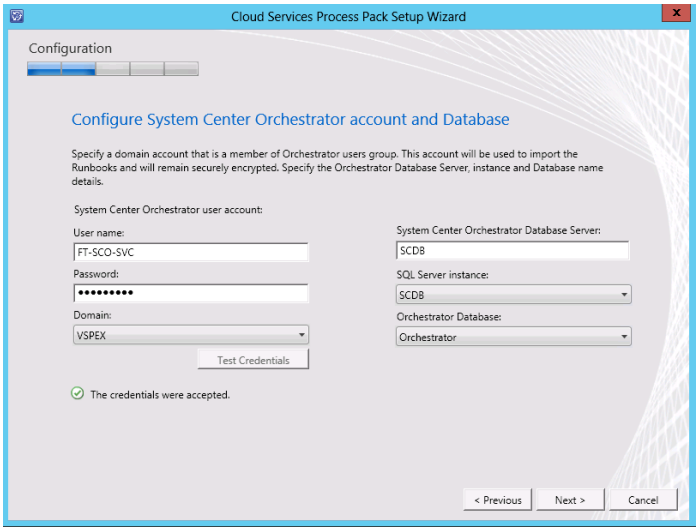
Click **Next** to continue.

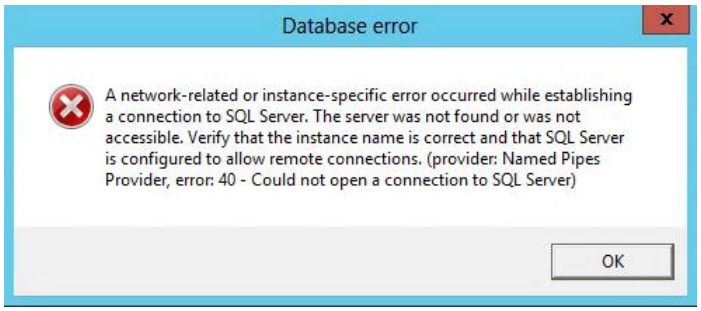
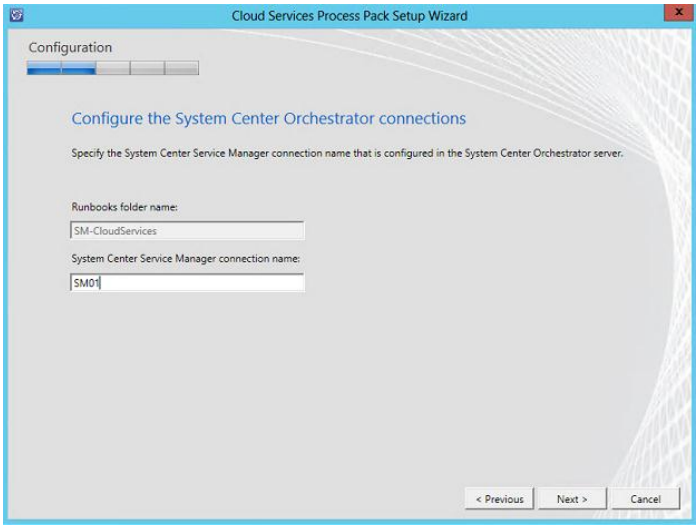
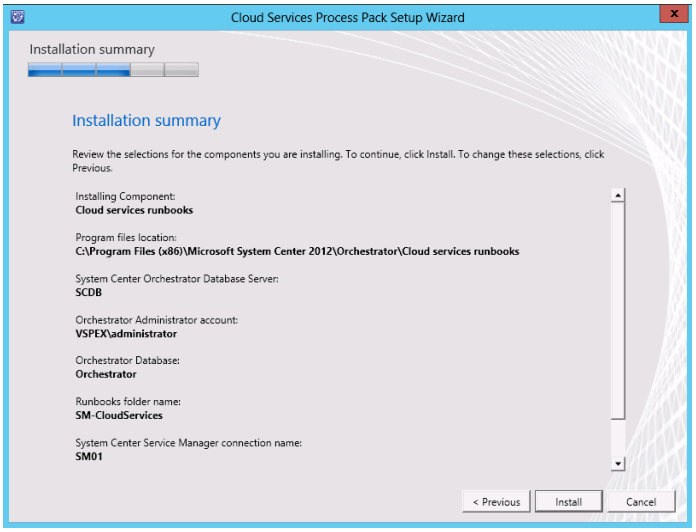


The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog.
When verified, click **Next** to continue.

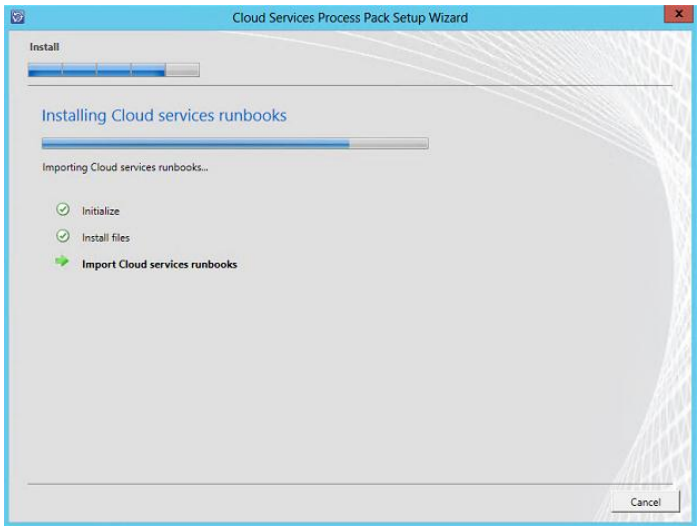


In the **Configure System Center Orchestrator account and Database** dialog, specify the Orchestrator service account in the dialog and click **Test Credentials**. Specify the Orchestrator database server name, the instance and database. When selected, click **Next** to continue.



Note: If the SCDB instance is not configured to use port 1433, the following error will appear when attempting to enumerate the Orchestrator database from the SQL named instance. Setup will not continue if this is the case.	
In the **Configure the System Center Orchestrator connections** dialog, specify the name of the Service Manager Orchestrator connector name created in the Orchestrator post-installation steps earlier. Click **Next** to continue.	
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation



15 Cisco Integration Components

Cisco has created several integration components to assist organizations in running the Microsoft Private Cloud on Cisco UCS environments.

- PowerTool
- Operations Manager Management Pack
- Orchestrator Integration Pack
- Virtual Machine Manager User Interface Extension
- Cisco Nexus 1000V

Check the Software Revision table (Table 2) for the location from which these components can be downloaded.

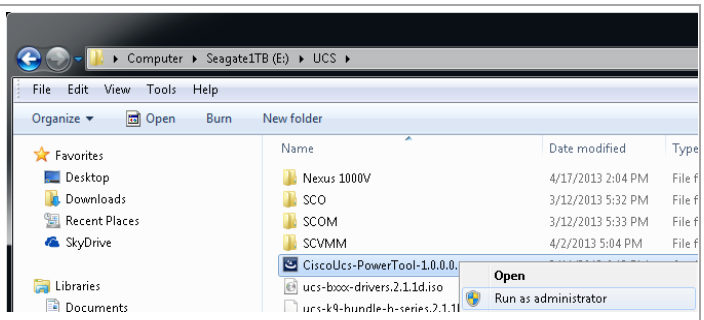
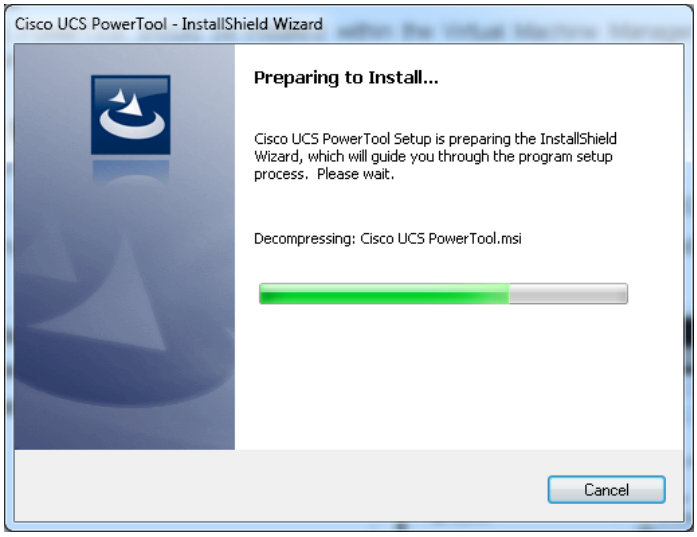
15.1 Cisco UCS PowerTool

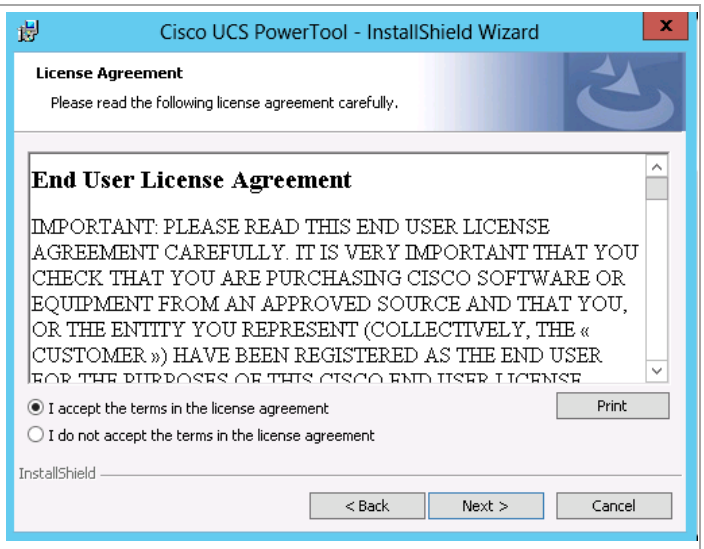
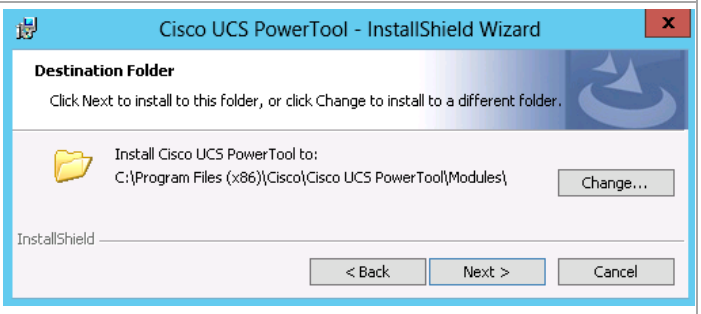
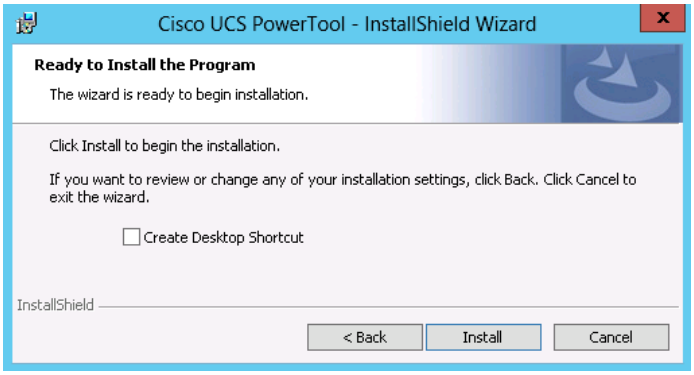
The Cisco UCS PowerTool should be installed within the Virtual Machine Manager and must be installed on the Orchestrator runbook servers.

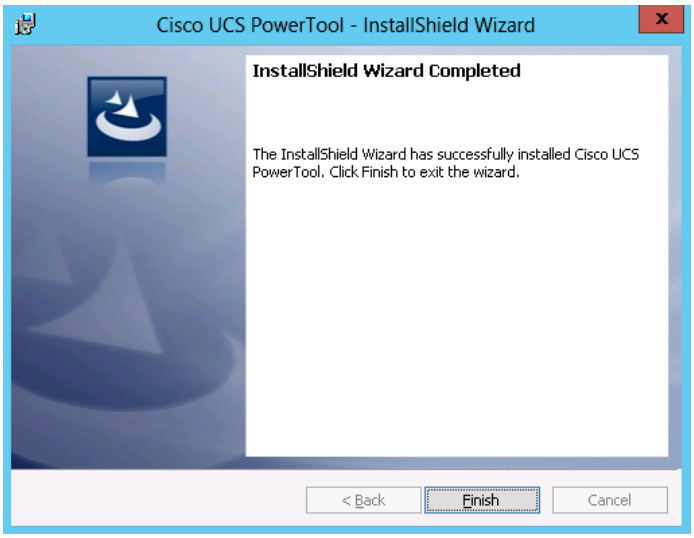
Before You Begin

- Ensure you have PowerShell v2.0 or above installed in your system (Windows Server 2012 and Windows 8 have PowerShell v3.0).
- Uninstall all versions of Cisco UCS Power Tool that are older than Cisco UCS PowerTool, Release 0.9.1.0.
- Close any instances of PowerShell running with the PowerTool module loaded.

Install PowerTool

Navigate to the location you have copied the CiscoUcs-PowerTool-1.0.0.0.exe file. Execute it from an elevated command prompt.	
A splash screen shows as the compacted file is expanded for installation.	
The routine checks to ensure no other instances of PowerShell are running. If so, it is necessary to stop those running instances before proceeding. Click **Next** to continue.	

Click the radio button by **I accept the terms in the license agreement**. Click **Next** to continue.	
If you want to change the location of the installation files, click the **Change…** button. Otherwise, accept the default location and click **Next** to continue.	
If you wish to create a desktop shortcut, click the check box by **Create Desktop Shortcut**. Otherwise, just click **Install** to continue.	

A progress bar will show the installation status.	
When complete, click the **Finish** button to complete the installation.	

To manually load into a different PowerShell environment, such as Microsoft's ISE or PowerGUI, modify your PowerShell startup file, or manually import the module with the PowerShell command:

Import-Module CiscoUcsPs

To test the installation, from the PowerShell prompt enter the following commands:

Import-Module CiscoUcsPs

Connect-Ucs <FI cluster FQDN or IP>.

When prompted, enter admin for the user name, enter the administrative password, and click Login to log in to the Cisco UCS Manager software.

15.2 System Center 2012 SP1 Operations Manager Management Pack

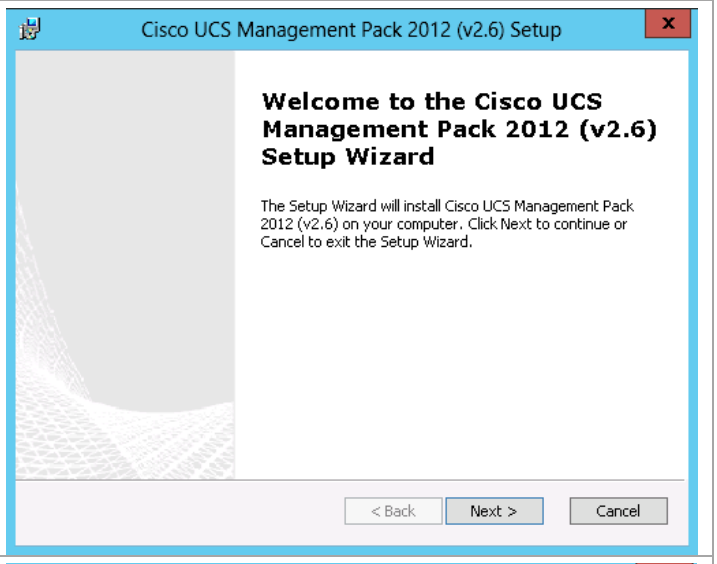
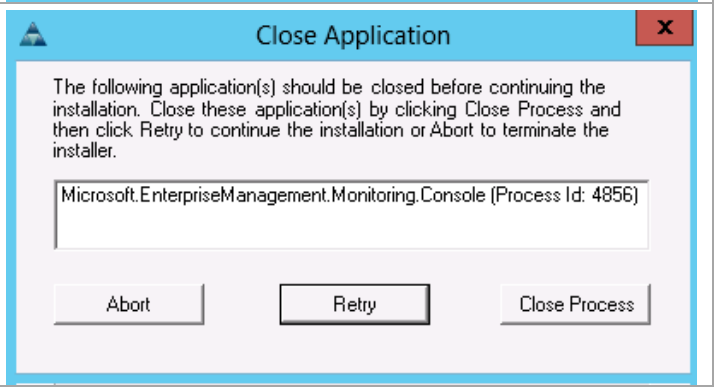
The Cisco UCS SCOM (System Center Operations Manager) Management Pack is a plug-in for System Center Operations Manager. It is used to monitor the health of the UCS system in the data center. With this plug-in, you can monitor chassis, blades, and service profiles across multiple UCS systems. Additionally, the Cisco UCS SCOM management pack enables correlation of faults and events between the Cisco UCS infrastructure and both bare-metal and virtualized operating systems already managed by SCOM.

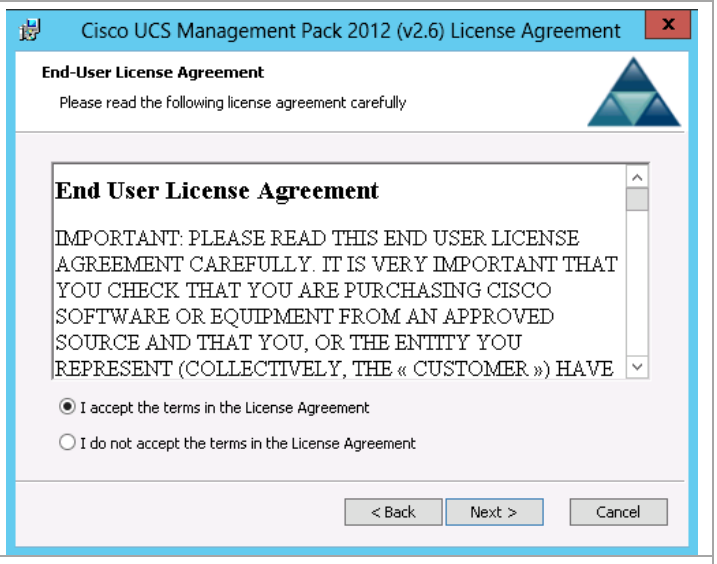
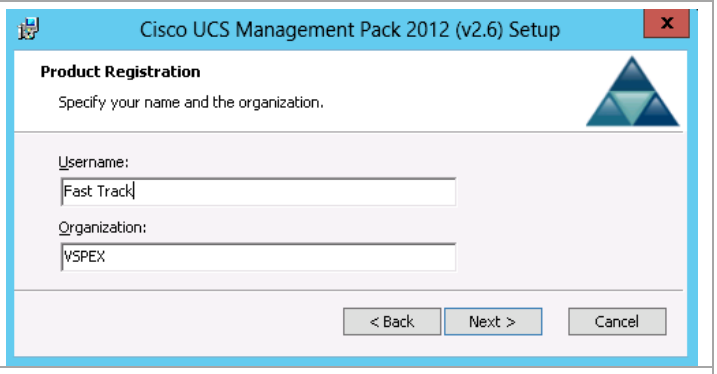
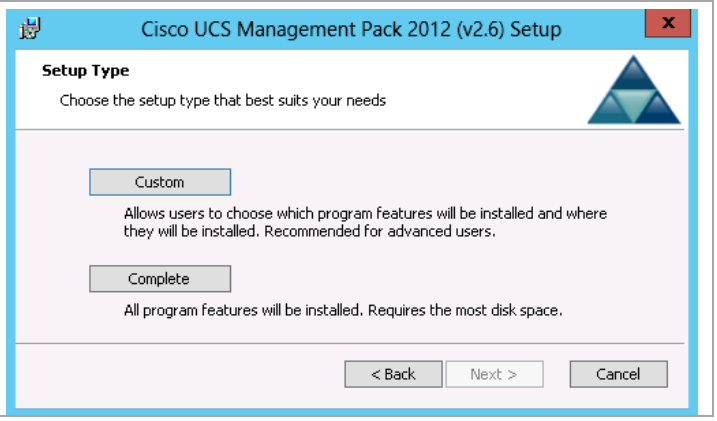
The Cisco UCS Management Pack for Operations Manager installation and configuration processes are comprised of the following high-level steps:

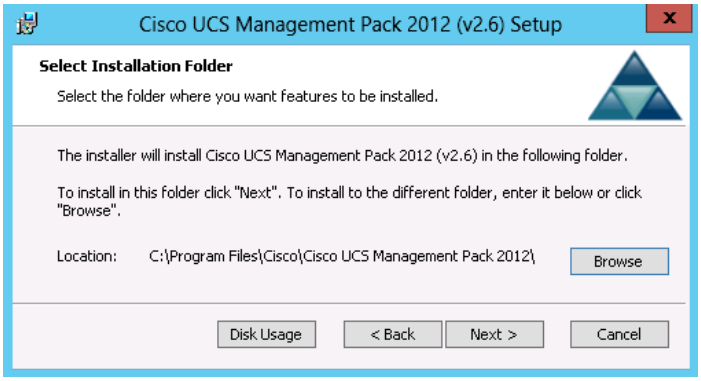
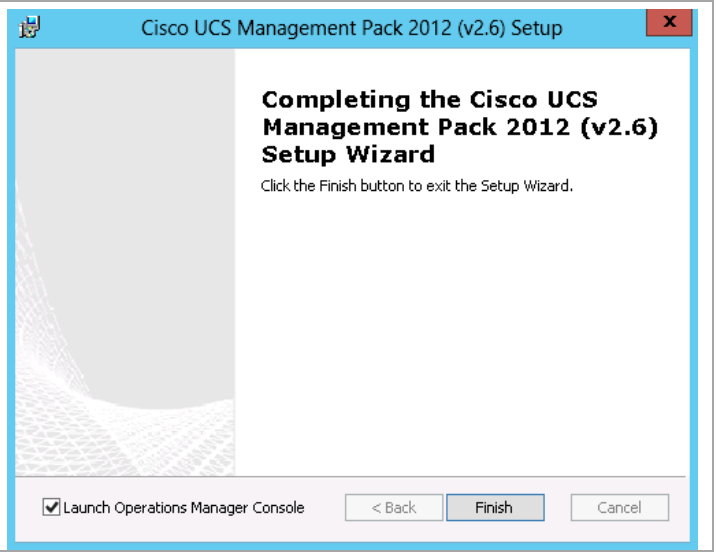


Install the Management Pack

▶ Perform the following steps on the first **System Center 2012 SP1 Operations Manager management server** virtual machine.

Launch the management pack installer, Cisco.UCS.MP.2012.v2.6.1-x64.msi Click **Next**.	
If you have the Operations Manager management console open, you will receive this warning. Close the console by clicking **Close Process** and click **Retry** to continue.	

Click **I accept the terms in the License Agreement** radio button. Click **Next**.	
Enter a user name in the **UserName** field. This field is required. Optionally, enter an organization in the **Organization** field.	
In the **Setup Type** screen, click on **Complete**.	

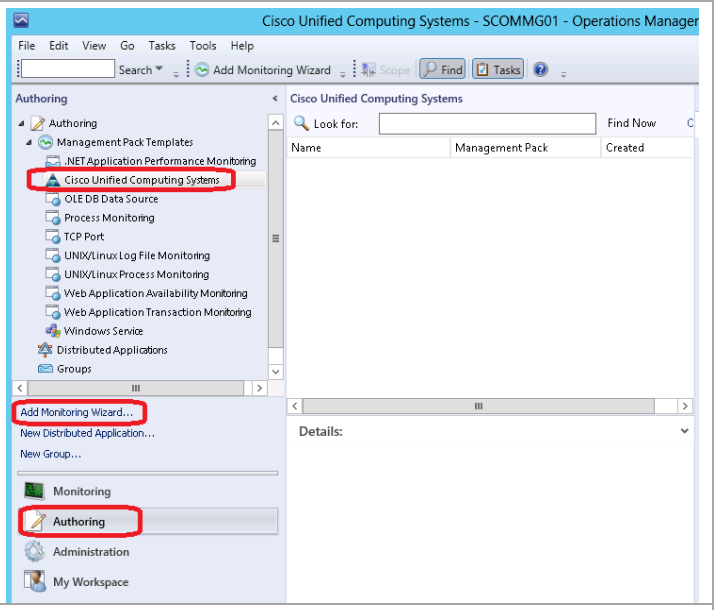
In the **Select Installation Folder**, you can accept the default location or specify a different location. Click **Next**. Click **Install** on the next screen to start the installation.	
After successful installation, you will receive the **Installation Complete** screen. Ensure the check box by **Launch Operations Manager Console** is checked. Click **Finish** to launch to console and continue configuring the management pack.	

Add Cisco UCS Domains to Operations Manager

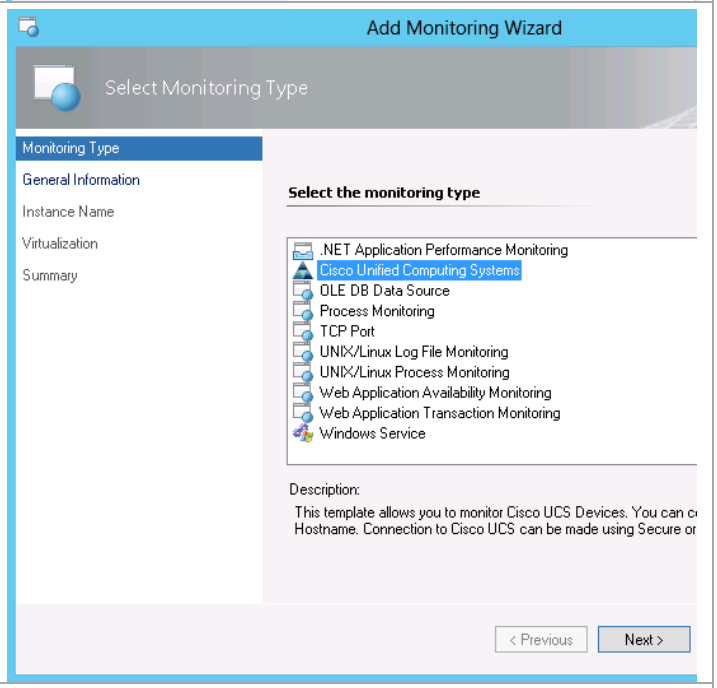
There are multiple combinations of how you may want to deploy the Cisco UCS management pack when deploying within an environment with multiple Operations Manager management servers. You can just deploy on the first management server, or you can deploy on both. These instructions provide the steps to deploy to the first management server.

To monitor Cisco UCS through SCOM:

- In the SCOM application, click the **Go** tab in the menu bar.
- Select **Authoring** from the drop-down menu.
- In the Authoring column, select **Cisco Unified Computing Systems**.
- In the **Tasks** panel, click the **Add Monitoring Wizard**.

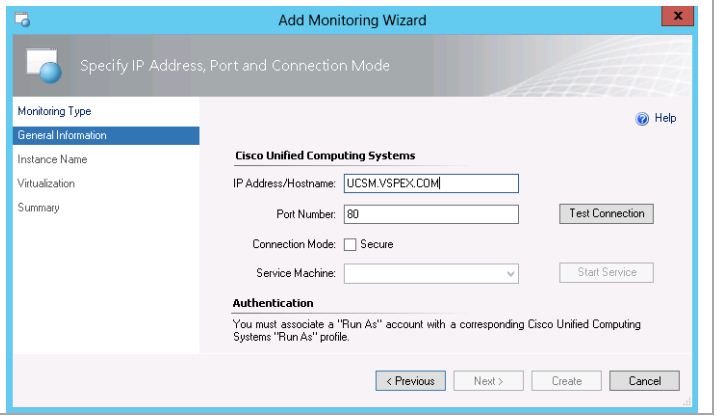


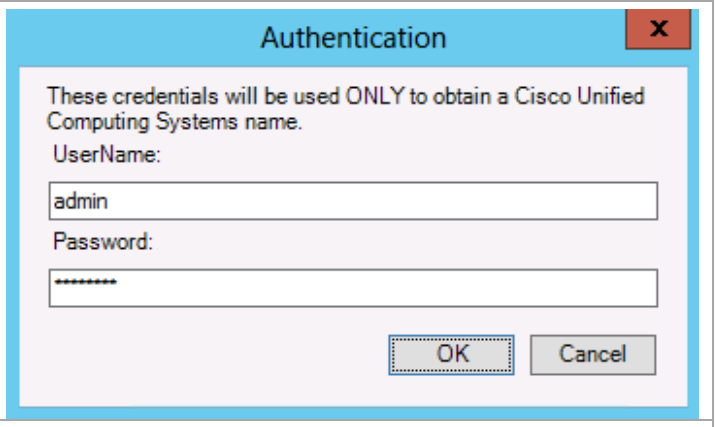
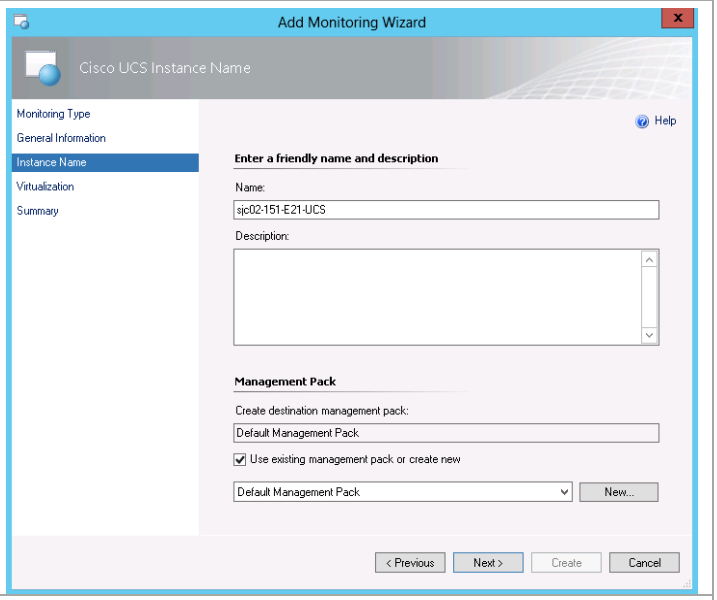
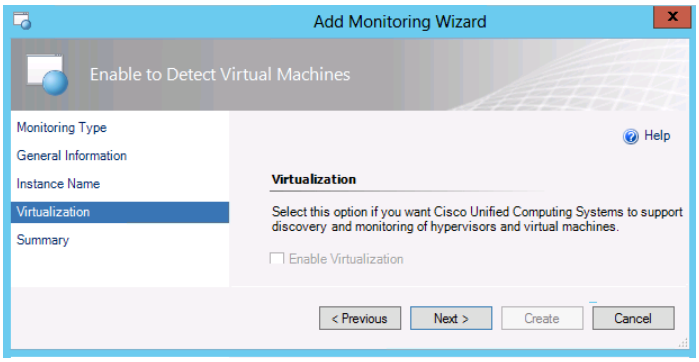
In the **Select Monitoring Type** screen, select **Cisco Unified Computer Systems**.
Click **Next**.

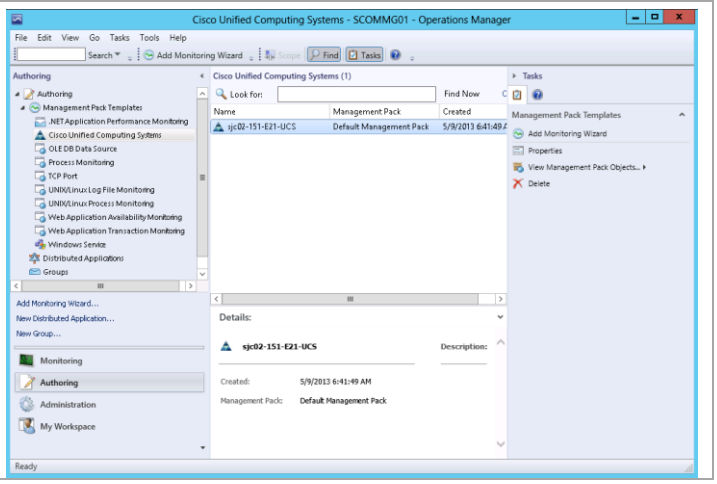


On the **General Information** screen, specify the IP address or host name of the UCS Management console.
Uncheck the **Connection Mode** box to use the default port of 80 for communication.
Click on **Test Connection** to test the connection to Cisco UCS Manager.

Note: A security alert is likely to appear due to an issue with the server certificate. Click **Yes** to continue.

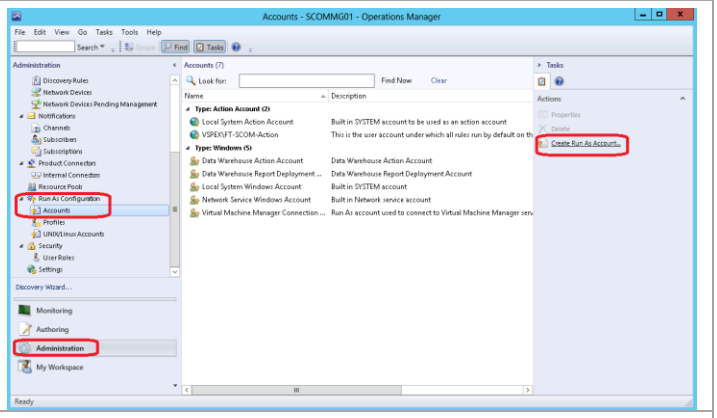
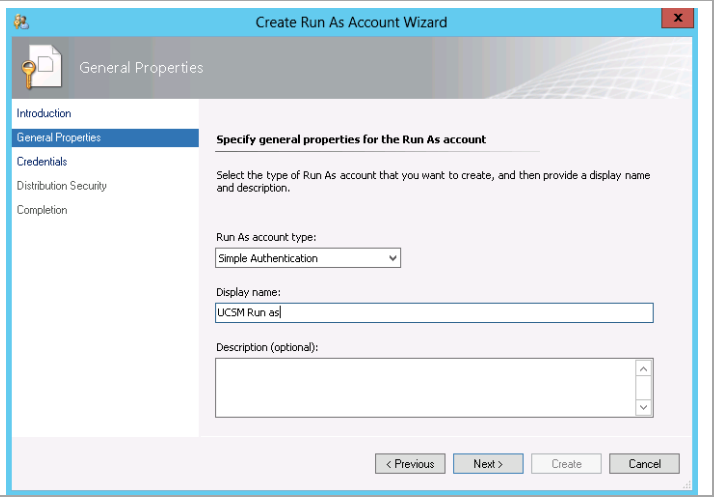


An authentication dialog window appears. Enter the proper UCS username and password to connect to UCS. Click **OK**. Upon successful connection, a message box indicating success will appear. Click **OK**. Click **Next**.	
On the **Cisco UCS Instance Name** screen, the instance name is set by default as the UCS host name. Click **Next**. **Note:** It is recommended that the default instance name is not modified. Optionally, you may enter a description for the UCS Domain. Check the box by Use existing management pack or create. **Note:** It is recommended that the default management pack be used.	
The Virtualization feature is not supported in this release. Click **Next**. The **Configuration Summary** screen appears. Review your entries and click **Create**.	

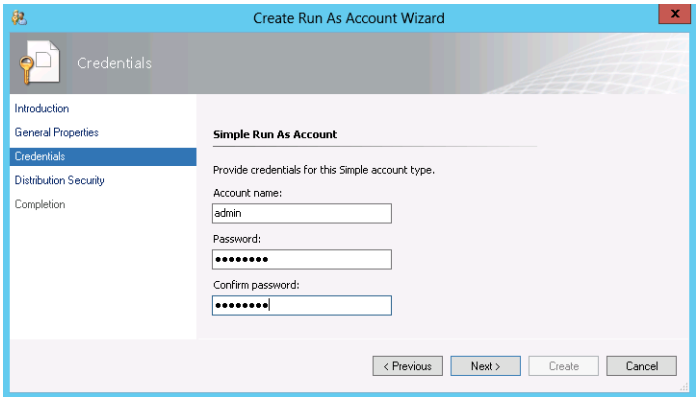
The created template for the management pack is shown in the Operations Manager console.	

Configure Administrator Account

Operations Manager uses Run As accounts to establish a connection to a Cisco UCS domain. The Run As account must be an administrator account.

Select the **Administration** section. Scroll down and expand **Run As Configuration**. Click on **Accounts**. From the **Tasks** pane on the right-hand side, click **Create Run As Account...** Click **Next** on the Introduction page.	
From the **Run As account type** drop-down, select **Simple Authentication**. Enter a name for this account in the **Display Name** field. Click **Next** to continue.	

In the **Credentials** screen, enter the credentials that will be used for access the UCS domain.
Click **Next** to continue.

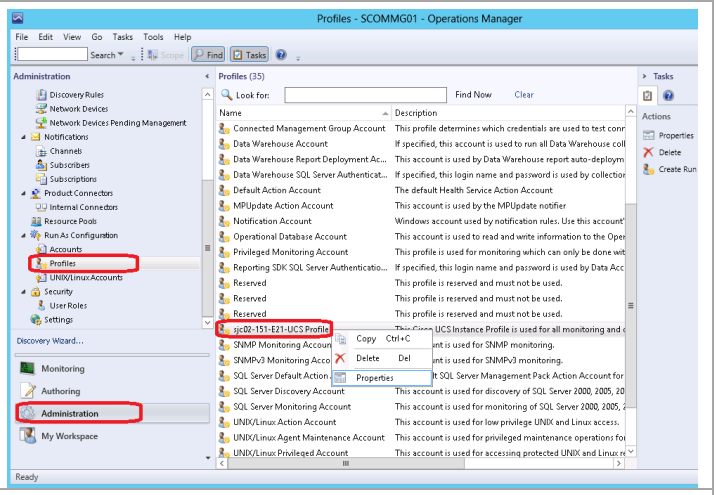


In the **Distribution Security** page, select the radio button by **Less Secure**.
Click **Create** to create the UCS run as account.

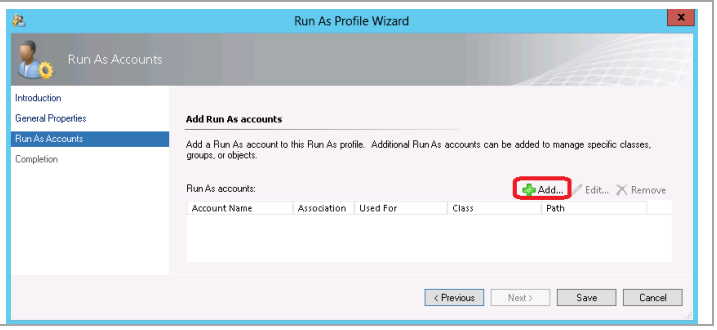
Note: Cisco UCS does not use the Windows operating system for Cisco UCS Manager. The More Secure option is intended for management packs that target computers or devices equipped with the Windows operating system.



Click **Close** on the successful completion page.
In the Operations Manager Console, select **Profiles** (right below the previous **Accounts** selection).
Scroll through the Profiles to find the profile you just created. Right-click the profile and select **Properties**.



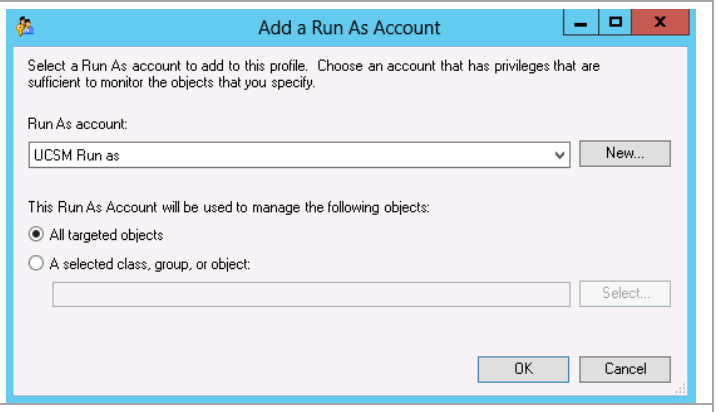
In the **Run As Profile Wizard** screen, select **Run As Accounts**.
Click the **Add...** icon.



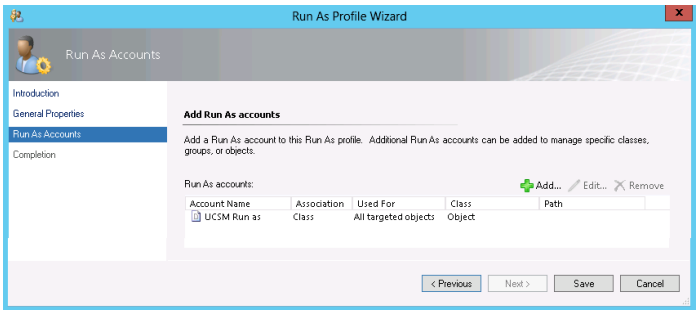
From the **Run As account** drop-down, select the run as account you just created for communicating with Cisco UCS.
Select the radio button by **All targeted objects**.

Note: If you have run this management pack previously, and know exactly what you want to monitor, you can make the other selection and pick your items.

Click **OK** to continue.

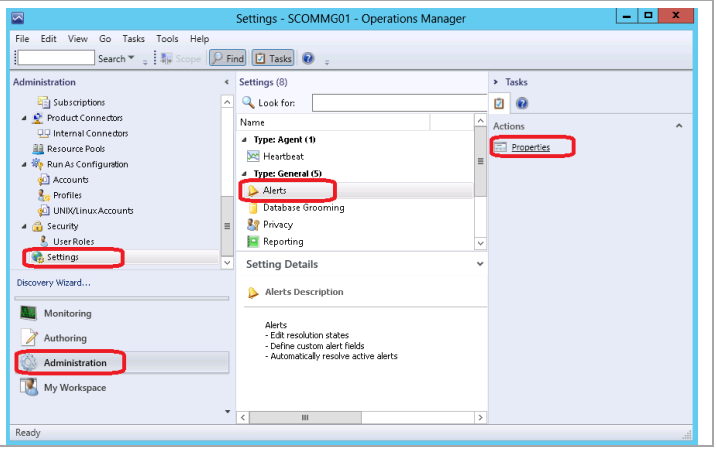


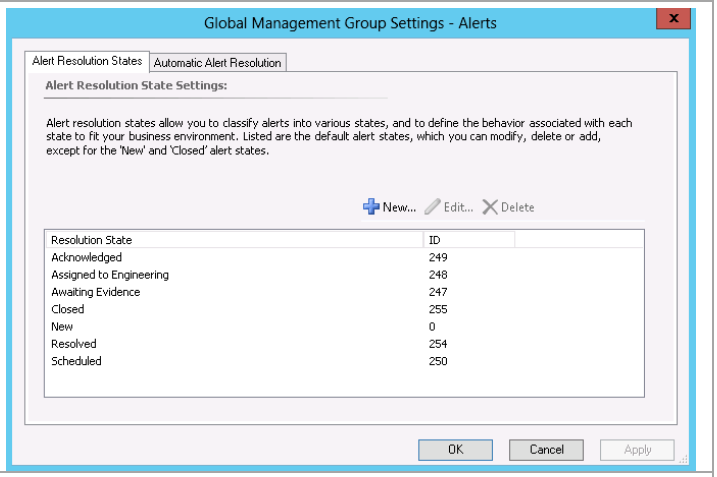
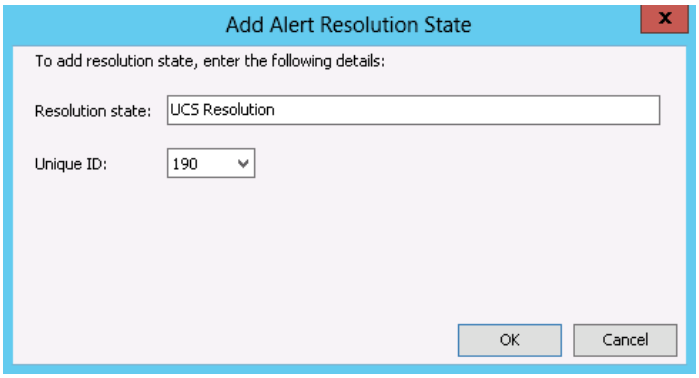
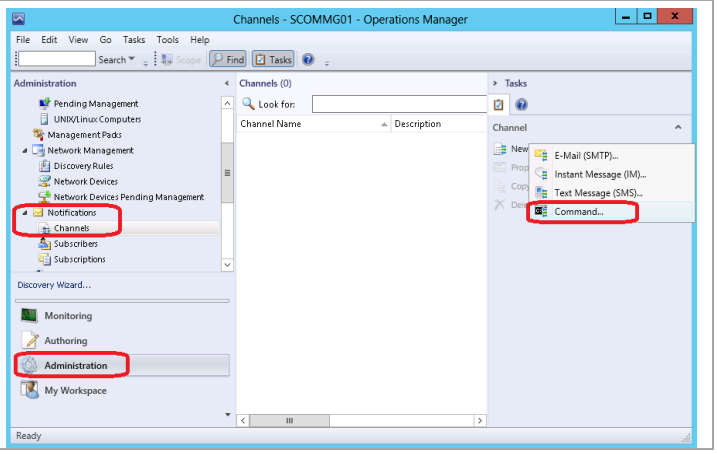
Back in the **Run As Profile Wizard** screen, click **Save** to continue.
On the successful completion page, click **Close**.



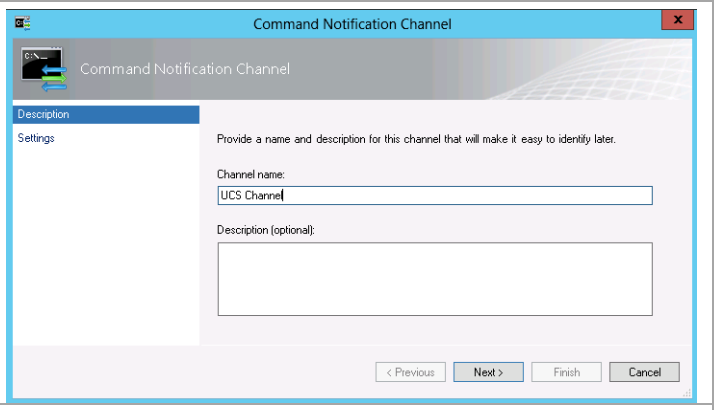
Configure Fault Acknowledgement

In the Operations Manager console, select **Administration**. Scroll to the bottom of the list on the left-hand side and select **Settings**.
Select **Alerts** from the Settings in the center pane, and click on the **Properties** task.

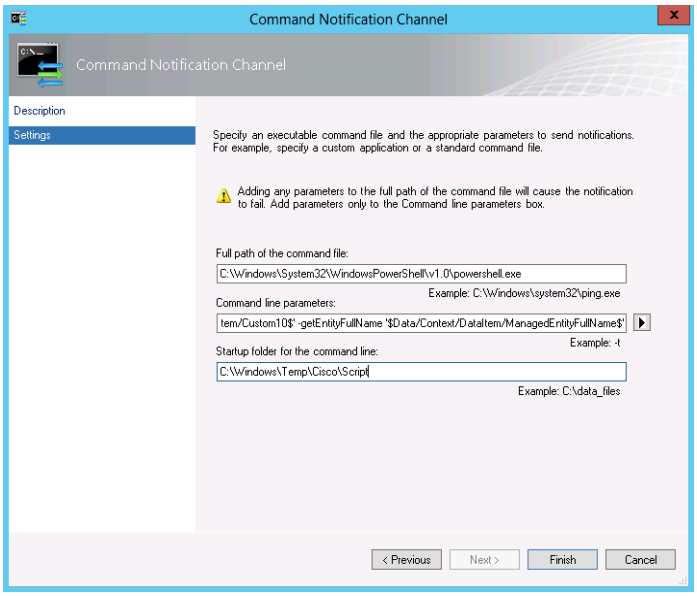


In the **Global Management Group Settings – Alerts** window, click **New…**	
In the **Resolution state** field, enter a name for this resolution state. In the **Unique ID** drop-down list, select an available identifier. Click **OK** to continue. Click **OK** in the Global Management Group Settings – Alerts window to continue.	
Select **Administration > Notifications > Channels** in the Operations Manager console. Under **Tasks** click **New** and select **Command…** from the drop-down list.	

In the **Command Notification Channel** screen, enter a value into the **Channel Name** field. Optionally, enter a description.
Click **Next** to continue.



In the **Settings** page, enter the following for the **Full path of the command file:**
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
In the **Command line parameters** field enter the following:
`-Command "& '"C:\Windows\Temp\Cisco\Script\Bidirectional.ps1"'" -getDnValue '$Data/Context/DataItem/Custom6$' -getFaultID '$Data/Context/DataItem/Custom7$' -getWebProxyUrl '$Data/Context/DataItem/Custom10$' -getEntityFullName '$Data/Context/DataItem/ManagedEntityFullName$'`
In the **Startup folder for the command line** field enter the following:
`C:\Windows\Temp\Cisco\Script`
Click **Finish** to continue and **Close** upon successful completion.



Click **Finish** to continue and **Close** upon successful completion.

Note: The installation of the Cisco UCS Management Pack places the Bidirectional.ps1 file into the C:\Windows\Temp\Cisco\Script directory. If you want to change the location, be sure to change both the command line parameter and the startup folder values above.

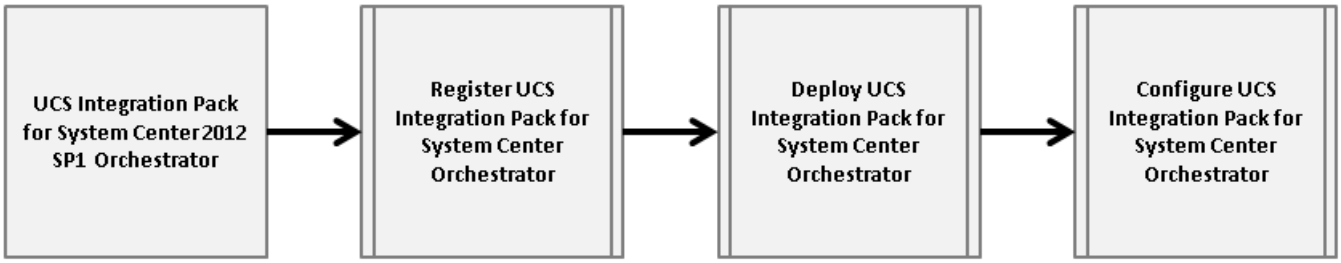
Configure Cisco UCS Management Service

For further information about the various configuration options that can be executed to tailor the monitoring to your environment, download the Cisco UCS Management Pack User Guide, Release 2.6 from
http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/msft_tools/scom/scom_2.6/scom_2.6_user_guide/scom_2_6_userguide.html.

15.3 System Center 2012 SP1 Orchestrator Integration Pack

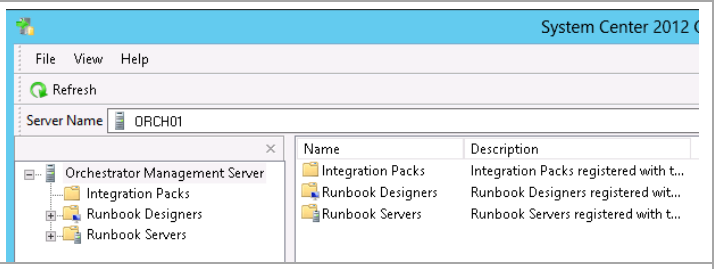
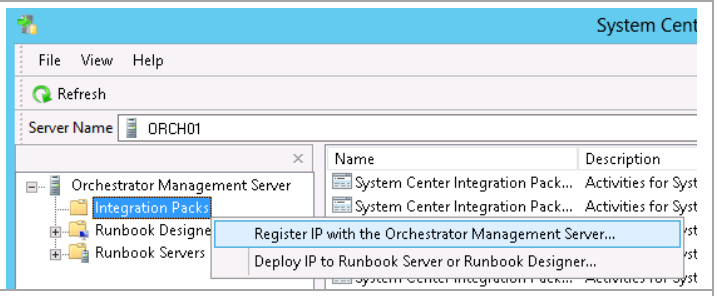
The Cisco UCS OIP (Orchestrator Integration Pack) is a plug-in for System Center 2012 Orchestrator. It is used to develop runbooks for automating processes that need to read and modify information within UCSM.

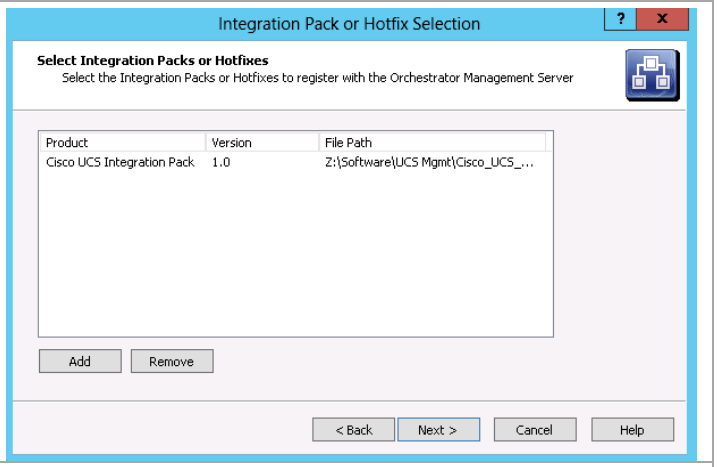
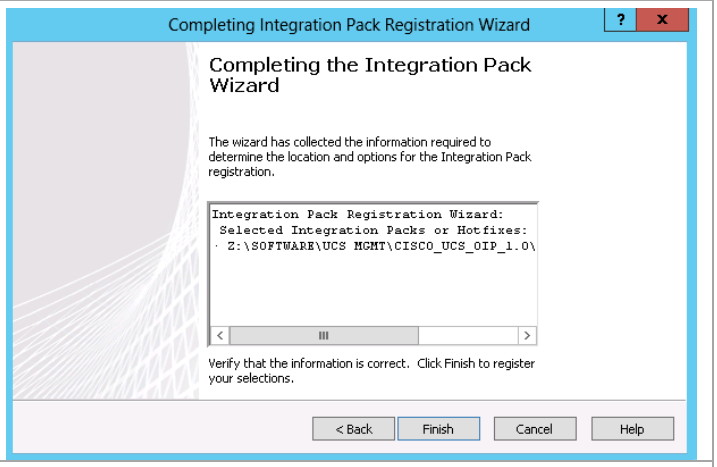
The Cisco UCS Management Pack for Orchestrator registration and deployment processes are comprised of the following high-level steps:



Register the Cisco UCS OIP

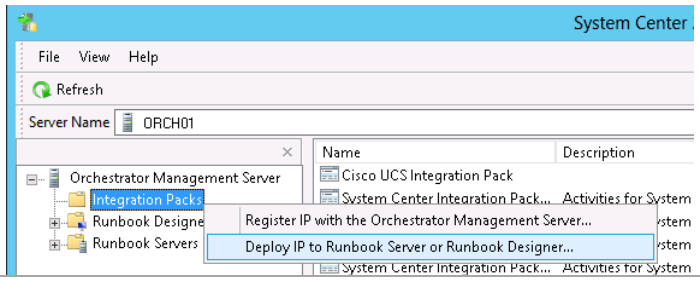
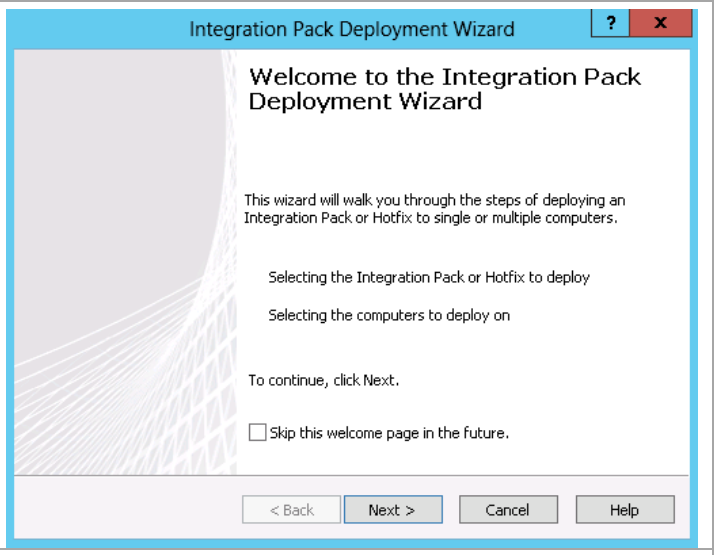
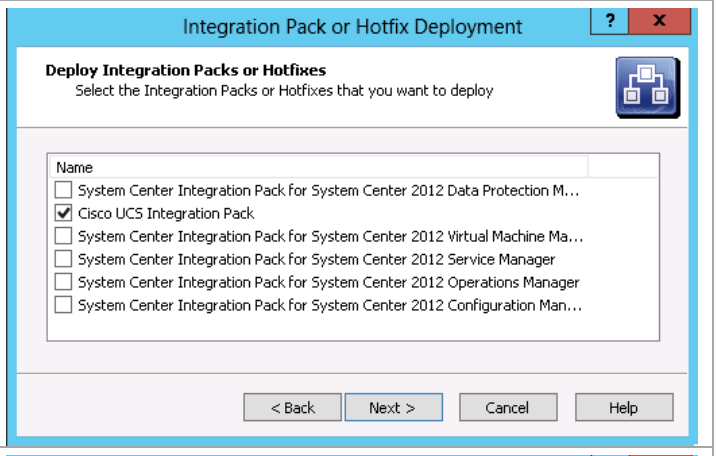
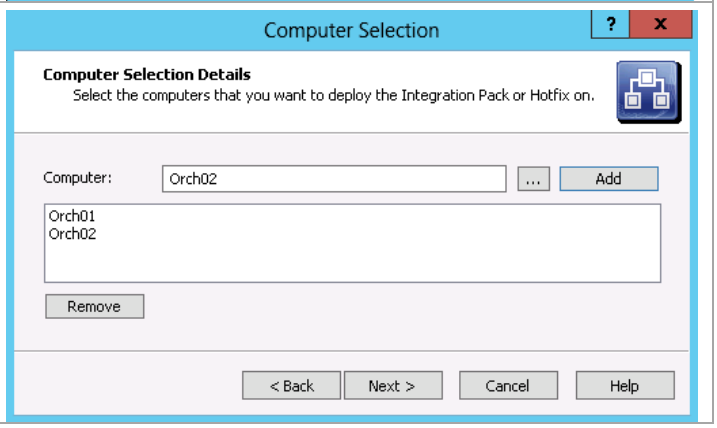
After downloading the Cisco UCS OIP, extract the installation file from the zip file. Ensure that Cisco UCS PowerTool has been installed on all Orchestrator management servers. Then perform the following steps on all Orchestrator management servers to register the integration pack.

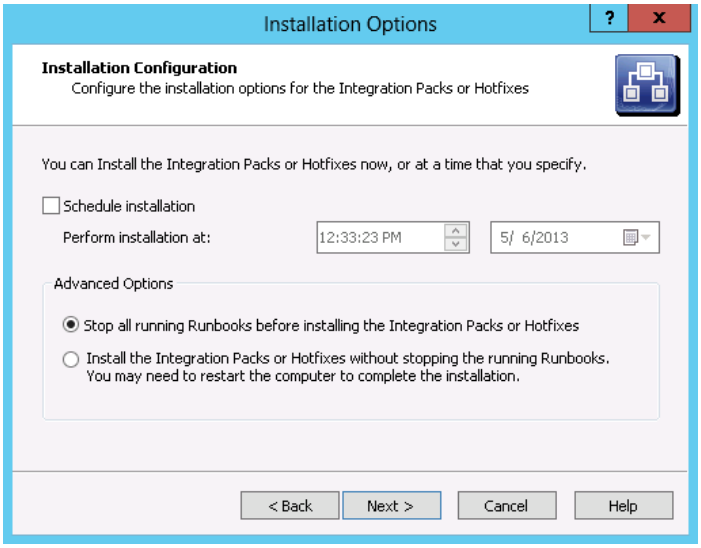
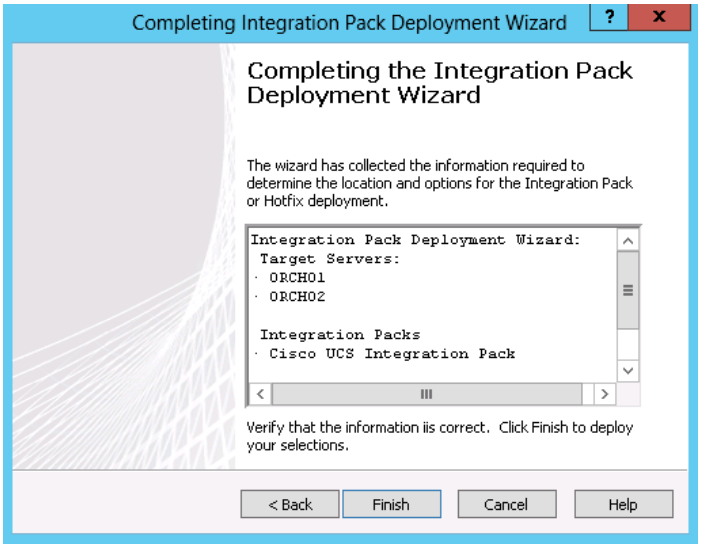
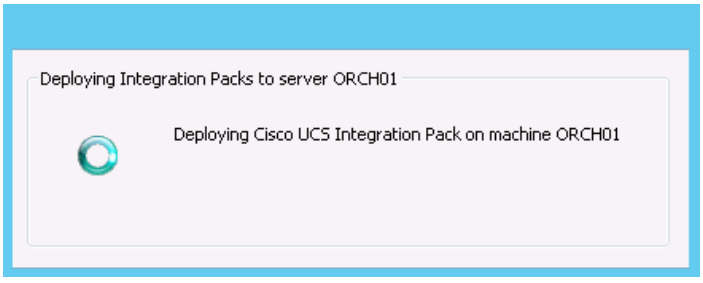
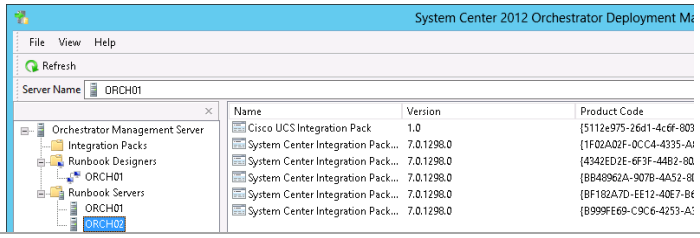
Launch the System Center 2012 Orchestrator Deployment Manager.	
Right-click **Integration Packs** and select **Register IP with the Orchestrator Management Server**.	
On the Welcome screen, click **Next** to continue.	

In the **Select Integration Packs or Hotfixes** dialog, click the **Add** button, navigate to where you extracted the OIP file, and select the file. Click **Next** to continue.	
On the summary page, click **Finish** to continue.	
Click **Accept** on the End User License Agreement page to complete the installation.	

Deploy the Cisco UCS OIP

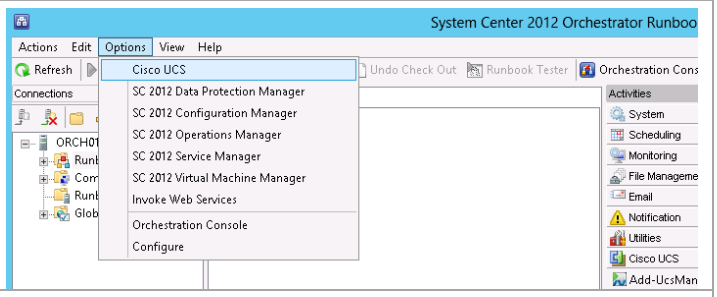
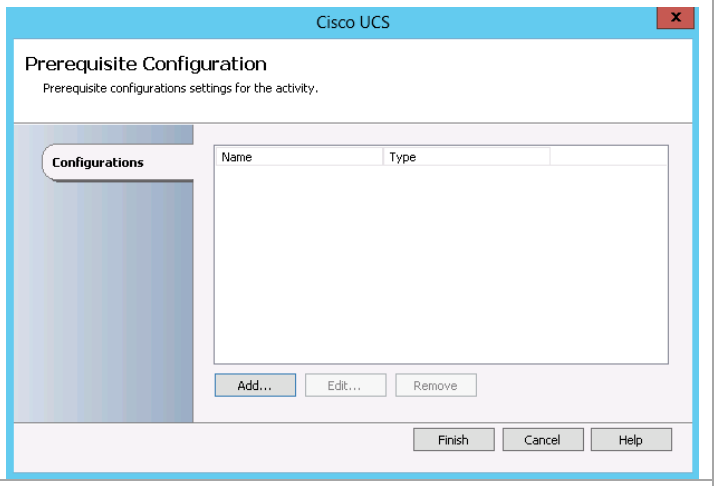
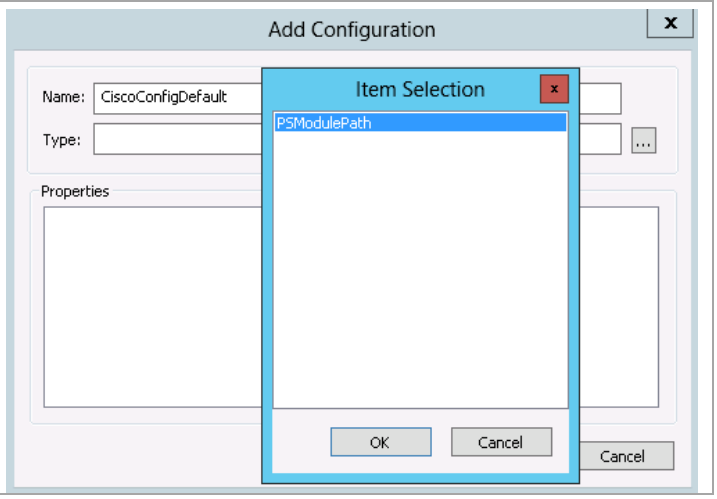
On each Runbook Server or Runbook Designer system, deploy the Cisco UCS OIP.

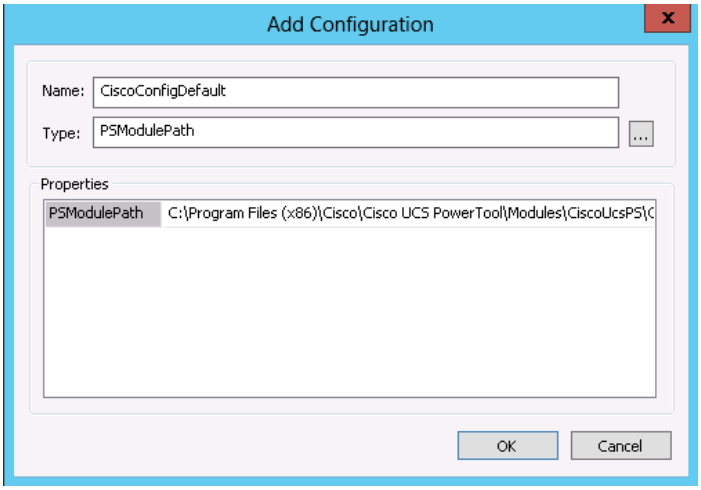
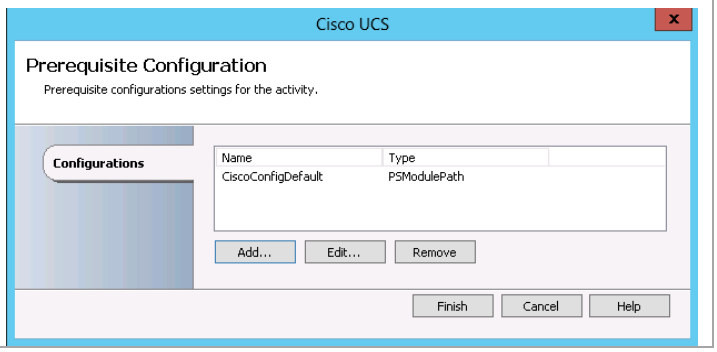
From the Deployment Manager, right-click **Integration Packs** and select **Deploy IP to Runbook Server or Runbook Designer…**	
On the Welcome page, click **Next** to continue.	
In the **Deploy Integration Packs or Hotfixes** dialog, select the **Cisco UCS Integration Pack**. Click **Next** to continue.	
In the **Computer Selection Details** dialog, enter the names of the runbook servers. Click **Next** to continue.	

Ensure the radio button by **Stop all running Runbooks before installing the Integration Packs or Hotfixes** is selected. Click **Next** to continue.	
On the summary page, click **Finish** to continue.	
A status window will show the progress of the deployment.	
Back in the Orchestrator Deployment Manager, ensure that the Cisco UCS OIP has been deployed to the target servers. Expand **Runbook Servers** and then click on each server listed to see that the Cisco UCS Integration Pack is listed.	

Configure the Cisco UCS OIP

On each system running the Orchestrator Runbook Designer, configure the Cisco UCS OIP.

Launch the Orchestrator Runbook Designer. Select **Options** and then **Cisco Ucs**.	
In the **Prerequisite Configuration** dialog, click the **Add…** button.	
Provide a value in the **Name** field. Click on the **…** at the end of the **Type** field. Select **PsModulePath** from the Item Selection window and click **OK**.	

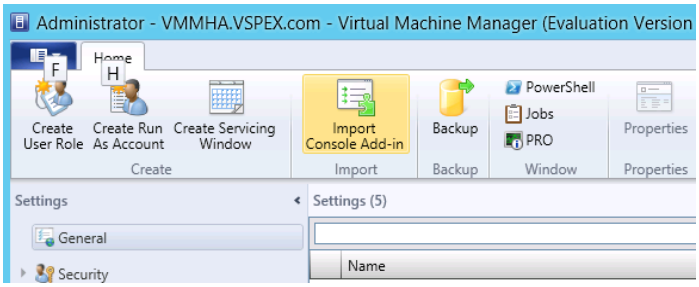
In the **Properties** of the **PsModulePath** field, enter the location of where the Cisco UCS PowerTool PowerShell data file was installed. By default, it is located at `C:\Program Files (x86)\Cisco\Cisco UCS PowerTool\Modules\CiscoUcsPS\CiscoUcsPS.psd1`. Click **OK** to continue.	
Click **Finish** to complete the configuration.	

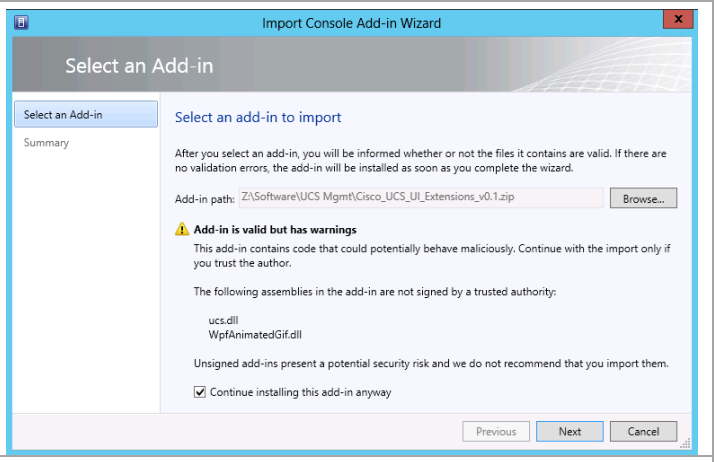
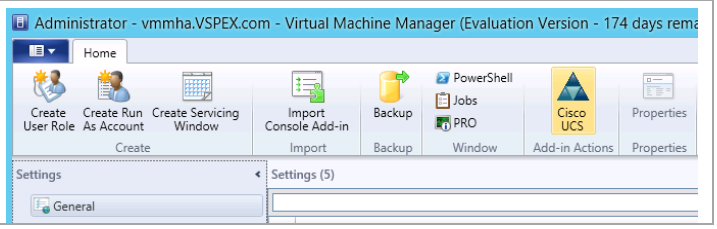
15.4 System Center 2012 SP1 Virtual Machine Manager UI Extension

The Cisco UCS Add-in for Microsoft System Center 2012 Virtual Machine Manager enables management of Cisco UCS from within SCVMM.

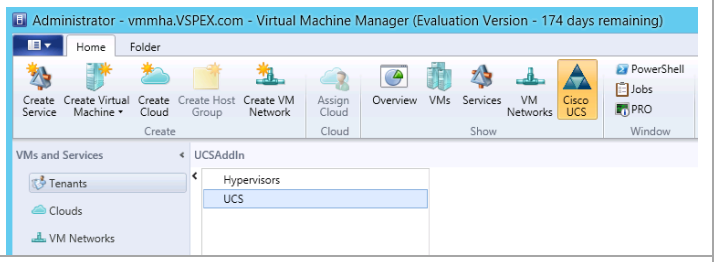
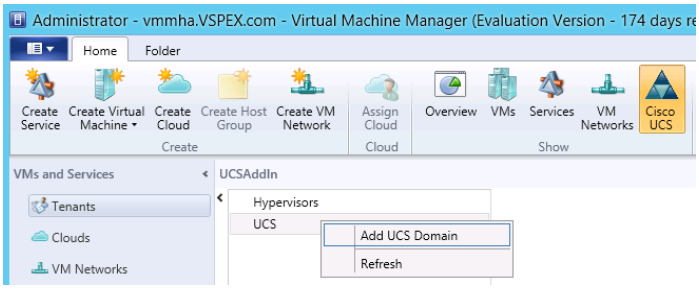
Installation of this add-in requires that Cisco UCS PowerTool is already installed on the servers to which the UI extensions add-in will be added. The add-in needs to be installed on any VMM console from which you want to use the extensions.

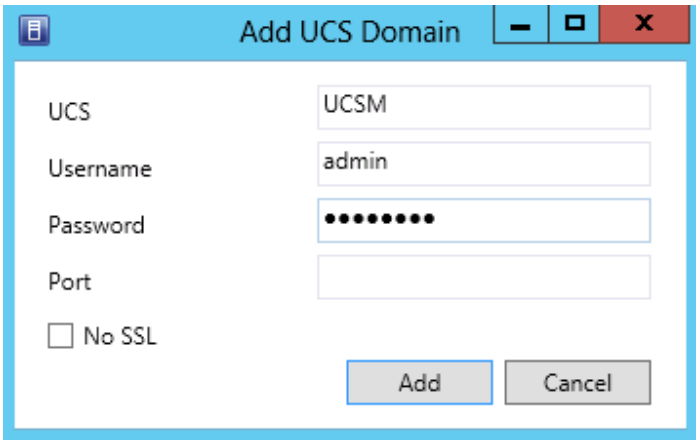
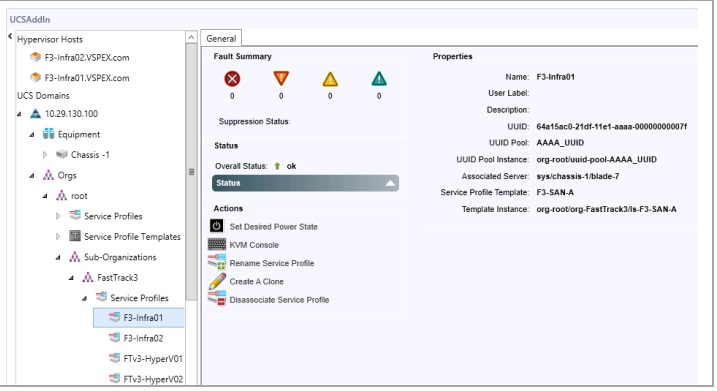
Importing the Add-in

Launch the SCVMM console, and navigate to **Settings**. Click on **Import Console Add-in**.	

In the **Select an add-in to import** dialog, browse to the location where you stored the downloaded zip file and select it. You will be presented with a warning about potential malicious code because it is not part of the VMM distribution. Click the **Continue installing this add-in anyway** box. Click **Next** to continue. On the Summary page that display, click **Finish** to complete the installation.	
Upon completion of the installation, you will see an icon for **Cisco UCS** in the tool bar ribbon.	

Configure and Use the Cisco UCS Add-in

From the **VMs and Services** selection, click on the **Cisco UCS** icon.	
Right-click **UCS** under UCSAddin. Select **Add UCS Domain**.	

Enter the DNS name or IP address of your Cisco UCS Manager into the **UCS** field. Enter a **Username** and **Password** for logging into UCSM. Optionally, dependent upon your Cisco UCS Manager installation, you may enter Port and SSL designation. **Note:** If your Cisco UCS Manager installation is integrated with Active Directory, these can be AD credentials. Otherwise, they will be credentials local to Cisco UCS Manager.	
At this point, you will be able to view and manipulate a subset of items from within Cisco UCS directly from the VMM console.	

15.5 Cisco Nexus 1000V

Cisco Nexus 1000V Series Switches provide a comprehensive and extensible architectural platform for virtual machine and cloud networking. The switches are designed to accelerate server virtualization and multi-tenant cloud deployments in a secure and operationally transparent manner for environments like Microsoft's Private Cloud. Download the distribution software from the location specified in the Software Revision table at the beginning of this document and expand it into a temporary directory.

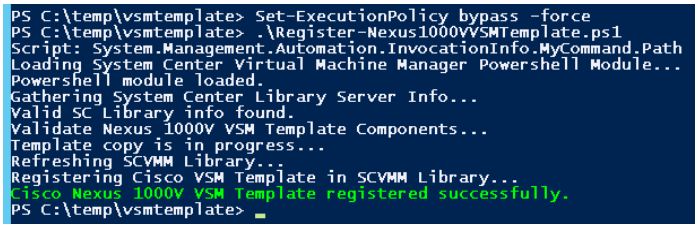
Create Two Virtual Supervisor Module VMs

The Nexus 1000V runs as a pair of virtual machines for high availability purposes. The Nexus 1000V distribution contains an ISO file (nexus-1000v.5.2.1.SM1.5.1.iso) that is used in the creation of the virtual machines that will run the Nexus 1000V software. Copy it to the Virtual Machine Manager library. (The VMM library is a standard Windows share, so normal procedures for putting simple files into the share work.) Refresh the library location after the copy is completed.

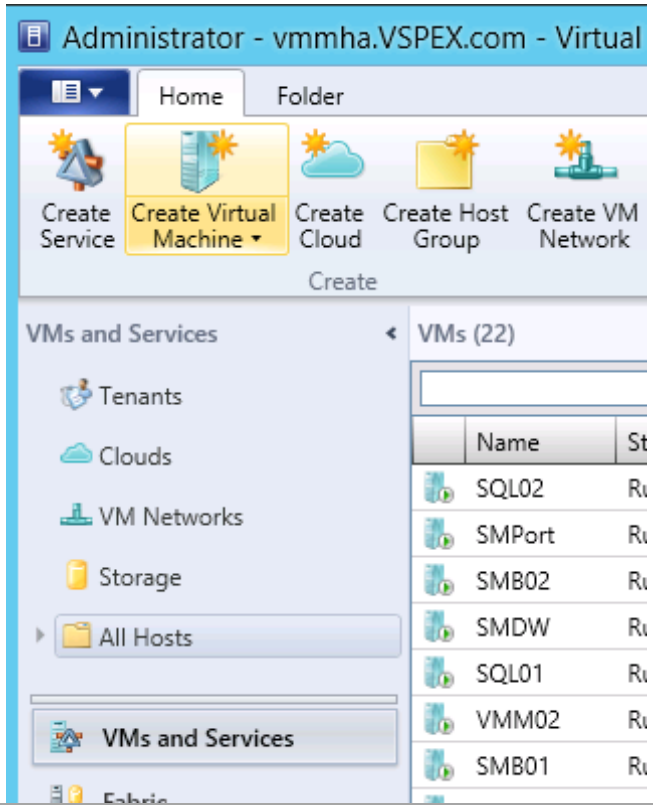
From an elevated PowerShell window on a Virtual Machine Manager machine, navigate to the directory containing the extracted contents of the Nexus 1000V distribution. Find the **Register-Nexus1000VVSMTemplate.ps1** script and execute it.

Note: You must execute this script from the directory in which it is found. It assumes a specific directory hierarchy.

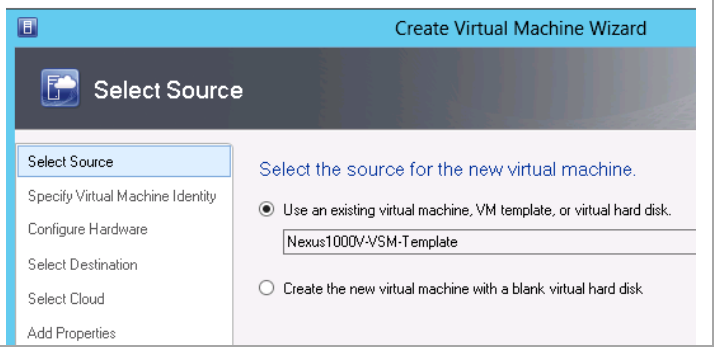
Note: You might have to set the execution policy to bypass to get the script to run.

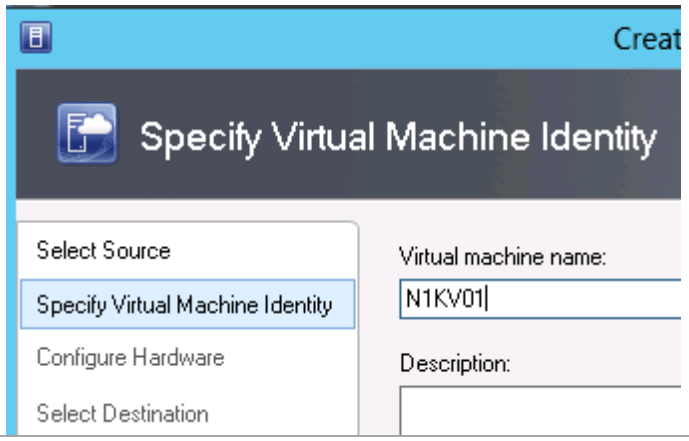
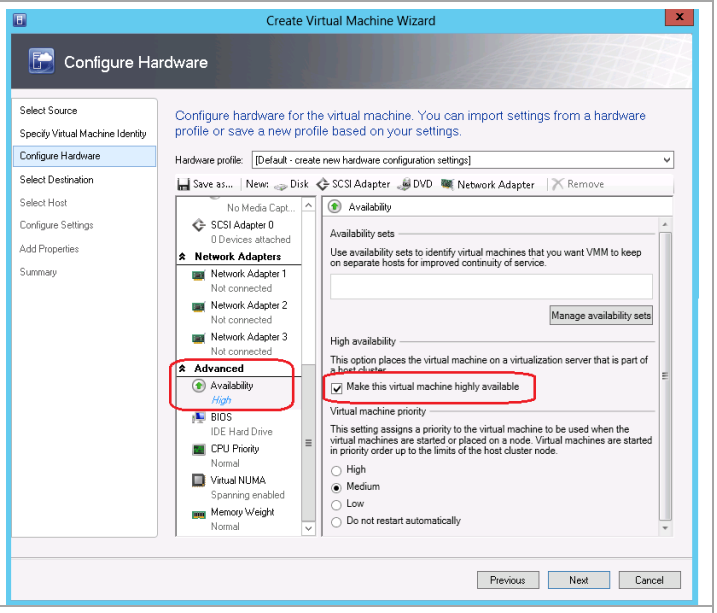
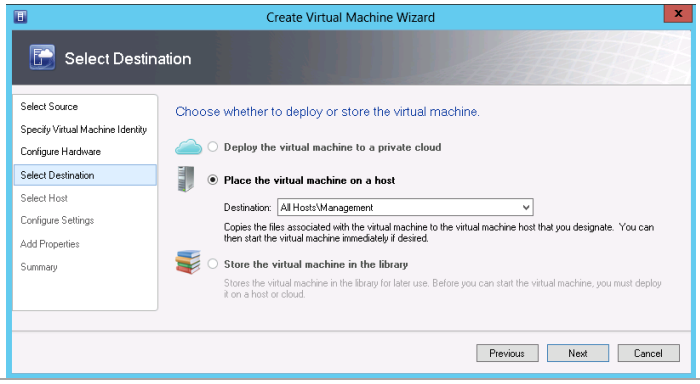


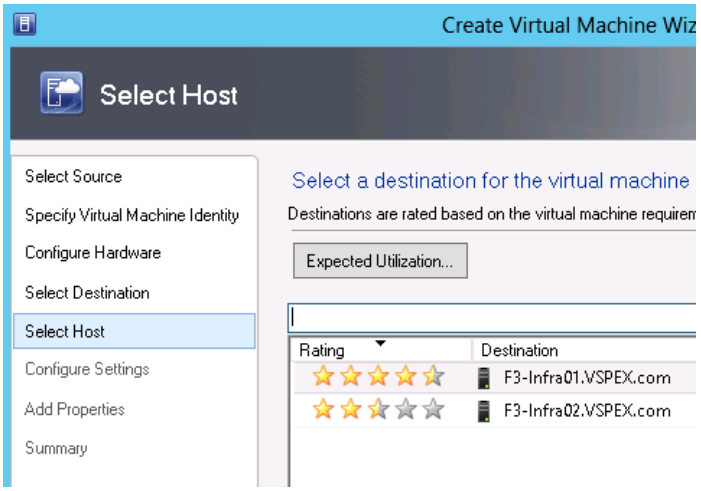
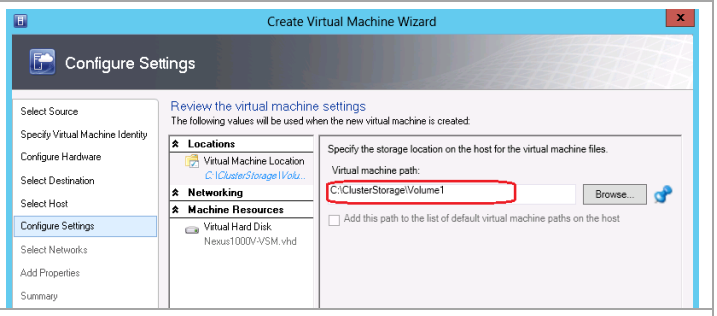
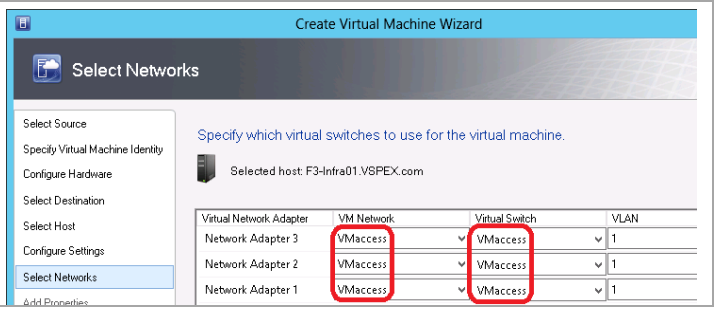
From one of the Virtual Machine Manager consoles, select **VMs and Services**.
Double-click on **Create Virtual Machine**. This will launch a wizard to assist in creating a virtual machine to be used for installing the Nexus 1000V software image.



In the **Select Source** dialog window, select the radio button by **Use an existing virtual machine, VM template, or virtual hard disk**. Click **Browse**. This launches a window that presents the contents of the VMM library. Select the **Nexus1000V-VSM-Template** and click **OK**.
Click **Next** to continue.



In the **Specify Virtual Machine Identity** dialog window, enter the name of the virtual machine. Click **Next** to continue.	
In the **Configure Hardware** dialog window, navigate to the **Advanced** settings and select **Availability**. Click the check box by **Make this virtual machine highly available**. Click **Next** to continue.	
In the **Select Destination** dialog window, select the management group you have defined for your fabric management cluster. Click **Next** to continue.	

In the **Select Host** dialog window, select one of the fabric management hosts for deployment. Click **Next** to continue.	
In the **Configure Settings** dialog window, ensure the **Virtual machine path** is pointing to the location you want to store the VM. This should be on one of the Cluster Shared Volumes. Click **Next** to continue.	
In the **Select Networks** dialog window ensure all network connections are to the VMaccess network. Click **Next** to continue. Click **Next** on the **Add Properties** dialog window. Click **Create** on the **Summary** dialog window. Do **not** select the option to start the virtual machine. Repeat the process to create a second VSM virtual machine.	

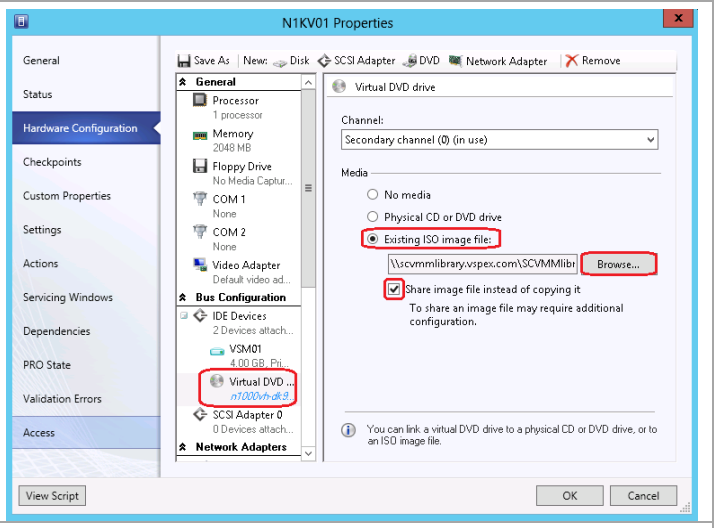
Configure the VSM

One of the components of the Nexus 1000V distribution media is an ISO file used for installing the software. As one of the first steps of this installation, you should have copied this ISO file to the VMM library.

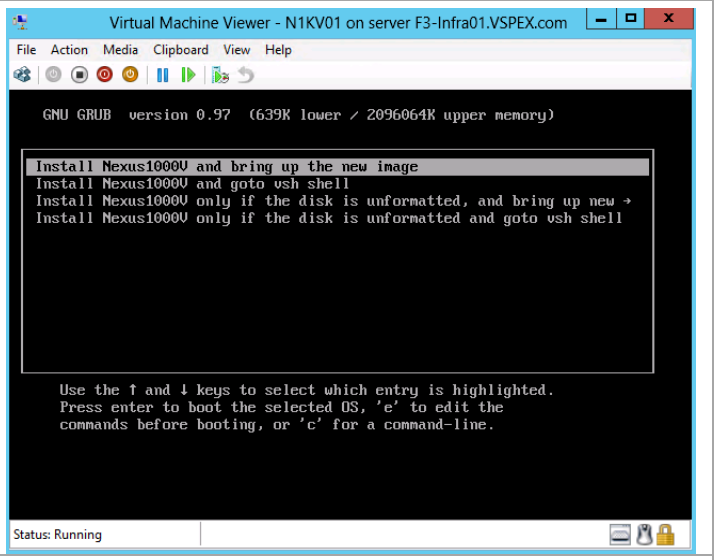
Note: Ensure the name to be used as the switch name has a DNS and (optionally) an associated pointer (PTR) record in your DNS server. The switch name is a value entered during configuration, so it is not the name of the VMs. VMM uses DNS to find this VSM.

Within the VMM console, right-click the N1KV virtual machine, and select **Properties**.
On the Properties window, select **Hardware Configuration**. Select the **Virtual DVD** component.
Click the radio button by **Existing ISO image file**. VMM will display the ISO files within its library. Select the nexus-1000v.5.2.1.SM1.5.1.iso file.
If you have configured Constrained Delegation, click the check box by **Share image file instead of copying it**.

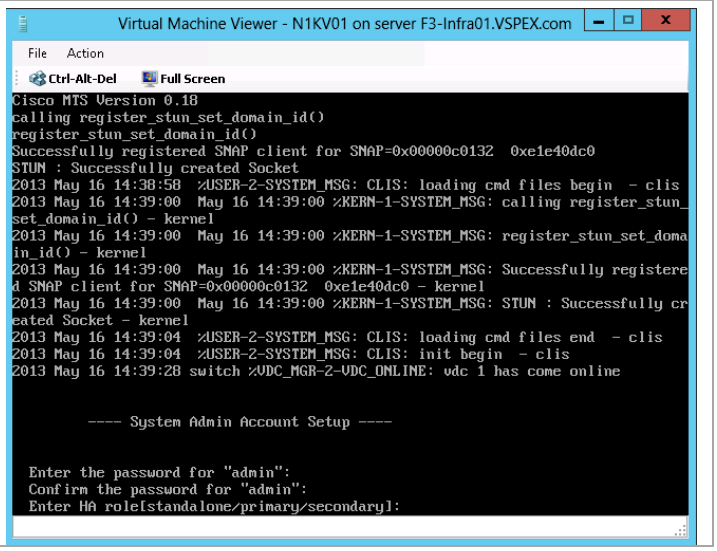
Note: Configuration of Constrained Delegation is covered in the section on setting up the VMM virtual machines.



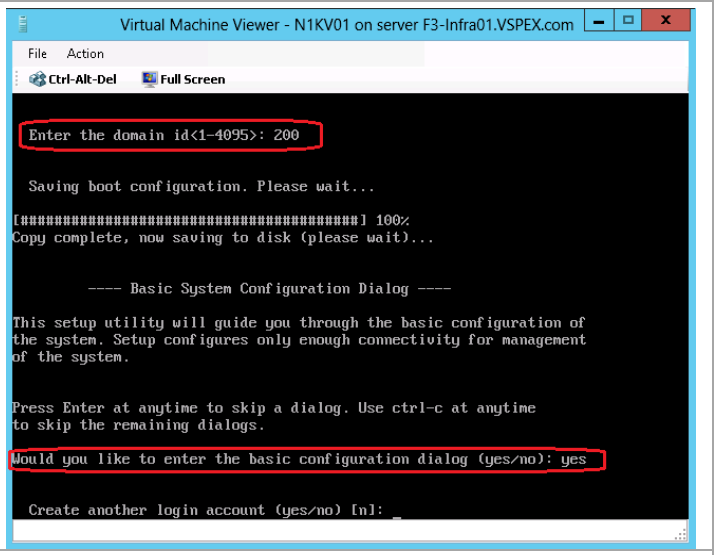
In VMM select the first N1KV virtual machine. Start it and connect to it through the console.
By default, **Install Nexus 1000V and bring up the new image** is highlighted. Either enter a return or let the timeout expire and the installation will begin.
There are two subsequent questions that will be answered with **y** automatically if you are not watching for them.
Do you want to format it (y/n)
Perform r/w tests (takes very long time) on target disks (y/n)



After some configuration, the system prompts for a new password for the admin account. Enter it and confirm it.
On the first VSM virtual machine, select **primary** for the HA role.
On the second VSM virtual machine, select **secondary** for the HA role.

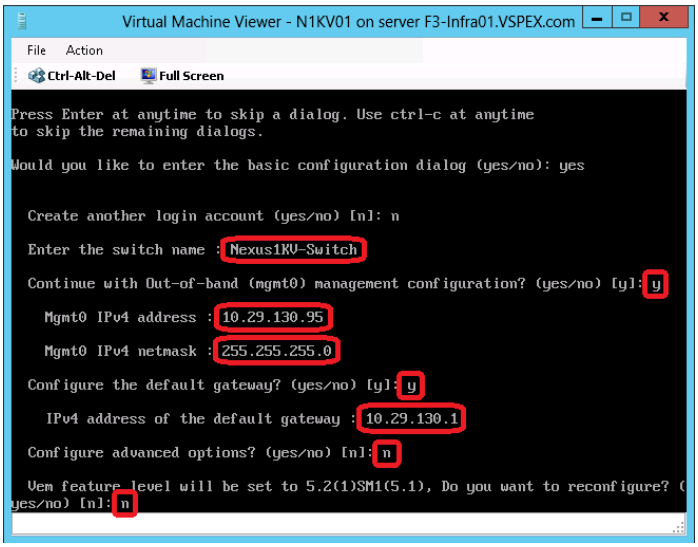


After selecting the HA role, you are asked for a **domain id** in the range 1-4095. This number is used when configuring HA, so it will be entered for both installs. <***200***>
The next question is asking to run the basic configuration dialog. Answer **yes**.
For the question to create another account, accept the default **n**.

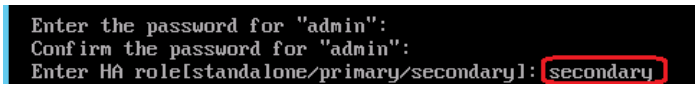


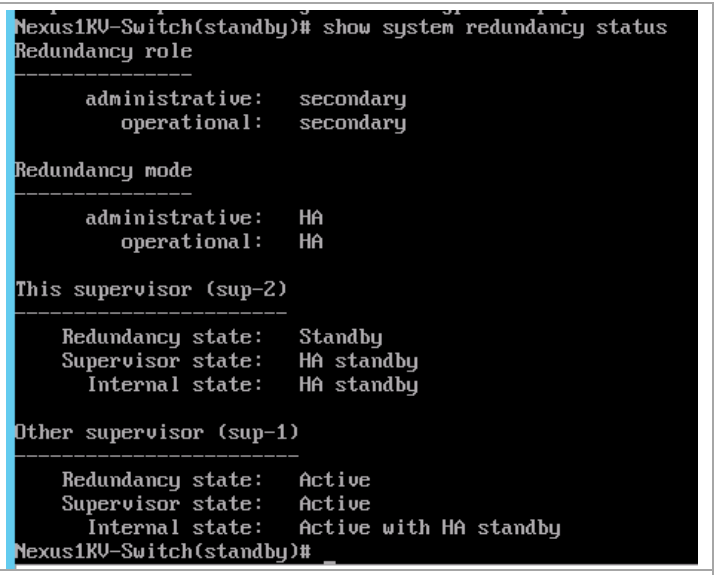
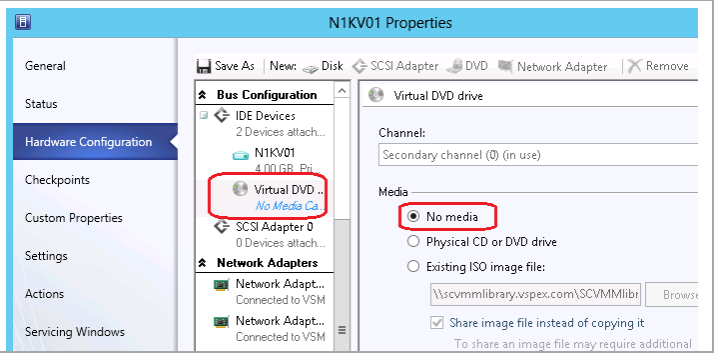
The next series of commands are answers similar to configuring a typical Nexus switch for out-of-band management.
Provide a character string to **name** the switch. (This is the name that needs the DNS entry). <***Nexus1KV-Switch***>
Configure out-of-bound management - **y**
Enter the **IPv4 address** that will be used for managing the switch. <***10.29.130.95***>
Enter the **netmask** for the address. <***255.255.255.0***>
Configure the default gateway - **y**
Enter the address for the **default gateway**. <***10.29.130.1***>
Configure advanced options – **n**
Reconfigure feature level – **n**
The next display is a summary of what has been entered and gives you the option to edit it if you need to change something.
Once the configuration is saved, you are presented with a login prompt.

Note: The **name** and **IPv4 address** is the name and address to be entered into your DNS.



Repeat the process for the second VSM virtual machine, using the same admin password.
Answer the **HA role** with **secondary**.
It will ask to reboot and then ask for the domain number. Enter the same domain number as was entered when setting up the first VM.
The system will reboot and come up in standby mode.



From both nodes you should be able to issue the command **show system redundancy status** and receive a display that looks something like this screenshot. This is from the standby N1KV.	
Within the VMM console, remove the ISO file from both virtual machines.	

Work from the primary VSM to continue with the configuration.
Enter the commands shown at right.
<***FastTrack3***> - user-defined name that will be used when defining a logical switch in VMM
<***Fabric-Mgmt***> - user-defined name of the management fabric. Member of just defined logical network.
<***N1KV-pool-15***> - user-defined name for a fabric management IP pool. Multiple pools can be created when managing multiple networks with N1KV.
<***192.168.15.100 192.168.15.199***> - pool of IP addresses to be managed
<***192.168.15.0 255.255.255.0***> - pool IP subnet and netmask
<***192.168.15.1***> - pool default gateway
<***N1KV-MF-Public***> - user-defined network segment name. Different network segments can be defined using different IP pools.
<***15***> - VLAN tag for management network
<***AllAccess***> - port profile created for later use in the definition of logical switch in VMM when configuring the virtual port.
<***N1KV-MF-Uplink***> - uplink port profile created for later use in the definition of the logical switch in VMM.
<***N1KV_Uplink_Policy_FastTrack***> uplink port profile for physical NIC.

```
conf t

feature telnet

nsm logical network  <FastTrack3>
 exit

nsm network segment pool <Fabric-Mgmt>
 member-of logical network  <FastTrack3>
 exit

nsm ip pool template <N1KV-pool-15>
  ip address <192.168.15.100 192.168.15.199>
  network <192.168.15.0 255.255.255.0>
  default-router <192.168.15.1>
  exit

nsm network segment <N1KV-MF-Public>
  member-of network segment pool <Fabric-Mgmt>
  switchport access vlan <1>
  ip pool import template <N1KV-pool-15>
  publish network segment
  exit

port-profile type vethernet <AllAccess>
 no shutdown
 state enabled
 publish port-profile
 exit

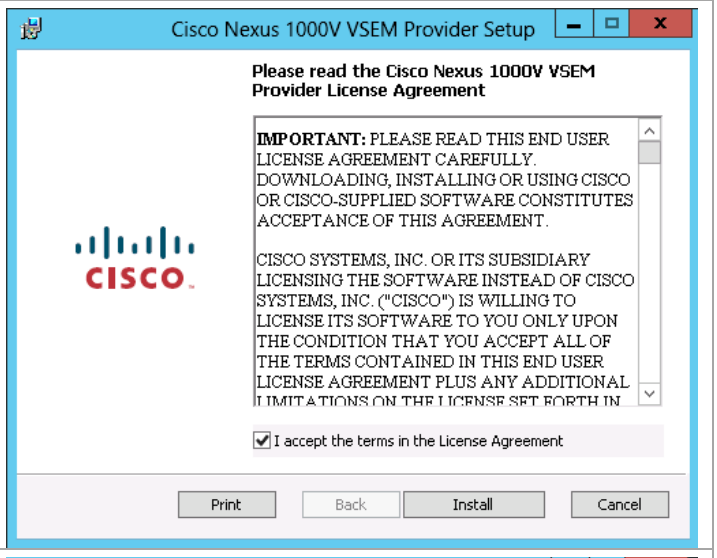
port-profile            type            ethernet
<N1KV_Uplink_Policy_FastTrack>
  channel-group auto mode on mac-pinning
  no shutdown
  state enabled
  exit

nsm network uplink <N1KV-MF-Uplink>
  import                          port-profile
<N1KV_Uplink_Policy_FastTrack>
  allow network segment pool <Fabric-Mgmt>
  system network uplink
  publish network uplink
  exit

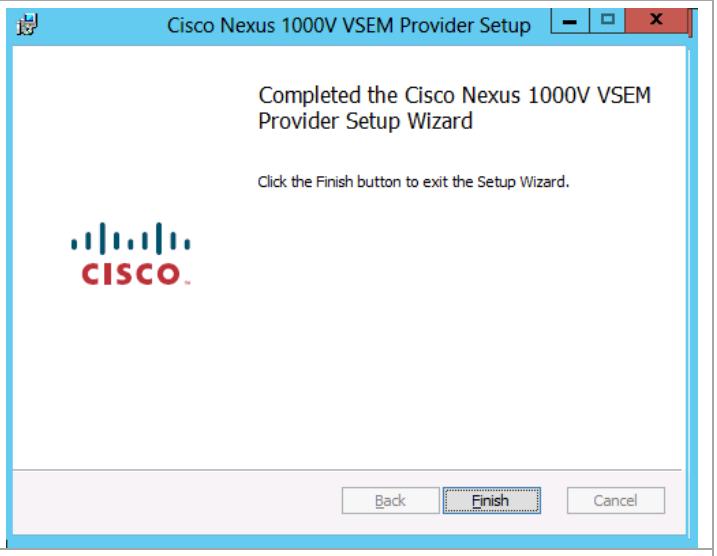
copy running-config startup-config
```

Configure Virtual Switch Extension Manager in VMM

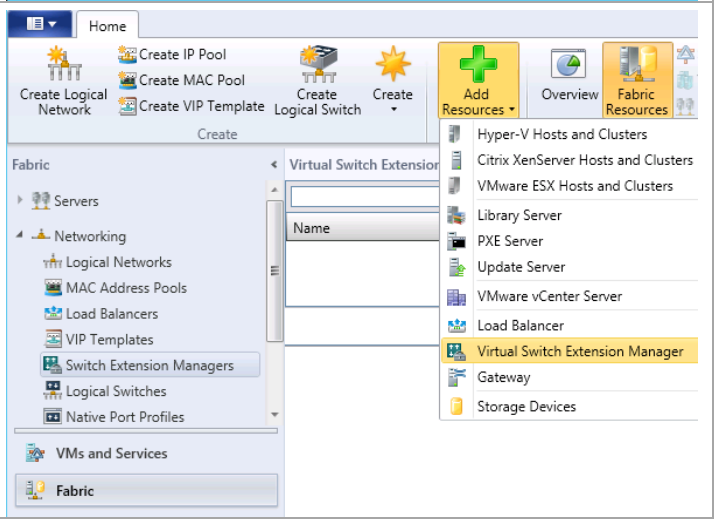
On the Virtual Machine Manager virtual machine that is currently running the highly available Virtual Machine Manager service, install the Cisco Nexus 1000V switch extensions by running Nexus1000V-VSEMProvider-5.2.1.SM1.5.1.0.msi from an elevated PowerShell or command window.
Select the check box by the **I accept the terms in the Licensing Agreement** statement.
Click **Install** to continue.

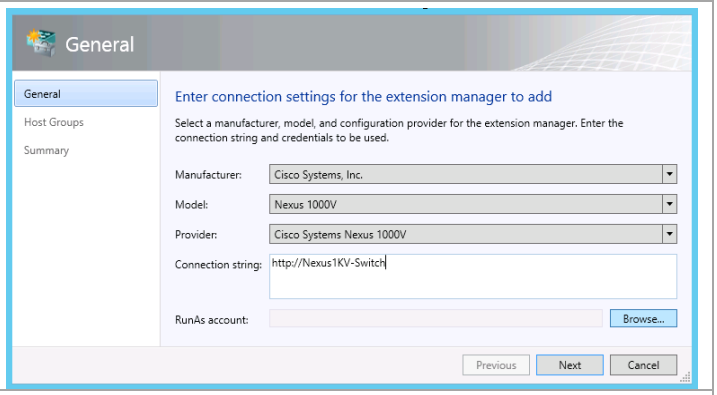
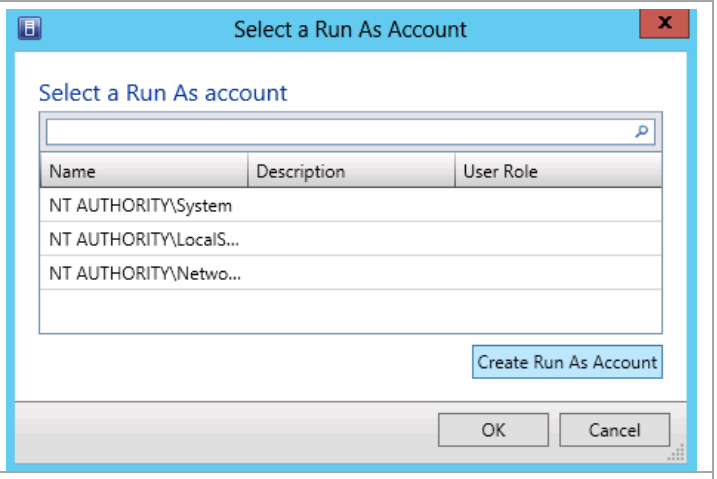
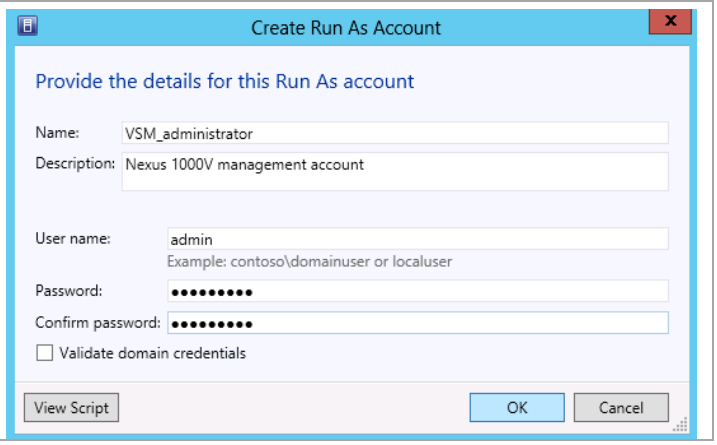


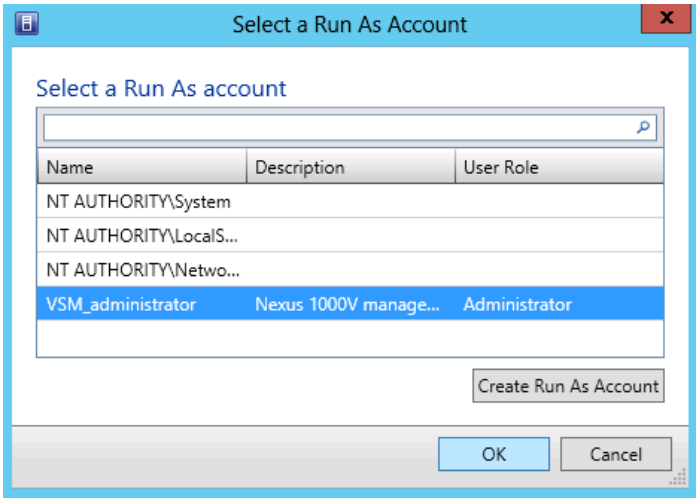
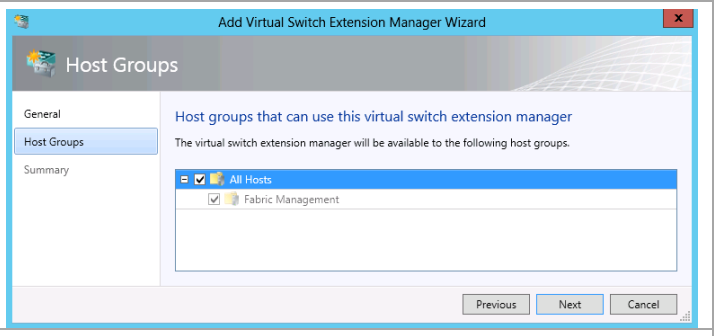
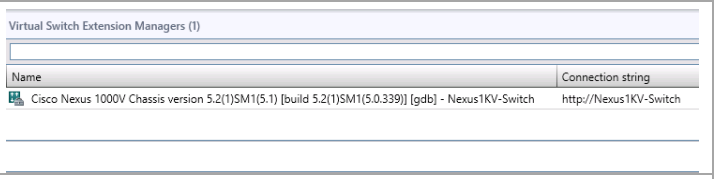
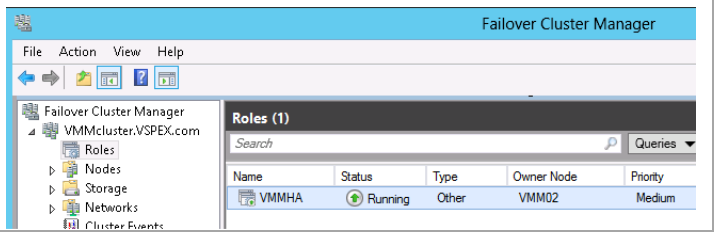
A status screen will show the progress of the installation.
Click **Finish** to complete the installation.
This may cause a loss of connection to the VMM console and you will have to reconnect.



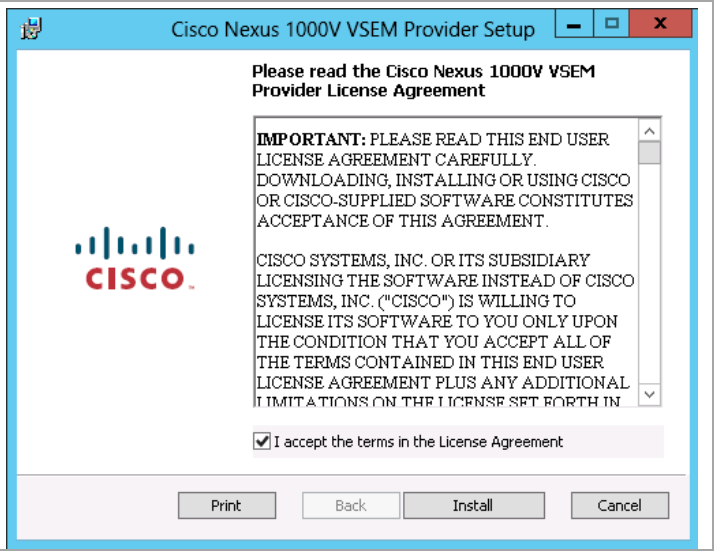
In the VMM console, select **Fabric**. Under **Networking**, select **Switch Extension Manager**.
Click **Add Resources** and from the drop-down menu select **Virtual Switch Extension Manager.**



In the **Enter connection setting for the extension manager to add** dialog window, enter **http://*<Nexus1KV-Switch>*** for accessing the Nexus 1000V VSM you created earlier. This is the name you provided for the switch and for which you created the DNS entry, not the name of the virtual machine. Click **Browse** to enter credentials for connecting to the VSM.	
In the **Select a Run As Account** dialog window, click on the **Create Run As Account**.	
In the **Provide the details for this Run As account** dialog window, enter a **Name** to be used for this account. Optionally, enter a **Description**. In the **User name** box, enter the user ID for the administrative account (admin) created on the Nexus 1000V virtual machine. Enter and confirm the **Password** for the administrator account on the Nexus 1000V virtual machine. Ensure the check box by **Validate domain credentials** is cleared, as this account is not in AD. Click **OK** to continue.	

In the **Select a Run As account** dialog window, select the newly create VSM administrator account. Click **OK** to continue. Click **Next** when you return to the **General** screen to move to the **Host Groups** screen.	
Select the box next to the **All Hosts** group. Click **Next** to continue. The next screen is a summary screen. Validate that entries were properly made. Click **Finish** when you have the correct values.	
You will now see a listing for the Virtual Switch Extension Manager within VMM.	
Using the **Cluster Failover Manager** on the VMM cluster, move the highly available Virtual Machine Manager instance to the second Virtual Machine Manager node.	

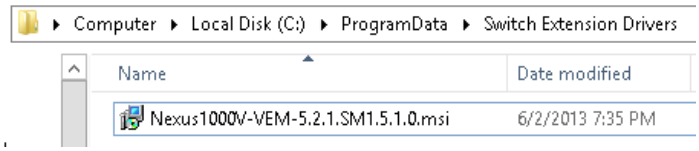
Connect to the second Virtual Machine Manager node. Install the Cisco Nexus 1000V switch extensions by running Nexus1000V-VSEMProvider-5.2.1.SM1.5.1.0.msi.
Select the checkbox by **I accept the terms in the License Agreement** and click **Install**. Click **Finish** when the installation completes.



Copy Virtual Ethernet Module Installation Packager to the VMM Virtual Machines

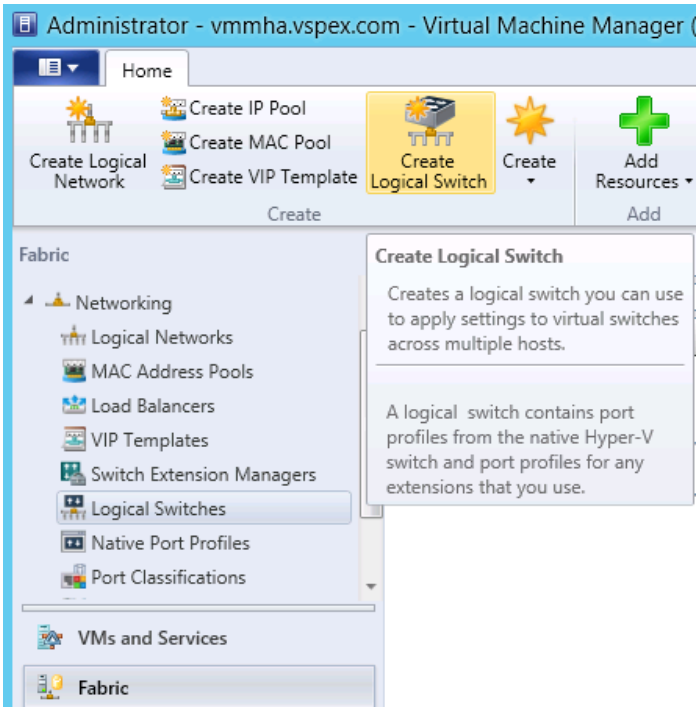
▶ Perform the following procedure on each Virtual Machine Manager node.

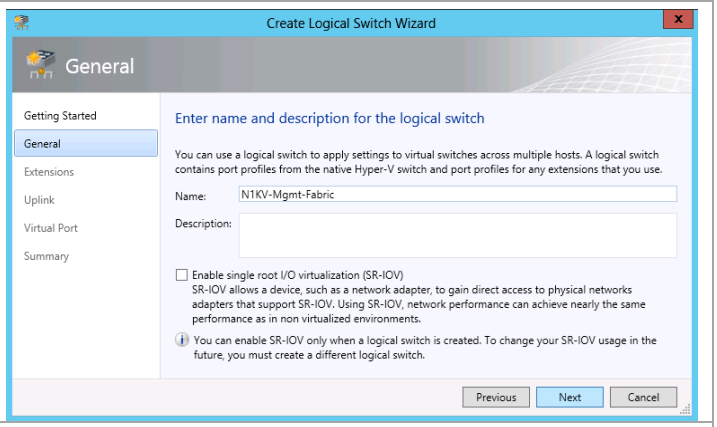
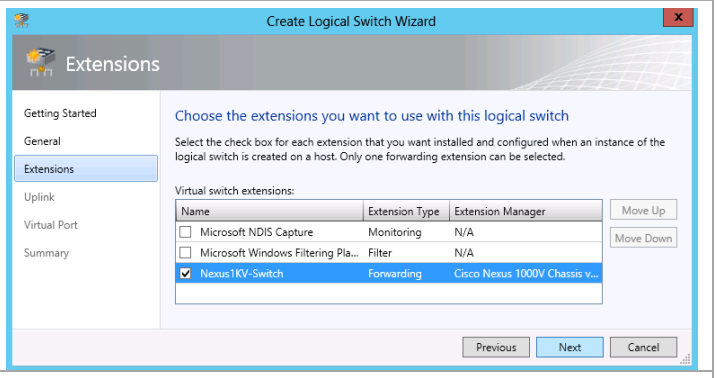
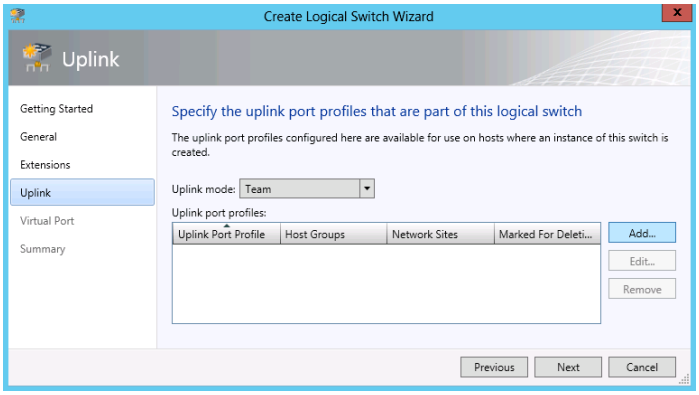
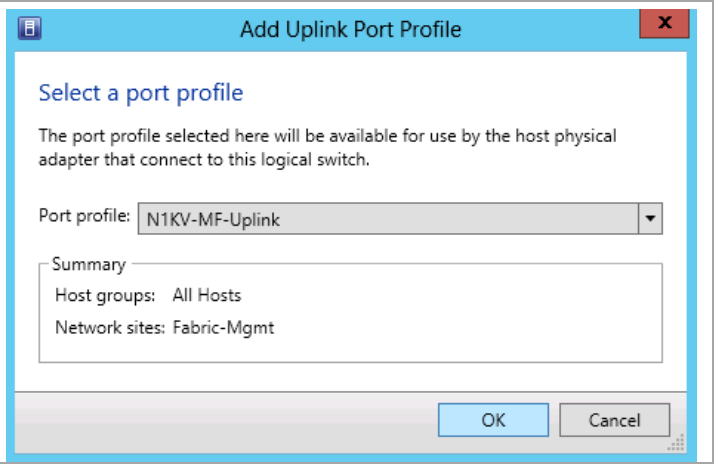
Copy Nexus1000V-VEM-5.2.1.SM1.5.1.0.msi to the following directory on each Virtual Machine Manager server:
C:\ProgramData\Switch Extensions Drivers

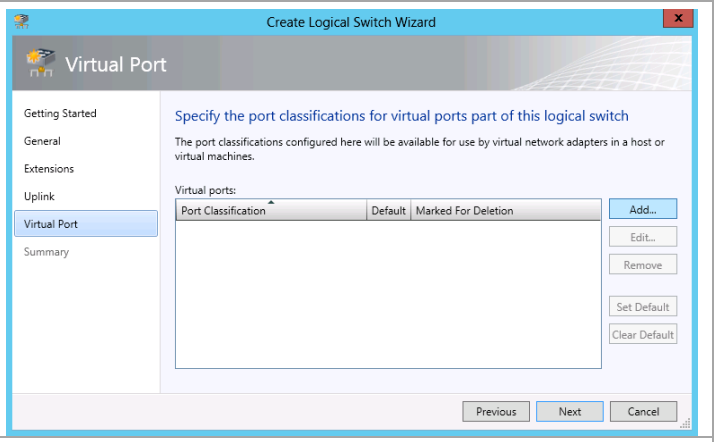
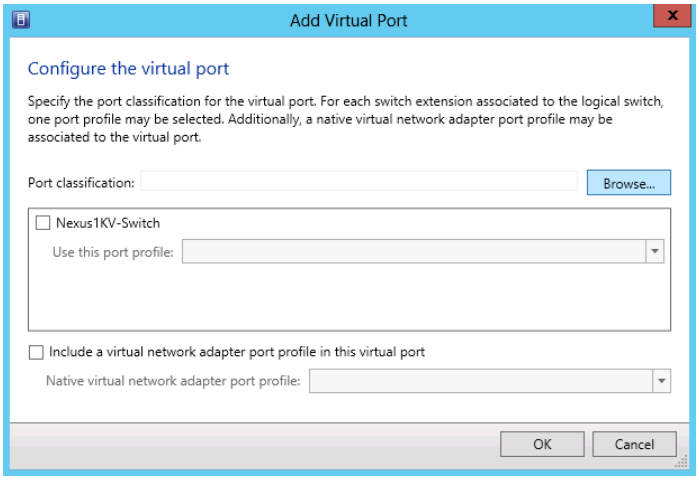
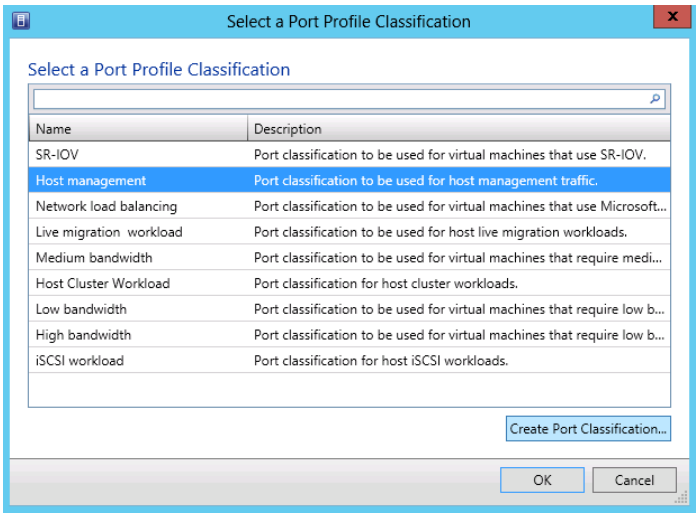


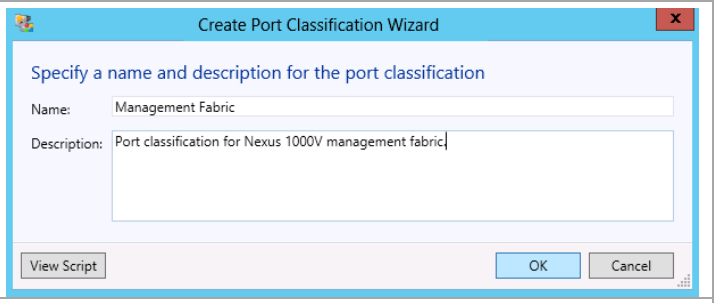
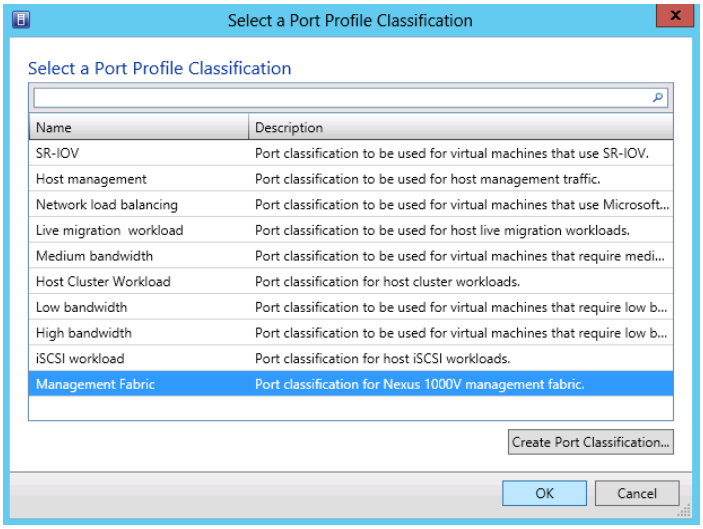
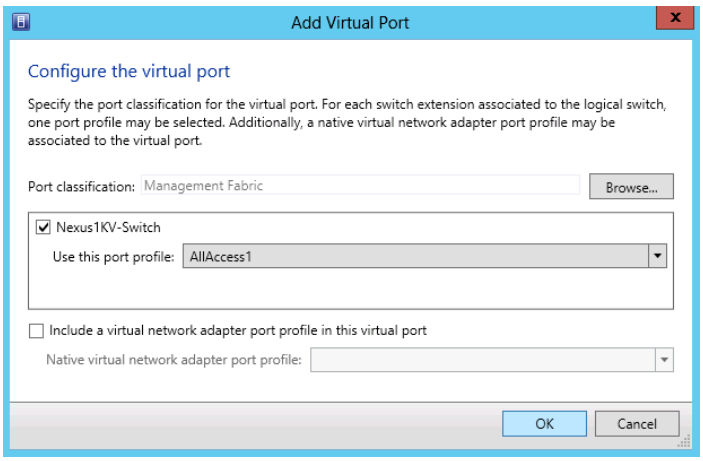
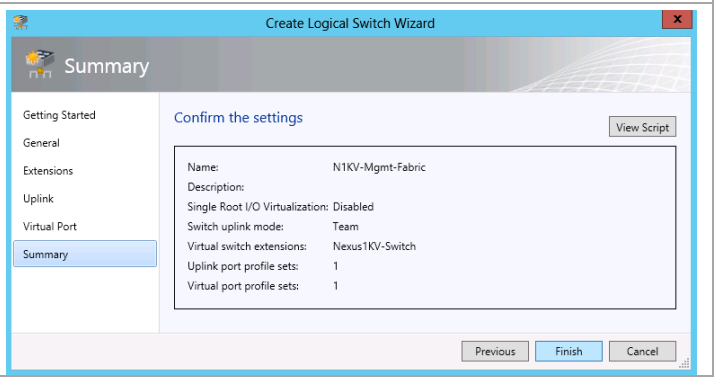
Configure a Logical Switch in VMM

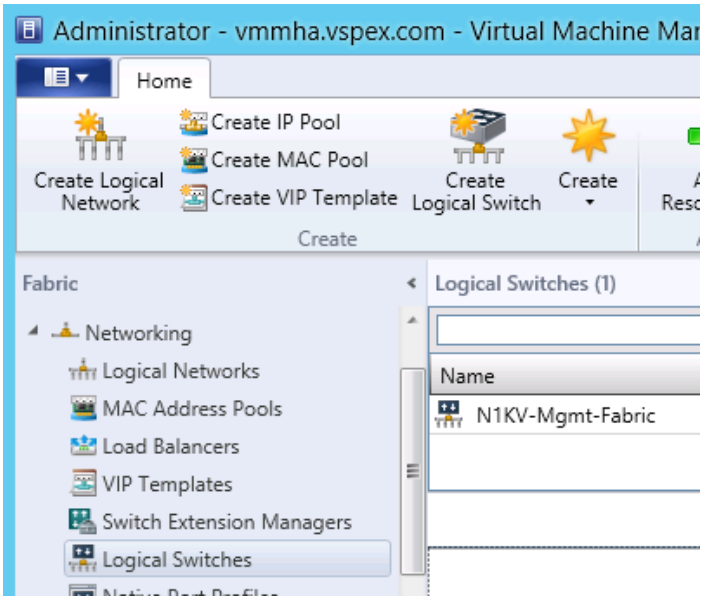
In the VMM console, select **Fabric**. Under **Networking** select **Logical Switches**.
Click on **Create Logical Switch** in the ribbon.
Click **Next** on the Getting Started page.



Enter a **Name** and optional description for the logical switch being created. Click **Next** to continue.	
On the **Extensions** dialog window, clear the check box by Microsoft Windows Filtering Platform. Select the check box by ***<Nexus1KV-Switch>***. Click **Next** to continue.	
In the **Uplink** dialog window, select **Team** from the **Uplink mode** drop-down menu. Click **Add…** to select the uplink profile previously created.	
Select the **Port profile** that was created earlier when configuring VSM. Click **OK** to continue. Click **Next** on the **Uplink** dialog window.	

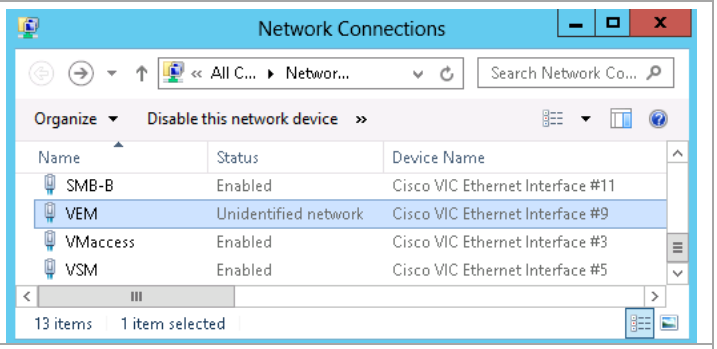
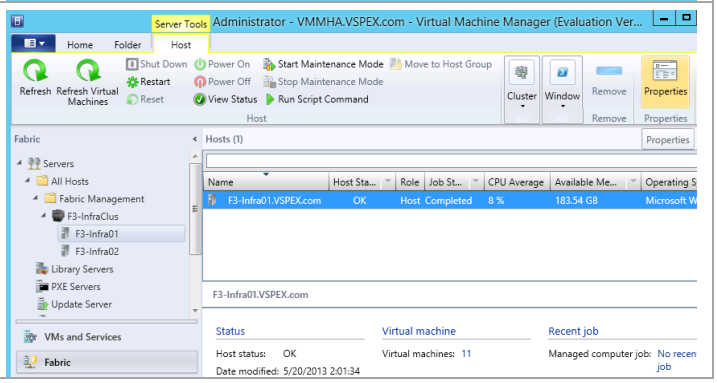
In the **Virtual Port** dialog window, click **Add…**	
In the **Configure the virtual port** dialog window, click **Browse…**	
In the **Select a Port Profile Classification** dialog window, select **Host Management**. Click **Create Port Classification…**	

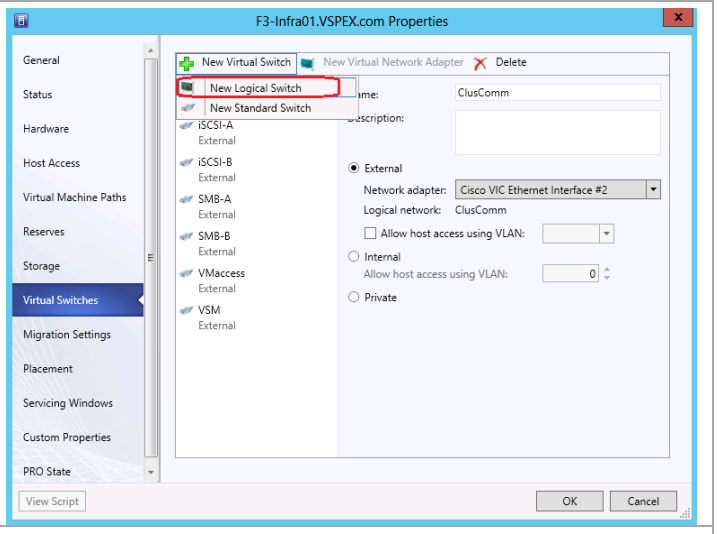
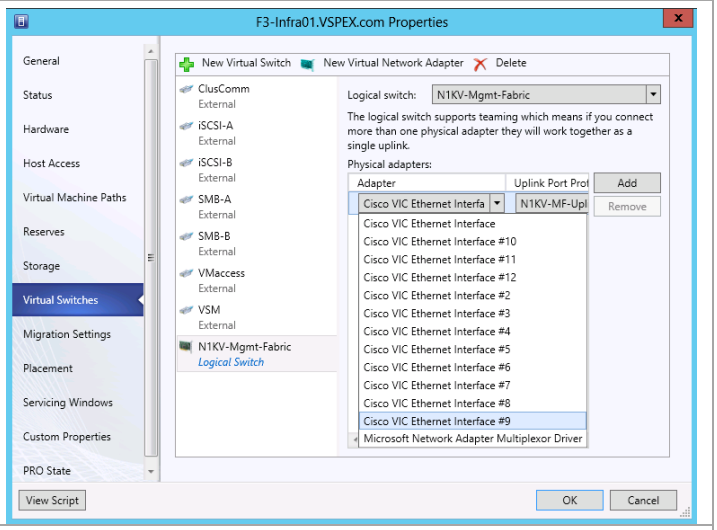
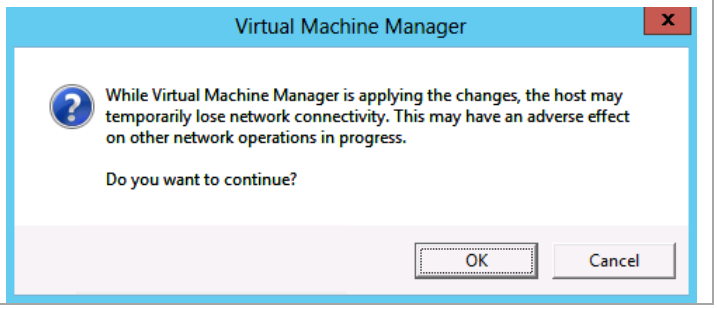
Enter a **Name** and **Description** to be used for the port classification. Click **OK** to continue.	
Select the just created port profile classification, and click **OK** to continue.	
Back in the **Configure the virtual port** dialog window, select the check box by your virtual switch, and select the port profile created earlier from the drop-down box. Click **OK** to continue. That takes you back to the **Virtual Port** dialog window. Click **Next** in that window to bring up a **Summary** window.	
In the **Summary** window, review your inputs. Click **Finish** to continue.	

Back in the VMM console, you will see the newly created Logical Switch.	

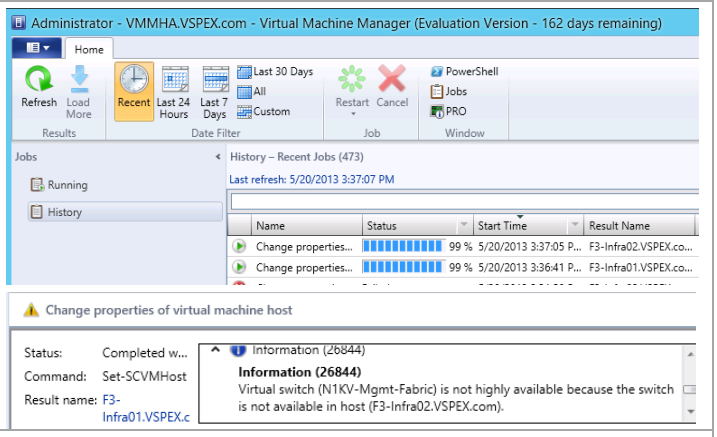
Create the Logical Switch on the Hyper-V Hosts

▶ Perform the following on each clustered Hyper-V node used for Fabric Management.

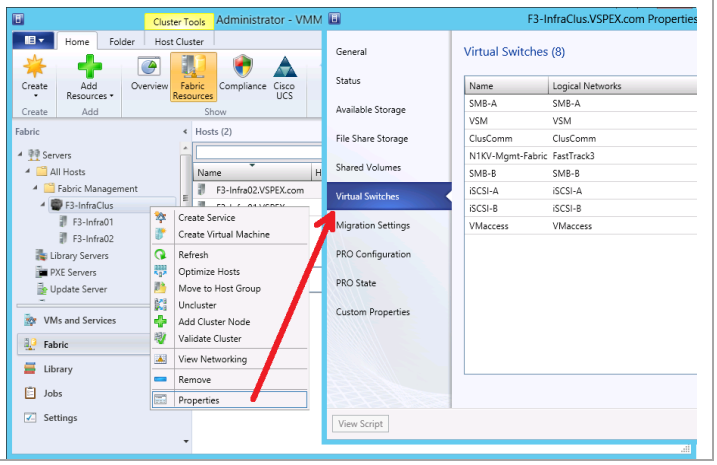
On the physical host, type **ncpa.cpl** from a PowerShell or command window to launch **Network Connections**. Find the network adapter that will be used for the new logical switch and note the interface number (#9 in the shown screen shot). This is quite likely to be different on each node.	
From the VMM console, select **Fabric**. Expand **Servers > All Hosts > <*host-group*>** Select the host from the previous step. Select **Properties**.	

In the **Properties** window, select **Virtual Switches** from the left-hand column. Click **New Virtual Switch** and select **New Logical Switch** from the drop-down menu.	
Select the new logical switch in the center panel. Select the Cisco VIC Ethernet Interface with the number obtained in the first step of this process. Click **OK** to continue.	
Click **OK** in the warning message to continue. Repeat this process for each host in the cluster before proceeding to the next step.	

Click **Jobs** to monitor the jobs progress. When completed it will show a status of **Completed w/ Info** until the logical switch is installed on all hosts in the cluster.

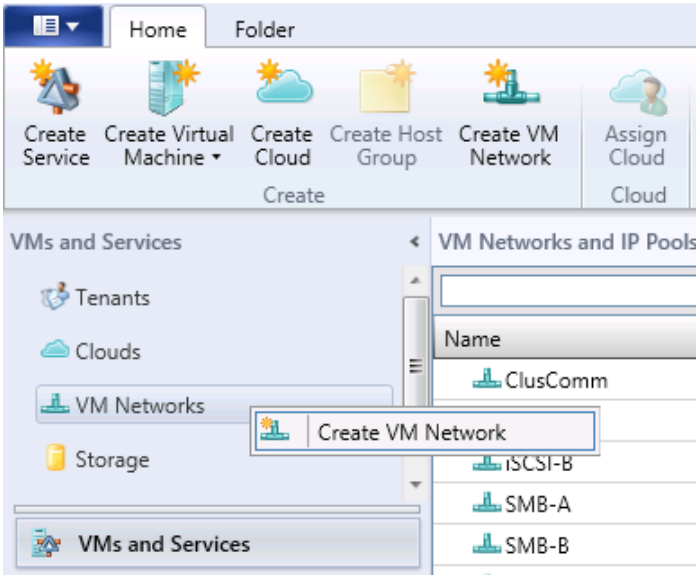


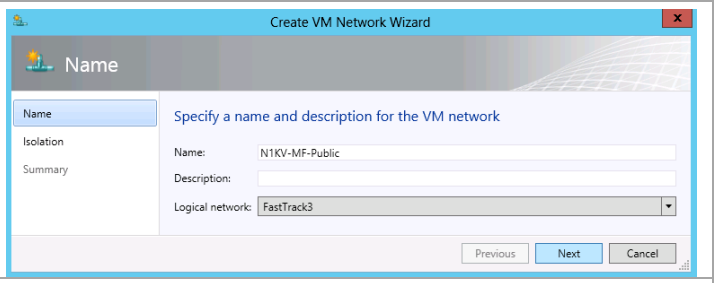
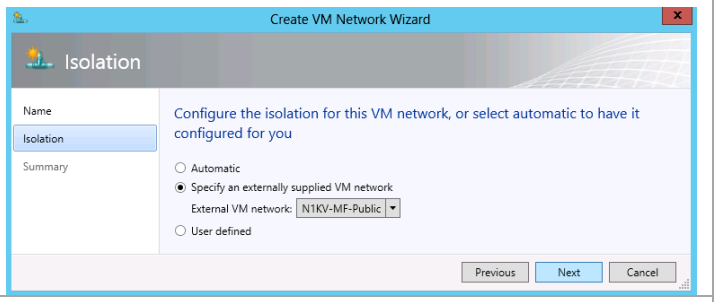
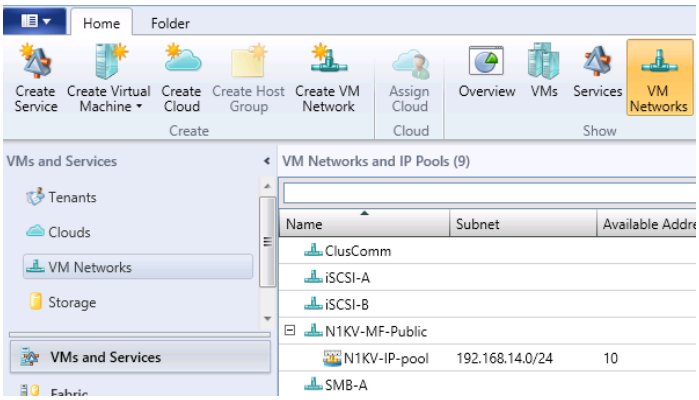
Open the **Properties** of the cluster and select **Virtual Switches** to see that the newly created logical switch is available to the cluster.
Click **Cancel** to exit the cluster properties window.



Create a VM Network

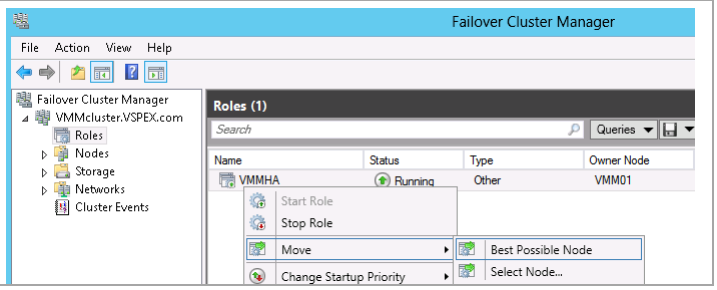
In the Virtual Machine Manager console, select **VMs and Services**. Right-click **VM Networks** and select **Create VM Network**.



Enter a **Name** for the network. Ensure that the **Logical network** you are deploying is selected. Click **Next** to continue.	
In the **Isolation** dialog window, click the radio button by **Specify an externally supplied VM Network**. From the drop-down list for External VM network, select the network segment defined when configuring the VSM. Click **Next** to continue. On the **Summary** window, click **Finish**.	
You can see the definition of the VM network in the VMM console.	

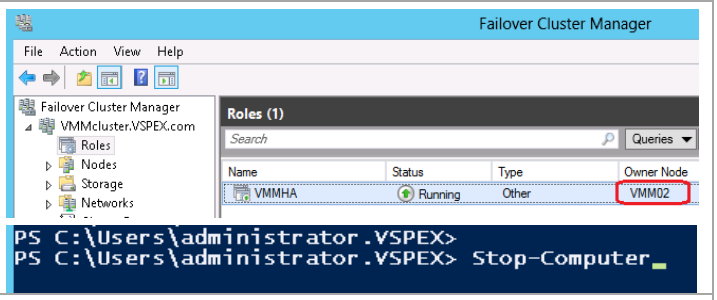
Configure the Virtual Machine Manager Virtual Machine Properties

This example shows how to add the network managed by the Nexus 1000V to the VMM virtual machines. The same procedure would be used to add network adapters on this managed network to other virtual machines.

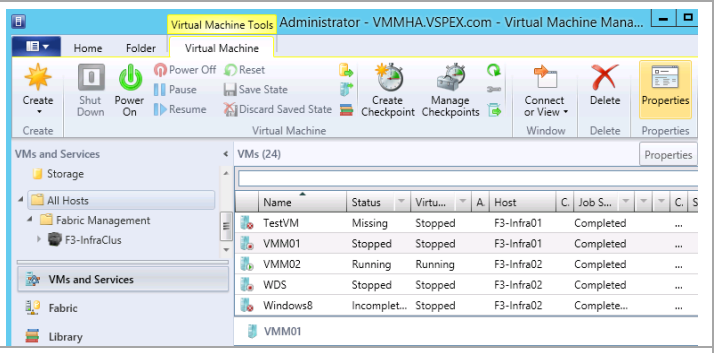
Login to the first Virtual Machine Manager virtual machine. Using Failover Cluster Manager console, identify the owner of the highly available Virtual Machine Manager instance. Move the Virtual Machine Manager instance to the second node, if it is owned by the first node, by right-clicking on the role, selecting **Move > Best Possible Node**.	

When you see the role has successfully moved to the other node, shutdown the first VMM virtual machine by running following PowerShell command:

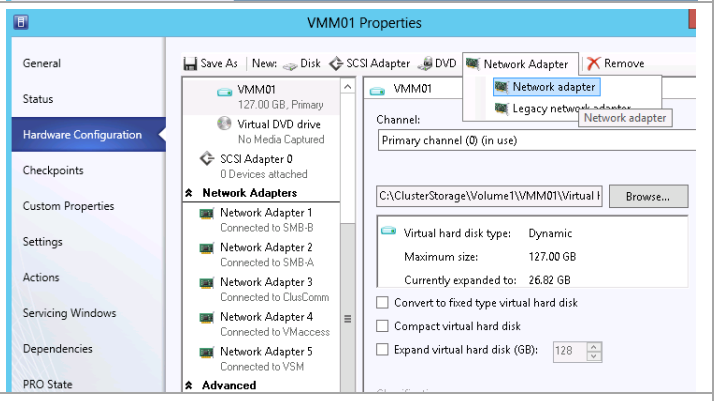
```
Stop-Computer
```



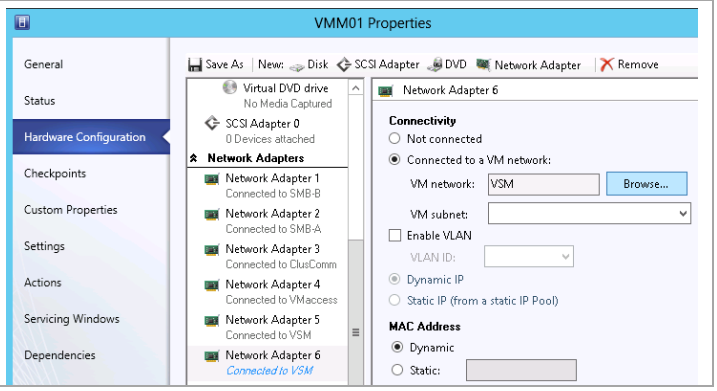
Log into the second VMM virtual machine and start the Virtual Machine Manager console. Select **VMs and Services**. Click **All hosts**.
Click the first Virtual Machine Manager virtual machine that is in a stopped state and select **Properties**.

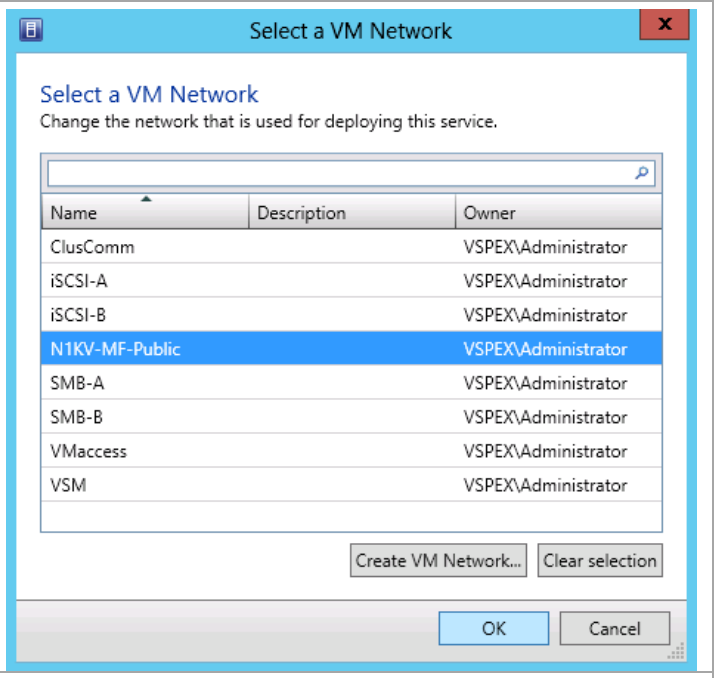
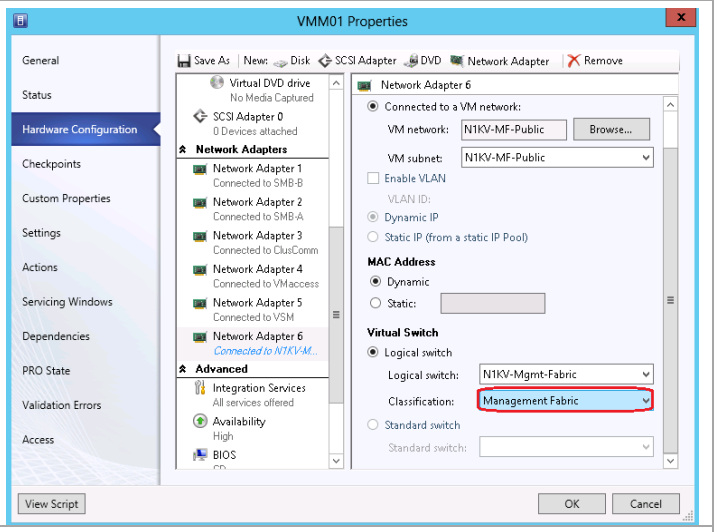
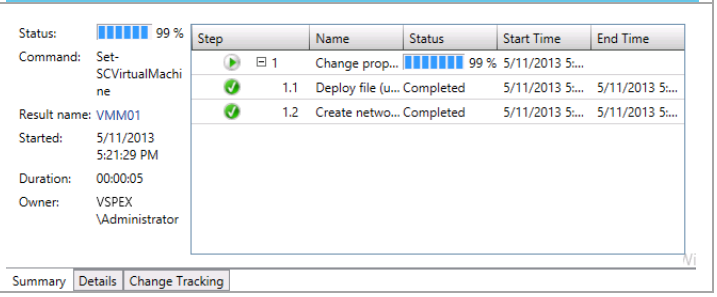


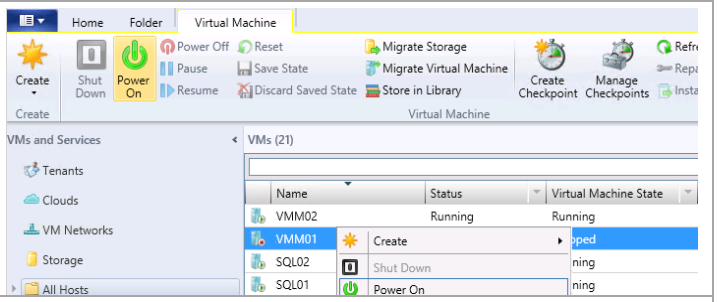
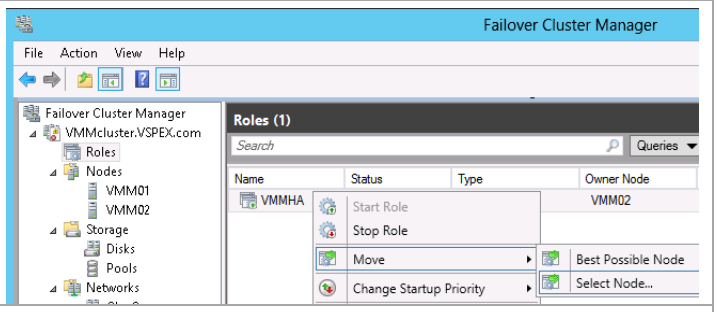
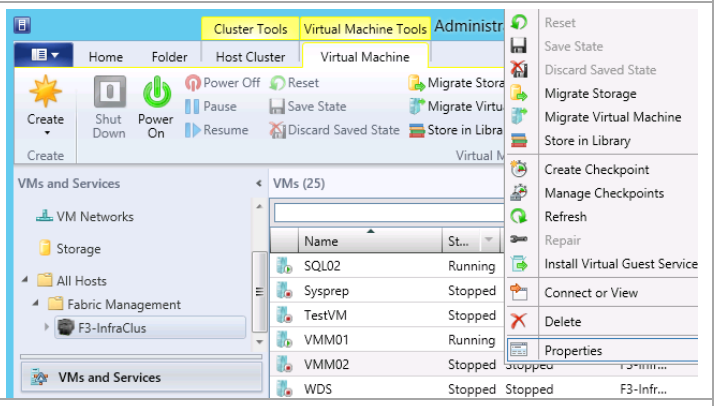
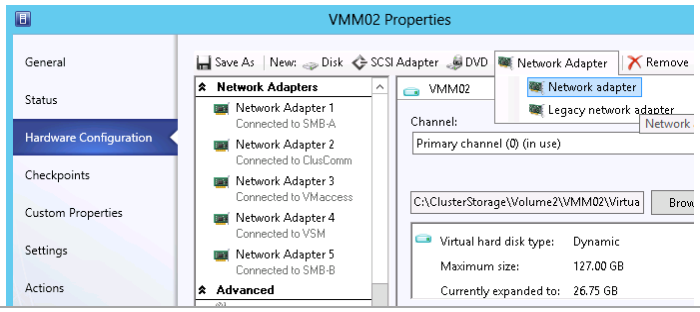
Add a net network adapter to the VMM virtual machine by selecting **Hardware Configuration** from the left column. Click on **Network Adapter** and select **Network Adapter** from the drop-down list.

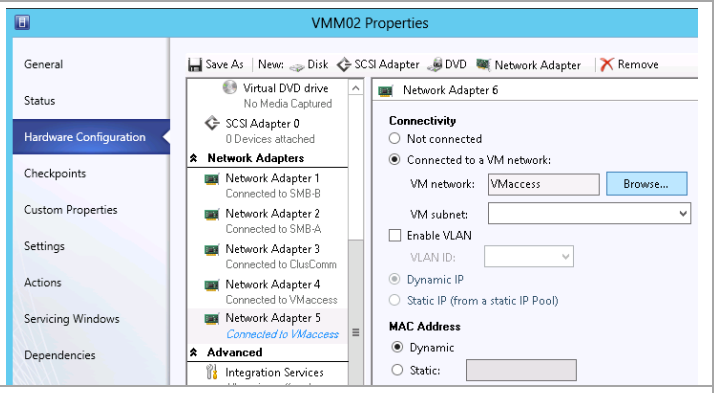
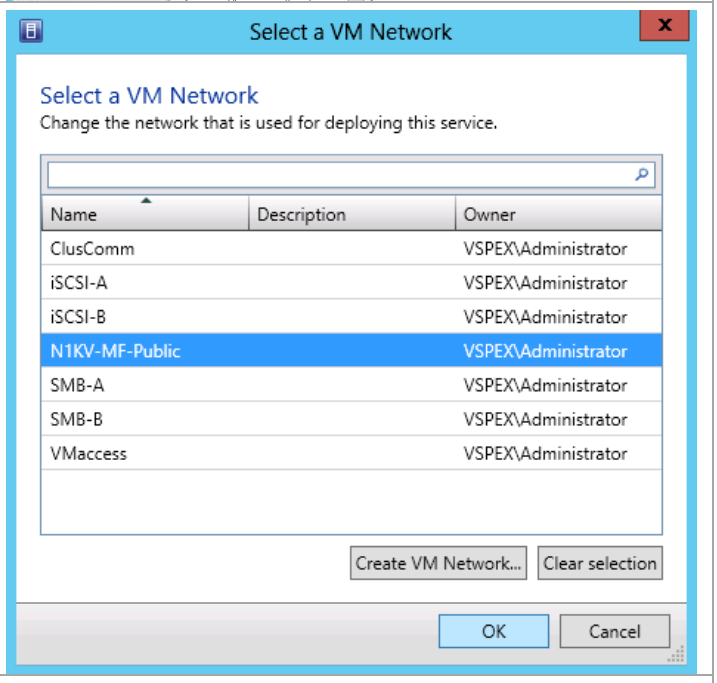
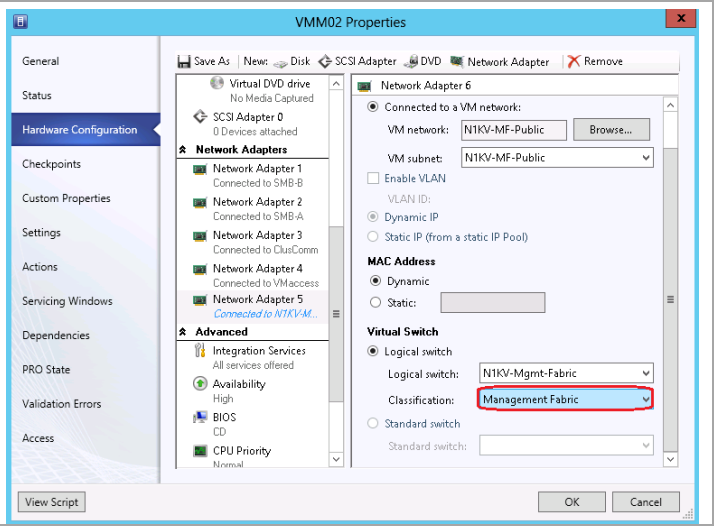


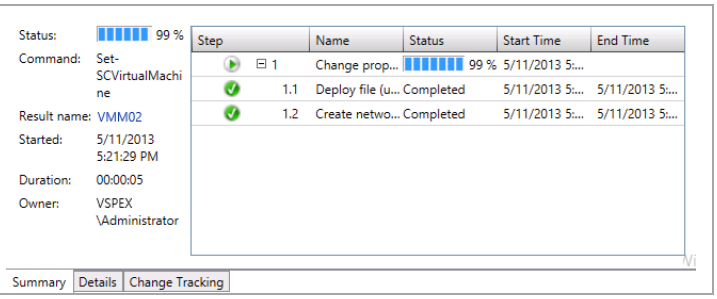
A new adapter will be created and added to the end of the list of existing adapters in the center pane. Select the newly created adapter.
Click the radio button by **Connected to a VM Network**.
Click **Browse…**



In the **Select a VM Network** dialog window, select the VM network created in the previous steps. Click **OK** to continue.	
Select **Management Fabric** from the Classification drop-down list under **Virtual Switch**. Click **OK** to continue.	
Select **Jobs** and monitor the job completion progress.	

Start the VMM virtual machine by right-clicking on the VM and selecting **Power On**.	
Log into the first VMM virtual machine. Using the Failover Cluster Manager console, move the highly available VMM role to the first VMM virtual machine.	
Stop the second VMM virtual machine by issuing the following PowerShell command: `Stop-Computer -ComputerName <VMM02> -Force`	
Start the VMM console and select **VMs and Services**. Expand **All Hosts**. Right-click the stopped VMM virtual machine and select **Properties**.	
Select **Hardware Configuration**. Scroll to **Network Adapters** in the center pane. Click **Network Adapter** and select **Network adapter** from the drop-down list to add a new network adapter to the virtual machine.	

A new adapter will be created and added to the end of the list of existing adapters in the center pane. Select the newly created adapter. Click the radio button by **Connected to a VM Network**. Click **Browse…**	
In the **Select a VM Network** dialog window, select the VM network created in the previous steps. Click **OK** to continue.	
Select **Management Fabric** from the drop-down list under **Virtual Switch**. Click **OK** to continue.	

Select **Jobs** and monitor the job completion progress. When the job completes, start the VMM virtual machine.	

16 EMC Integration Components

16.1 EMC Software Installation Locations

There are several EMC management software components which are recommended to be installed in the Fast Track environment. Some of the components, specifically ESI PowerShell and Navisphere CLI can be installed on a configuration workstation to assist in the initial setup of the Fast Track infrastructure. After the initial deployment, a management VM can be configured to host all of the EMC software components. The list below outlines the components and their installation locations as tested during the Fast Track validation.

- EMC Navisphere CLI (naviseccli)
  - Configuration Workstation
  - EMC Management VM
- EMC Storage Integrator PowerShell Toolkit
  - Configuration Workstation
  - EMC Management VM
- EMC SMI-S Provider
  - EMC Management VM
- EMC Storage Integrator Service
  - EMC Management VM
- EMC System Center Operations Manager Management Packs
  - SCOM Server

16.2 Install and Configure the EMC Storage Integrator Management Pack for System Center Operations Manager

The EMC Storage Integrator System Center Operations Manager (ESI SCOM) Management Packs and the ESI Service work in conjunction with Microsoft System Center Operations Manager for centralized discovery and monitoring of supported EMC storage systems and storage-system components. The ESI Service views and reports information to SCOM regarding all registered EMC storage systems and storage-system components. The ESI SCOM Management Packs integrate EMC storage systems with SCOM by providing the following functionality:

- Consolidated and simplified dashboard view of storage entities
- Health status and events from the storage system
- Alerts for possible problems with disk drives, power supplies, storage pools and other types of physical and logical components in SCOM

The installation and configuration of ESI and the SCOM management pack includes several steps outlined below:

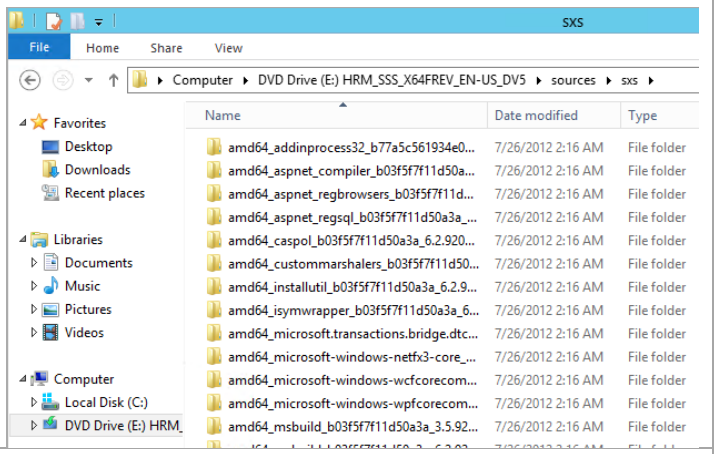
- Install the ESI Service and ESI Service PowerShell Toolkit
- Register the VNX array with the ESI Service
- Create an ESI Service user for the SCOM Management Pack RunAs Account
- Install the ESI SCOM Management Packs
- Import the ESI SCOM Management Packs
- Create an ESI RunAs Account and associating the account with a Profile
- Set Overrides for the EMC SI Service Discovery

Additional information can be found in the EMC Storage Integrator online help file, specifically the "ESI Service and ESI SCOM Management Packs" section.

16.3 Install the ESI Service and ESI Service PowerShell Toolkit

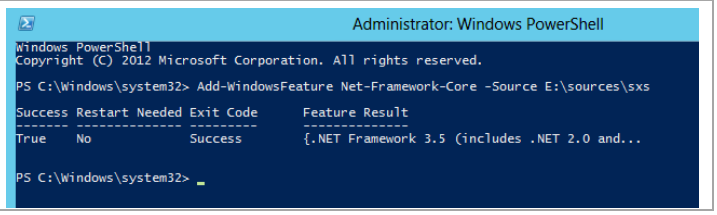
▶ Perform the following steps on the **EMC Management** virtual machine.

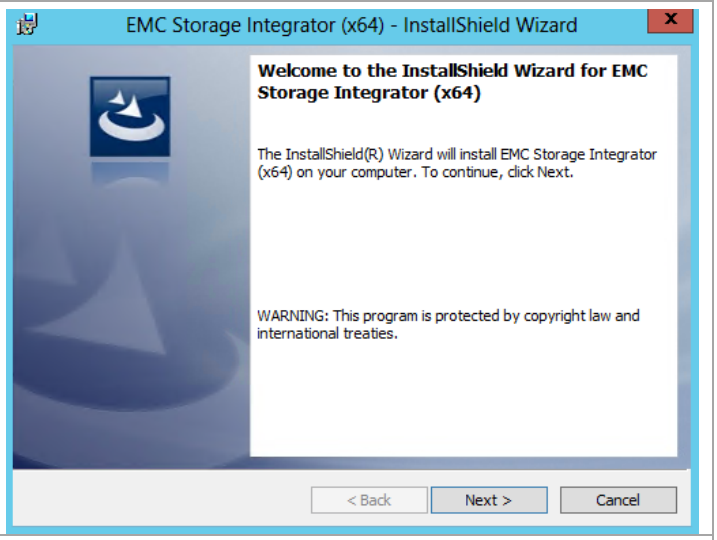
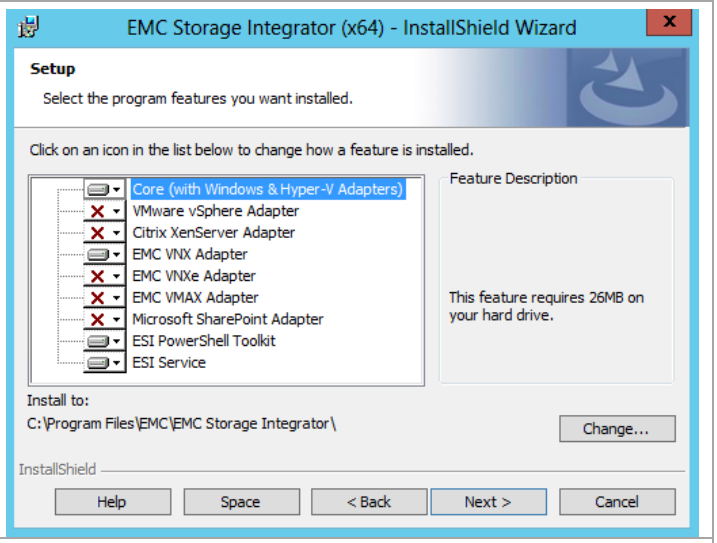
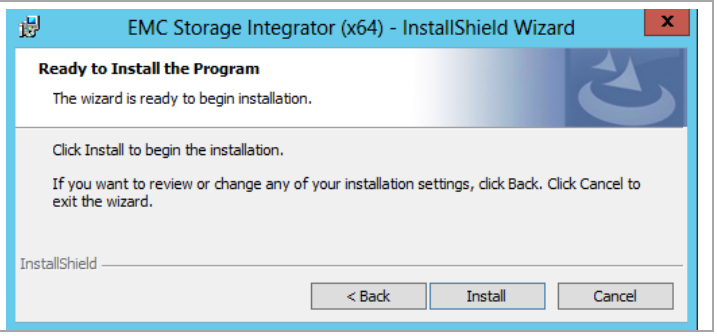
Obtain a copy of the Windows Server 2012 source files. The source files can be found on the installation media in the "\sources\sxs" folder



Install .Net Framework 3.5 using the source files from the previous step. From PowerShell run the following command:

```
Add-WindowsFeature Net-Framework-Core -Source E:\sources\sxs
```



Run the EMC Storage Integrator (x64) installer	
Select the following components • Core (with Windows & Hyper-V Adapters) • EMC VNX Adapter • ESI PowerShell Toolkit • ESI Service Click **Next**	
Select **Install**	

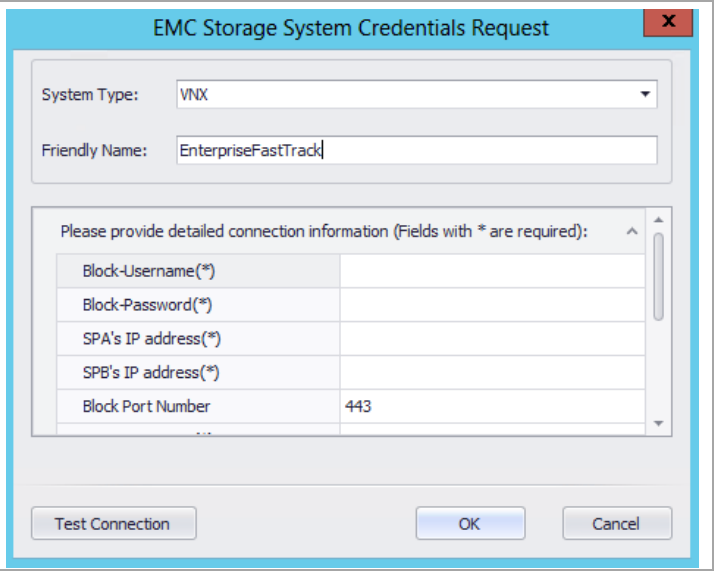
Register the VNX with the ESI Service

▶ Perform the following steps on the **EMC Management** virtual machine.

From PowerShell command window run ***Add-EmcSystem***
When prompted choose the appropriate **System Type:**

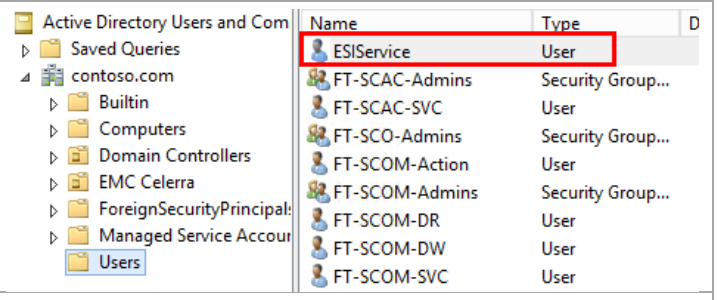
- "VNX" for a Unified System
- "VNX-Block" for a block only system

Enter the credentials and IP address information.
Select **Add host Key If Missing**
Select **Test Connection** to ensure connectivity
Select **OK**



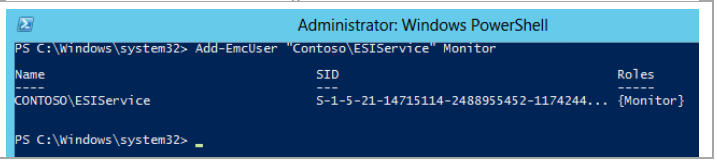
Create an ESI Service User for the SCOM Management Pack Run As Account

Create an ESI Service user account within the Active Directory domain. The user does not need administrative access to the host running the ESI Service.



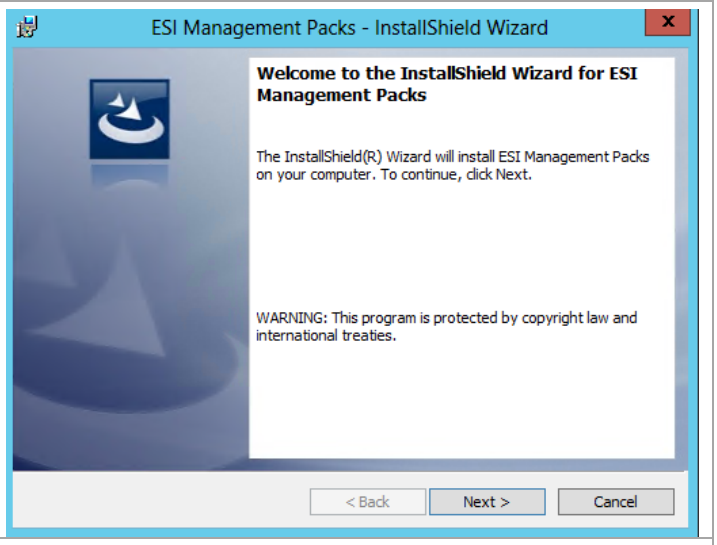
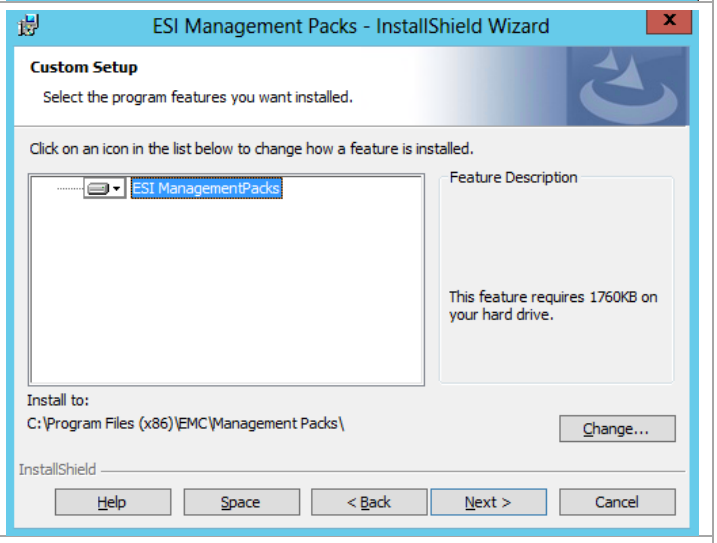
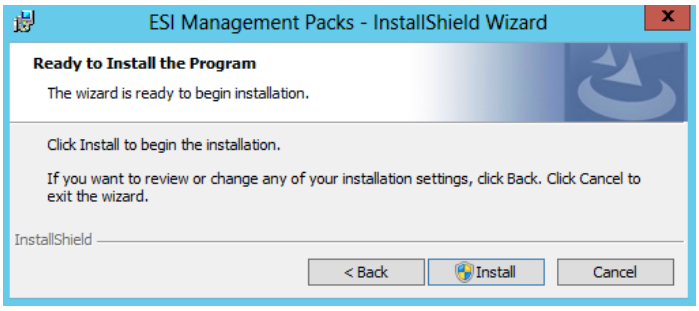
From the host running the ESI Service, run the ***Add-EMCUser*** PowerShell command and give the ESI Service user "Monitor" access:

```
Add-EmcUser "Contoso\ESIService" Monitor
```



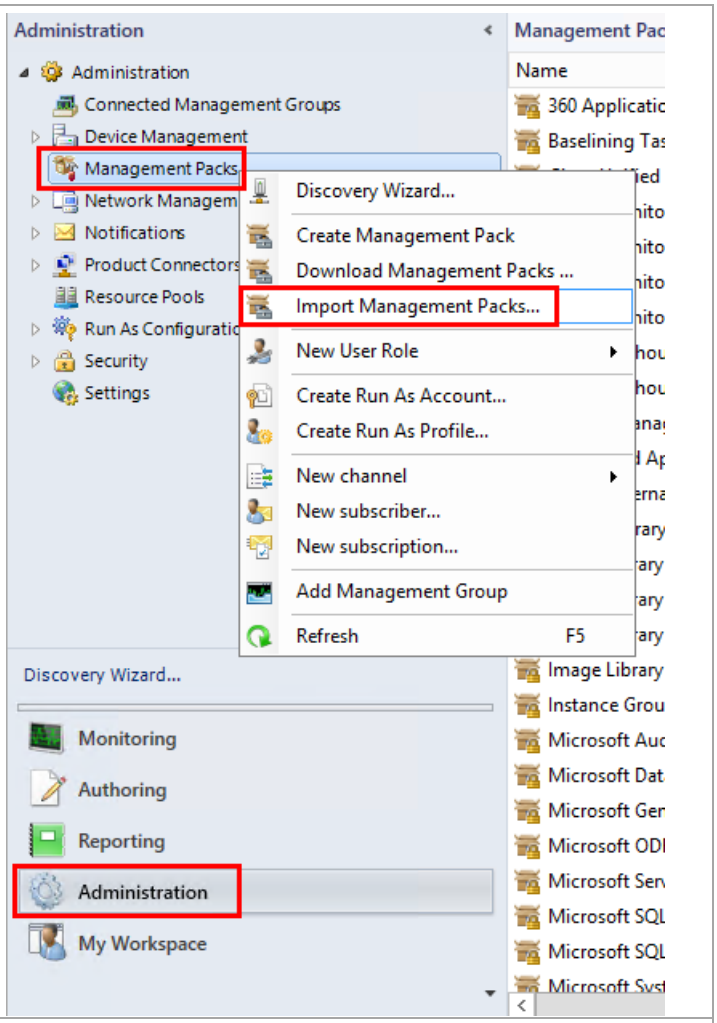
16.4 Install the ESI SCOM Management Packs

▶ Perform the following steps on the **SCOM** virtual machine.

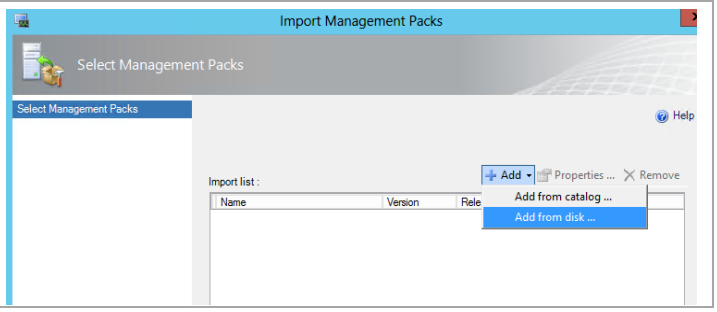
From the SCOM host run the ESI SCOM Management Packs installer	
Select or note the installation location Select **Next**	
Select **Install** and then **Finish**	

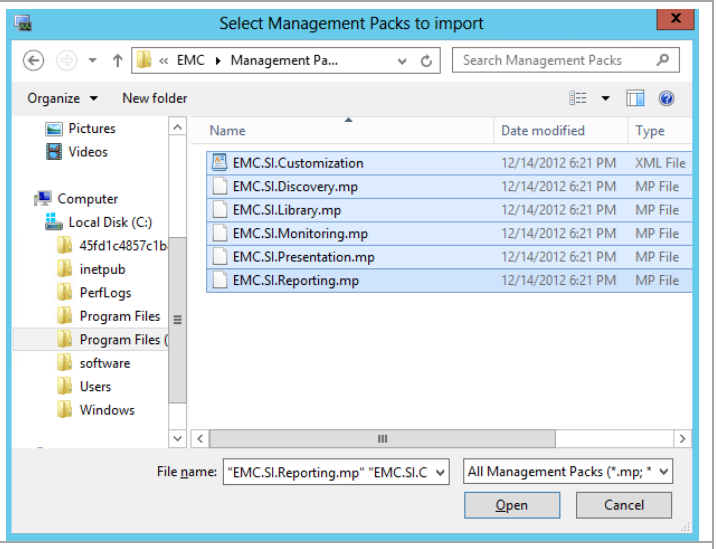
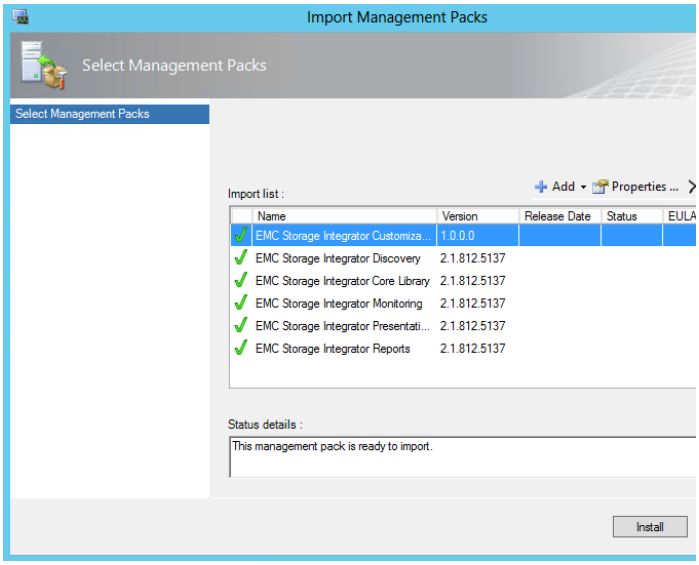
Import the ESI SCOM Management Packs

From within the Operations Manager console go to **Administration** > **Management Packs**
Right click on **Management Packs** and select **Import Management Packs**



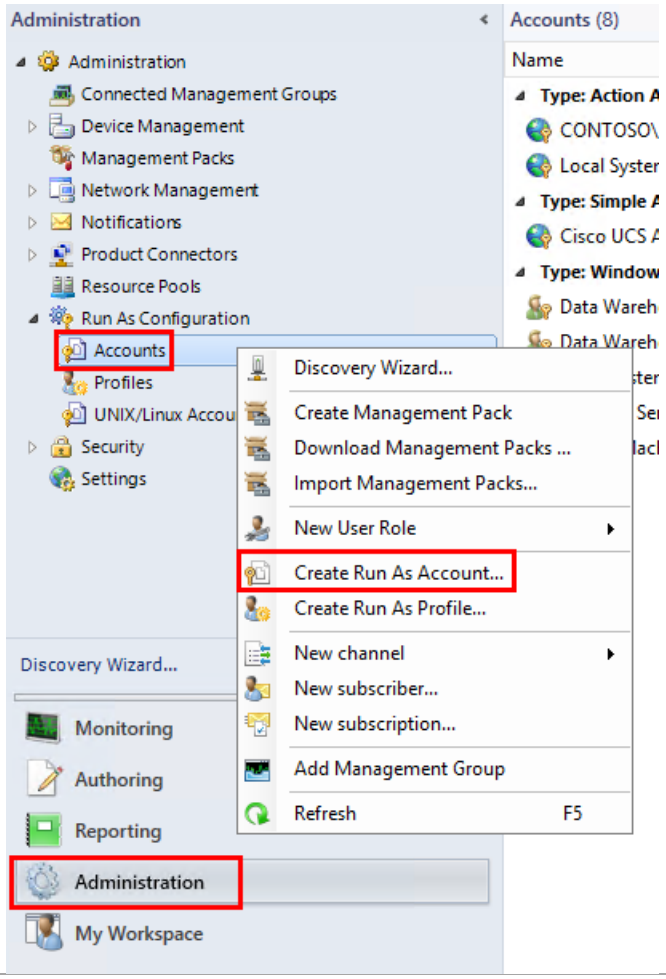
Select **Add** and then **Add from disk ...**



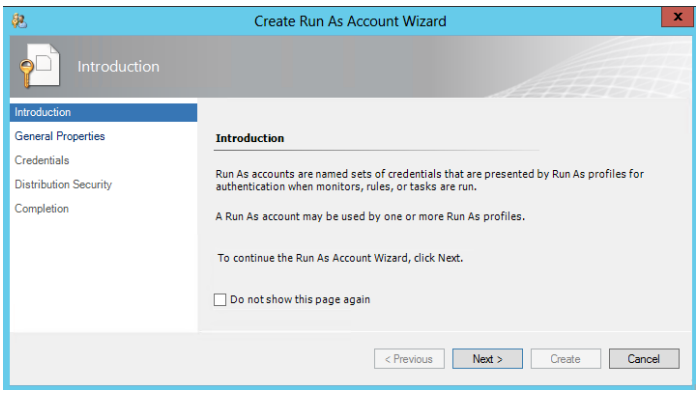
Browse to the management pack installation directory and select the 5 .MP and 1 .XML file in that directory. Select **Open**	
Select **Install** Then **Close** the wizard following successful completion.	

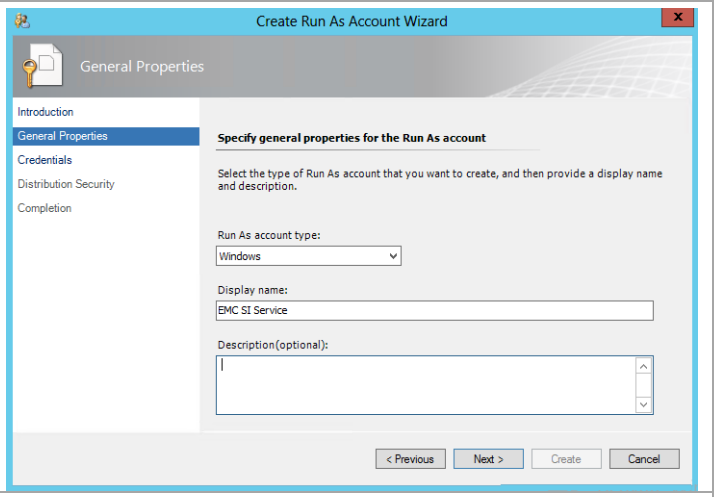
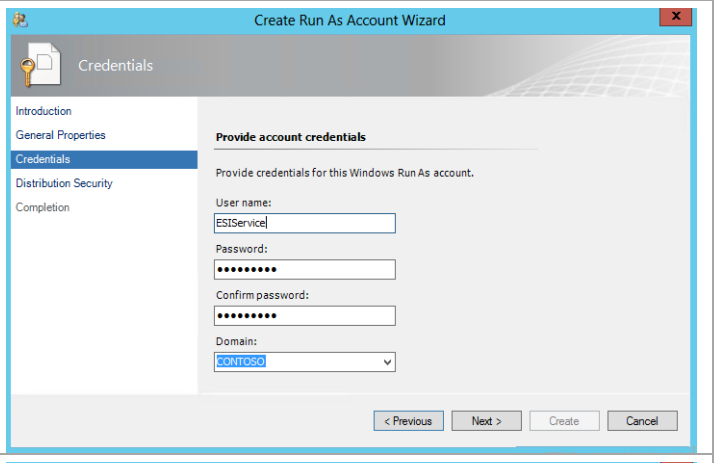
Create ESI Run As Account and Associate with a Profile

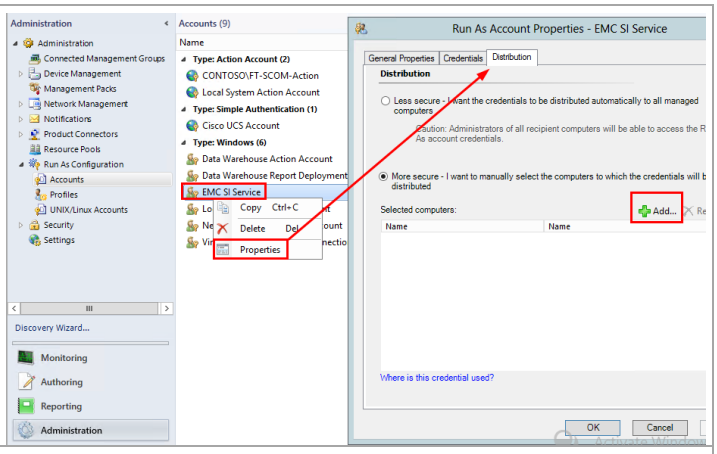
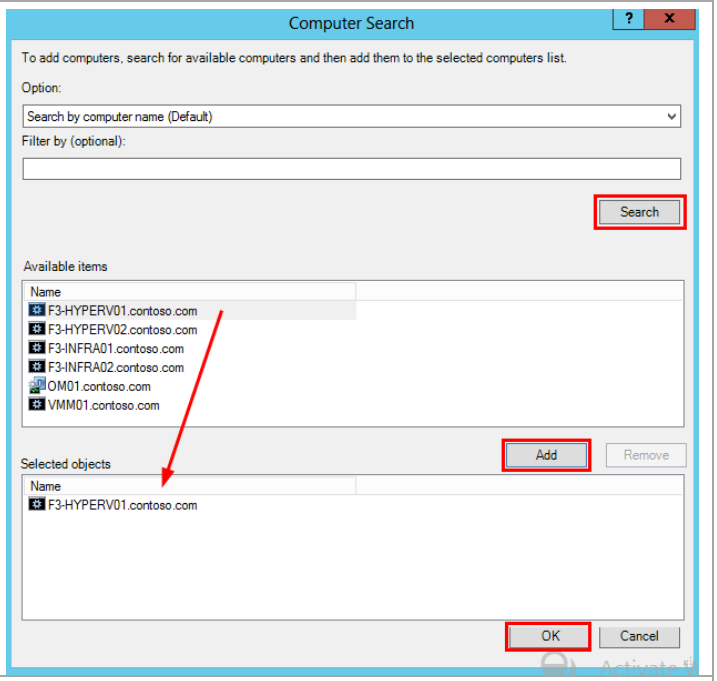
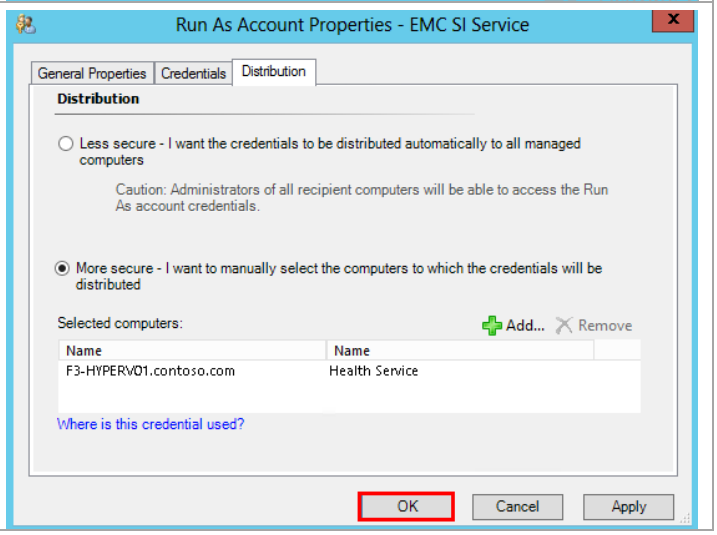
From within the Operations Manager console go to **Administration** > **Run As Configuration** > **Accounts**
Right click on **Accounts** and select **Create Run As Account…**

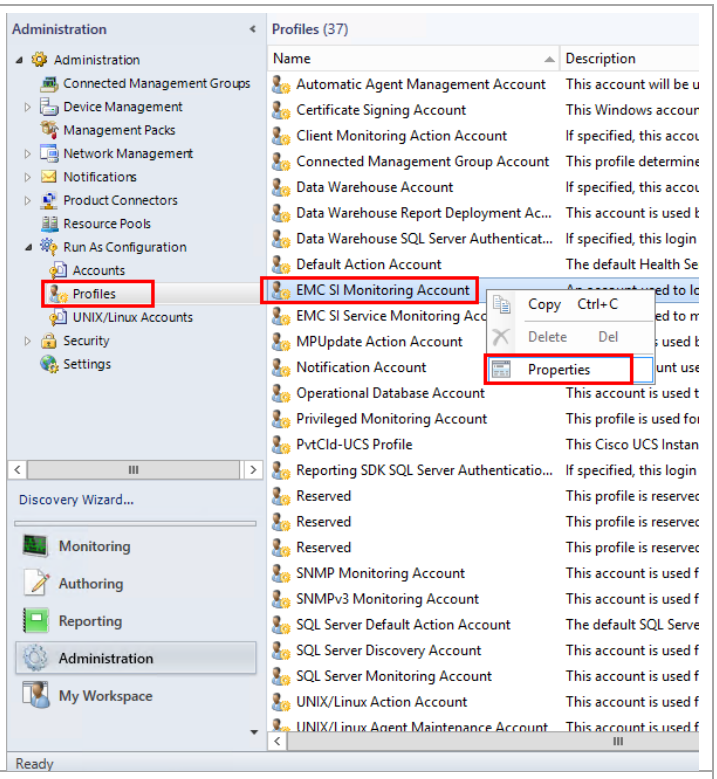
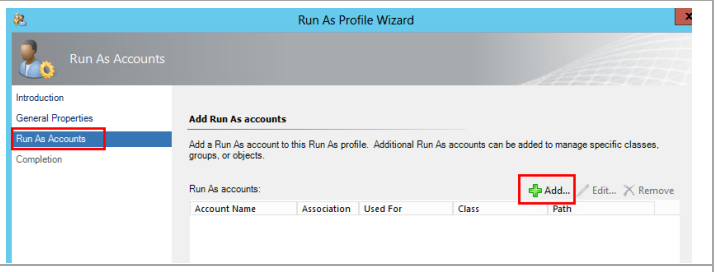
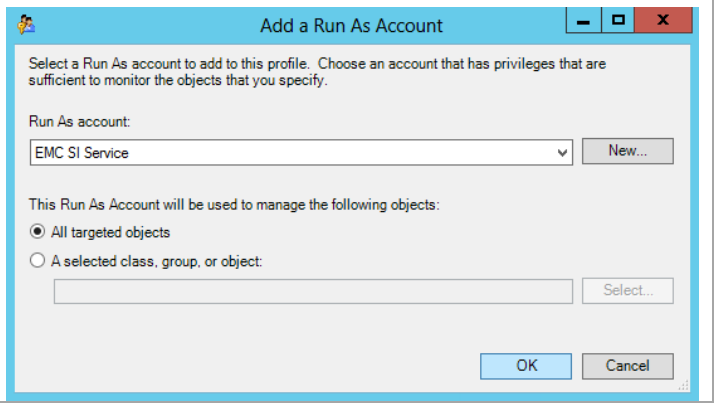


Select **Next**

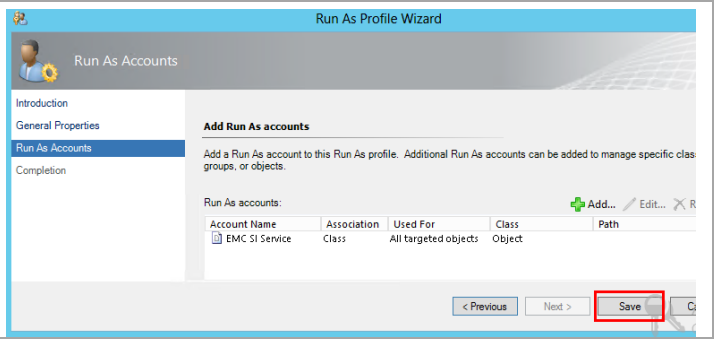


Choose a Run As account type of **Windows** and type in the desired Display Name and Description. Select **Next**	
Enter the account details for the domain account created in the previous steps that was assigned "Monitor" access to the ESI Service. Select **Next**	
Choose the desired security option and select **Create** and then **Close.**	

If the **More secure** security option was selected, go to the **Properties** of the Run as account and select the **Distribution** tab	
Select **Add** Select **Search** to get a list of the available hosts, running the SCOM agent that can be used to communicate with the ESI Service. **Add** the desired server or VM running the SCOM agent and select **OK**.	
Select **OK** to save the change to the run as account	

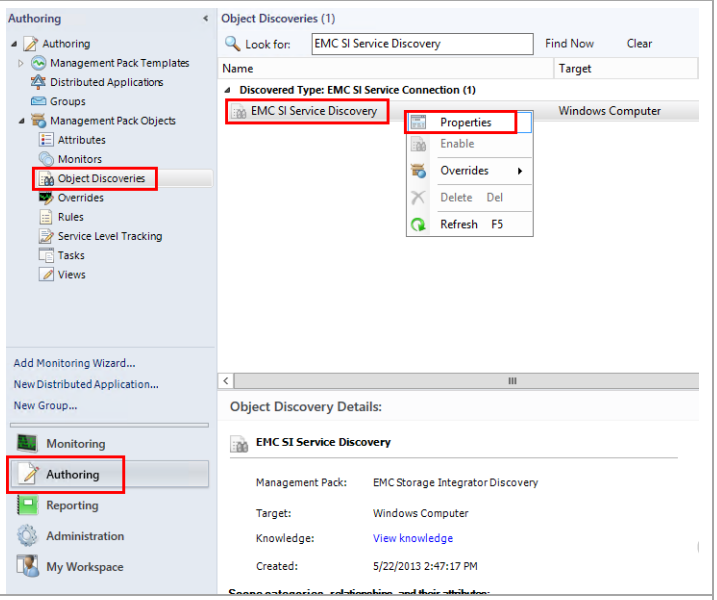
Go to **Administration > Run As Configuration > Profiles** Within Profiles find the **EMC SI Monitoring Account** profile. Right click on that profile and select **Properties**.	
Select **Run As Accounts** and then select A**dd…**	
Select the run as account created in the previous steps and click **OK**	

Select **Save** to commit the change
Select **Close** at the following screen

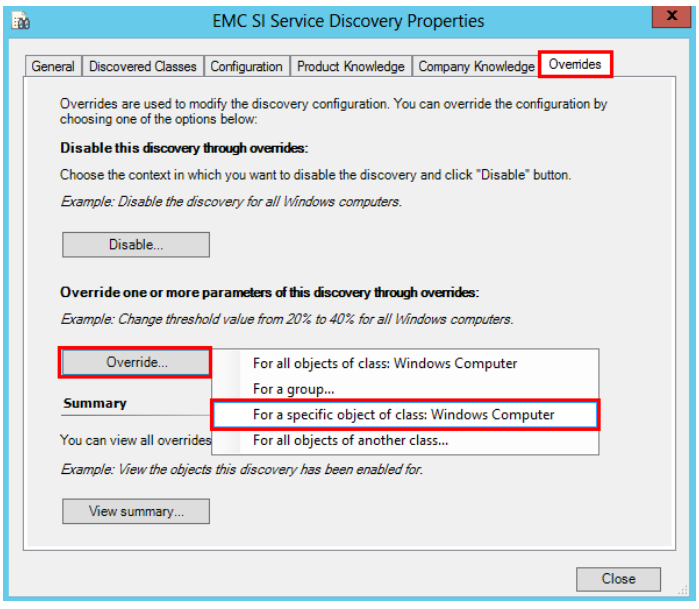


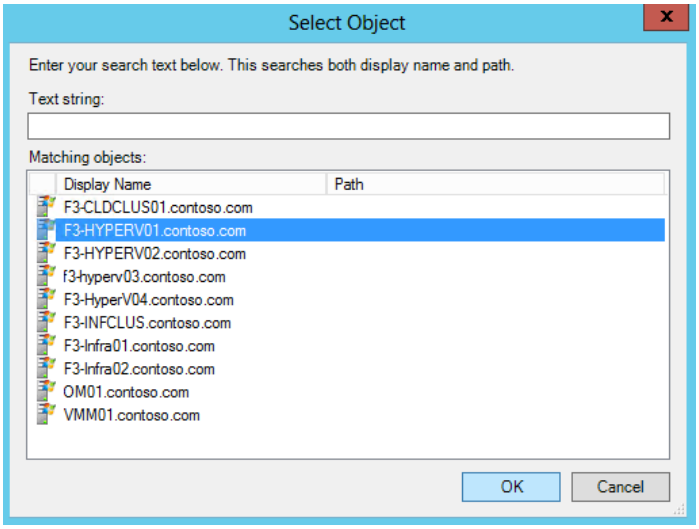
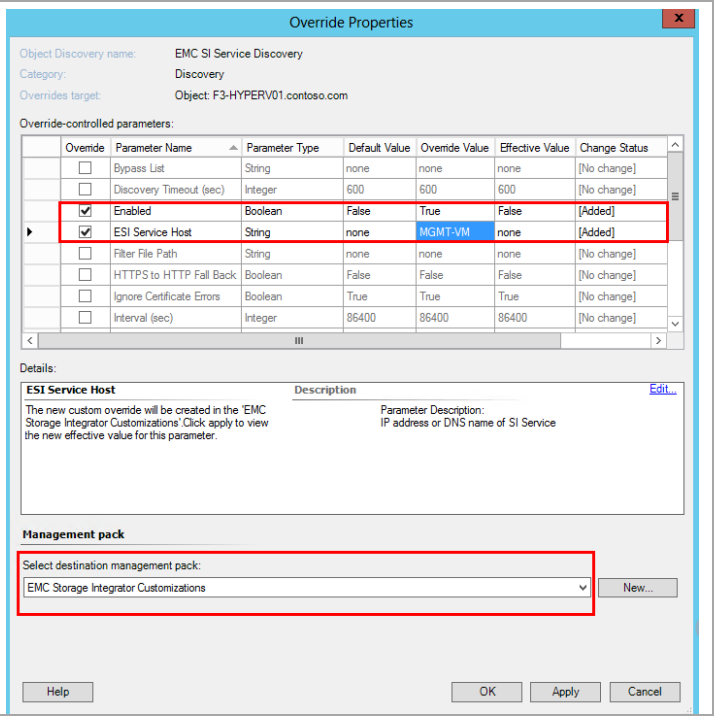
Setting Overrides for the EMC SI Service Discovery

From within the Operations Manager console go to **Authoring > Management Pack Objects > Object Discoveries**
Find the **EMC SI Service Discovery** entry
Right click on EMC SI Service Discovery and select **Properties**



Go to the **Overrides** tab
Click **Override...** and select **For a specific object of class: Windows Computer**



Select the desired host that will be used to communicate with the ESI Service. If the "more secure" run as account option was selected in the previous steps, ensure to use the host where the credentials were distributed. Select **OK**	
Within the override properties the following parameters are required to be changed: Parameter Name: **Enabled** Override Value: **True** Parameter Name: **ESI Service Host** Override Value: **Name or IP Address of EMC Service Host** For **Select destination management pack** choose "**EMC Storage Integrator Customizations"** Select **OK** For more details on additional parameters that can optionally be modified, see the ESI SCOM Management Pack online help	

16.5 Install and Configure the EMC SMI-S Provider for System Center Virtual Machine Manager integration

VMM storage integration requires an SMI-S provider instance to communicate with the VNX storage array. The following sections outline the minimum requirements for configuring the SMI-S provider and VMM environment to allow for VMM to manage VNX storage and perform rapid virtual machine deployment. At a high level the required steps include:

- Installing the EMC SMI-S Provider
- Registering the VNX with the Provider
- Creating the SMI-S user for the SCVMM run as account

- Creating the run as account within SCVMM
- Registering the EMC SMI-S provider with SCVMM
- Creating classifications and choosing storage pools for management
- Allocating Storage Pools to Host Groups
- Configuring the Library Server
- Creating a San Copy Capable Template
- Selecting the Rapid Provisioning Deployment Method

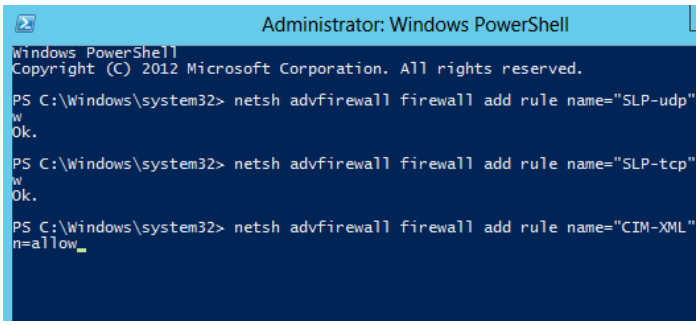
Additional information can be found in the document titled "Storage Automation with System Center 2012 and EMC Storage Systems using SMI-S" available at https://support.emc.com

Install the EMC SMI-S Provider

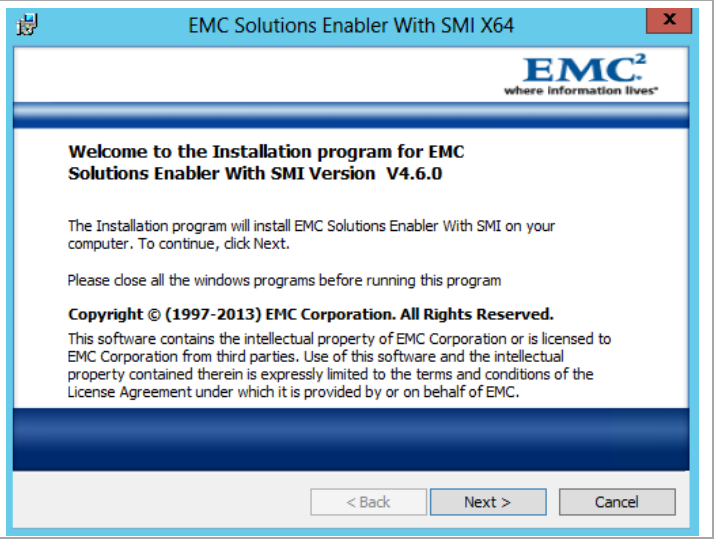
▶ Perform the following steps on the **EMC Management** virtual machine.

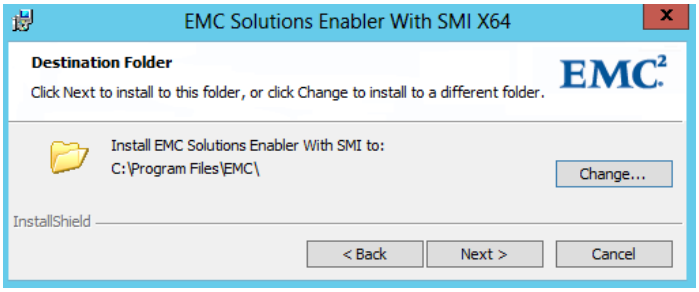
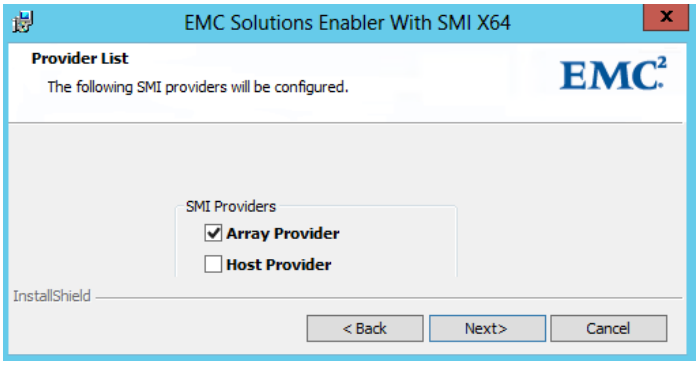
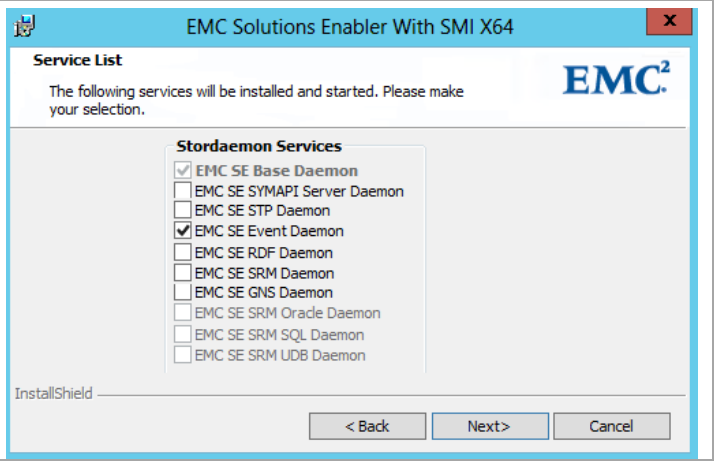
From an elevated PowerShell session run the following commands to open the ports required for the SMI-S provider:

```
netsh advfirewall firewall add rule name="SLP-udp" dir=in protocol=UDP localport=427 action=allow
netsh advfirewall firewall add rule name="SLP-tcp" dir=in protocol=TCP localport=427 action=allow
netsh advfirewall firewall add rule name="CIM-XML" dir=in protocol=TCP localport=5988-5989 action=allow
```



Run the se7600-WINDOWS-x64-SMI.exe installer
Click **Next**



Install to the desired location Click **Next**	
Ensure **Array Provider** is selected and click **Next**	
Accept the default service list and click **Next** Then select **Install** to start the installation. Select **Finish** to close the installer upon completion	

Register the VNX with the Provider

▶ Perform the following steps on the **EMC Management** virtual machine.

From a command or PowerShell prompt, change directory to C:\Program Files\emc\ECIM\ECOM\bin

Run the **TestSmiProvider.exe** command and accept all defaults by hitting **Enter** when prompted.

```
PS C:\Program Files\emc\ECIM\ECOM\bin> .\TestSmiProvider.exe
Connection Type (ssl,no_ssl,native) [no_ssl]:
Host [localhost]:
Port [5988]:
Username [admin]:
Password [#1Password]:
Log output to console [y|n (default y)]:
Log output to file [y|n (default y)]:
Logfile path [Testsmiprovider.log]:
Connecting to localhost:5988
Using user account 'admin' with password '#1Password'

##########################################################################
##                                                                      ##
##                  EMC SMI Provider Tester                             ##
##   This program is intended for use by EMC Support personnel only.    ##
##   At any time and without warning this program may be revised        ##
##   without regard to backwards compatibility or be                    ##
##   removed entirely from the kit.                                     ##
##########################################################################
  slp    - slp urls                    slpv    - slp attributes
  cn     - Connect                     dc      - Disconnect
  disco  - EMC Discover                rc      - RepeatCount
  addsys - EMC AddSystem               remsys  - EMC RemoveSystem
  refsys - EMC RefreshSystem

  ec     - EnumerateClasses            ecn     - EnumerateClassNames
  ei     - EnumerateInstances          ein     - EnumerateInstanceNames
  ens    - EnumerateNamespaces         miner   - Mine classes

  a      - Associators                 an      - AssociatorNames
  r      - References                  rn      - ReferenceNames

  gi     - GetInstance                 gc      - GetClass

  ci     - CreateInstance              di      - DeleteInstance
  mi     - ModifyInstance              eq      - ExecQuery
  gp     - GetProperty                 sp      - SetProperty

  tms    - TotalManagedSpace           tp      - Test pools
  ecap   - Extent Capacity             pd      - Profile Discovery

  im     - InvokeMethod                active  - ActiveControls
  ind    - Indications menu            tv      - Test views

  st     - Set timeout value           lc      - Log control
  sl     - Start listener              dv      - Display version info
  ns     - NameSpace                   vtl     - VTL menu

  chp    - consolidated host provider menu


  q      - Quit                        h       - Help
##########################################################################
Built with EMC SMI-S Provider: V4.6.0
```

Run the **addsys** command
For **Add System** enter **y**
For **ArrayType** enter **1**
For **IP address or hostname** enter the IP for **SPA** and hit **enter**
For **IP address or hostname 2 enter the IP** for **SPB** and hit **enter**
For **Address Type** enter **2** for each entry
Enter the appropriate **User and Password** with access to run privileged commands to the array
Resulting output should be **0**
Press **enter** to continue
Press **q** to quit

```
##########################################################################
Built with EMC SMI-S Provider: V4.6.0
Namespace: root/emc
repeat count: 1
(localhost:5988) ? addsys
Add System {y|n} [n]: y

ArrayType (1=Clar, 2=Symm) [1]:
One or more IP address or Hostname or Array ID

Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 10.5.223.128
IP address or hostname or array id 1 (blank to quit): 10.5.223.129
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]:
Address Type (1) [default=2]:
User [null]: admin
Password [null]: P@ssw0rd
++++ EMCAddSystem ++++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Failed
       5=Invalid Parameter
       4096=Job Queued, 4097=Size Not Supported
Note: Not all above values apply to all methods - see MOF for the method.

System : //10.5.177.133/root/emc:Clar_StorageSystem.CreationClassName="Clar_Stora
"

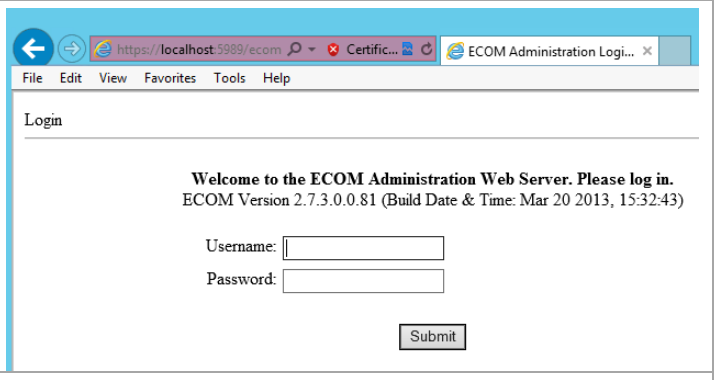
In 12.420784 Seconds

Please press enter key to continue...
```

Create the SMI-S User for the SCVMM Run As Account

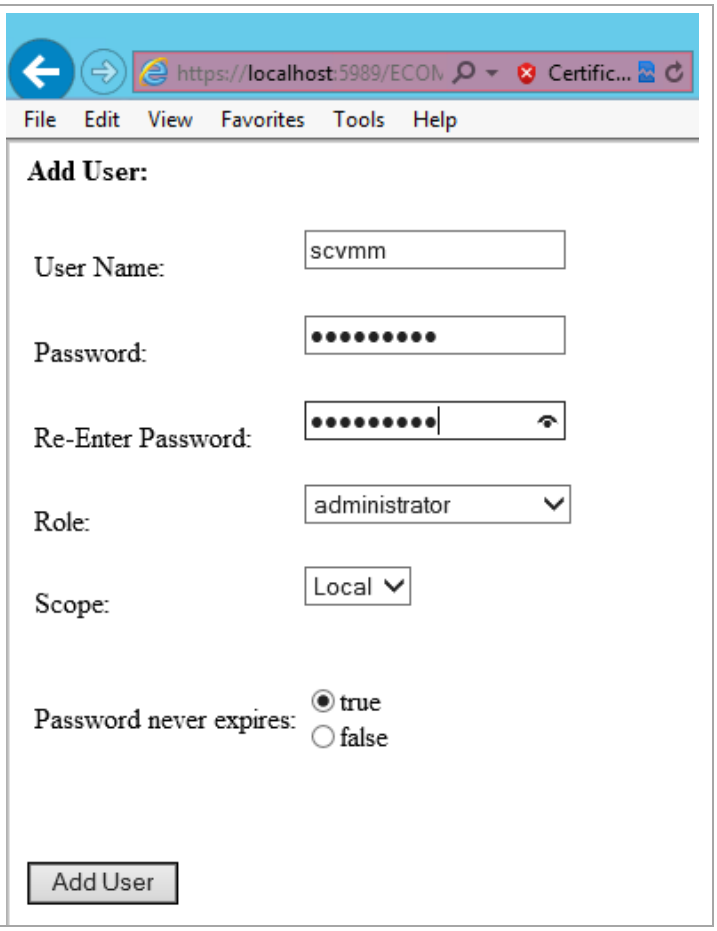
▶ Perform the following steps on the **EMC Management** virtual machine.

From a web browser go to https://localhost:5989/ecomconfig
Log in as:
Username: admin
Password: #1Password



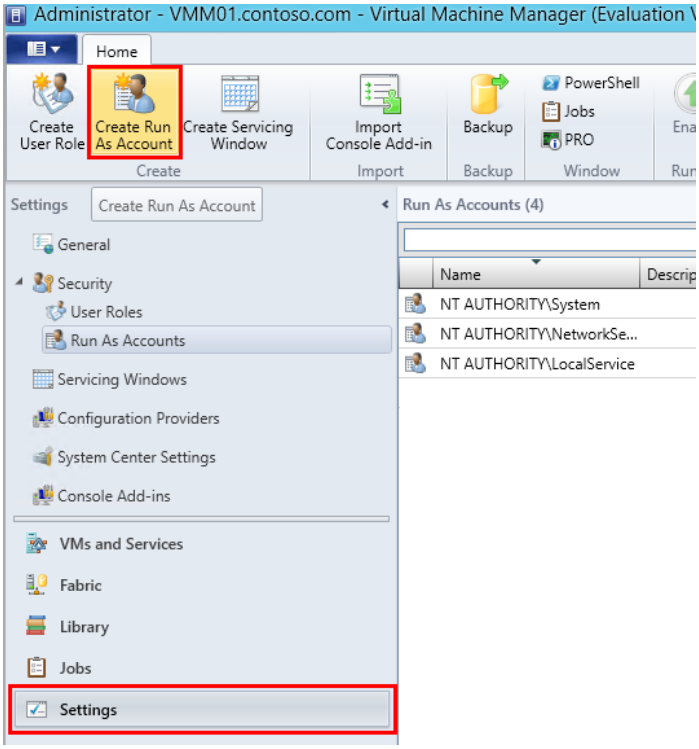
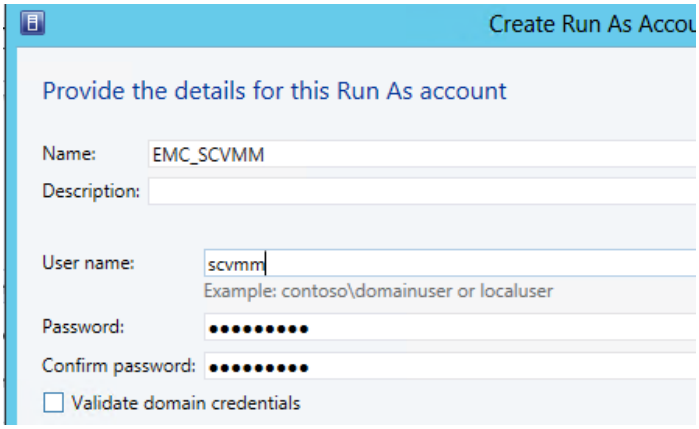
Select **Add User**



Insert the desired **User Name** and **Password** For **Role** choose **administrator** For **Scope** choose Local If **Password never expires** is set to **false** the password for this user will expire in 90 days. Select **Add User**	

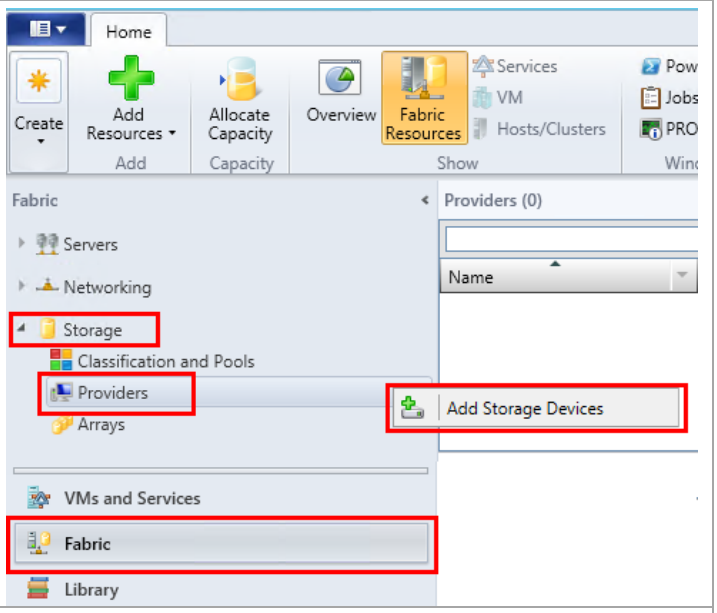
Create the Run As Account within SCVMM

This section assumes that SCVMM has already been installed in the environment

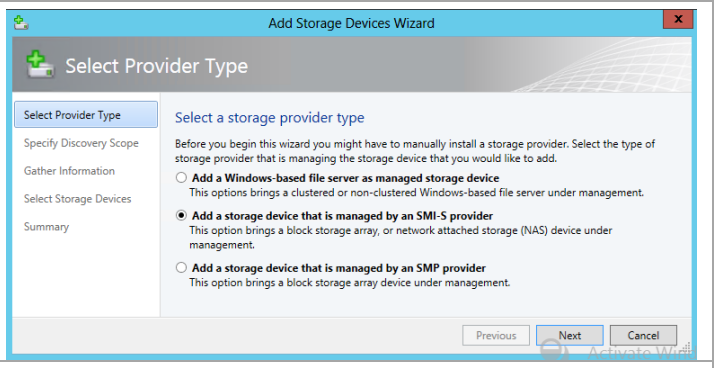
▶ Perform the following steps on the **SCVMM** virtual machine.	
From within the Virtual Machine Manager console, go to **Settings** > **Security** > **Run As Accounts** Select **Create Run As Account**	
Enter the appropriate information, including the **User name** and **Password** used when creating the account on the SMI-S provider host. Select **OK**	

Register the EMC SMI-S provider with SCVMM

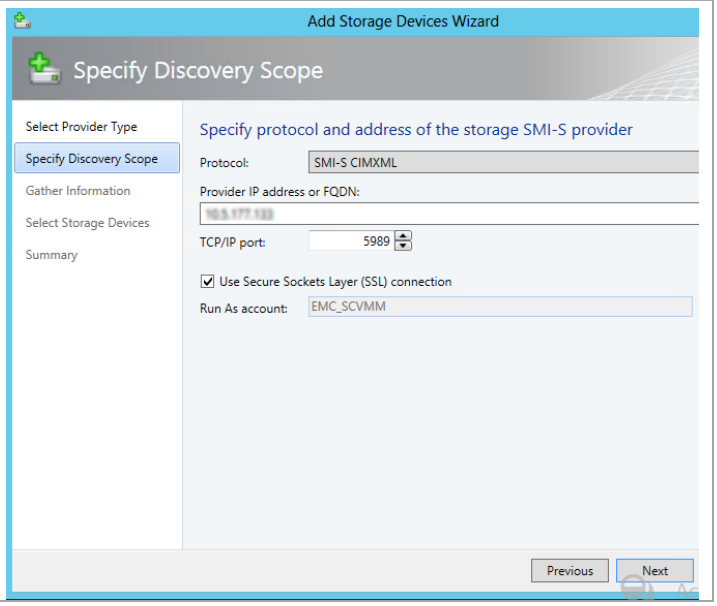
From within the Virtual Machine Manager console, go to **Fabric > Storage > Providers**
Right click on **Providers** and select **Add Storage Devices**

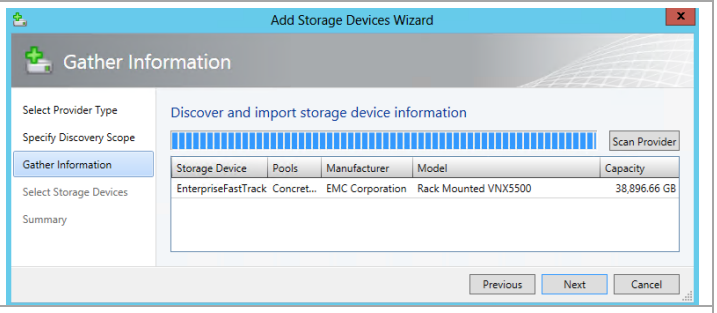
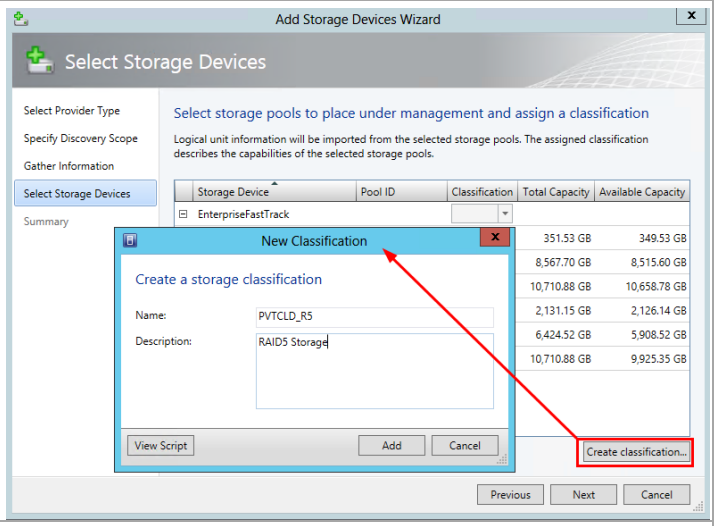
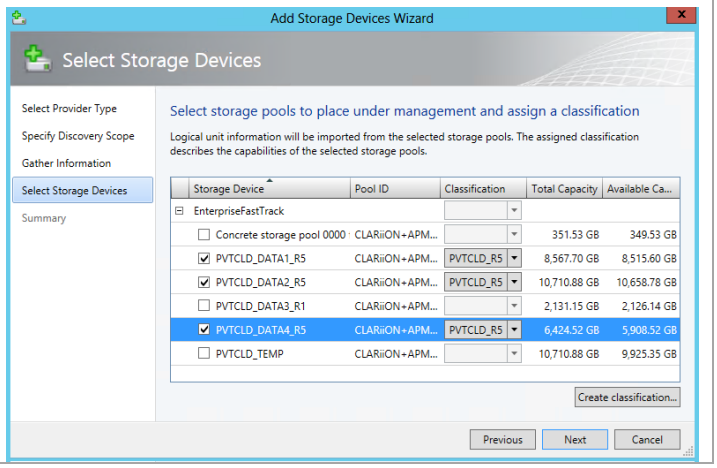


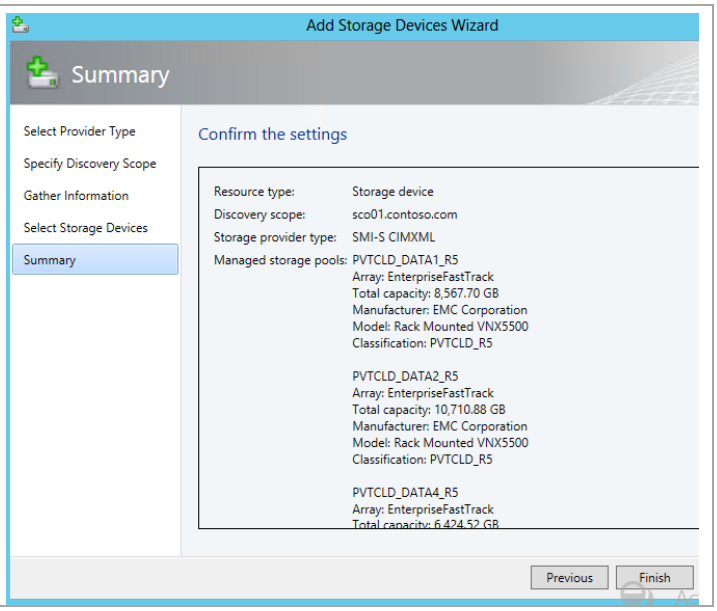
Select **Add a storage device that is managed by an SMI-S provider**
Select **Next**



Enter the following information:
Protocol:
Choose "SMI-S CIMXML"
Provider IP address or FQDN:
Enter the IP or Name of the SMI-S provider host
TCP/IP port:
If SMI-S provider was not modified, keep the default port selection
Use SSL:
Optionally select SSL
Run As account:
Select the Run As account previously created which will connect to the SMI-S Provider host.
Select **Next**
If SSL was selected, import the certificate when prompted.

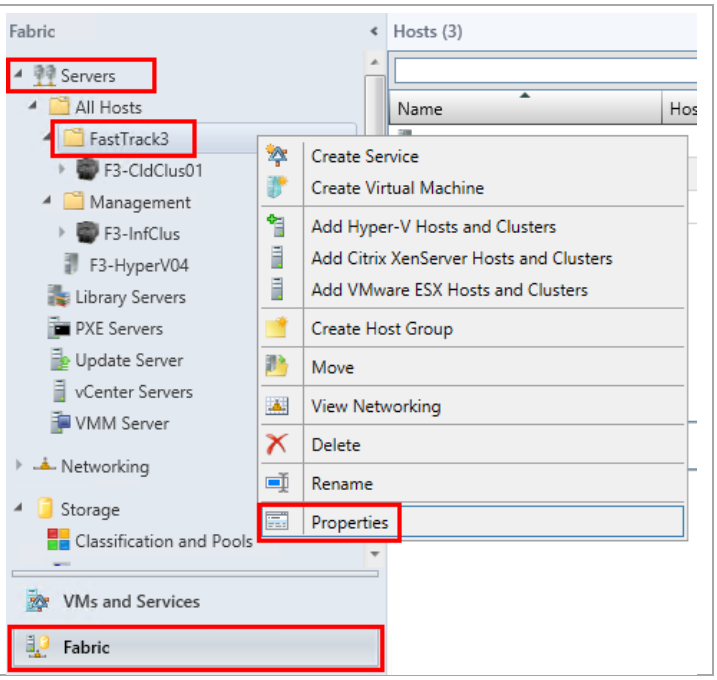


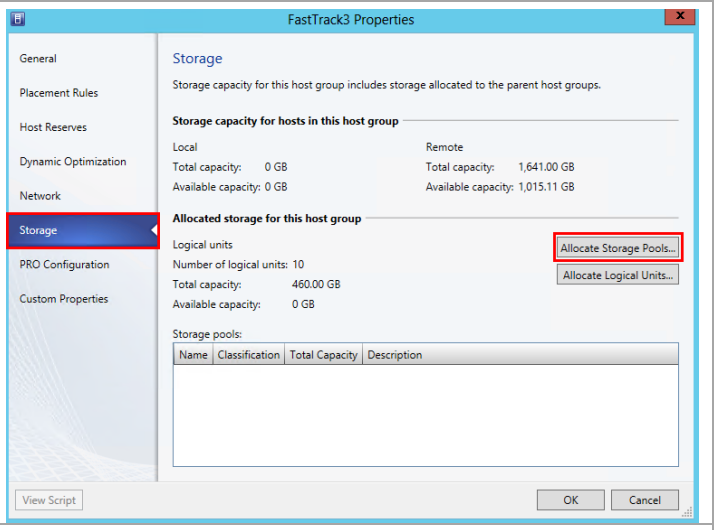
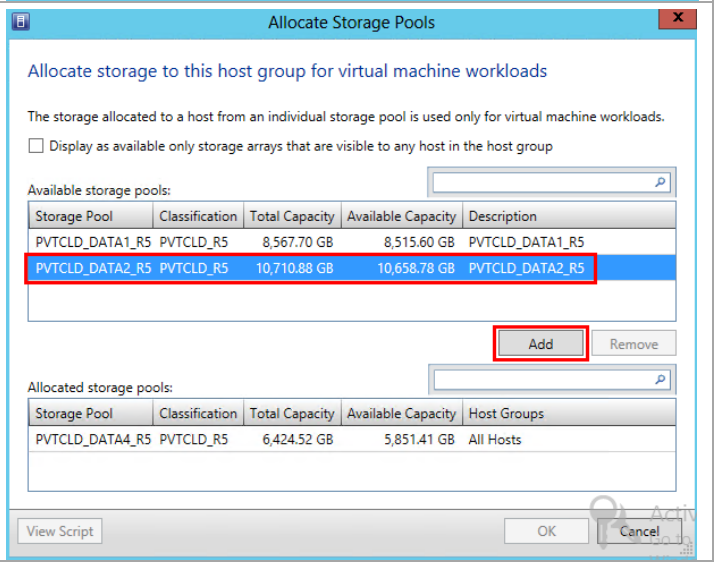
Verify the storage device following a successful discovery operation. Select **Next**	
Select **Create classification** and create one or multiple classifications based on the storage types in your environment. Select **Add**	
Select the pools to be managed within SCVMM and assign the previously created Classification(s) Select **Next**	

Confirm the settings and select **Finish**	

Allocate Storage Pools to Host Groups

This section assumes that SCVMM has already been installed in the environment and physical hosts have been added to host groups within VMM. Allocating a storage pool to a VMM host group makes that storage pool available for use by the hosts or clusters within that group.

From within the Virtual Machine Manager console, go to **Fabric** > **Servers** Expand the **Servers** folder Right click on the appropriate host folder and select **Properties**	

Go to the **Storage** menu and select **Allocate Storage Pools….**	
Select the desired storage pools and click **Add** Select **OK** to commit and exit.	

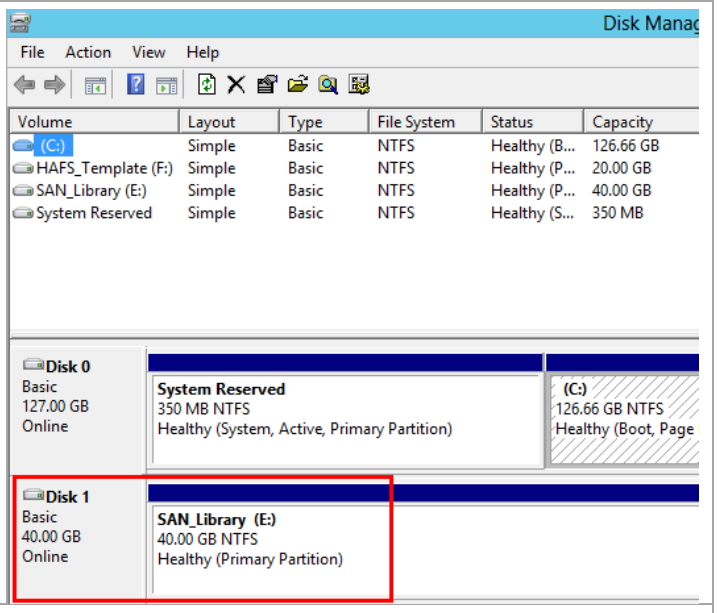
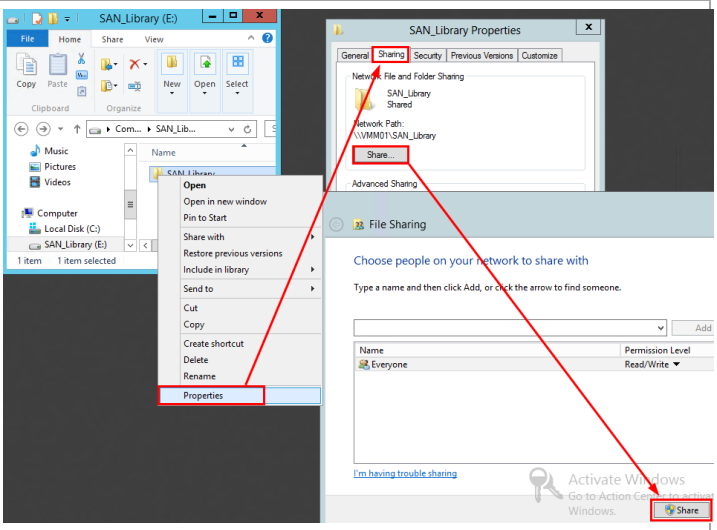
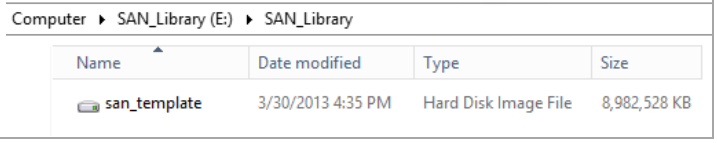
16.6 Configure the Library Server

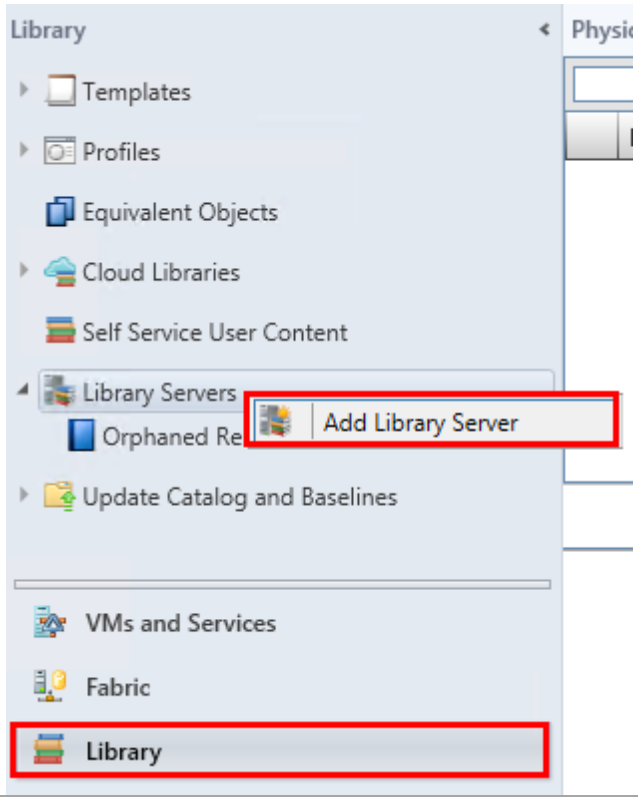
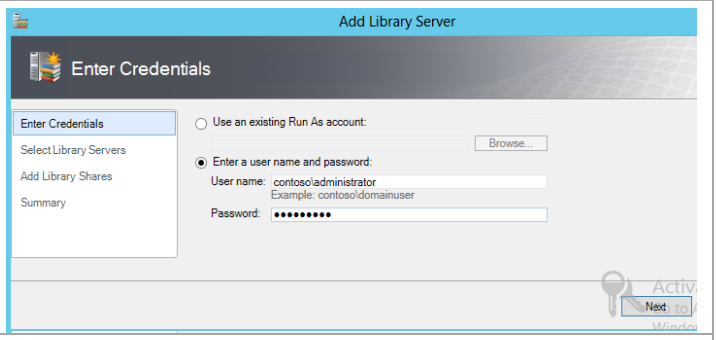
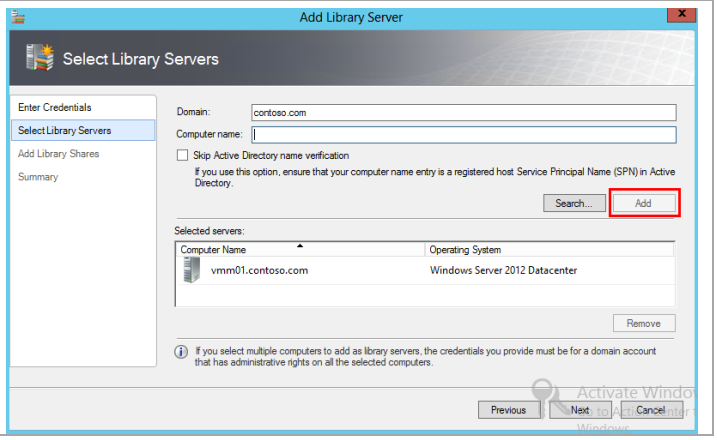
SCVMM supports rapid virtual machine deployment with the use of array snapshots or clones. To support this functionality a library server can be configured to support a "San Copy Capable" template as a source for the replicas. The library server must be hosted by a stand-alone Hyper-V host or VM, with a physical LUN presented over either FC, iSCSI or as a pass through disk. The LUN presented to the library server must contain a single virtual hard disk. If multiple virtual hard disks reside on the template LUN then it will not be considered San Copy Capable.

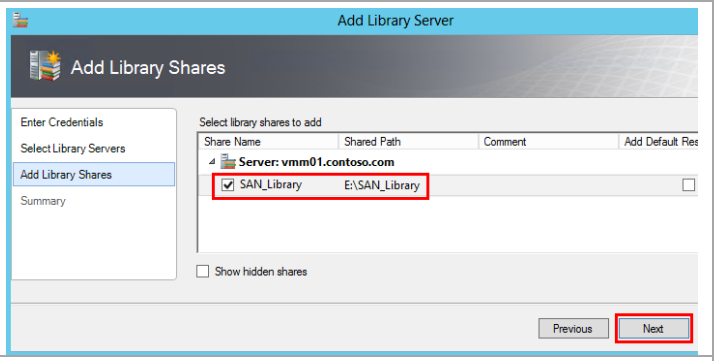
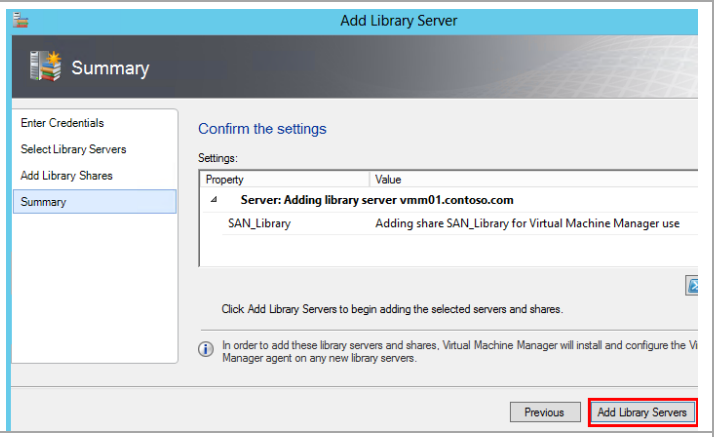
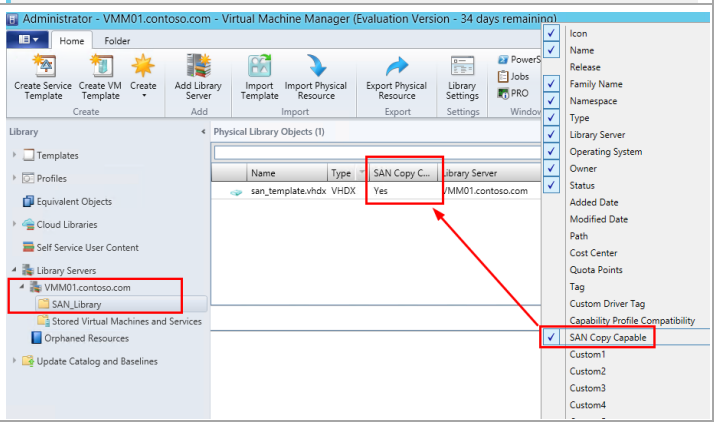
If iSCSI is used in the environment, it is recommended to configure the library server as a clustered virtual machine, with the template LUN presented over iSCSI. If iSCSI is not used, then a virtual machine with pass through storage can be used. The VM using pass through disks may be clustered, however, testing has shown problems with live migration where a clustered VM uses pass through storage.

Note: The LUN presented to the library server must be created in a pool which is managed by VMM. Also, the pool where this LUN resides must also be allocated to the appropriate host group where deployment is planned.

After the appropriate LUN is presented to the planned library server, execute the following steps:

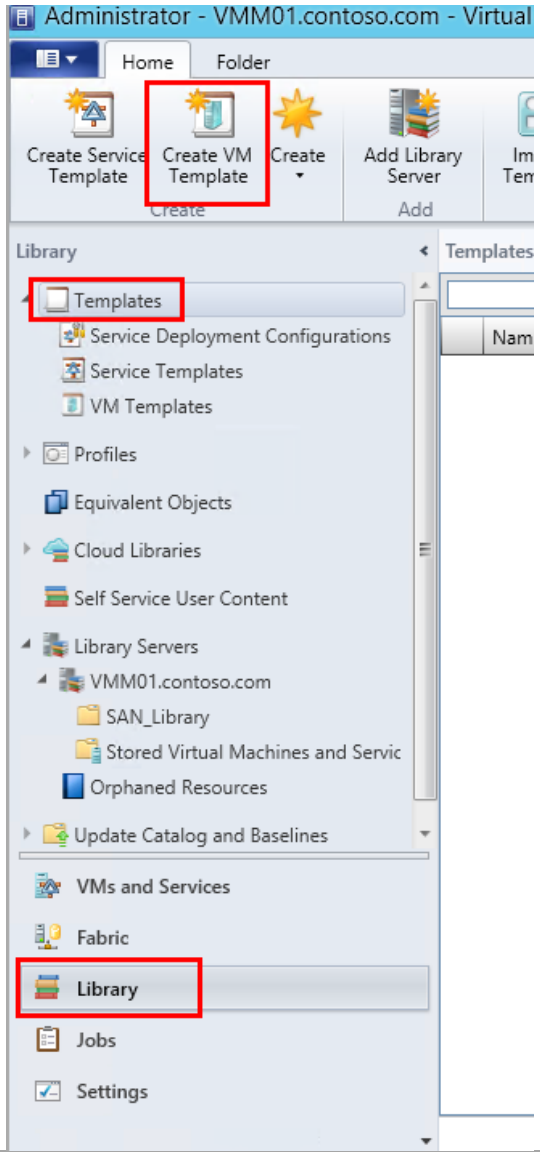
Mount the LUN to the desired mount point or drive letter	
Go to the drive letter or mount point in Windows Explorer and create a folder. Right click on the newly created folder and select **Properties** Go to the Sharing tab and select **Share** to share out the folder. For permissions, Microsoft states the following: *For a library share to function through VMM, the minimum required permissions are that the Local System (SYSTEM) account has full control permissions at both the share and the NTFS file system level. By default, the Local System account has full control permissions when you create a file share and then add the library share to VMM management.* *However, to add resources to a library share, an administrator typically needs to access the share through Windows Explorer. They can do this either outside VMM or through the VMM console, where they can right-click the library share, and then click **Explore**. Because of this, ensure that you assign the appropriate access control permissions outside VMM. For example, we recommend that you assign full control share and NTFS permissions to the Administrators group.*	
Add the desired virtual hard disk representing a sysprepped operating system image to the share. This virtual hard disk will be used for creating a san copy capable template.	

From the **Library** node of the VMM console go to **Library Servers**. Right click on library servers and select **Add Library Server**	
Enter a user which has administrator access to the planned library server and select **Next**	
Enter the **Computer name** of the library server and choose **Add**. Then select **Next** to continue.	

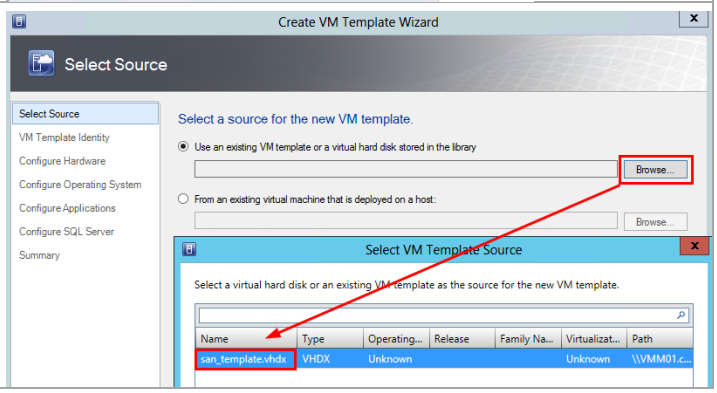
Select the previously created library share and click **Next**	
Select **Add Library Servers** to complete the wizard and start the Add Library Server job.	
Following the successful add library server job, return to the Library area of VMM and expand the newly added library server Select the library share and view the virtual hard disk within the share. Right click on a column grouping and find the "**San Copy Capable"** column to add. Ensure the San Copy Capable column displays **Yes** If San Copy Capable displays as "No" ensure the pool where the LUN supporting the .vhdx resides is managed by VMM. Also ensure that the pool is allocated to a host group.	

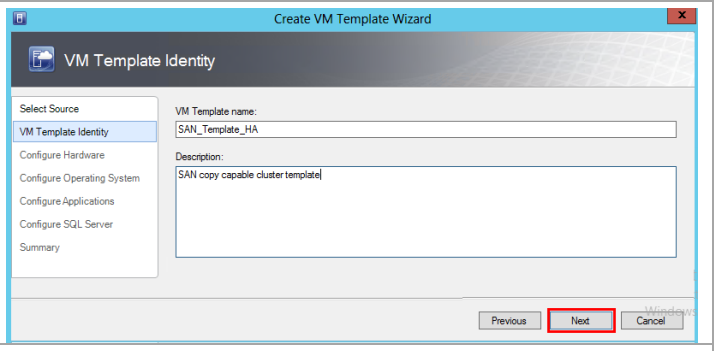
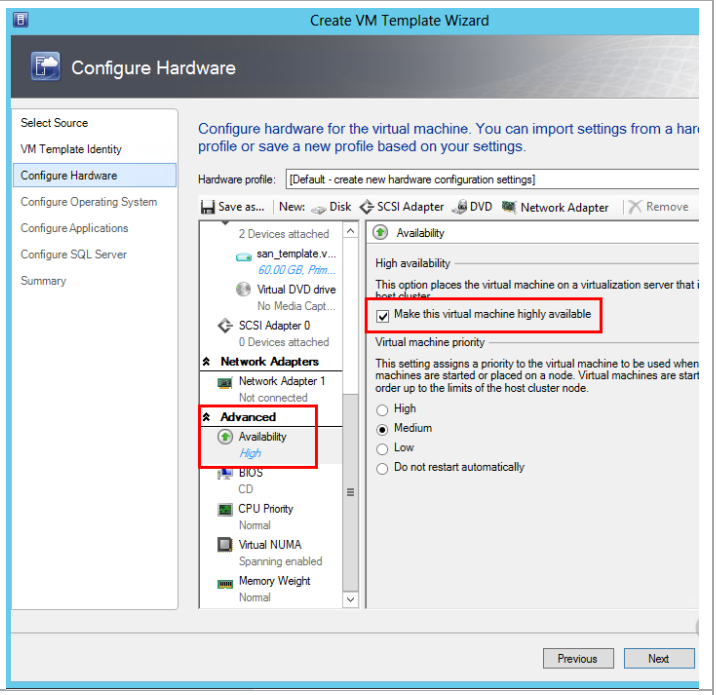
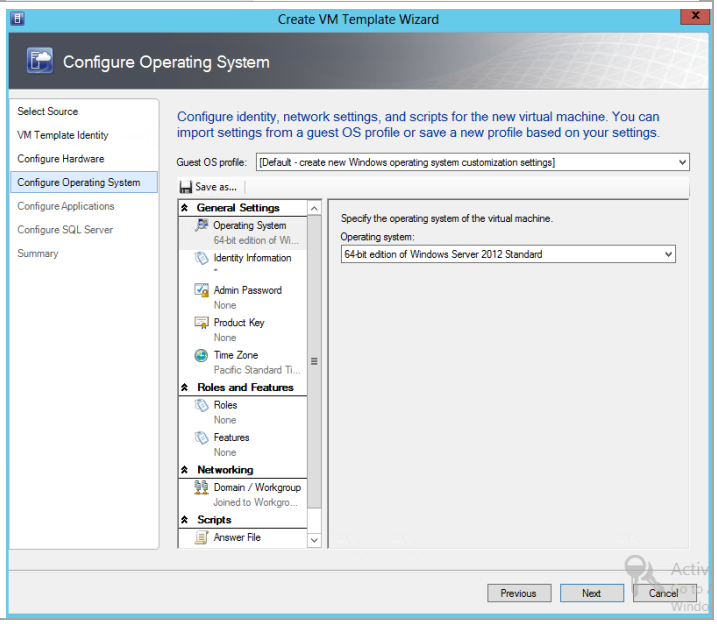
16.7 Create a SAN Copy Capable Template

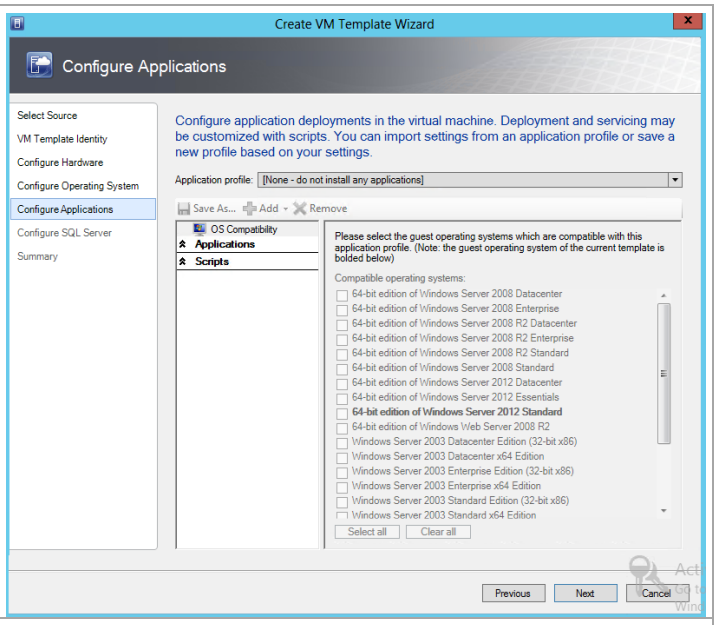
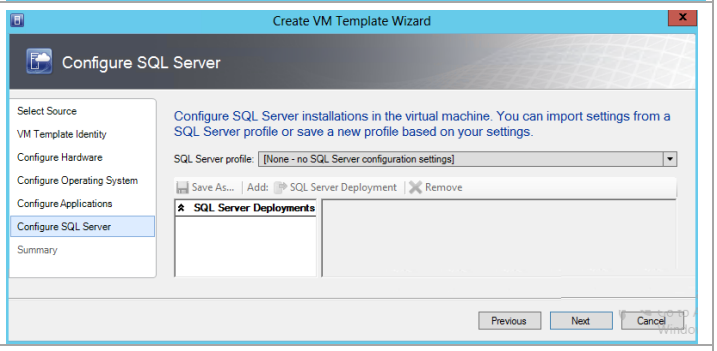
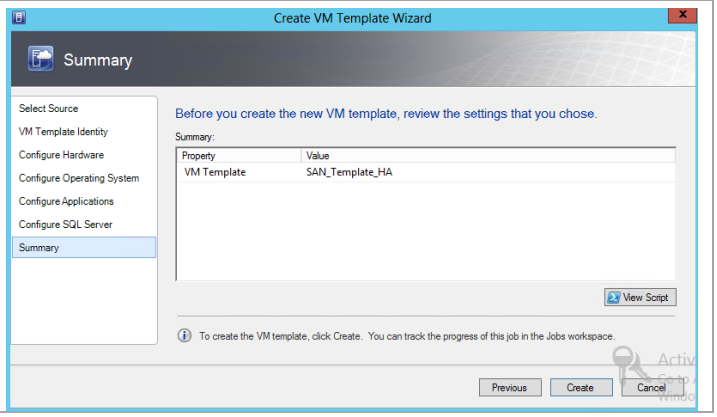
From within the Virtual Machine Manager console, go to **Library** > **Templates**
Select **Create VM Template**



Select **Use an existing VM template or a virtual hard disk stored in the library** and choose **Browse**
Select the San Copy Capable virtual hard disk and select **OK**
Select **Next**



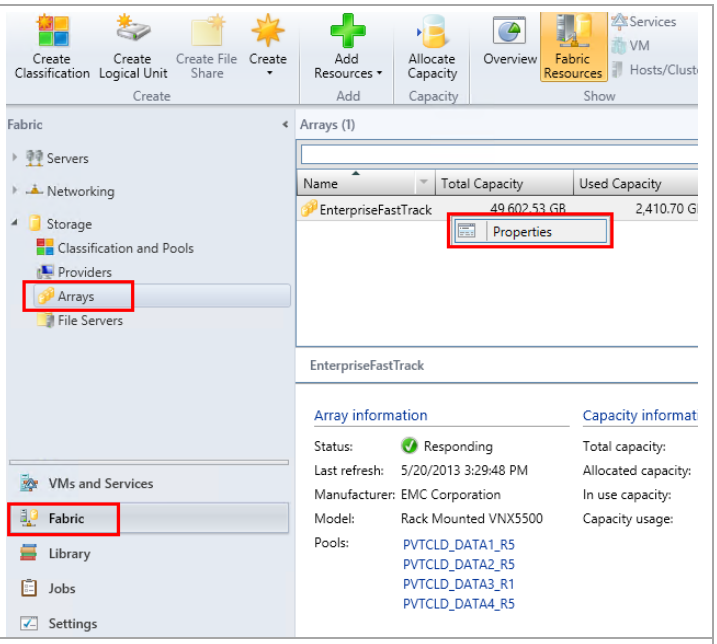
Name the template and select **Next**	
Select the appropriate hardware customizations. If the template is intended for cluster deployment, go to **Advanced > Availability** and select **Make this virtual machine highly available** Select **Next**	
Choose the desired operating system customization and select **Next**	

Choose optional application deployments and select **Next**	
Optionally choose the SQL Server configuration for the template and choose **Next**	
Select create to start the Create template job and complete the wizard.	

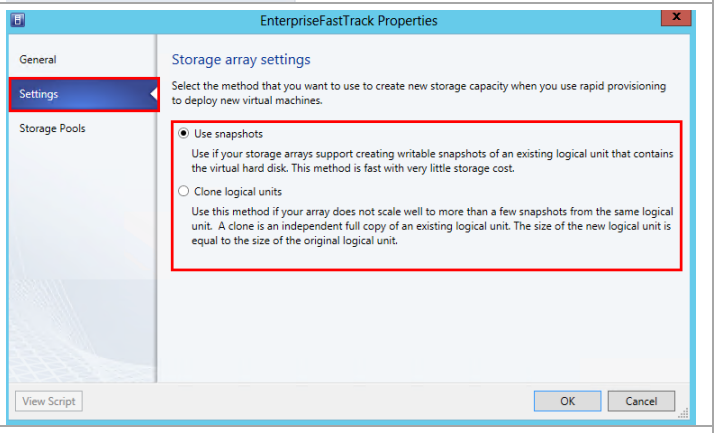
16.8 Select the Rapid Provisioning Deployment Method

SCVMM supports both clones and snapshots for SAN Copy based deployments. The copy method can be changed via PowerShell or from the GUI. The following steps detail how to change this setting using either method.

From within the Virtual Machine Manager console, go to **Fabric > Storage > Arrays**
Right click on the VNX entry and select **Properties**



Go to the **Settings** menu
From the Settings menu **Use snapshots** can be selected to use VNX Snapshots, where up to 256 snapshots can be taken per template LUN.
Alternatively **Clone logical units** can be chosen to do full copy clones of the template LUN.
Select **OK** to change the setting.

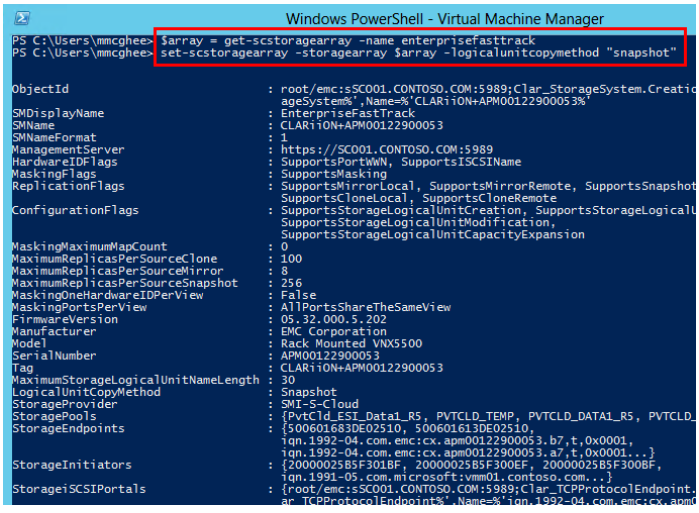


For scripting purposes, the storage array setting for choosing snapshots or clones can be modified for a particular job. Use the following command to set either "snapshot" or "clone" for the copy method:

```
$array = get-scstoragearray -name enterprisefasttrack

#For Snapshots
set-scstoragearray -storagearray $array -logicalunitcopymethod "snapshot"

#For Clones
set-scstoragearray -storagearray $array -logicalunitcopymethod "clone"
```



17 Appendix A: SQL Cluster Named Instance Worksheet

Table 37 Example Customer Worksheet for Naming SQL Instances

Component	Service Manager management server	Service Manager Data Warehouse server	Service Manager analysis server	App Controller, Orchestrator, Microsoft SharePoint® services Farm and WSUS	Virtual Machine Manager	Operations Manager	Operations Manager Data Warehouse
SQL Server Instance Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance Failover Cluster Network Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance DATA Cluster Disk Resource							
SQL Server Instance LOG Cluster Disk Resource							
SQL Server Instance Install Drive							
SQL Server Instance DATA Drive							
SQL Server Instance LOG Drive							
SQL Server Instance TEMPDB Drive							
Cluster Service Name	SQL Server (SCSMDB)	SQL Server (SCSMDW)	SQL Server (SCSMAS)	SQL Server (SCDB)	SQL Server (SCVMMDB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)
Clustered SQL Server Instance IP Address							
Host Cluster Public Network Interface Subnet Mask							
Host Cluster Public Network Interface Name							
SQL Server Instance Listening TCP/IP Port				1433[23]			
SQL Server Instance Preferred Owners	Node2, Node4	Node2, Node4	Node2, Node4	Node1, Node4	Node1, Node4	Node3, Node4	Node3, Node4

[23] Note that the SCDB instance must use port 1433 if the Cloud Services Process Pack will be used in the environment.

18 Appendix B: Sample PowerShell Scripts

These are some sample PowerShell scripts and input files to create accounts and groups used by System Center 2012. These are for sample purposes only. They should be reviewed for compliance with customer policies and naming conventions. They were tested within the lab environment where this system was configured. Security in your environment may not allow these scripts to run in your environment. No warranty or support is implied by their inclusion within this document. They were included to provide you with a starting point if you want to automate some steps.

18.1 Populate Domain Accounts and Security Groups

Add-FTUsers.ps1

```
<#

Simple script to add the Accounts required for the System Center
installation.
This script relies on a .csv file - AddFTUsers.csv - in a specific
format.
The .csv file can be changed to meet the customer requirements

This simply adds the accounts.  It does not put them into groups or
assign specific permissions.

#>

Import-Module ActiveDirectory

$Users = Import-Csv -Delimiter ";" -Path ".\AddFTUsers.csv"
foreach ($User in $Users)
{
    $OU = $User.OU
    $Password = $User.Password
    $Name = $User.Name
    $Description = $User.Description
    New-ADUser -Name $Name -SamAccountName $Name -UserPrincipalName
$Name -DisplayName $Name -Surname $Name -AccountPassword (ConvertTo-
SecureString $Password -AsPlainText -Force) -PasswordNeverExpires $true
-Enabled $true -Path $OU -Description $Description
}
```

AddFTUsers.csv

Note: You must change the OU definition to reflect your environment.

```
Name;Password;OU;Description
FT-SCAC-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"AppController
service account"
FT-SCInstall;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"Optional for SC
2012 install"
FT-SCOM-Action;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"OM monitoring"
FT-SCOM-DR;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"OM data reader for
SQL SRS"
FT-SCOM-DW;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"OM Data warehouse"
FT-SCOM-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"OM service
account"
```

```
FT-SCO-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"Orchestrator
service account"
FT-SCSM-ADCI;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM-AD connector"
FT-SCSM-OCI;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM-Orchestrator
connector"
FT-SCSM-OLAP;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM  SQL  Analysis
Services"
FT-SCSM-OMAlert;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM-OM    alert
connector"
FT-SCSM-OMCI;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM-OM connector"
FT-SCSM-SSRS;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM  SQL  SRS  for
datamart"
FT-SCSM-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM         service
account"
FT-SCSM-Users;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM users"
FT-SCSM-VMMCI;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM-VMM
connector"
FT-SCSM-WF;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SM workflows"
FT-SQL-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"SQL         service
account"
FT-VMM-SVC;OEM@ftv3!;"OU=FastTrack,DC=VSPEX,DC=com";"VMM         service
account"
```

Add-FTGroups.ps1

```
<#

Simple script to add the AD security Groups required for the System
Center installation.
This script relies on a .csv file - AddFTGroups.csv - in a specific
format.
The .csv file can be changed to meet the customer requirements

This simply adds the groups.

#>

Import-Module ActiveDirectory

$Groups = Import-Csv -Delimiter ";" -Path ".\AddFTGroups.csv"
foreach ($Group in $Groups)
{
    $OU = $Group.OU
    $Name = $Group.Name
    $Scope = $Group.Scope
    $Description = $Group.Description
    New-ADGroup -Name $Name -DisplayName $Name -GroupCategory Security
-GroupScope $Scope -Path $OU -Description $Description
}
```

AddFTGroups.csv

Note: You must change the OU definition to reflect your environment.

```
Name;OU;Scope;Description
FT-SCAC-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"Application
Controller Admins"
```

```
FT-SC-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"Full Admins on all
SC components"
FT-SCO-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"Orchestrator
Admins"
FT-SCO-Operators;"OU=FastTrack,DC=VSPEX,DC=com";Global;"Orchestrator
Operators"
FT-SCOM-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"OM
Administrators"
FT-SCSM-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"SM
Administrators"
FT-SCVMM-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"VMM
Administrators"
FT-SCVMM-AppAdmins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"VMM
Application Administrators"
FT-SCVMM-FabricAdmins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"VMM Fabric
Administrators"
FT-SCVMM-ROAdmins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"VMM Read-Only
Administrators"
FT-SCVMM-TenantAdmins;"OU=FastTrack,DC=VSPEX,DC=com";Global;"VMM Tenant
Administrators"
FT-SQL-Admins;"OU=FastTrack,DC=VSPEX,DC=com";Universal;"sysadmins on
all SQL instances/local Admin on SQL nodes"
```

18.2 Add-UcsHyperVFeatures.ps1

```
Write-Host ""
Write-Host "Install the MPIO and Failover Clustering features and the
Hyper-V role"
Write-Host ""
Write-Host -ForegroundColor Yellow "Installing Hyper-V will cause the
system to reboot"
Write-Host ""

$srvr = Read-Host "Enter computer name of server on which to install
MPIO"

Write-Host ""
Write-Host "Installing the MPIO feature"
Install-WindowsFeature -Name Multipath-IO -ComputerName $srvr -
IncludeManagementTools

Invoke-Command -ComputerName $srvr -ScriptBlock `
{
    Set-Service -Name MSiSCSI -StartupType Automatic
    Start-Service -Name MSiSCSI
    Write-Host "Add new vendor and product IDs for MPIO"
#   Values for EMC VNX
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "LUNZ"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "VDISK"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 0"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 1"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 10"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 5"
    $trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "VRAID"
    Write-Host "List of configured vendor and product IDs"
    Get-MSDSMSupportedHW | Select VendorId, ProductId | ft
```

```
}

Write-Host ""
Write-Host "Installing the Failover Clustering feature"
Install-WindowsFeature -Name Failover-Clustering -ComputerName $Srvr -
IncludeManagementTools

Write-Host ""
Write-Host "Installing the Hyper-V role"
Install-WindowsFeature    -Name    Hyper-V    -ComputerName    $Srvr    -
IncludeManagementTools -Restart
```

18.3 Create-UcsFtVms.ps1

```
<#

 Build the VM definitions for the Private Cloud VMs

   W A R N I N G
   W A R N I N G
   W A R N I N G

 Ensure that all the Cluster Shared Volumes are owned by the host on
which this
 runs.

 This script MUST be run from an elevated PowerShell environment.

 The variables in this script should be modified to reflect the
customer
 environment.


 The VMs are built onto the cluster, so even though all are built
 on one host, they will be available to other nodes after the Failover
Cluster
 refreshes.

 The CSV volume on which each VM is created is alternated.  The 'odd
numbered' VMs
 are placed on C:\ClusterStorage\Volume1, and the 'even numbered' VMs
are placed on
 C:\ClusterStorage\Volume2.  Similarly, cluster nodes to which they are
assigned
 are alternated.  Therefore, for every other VM creation below, you
will see a
 command to move it to a different host

NOTE:  The Service Manager Portal VM is not created by this routine.
This routine assumes a sysprepped Windows Server 2012 image, and the
Portal server must run Windows Server 2008 R2 SP1.

#>

# Variables to be edited for the customer environment

# Virtual Switch Names
```

```
$VMaccess = "VMaccess"
$Mgmt = "Mgmt"
$ClusComm = "ClusComm"
$iSCSIA = "iSCSI-A"
$iSCSIB = "iSCSI-B"

# Corresponding VLAN IDs

$VMaccessVLAN = "10"
$MgmtVLAN = "1"
$ClusCommVLAN = "13"
$iSCSIAVLAN = "18"
$iSCSIBVLAN = "19"

$otherNode = "F3-Infra01"

$TemplateSource = "D:\VMs\Sysprep\Virtual Hard Disks\Sysprep.vhdx"
$VHD = "\Virtual Hard Disks\"

# Since good practice would have the sysprepped disk read-only,
# this variable is used to reset the file after copying.

New-Variable -Name read_only -Value 1 -Option readonly


# Virtual Machine Names

$VMArray = @()
$VMArray +=, ("SQL01", "C:\ClusterStorage\Volume1\", 16384MB, 8)
$VMArray +=, ("SQL02", "C:\ClusterStorage\Volume2\", 16384MB, 8)
$VMArray +=, ("VMM01", "C:\ClusterStorage\Volume1\", 8192MB, 4)
$VMArray +=, ("VMM02", "C:\ClusterStorage\Volume2\", 8192MB, 4)
$VMArray +=, ("Orch01", "C:\ClusterStorage\Volume1\", 8192MB, 4)
$VMArray +=, ("Orch02", "C:\ClusterStorage\Volume2\", 8192MB, 4)
$VMArray +=, ("SM01", "C:\ClusterStorage\Volume1\", 16384MB, 4)
$VMArray +=, ("SM02", "C:\ClusterStorage\Volume2\", 16384MB, 4)
$VMArray +=, ("SMDW", "C:\ClusterStorage\Volume1\", 16384MB, 8)
$VMArray +=, ("AC01", "C:\ClusterStorage\Volume2\", 8192MB, 4)
$VMArray +=, ("WDS", "C:\ClusterStorage\Volume1\", 4096MB, 2)
$VMArray +=, ("OM01", "C:\ClusterStorage\Volume2\", 16384MB, 8)
$VMArray +=, ("OM02", "C:\ClusterStorage\Volume1\", 16384MB, 8)
$VMArray +=, ("OMRS", "C:\ClusterStorage\Volume2\", 16384MB, 8)



$i = 0
While ($i -lt $VMArray.length)
{
    $Element = $VMArray[$i]
    $VMName = $Element[0]
    $VMPath = $Element[1]
    $VMMem = $Element[2]
    $VMCpu = $Element[3]
    Write-Host "*********"
    Write-Host "*"
    Write-Host "*  Creating:" $VMName "at" (Get-Date)
```

```
    Write-Host "*"
    Write-Host "*********"
    $Dest = $VMPath + $VMName + $VHD + $VMName + ".vhdx"
    $LocDir = $VMPath + $VMName + $VHD
    $vm = New-VM -Name $VMName -Path $VMPath -MemoryStartupBytes $VMMem
    $trash = New-Item -Path $LocDir -ItemType Directory
    copy $TemplateSource $Dest
    Get-ChildItem -Path $dest |  Where-Object { $_.attributes -match
'readonly' } |
       ForEach-Object {$_.attributes = $_.attributes -Bxor $read_only }
    $vm | Add-VMHardDiskDrive -ControllerType IDE -ControllerNumber 0 -
ControllerLocation 0 -Path $Dest
    $vm_1 = $vm | Get-VMNetworkAdapter
    $vm_1 | Remove-VMNetworkAdapter
    $vm | Add-VMNetworkAdapter -Name $VMaccess -SwitchName $VMaccess
    $vm_1 = $vm | Get-VMNetworkAdapter
    $vm_1 | Set-VMNetworkAdapterVlan -Access -VlanId $VMaccessVlan
    $vm | Set-VM -ProcessorCount $VMCpu
    Add-ClusterVirtualMachineRole -VirtualMachine $VMName

 # When $i is an odd number, place on second node in cluster
    if ($i%2)
    {
        Move-ClusterGroup -Name $VMName -Node $otherNode
    }
    $i++
}


Write-Host "Completed at:" (Get-Date)
```

18.4 Set-UcsHyperVAdapters.ps1

```
# Note that the $ucsIP variable needs to be changed to reflect customer
environment

$ucsIP     = "192.168.14.100"

if  ((Get-Module  |  Where  {$_.Name  -ilike  "CiscoUcsPS"}).Name  -ine
"CiscoUcsPS")
      {
      Write-Host "Loading Module: Cisco UCS PowerTool Module"
      Import-Module CiscoUcsPs
      }

$trash   =   set-ucspowertoolconfiguration   -supportmultipledefaultucs
$false

# Connect to UCSM

$ucsCreds = Get-Credential
$UCSMHandle = Connect-Ucs $UcsIP $ucsCreds

Write-Host ""
```

```
Write-Host -ForegroundColor Yellow "Entered name of host must match
case of service profile name"
$srvr = Read-Host "Enter the name of the Hyper-V host to target"
Write-Host ""
[int]$hostNum = Read-Host "Enter a numeric value between 1-254 to use
as the host number"

Write-Host ""
Write-Host "Not all NICs should have their IP address altered, e.g.
Mgmt and iSCSI boot NICs"
$in = Read-Host "Enter a comma separated list of NICs to ignore"
$in2 = $in -replace " ",""
$ignoreNic = $in2 -split ","

Write-Host ""
$org = Read-Host "Enter Sub-Organization name of Service Profile, or
'root'"
If ($org.Length -eq 0) {$org = "root"}
$orgLevel = Get-UcsOrg -Name $org
$svcProfile = $orgLevel.DN + "/" + $srvr
Write-Host ""

# Retrieve table of NICs from the UCS Profile

$ducsVnics = Get-UcsVnic -ServiceProfile $svcProfile
If ($ducsVnics.length -eq 0)
{
    Write-Host -ForegroundColor Red "Invalid Service Profile name -
$svcProfile"
    Disconnect-Ucs
    Exit
}

# This is a special check to remove the dyanmic virtual function vNICs
created by having VM-FEX defined
$ucsVnics = @()
Foreach ($d in $ducsVnics)
{
    If ($d.addr -ne "derived")
    {
        $ucsVnics +=, $d
    }
}

Write-Host "$srvr has the following vNICs"
$ucsVnics.Name

$vlans = Get-UcsLanCloud | Get-UcsVlan | Select Name, Id
$assignedIP = @()

# Rename the NICs on the server to match the NIC name of the service
profile
# If NIC is not one entered to be ignored, change the IP address

ForEach ($u in $UcsVnics)
{
```

```
    $adapterConfig = (Get-WMIobject Win32_NetworkAdapterConfiguration -
namespace "root\CIMV2" -computername $srvr | `
        Where-Object {$_.MACaddress -eq $u.Addr})
    $hostNic = (Get-WMIobject Win32_NetworkAdapter -computername $srvr
| Where-Object {$_.Index -eq $adapterConfig.Index})
    If ($hostNic.NetconnectionID -ne $u.name)
    {
        $tmp = $hostNic.NetconnectionID ; $tmp_1 = $u.Name
        Write-Host "Changing NIC $tmp to be named $tmp_1"
        $hostNic.NetconnectionID=$u.Name
        $trash = $hostNic.Put()
    }
    $check = $FALSE

    Foreach ($ig in $ignoreNic)
    {
        If ($ig -eq $u.Name) {$check = $TRUE}
    }

    If (!$check)
    {
        Foreach ($v in $vlans)
        {
            If ($v.Name -eq $u.name)
            {
                $adapterConfig.DHCPenabled = $False
                    $adapterConfig.SetDynamicDNSRegistration($false)    |
out-null
                $newIP = "192.168." + $v.Id + "." + $hostNum
                Foreach ($aIP in $assignedIP)
                {
                    If ($newIP -eq $aIP)
                    {
                        $octets = ($newIP.split("."))
                        [int]$lastOctet = $octets[3]
                        $lastOctet++
                        $newip = $octets[0] + "." + $octets[1] + "." +
$octets[2] + "." + $lastOctet
                    }
                }
                $adapterConfig.enablestatic($newIP,"255.255.255.0")    |
out-null
                $assignedIP +=, $newIP
                Write-Host $u.Name "new IP > $newIP"
            }
        }
    }
}
```

18.5 Set-UcsHyperVRemoteMgmt.ps1

```
#
#  Set-UcsHyperVRemoteMgmt.ps1
#
# This script works on a variety of settings that are easiest done from
the
```

```
# local machine to make it remotely manageable by a management
workstation.

# Ensure Server Manager remoting is enabled
Configure-SMRemoting.exe -Enable

# Set some firewall rules

#  Enable ping requests in and out
Set-NetFirewallRule –Name “FPS-ICMP4-ERQ-In” –Enabled True
Set-NetFirewallRule –Name “FPS-ICMP6-ERQ-In” –Enabled True
Set-NetFirewallRule –Name “FPS-ICMP4-ERQ-Out” –Enabled True
Set-NetFirewallRule –Name “FPS-ICMP6-ERQ-Out” –Enabled True

#  Enable remote volume management - firewall rules need to be set on
both
#  source and destination computers
#  ***NOTE*** Policy must also be set on system to "Allow remote access
#  to the Plug and Play interface"
#  This is done with gpedit.msc locally or gpedit for domain policy
Set-NetFirewallRule –Name “RVM-VDS-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RVM-VDSLDR-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RVM-RPCSS-In-TCP” –Enabled True

#  Enable DCOM management requests in
Set-NetFirewallRule –Name “ComPlusNetworkAccess-DCOM-In” –Enabled True

#  Enable remote service management
Set-NetFirewallRule –Name “RemoteSvcAdmin-In-TCP” –Enabled True
Set-NetFirewallRule –Name "RemoteSvcAdmin-NP-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RemoteSvcAdmin-RPCSS-In-TCP” –Enabled True

#  Enable Remote Event Log Management
Set-NetFirewallRule –Name "RemoteEventLogSvc-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RemoteEventLogSvc-NP-In-TCP” –Enabled True
Set-NetFirewallRule  –Name  “RemoteEventLogSvc-RPCSS-In-TCP”  –Enabled
True

#  Enable Remote Scheduled Tasks Management
Set-NetFirewallRule –Name “RemoteTask-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RemoteTask-RPCSS-In-TCP” –Enabled True

#  Enable Windows Firewall Remote Management
Set-NetFirewallRule –Name “RemoteFwAdmin-In-TCP” –Enabled True
Set-NetFirewallRule –Name “RemoteFwAdmin-RPCSS-In-TCP” –Enabled True

#  Enable WMI management requests in
Set-NetFirewallRule –Name “WMI-WINMGMT-In-TCP” –Enabled True

#  Enable Remote Shutdown
Set-NetFirewallRule  –Name  “Wininit-Shutdown-In-Rule-TCP-RPC”  –Enabled
True

#  Set some services to automatically start and start them.
Set-Service -Name PlugPlay -StartupType Automatic
Start-Service PlugPlay
Set-Service -Name RemoteRegistry -StartupType Automatic
```

```
Start-Service RemoteRegistry
Set-Service -Name vds -StartupType Automatic
Start-Service vds

#  Enable Remote Desktop
(Get-WmiObject          Win32_TerminalServiceSetting          -Namespace
root\cimv2\TerminalServices).SetAllowTsConnections(1,1) | Out-Null
(Get-WmiObject      -Class      "Win32_TSGeneralSetting"      -Namespace
root\cimv2\TerminalServices          -Filter          "TerminalName='RDP-
tcp'").SetUserAuthenticationRequired(0) | Out-Null
```

18.6 Fast Track Software Download

FastTrackDownloadSoftware.ps1

```
$downloadDirectory = "E:\Temp\"
$path = (Get-Location)
$validate = $True

Write-Host ""
Write-Host "Start time:" (Get-Date)

# Elevate
Write-Host "Checking for elevation... "
$currentUser     =     New-Object     Security.Principal.WindowsPrincipal
$([Security.Principal.WindowsIdentity]::GetCurrent())
if
(($currentUser.IsInRole([Security.Principal.WindowsBuiltinRole]::Admini
strator)) -eq $False)
{
    $validate = $False
    Write-Host "Script must be run from elevated account."
    Exit
}

# Check PS host
If ($Host.Name -ne 'ConsoleHost')
{
    $validate = $False
    Write-Host  "FastTrackDownloadSoftware.ps1  should  not  be  run  from
ISE" -ForegroundColor Red
}

If (Test-Path "$Path\FastTrackDownloads.xml")
{
    try          {$download          =          [XML]          (Get-Content
"$Path\FastTrackDownloads.xml")}
    catch      {$validate      =      $false;      Write-Host      "Invalid
FastTrackDownloads.xml" -ForegroundColor Red}
}
    Else
    {
        $validate = $False
        Write-Host   "Missing   FastTrackDownloads.xml"   -ForegroundColor
Red
    }
```

```
If (!$validate) {Exit}

$webClient = New-Object System.Net.WebClient

$software = @()
$download.downloads.Item | ForEach-Object {
    $Item = $_
    $software += $Item
}

$software | ForEach-Object {
    $downloadName = $_.Name
    $downloadURL = $_.URL
    $downloadPath = $downloadDirectory + $_.File
    $downloadedSize = 0

# Get item download size
    $webRequest = [net.WebRequest]::Create($downloadURL)
    $webResponse = $webRequest.GetResponse()
    $downloadSize = $webResponse.ContentLength
    $webResponse.Close()
    $webRequest.Abort()
    $DownloadSizeInMB                                                    =
[System.Math]::Round(($DownloadSize/1024/1024),2)

    If ($webClient.IsBusy) {Start-Sleep 1}
    try
    {
        $webCLient.DownloadFileAsync($downloadURL,$downloadPath)
    }
    Catch
    {
        Write-Host $Error
        }

    While (!(Test-Path $downloadPath)) {Start-Sleep 1}
    While ((Get-Item $downloadPath).Length -lt $downloadSize)
    {
        $downloadCurrentSize = (Get-Item $downloadPath).Length
        $downloadCurrentSizeinMB                                         =
[System.Math]::Round(($downloadCurrentSize/1024/1024),2)
        Write-Progress -id 1 -Activity "Downloading $downloadName" -
Status   "$downloadCurrentSizeinMB   of   $downloadSizeInMB   MB"   -
PercentComplete (((Get-Item $downloadPath).Length / $downloadSize)*100)
    }
}

Write-Host "End time:" (Get-Date)
Write-Host ""
```

FastTrackDownloads.xml

```
<?xml version="1.0" encoding="utf-8"?>

<Downloads version="0.1">

    <Item>
```

```
        <Name>SystemCenter2012SP1OperationsManager </Name>

<URL>http://care.dlservice.microsoft.com/dl/download/0/3/F/03F1B876-
E7D7-45BE-8B0B-0BDBD02DD800/SC2012_SP1_SCOM_EN.exe </URL>
        <File>SC2012_SP1_SCOM_EN.exe </File>
    </Item>
    <Item>
        <Name>SystemCenter2012SPVirtualMachineManager1 </Name>

<URL>http://care.dlservice.microsoft.com/dl/download/4/8/5/485D6D85-
5811-4E7E-83F5-84F9492D3234/SC2012_SP1_SCVMM.exe </URL>
        <File>SC2012_SP1_SCVMM.exe </File>
    </Item>
    <Item>
        <Name>SystemCenter2012SP1Orchestrator </Name>

<URL>http://care.dlservice.microsoft.com/dl/download/9/9/4/99473D48-
B8E2-453D-9B34-33FEA42038F7/SC2012_SP1_SCO.exe </URL>
        <File>SC2012_SP1_SCO.exe </File>
    </Item>
    <Item>
        <Name>SystemCenter2012SP1ServiceManager </Name>

<URL>http://care.dlservice.microsoft.com/dl/download/B/F/5/BF5B6A61-
D12C-41F3-B220-6A127E24C57F/SC2012_SP1_SCSM.exe </URL>
        <File>SC2012_SP1_SCSM.exe </File>
    </Item>
    <Item>
        <Name>SystemCenter2012SP1AppController </Name>

<URL>http://care.dlservice.microsoft.com/dl/download/F/9/1/F916020F-
CCFF-427C-BF88-30318B72582F/SC2012_SP1_SCAC.exe </URL>
        <File>SC2012_SP1_SCAC.exe </File>
    </Item>
    <Item>
        <Name>SystemCenterCloudServicesProcessPack </Name>
        <URL>http://download.microsoft.com/download/2/A/4/2A495A01-
6016-4058-BC41-
CD07FE4D8C0A/System_Center_Cloud_Services_Process_Pack.zip </URL>
        <File>System_Center_Cloud_Services_Process_Pack.zip </File>
    </Item>
    <Item>
        <Name>SystemCenter2012SP1IntegrationPacks </Name>
        <URL>http://download.microsoft.com/download/1/6/5/16536A3A-
DD03-4FE8-AD32-
6DDA091FDC03/System_Center_2012_SP1_Integration_Packs.EXE </URL>
        <File>System_Center_2012_SP1_Integration_Packs.EXE </File>
    </Item>
    <Item>

<Name>SystemCenter2012ManagementPackMicrosoftWindowsServerLibrary</Name
>
        <URL>http://download.microsoft.com/download/f/7/b/f7b960c9-
7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.Library.mp </URL>
        <File>Microsoft.Windows.Server.Library.mp </File>
    </Item>
    <Item>
```

```
<Name>SystemCenter2012ManagementPackMicrosoftWindowsServer2008Discovery
</Name>
        <URL>http://download.microsoft.com/download/f/7/b/f7b960c9-
7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.2008.Discovery.mp
</URL>
        <File>Microsoft.Windows.Server.2008.Discovery.mp </File>
    </Item>
    <Item>

<Name>SystemCenter2012ManagementPackMicrosoftWindowsInternetInformation
ServicesCommonLibrary </Name>
        <URL>http://download.microsoft.com/download/F/F/1/FF13C2CF-
C955-4D3F-94EA-
4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.CommonLibrar
y.mp </URL>

<File>Microsoft.Windows.InternetInformationServices.CommonLibrary.mp
</File>
    </Item>
    <Item>

<Name>SystemCenter2012ManagementPackMicrosoftWindowsInternetInformation
Services2003 </Name>
        <URL>http://download.microsoft.com/download/F/F/1/FF13C2CF-
C955-4D3F-94EA-
4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2003.mp
</URL>
        <File>Microsoft.Windows.InternetInformationServices.2003.mp
</File>
    </Item>
    <Item>

<Name>SystemCenter2012ManagementPackMicrosoftWindowsInternetInformation
Services2008 </Name>
        <URL>http://download.microsoft.com/download/F/F/1/FF13C2CF-
C955-4D3F-94EA-
4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2008.mp
</URL>
        <File>Microsoft.Windows.InternetInformationServices.2008.mp
</File>
    </Item>
    <Item>
        <Name>SystemCenter2012ManagementPackMicrosoftSQLServerLibrary
</Name>
        <URL>http://download.microsoft.com/download/0/7/7/07714012-
3B7C-4691-9F2B-7ADE4188E552/Microsoft.SQLServer.Library.mp </URL>
        <File>Microsoft.SQLServer.Library.mp </File>
    </Item>
    <Item>
        <Name>SQLServer2012SP1 </Name>
        <URL>http://download.microsoft.com/download/3/B/D/3BD9DD65-
D3E3-43C3-BB50-0ED850A82AD5/SQLServer2012SP1-FullSlipstream-ENU-x64.iso
</URL>
        <File>SQLServer2012SP1-FullSlipstream-ENU-x64.iso </File>
    </Item>
    <Item>
```

```
        <Name>SQLServer2012AnalysisManagementObjects </Name>
        <URL>http://download.microsoft.com/download/4/B/1/4B1E9B0E-
A4F3-4715-B417-31C82302A70A/ENU/x64/SQL_AS_AMO.msi </URL>
        <File>SQL_AS_AMO.msi </File>
    </Item>
    <Item>
        <Name>SQLServer2008R2SP1AnalysisManagementObjects </Name>
        <URL>http://go.microsoft.com/fwlink/?LinkID=188448 </URL>
        <File>SQLSERVER2008_ASAMO10.msi </File>
    </Item>
    <Item>
        <Name>SQLServer2012SP1NativeClient </Name>
        <URL>http://download.microsoft.com/download/4/B/1/4B1E9B0E-
A4F3-4715-B417-31C82302A70A/ENU/x64/sqlncli.msi </URL>
        <File>sqlncli.msi </File>
    </Item>
    <Item>
        <Name>MicrosoftReportViewer2010SP1 </Name>
        <URL>http://download.microsoft.com/download/5/B/9/5B95F704-
F7E3-440D-8C68-A88635EA4F87/ReportViewer.exe </URL>
        <File>ReportViewer2010.exe </File>
    </Item>
    <Item>
        <Name>MicrosoftReportViewer2008SP1 </Name>
        <URL>http://download.microsoft.com/download/0/4/F/04F99ADD-
9E02-4C40-838E-76A95BCEFB8B/ReportViewer.exe </URL>
        <File>ReportViewer2008.exe </File>
    </Item>
    <Item>
        <Name>MicrosoftSharePointFoundation2010 </Name>
        <URL>http://download.microsoft.com/download/3/5/C/35C62B58-
0C29-4A8F-BC6B-D28CD1A6EEDD/SharePointFoundation.exe </URL>
        <File>SharePointFoundation.exe </File>
    </Item>
    <Item>
        <Name>MicrosoftSharePointFoundation2010SP1 </Name>
        <URL>http://download.microsoft.com/download/7/0/0/7002DFA1-
831C-414A-AE71-A5D18BEF1E32/sharepointfoundation2010sp1-kb2460058-x64-
fullfile-en-us.exe </URL>
        <File>sharepointfoundation2010sp1-kb2460058-x64-fullfile-en-
us.exe </File>
    </Item>
    <Item>
        <Name>WindowsAssessmentandDeploymentKit </Name>
        <URL>http://download.microsoft.com/download/9/9/F/99F5E440-
5EB5-4952-9935-B99662C3DF70/adk/adksetup.exe </URL>
        <File>adksetup.exe </File>
    </Item>
    <Item>
        <Name>Java7 </Name>

<URL>http://javadl.sun.com/webapps/download/AutoDL?BundleId=76862
</URL>
        <File>jre-7u21-windows-x64.exe </File>
    </Item>
    <Item>
        <Name>PuTTY </Name>
```

```
        <URL>http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
</URL>
        <File>putty.exe </File>
    </Item>
    <Item>
        <Name>PL2303USBtoSerialDriver </Name>

<URL>https://s3.amazonaws.com/plugable/bin/PL2303_Prolific_DriverInstal
ler_v1.7.0.zip </URL>
        <File>PL2303_Prolific_DriverInstaller_v1.7.0.zip </File>
    </Item>
</Downloads>
```

18.7 PowerShell Scripts for VNX5500 Management

Create-EMCHyperVSparesClones.ps1

```
#Replace VNX management IP address in the next line
$VNX="10.5.223.128"

#create raid group for clone private LUNs
naviseccli -h $VNX createrg 0 0_0_2 0_0_3

#create raid group and bind LUN for hot spares
naviseccli -h $VNX bind hs 4046 0_0_24
naviseccli -h $VNX bind hs 4047 0_1_23
naviseccli -h $VNX bind hs 4048 0_1_24

#bind clone private LUNs to raid group 0
Function bindcheck {
    Foreach ($lun in $lunarray)
    {
        $bound = naviseccli -address $vnx getlun $lun -bind
        Foreach ($entry in $bound)
        {
            $newentry = $entry -split ":"
            Foreach ($sentry in $newentry[1])
            {
                $sentry = $sentry.trim()
                $lun
                naviseccli -address $vnx getlun $lun -state
                naviseccli -address $vnx getlun $lun -owner
                write-host $sentry "% bound for lun $lun"
                If ($sentry -ne "100")
                {
                    Start-Sleep 20
                    bindcheck4044
                }
            }
        }
    }
}

naviseccli -h $VNX bind r1 4044 -rg 0 -cap 1 -sp a  -sq gb
naviseccli -h $VNX bind r1 4045 -rg 0 -cap 1 -sp b  -sq gb
$lunarray = 4044,4045
```

```
bindcheck

#add clone private luns
naviseccli -h $VNX clone -allocatecpl -Spa 4044 -Spb 4045 -o
If ($LastEXITCODE -ne 0)
{
    naviseccli -h $VNX clone -allocatecpl -Spa 4044 -Spb 4045 -o
    If ($LASTEXITCODE -EQ 0)
    {
        Write-Host "Retry was successful"
    }
    else
    {
        Write-Host "Retry failed"
    }
}
```

PrepMasterBoot-AddViaWWPN.ps1

```
#-----------------------------------------------------------------------
------------
# Filename:      PrepMasterBoot_AddViaWWPN.ps1
# Description:    Set up Cisco UCS ServiceProfile to do Boot from SAN
from
#                VNX5500
#-----------------------------------------------------------------------
------------
#
# Uses an XML file with the following schema.  This same schema is used
by
#  - PrepMastBoot-AddViaWWPN.ps1
#  - Process Storage Requests.ps1
#  - PostClone_AddViaWWPN.ps1
#
# <StorageParams>
# <Servers>
#   <Server>
#     <ServerName>F3-Infra01</ServerName>
#     <IPAddress>192.168.11.150</IPAddress>
#       <luns>
#         <label>MASTER-BOOT-2012</label>
#         <pool>PVTCLD_DATA1_R5</pool>
#         <size>60GB</size>
#       </luns>
#   </Server>
# </Servers>
# <Array>EnterpriseFastTrack</Array>
# <UCSAddress>10.5.177.10</UCSAddress>
# </StorageParams>
#
#-----------------------------------------------------------------------
------------

$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\CFG_STORAGE_LUNS.xml"

Function ReadStorageConfig ([String]$filename) {
    $xmlConfigFile = [xml](Get-Content $filename )
```

```
    $global:StorageConfig                                                    =
$xmlConfigFile.SelectSingleNode( '/StorageParams' )
}

ReadStorageConfig $myxmlfile

Import-Module CiscoUcsPS
Import-Module ESIPSToolkit

Function LUNExists {
      param ($TGTLUN)
      $Val = Get-EmcLUN $TGTLUN -Silent
      if ($Val -eq $null) {return $false} else {return $true}
}

Function reghostexists {
    param ($tgthost)
    $val = Get-EmcStorageRegisteredHost $tgthost
    If ($Val -eq $null) {Return $false}
    Else {Return $true}
}

$StorageArray = Get-EMCStorageSystem -ID $global:StorageConfig.Array -
Silent

If ($StorageArray -eq $null)
{
      Write-Host "ERROR: Array" $Array "is not known or registered
under that name."
      Exit 1
}


Update-EmcSystem $StorageArray

# Prompt user for connection to UCS environment
If      ($UCS      -eq      $null)      {$UCS      =      Connect-Ucs
$global:StorageConfig.UCSAddress}


ForEach ($entry in $global:StorageConfig.Servers.Server)
{
    ForEach ($lun in $entry.luns)
    {
        Write-Host $entry.Servername, $lun.label
    }
}
# Check for pre-existing LUN
If (LUNExists $global:StorageConfig.Servers.Server.luns.label)
{ # We present the LUN
    $MyServiceProfile = Get-UcsServiceProfile | where {$_.Name -eq
$global:StorageConfig.Servers.Server.ServerName}
      If ($MyServiceProfile -eq $null)
      {
          Write-Host     "ERROR:     Cannot     find     ServiceProfile"
$global:StorageConfig.Servers.Server.ServerName
            exit 1
```

```
      }
      Else
      {
#
# Extract out the WWPN initiator information for the Service Profile
#
            $MyvHBAs = Get-UcsVhba -ServiceProfile $MyServiceProfile
#
# Get the Gold Master that we plan to use
#
            $MasterLUN            =            get-EMCLun            -ID
$global:StorageConfig.Servers.Server.luns.label      -BlockStorageSystem
$StorageArray
#
# Add all the initiators from the Service Profile to the Storage Group
on the VNX
#
            ForEach ($vHBA in $MyvHBAs)
      {
                $HostRegistration = $vHBA.NodeAddr + ":" + $vHBA.Addr
            If                                          (reghostexists
$global:StorageConfig.Servers.Server.ServerName)
            {
                $rg=get-emcstorageregisteredhost
$global:StorageConfig.Servers.Server.ServerName
                Write-Host "New Init" $HostRegistration
                New-EmcStorageRegisteredInitiator -registeredhost $rg -
InitiatorIds $HostRegistration
            }
            Else
            {
                Write-Host "New Host" $HostRegistration
                New-EMCStorageRegisteredHost              -StorageSystem
$StorageArray  -HostName  $global:StorageConfig.Servers.Server.ServerName
-IpAddress       $global:StorageConfig.Servers.Server.IPAddress       -
HostBusAdapterIds $HostRegistration
            }
        }

      }
      If (LUNExists $MasterLUN)
    {
        Write-Host "unmask lun" $masterlun
        Set-EmcLunAccess -Lun $MasterLUN -InitiatorId $Hostregistration
-HostName       $global:StorageConfig.Servers.Server.ServerName       -
HostIPAddress $global:StorageConfig.Servers.Server.IPAddress -Available
      }
      Else
      { # We Fail, because the LUN cannot be found
            Write-host "ERROR: Cannot find the LUN:" $MasterLUN
            Exit 1
      }
}
```

ProcessStorageRequests.ps1

```
#-------------------------------------------------------------------------
------------
```

```
# Filename:      ProcessStorageRequests.ps1
# Description:   Create LUNs based on xml file
#
#-------------------------------------------------------------------------
------------
#
# Uses an XML file with the following schema.  This same schema is used
by
#  - PrepMastBoot-AddViaWWPN.ps1
#  - Process Storage Requests.ps1
#  - PostClone_AddViaWWPN.ps1
#
# <StorageParams>
# <Servers>
#   <Server>
#     <ServerName>F3-Infra01</ServerName>
#     <IPAddress>192.168.11.150</IPAddress>
#       <luns>
#         <label>MASTER-BOOT-2012</label>
#         <pool>PVTCLD_DATA1_R5</pool>
#         <size>60GB</size>
#       </luns>
#   </Server>
# </Servers>
# <Array>EnterpriseFastTrack</Array>
# <UCSAddress>10.5.177.10</UCSAddress>
# </StorageParams>
#
#-------------------------------------------------------------------------
------------

$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\CFG_STORAGE_LUNS.xml"

function ReadStorageConfig ([String]$filename) {
$xmlConfigFile = [xml](Get-Content $filename )
$global:StorageConfig                                                    =
$xmlConfigFile.SelectSingleNode( '/StorageParams' )
}

ReadStorageConfig $myxmlfile

Import-Module ESIPSToolkit

function LUNExists {
    param ($TGTLUN)
    $Val = Get-EmcLUN $TGTLUN -Silent
    if ($Val -eq $null) {return $false} else {return $true}
}

$StorageArray = get-EMCStorageSystem -ID $global:StorageConfig.Array -
silent

if ($StorageArray -eq $null)
{
    Write-Host "ERROR: Array" $Array "is not known or registered under
that name."
```

```
    exit 1
}

Update-EmcSystem $StorageArray

function createluns {
    foreach ($entry in $global:StorageConfig.Servers.Server) {
        foreach ($lun in $entry.luns) {
            IF (LUNExists $lun.label)
            { Write-Host "LUN" $lun.label "already exists."}
            else
          {
# We need to create the LUN
                write-host "Creating LUN" $lun.label
                $pool = get-emcstoragepool $lun.pool
                $Size = invoke-expression $lun.size
                $NewLUN = New-EmcLun -Pool $pool -Name $lun.label -
Capacity $Size -Description $lun.label
            }
        }
    }
}

createluns
```

ProcessClones.ps1

```
#-------------------------------------------------------------------------
------------
# Filename:      ProcessClones.ps1
#   Description:        Create   Clones   from   Source   LUN   based   on
ProcessClones.xml file
#
#-------------------------------------------------------------------------
------------
#
# Uses an XML file with the following schema
# <StorageParams>
# <SourceLUN>PVTCLD-MASTER-BOOT</SourceLUN>
# <TargetLUNs>
#   <lun>PVTCLD-INFRA1-BOOT</lun>
#   <lun>PVTCLD-INFRA2-BOOT</lun>
#   <lun>PVTCLD-HYPERV1-BOOT</lun>
#   <lun>PVTCLD-HYPERV2-BOOT</lun>
#   <lun>PVTCLD-HYPERV3-BOOT</lun>
#   <lun>PVTCLD-HYPERV4-BOOT</lun>
#   <lun>PVTCLD-HYPERV5-BOOT</lun>
#   <lun>PVTCLD-HYPERV6-BOOT</lun>
# </TargetLUNs>
# <CloneGroupName>Temp</CloneGroupName>
# <VNXBlockSPAAddress>10.5.223.128</VNXBlockSPAAddress>
# </StorageParams>
#
#-------------------------------------------------------------------------
------------
```

```
$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\ProcessClones.xml"
function ReadStorageConfig ([String]$filename) {
    $xmlConfigFile = [xml](cat $filename )
    $global:StorageConfig                                                    =
$xmlConfigFile.SelectSingleNode( '/StorageParams' )
    cls
    if ($global:StorageConfig.TargetLUNs.lun.count -gt "8")
    {
        write-host   "There   are"   $StorageConfig.TargetLUNs.lun.count
"clone targets, only 8 are supported concurrently"
        start-sleep 10
        exit
    }
}

ReadStorageConfig $myxmlfile

write-host "Warning You are about to overwrite the following LUNs:" -
foregroundcolor Black -backgroundcolor Yellow
foreach ($entry in $global:StorageConfig.TargetLUNs.LUN) {
    write-host $entry
}

write-host "With the contents of LUN" $global:StorageConfig.SourceLUN
$prompt =  Read-Host "Please type 'overwrite' to continue"
if ($prompt -ne "overwrite")
{
    write-host $prompt "is not valid, exiting"
    exit 1
}

function CloneStart {
    $clonesource = get-emclun $global:StorageConfig.SourceLUN
    write-host            "Creating            Clone            Group"
$global:StorageConfig.CloneGroupName
    write-host "Adding Source LUN" $clonesource
    naviseccli  -address  $global:StorageConfig.VNXBlockSPAAddress  clone
-createclonegroup   -name   $global:StorageConfig.CloneGroupName   -Luns
$clonesource.ArrayLunID -o

    foreach ($entry in $global:StorageConfig.TargetLUNs.LUN)
    {
        $clonetarget=get-emclun $entry
        write-host "Adding Clone Target LUN" $clonetarget
        naviseccli   -address   $global:StorageConfig.VNXBlockSPAAddress
clone   -addclone   -Name   $global:StorageConfig.CloneGroupName   -Luns
$clonetarget.ArrayLunId -syncrate high -o
    }
}

function CloneSyncCheck {
    $synchronized=naviseccli                                          -address
$global:StorageConfig.VNXBlockSPAAddress    clone    -listclone    -name
$global:StorageConfig.CloneGroupName   -percentsynced   |   select-string
PercentSynced
    foreach ($entry in $synchronized)
```

```
    {
        $test=$entry -split ":"
        foreach ($sentry in $test[1])
        {
            $sentry=$sentry.trim()
            write-host $sentry "% Copied per Clone target"
            if ($sentry -ne "100")
            {
                start-sleep 20
                CloneSyncCheck
            }
        }
    }
}

function CloneFracture {
    $fracture=naviseccli                                              -address
$global:StorageConfig.VNXBlockSPAAddress    clone    -listclone    -name
$global:StorageConfig.CloneGroupName | select-string CloneID
    foreach ($entry in $fracture)
    {
        $test=$entry -split ":"
        foreach ($sentry in $test[1])
        {
            $sentry=$sentry.trim()
            write-host "Fracturing Clone Target" $sentry
            naviseccli                                                -address
$global:StorageConfig.VNXBlockSPAAddress   clone   -fractureclone   -Name
$global:StorageConfig.CloneGroupName -CloneId $sentry -o
        }
    }
}

function CloneDelete {
    $cdelete=naviseccli                                               -address
$global:StorageConfig.VNXBlockSPAAddress    clone    -listclone    -name
$global:StorageConfig.CloneGroupName | select-string CloneID
    foreach ($entry in $cdelete)
    {
        $test=$entry -split ":"
        foreach ($sentry in $test[1])
        {
            $sentry=$sentry.trim()
            write-host "Deleting Clone Target" $sentry
            naviseccli                                                -address
$global:StorageConfig.VNXBlockSPAAddress   clone   -removeclone   -Name
$global:StorageConfig.CloneGroupName -CloneId $sentry -o
        }
    }
}

function CloneGroupDelete {
    write-host            "Deleting            Clone            Group"
$global:StorageConfig.CloneGroupName
    $cdelete=naviseccli                                               -address
$global:StorageConfig.VNXBlockSPAAddress clone -destroyclonegroup -name
$global:StorageConfig.CloneGroupName -o
```

```
}

CloneStart
CloneSyncCheck
CloneFracture
CloneDelete
CloneGroupDelete
```

PostClone_AddViaWWPN.ps1

```
#-------------------------------------------------------------------------
------------
# Filename:      PostClone_AddViaWWPN.ps1
# Description:    Set up Cisco UCS ServiceProfile to do Boot From SAN
from
#                VNX5500
#-------------------------------------------------------------------------
------------
#
# Uses an XML file with the following schema.  This same schema is used
by
#  - PrepMastBoot-AddViaWWPN.ps1
#  - Process Storage Requests.ps1
#  - PostClone_AddViaWWPN.ps1
#
# <StorageParams>
# <Servers>
#   <Server>
#     <ServerName>F3-Infra01</ServerName>
#     <IPAddress>192.168.11.150</IPAddress>
#       <luns>
#         <label>MASTER-BOOT-2012</label>
#         <pool>PVTCLD_DATA1_R5</pool>
#         <size>60GB</size>
#       </luns>
#   </Server>
# </Servers>
# <Array>EnterpriseFastTrack</Array>
# <UCSAddress>10.5.177.10</UCSAddress>
# </StorageParams>
#
#-------------------------------------------------------------------------
------------

$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\CFG_STORAGE_LUNS.xml"

function ReadStorageConfig ([String]$filename) {
    $xmlConfigFile = [xml](Get-Content $filename )
    $global:StorageConfig                                                =
$xmlConfigFile.SelectSingleNode( '/StorageParams' )
}

ReadStorageConfig $myxmlfile

Import-Module CiscoUcsPS
Import-Module ESIPSToolkit
```

```
function LUNExists {
    param ($TGTLUN)
    $Val = Get-EmcLUN $TGTLUN -Silent
    if ($Val -eq $null) {return $false} else {return $true}
}

function reghostexists {
    param ($tgthost)
    $val = get-emcstorageregisteredhost $tgthost
    if ($Val -eq $null) {return $false} else {return $true}
}

$StorageArray = get-EMCStorageSystem -ID $global:StorageConfig.Array -
silent

if ($StorageArray -eq $null)
{
    Write-Host "ERROR: Array" $Array "is not known or registered under
that name."
    exit 1
}


Update-EmcSystem $StorageArray

# Prompt user for connection to UCS environment
if      ($UCS      -eq      $null)      {$UCS      =      connect-ucs
$global:StorageConfig.UCSAddress}


foreach ($entry in $global:StorageConfig.Servers.Server) {
    foreach ($lun in $entry.luns) {
        write-host $entry.Servername, $lun.label

# Check for pre-existing LUN
        IF (LUNExists $lun.label)
        {
# We present the LUN
            $MyServiceProfile = Get-UcsServiceProfile | where {$_.Name
-eq $entry.ServerName}
            if ($MyServiceProfile -eq $null)
            {
                Write-Host   "ERROR:   Cannot   find   ServiceProfile"
$global:StorageConfig.Servers.Server.ServerName
                exit 1
            }
            else
            {
#
# Extract out the WWPN initiator information for the Service Profile
#

                $MyvHBAs       =       Get-UcsVhba       -ServiceProfile
$MyServiceProfile

#
# Get the Boot LUN that we plan to use
```

```
#
                $BootLUN    =    get-EMCLun    -ID    $lun.label    -
BlockStorageSystem $StorageArray

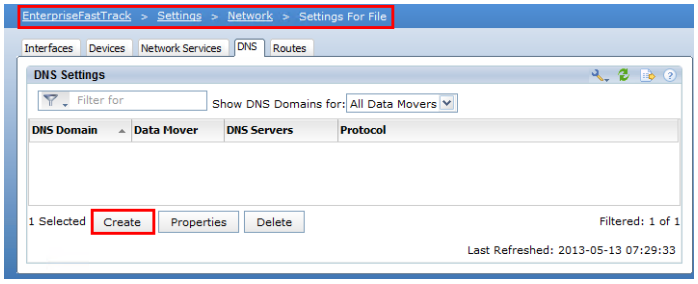
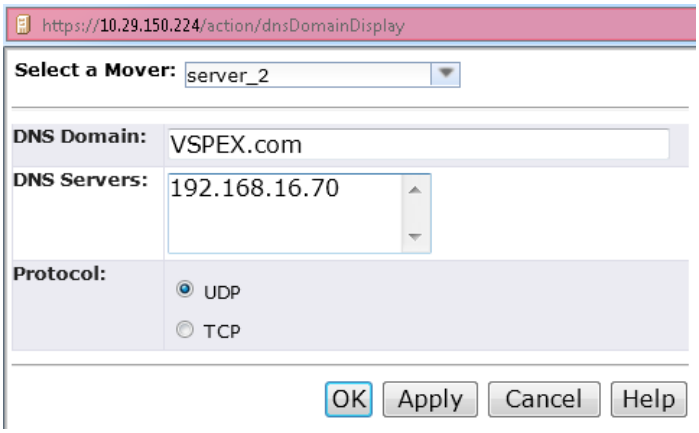
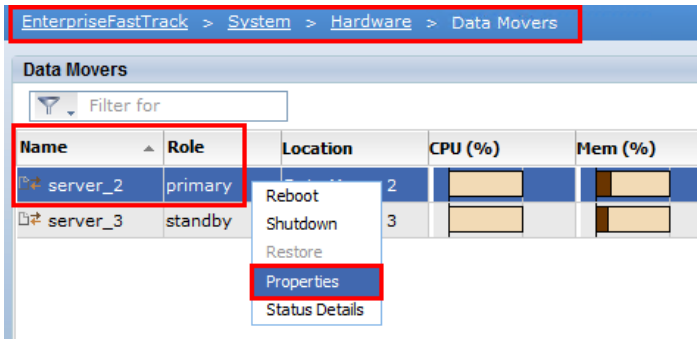
#
# Add all the initiators from the Service Profile to the Storage Group
on the VNX
#

                foreach ($vHBA in $MyvHBAs)
                {
                    $HostRegistration   =   $vHBA.NodeAddr   +   ":"   +
$vHBA.Addr
                    if (reghostexists $entry.ServerName)
                    {
                        $rg=get-emcstorageregisteredhost
$entry.ServerName
                        write-host "New Init" $HostRegistration
                        New-EmcStorageRegisteredInitiator              -
registeredhost $rg -InitiatorIds $HostRegistration
                    }
                    else
                    {
                        write-host "New Host" $HostRegistration
                        New-EMCStorageRegisteredHost      -StorageSystem
$StorageArray -HostName $entry.ServerName -IpAddress $entry.IPAddress -
HostBusAdapterIds $HostRegistration
                    }
                }
            }
            if (LUNExists $BootLUN)
            {
                write-host "unmask lun" $BootLun
                Set-EmcLunAccess     -Lun     $BootLUN     -InitiatorId
$Hostregistration     -HostName     $entry.ServerName     -HostIPAddress
$entry.IPAddress -unAvailable
            }
            else
            {
# We Fail, because the LUN cannot be found

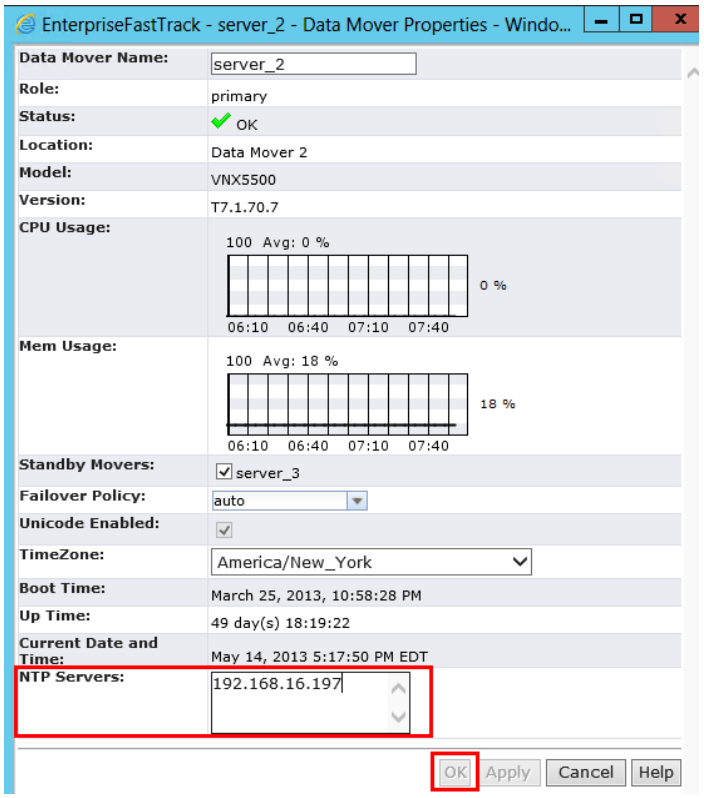
                Write-host "ERROR: Cannot find the LUN:" $BootLUN
                exit 1
            }
        }
    }
}
```

19 Appendix C: VNX5500 SMB 3.0 Configuration

19.1 Configure DNS and NTP

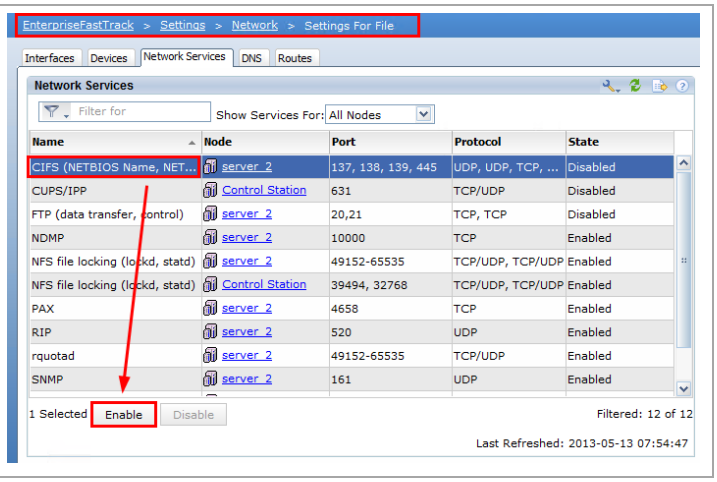
In Unisphere, go to **Settings > Network > Settings** for File Select the **DNS** tab and click **Create**.	
Enter the appropriate **DNS Domain** name and **DNS Server** addresses. Select UDP, then select **OK**	
In Unisphere, go to **System > Hardware > Data Movers** Right click on the primary blade and select **Properties**	

Enter in the appropriate **NTP Servers** and select **OK**



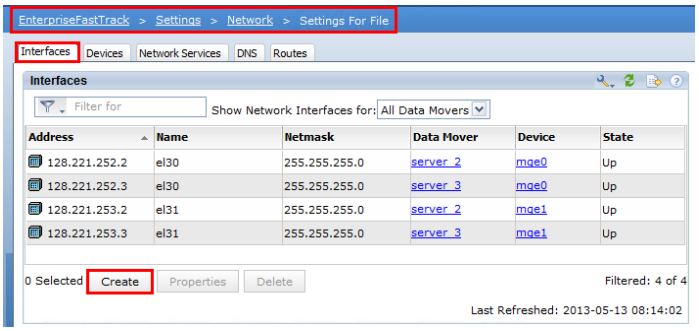
19.2 Configure Network Services

In Unisphere, go to **Settings > Network > Settings** for File
Select the **Network Services** tab
High-light **CIFS** and select **Enable**

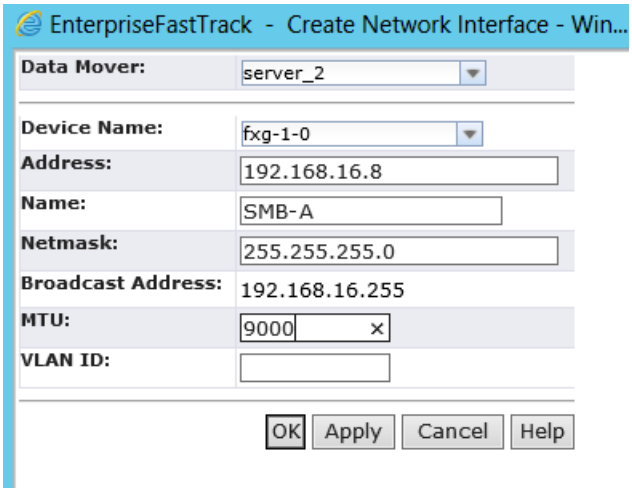


19.3 Configure Interfaces

In Unisphere, go to **Settings > Network > Settings for File**
Select the **Interfaces** tab and select **Create**

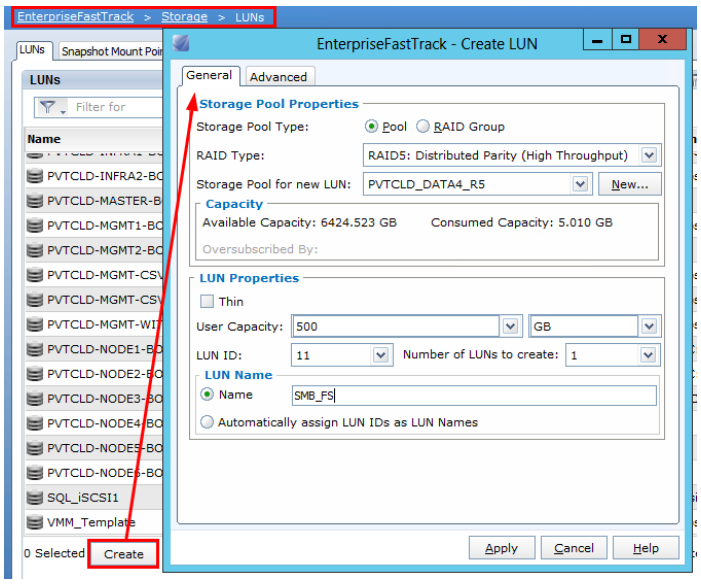


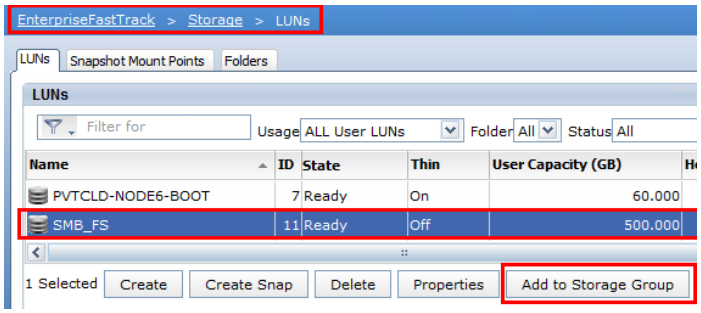
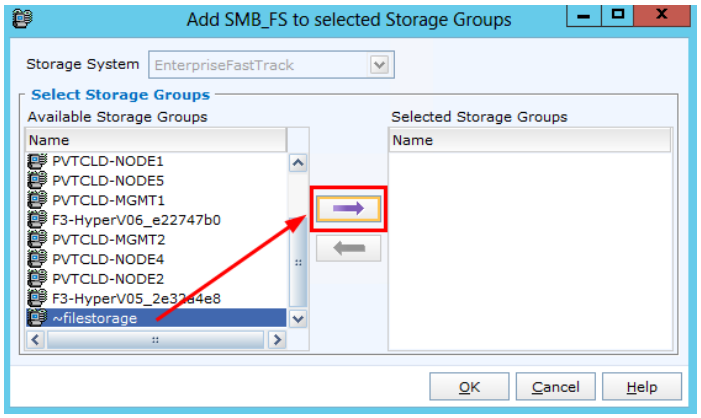
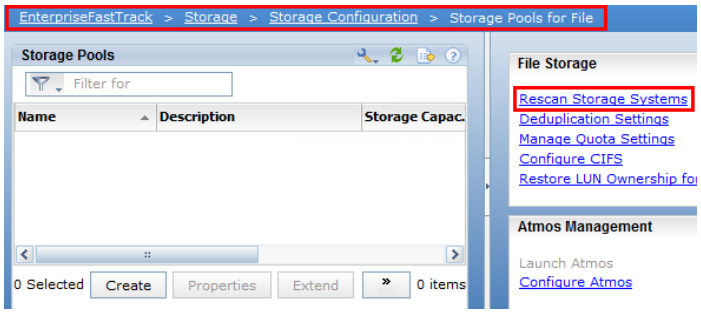
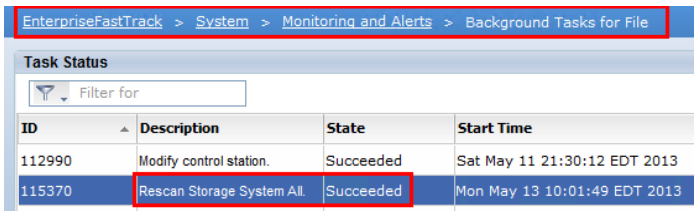
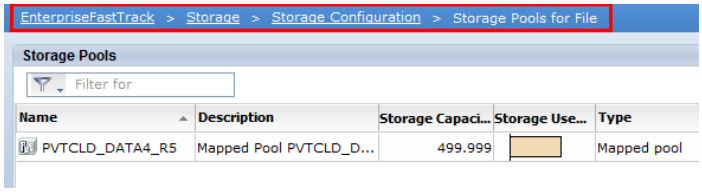
Select the appropriate device to match the desired IP address and subnet. Also set the **MTU** to **9000**.
Select **Apply**
Repeat this step to create an interface for the other physical device
Select **OK**



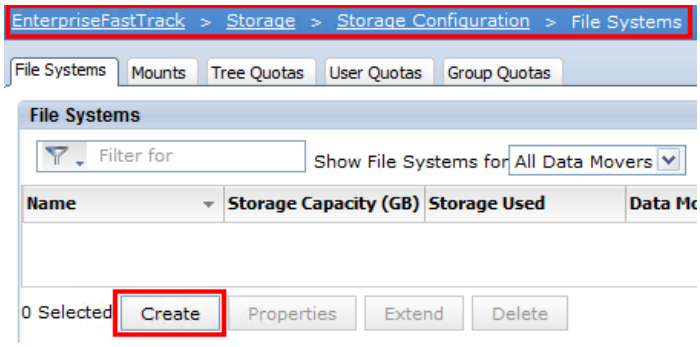
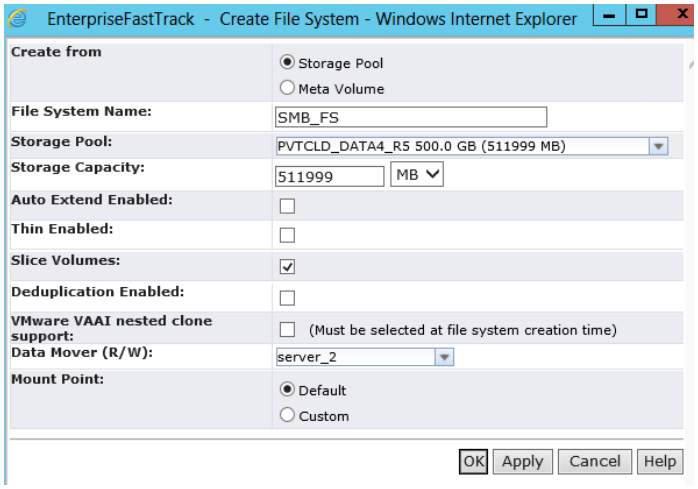
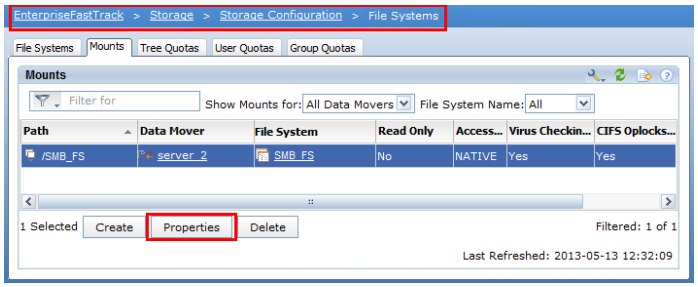
19.4 Configure Storage

In Unisphere, go to **Storage > LUNs**
Create a LUN intended for SMB use.

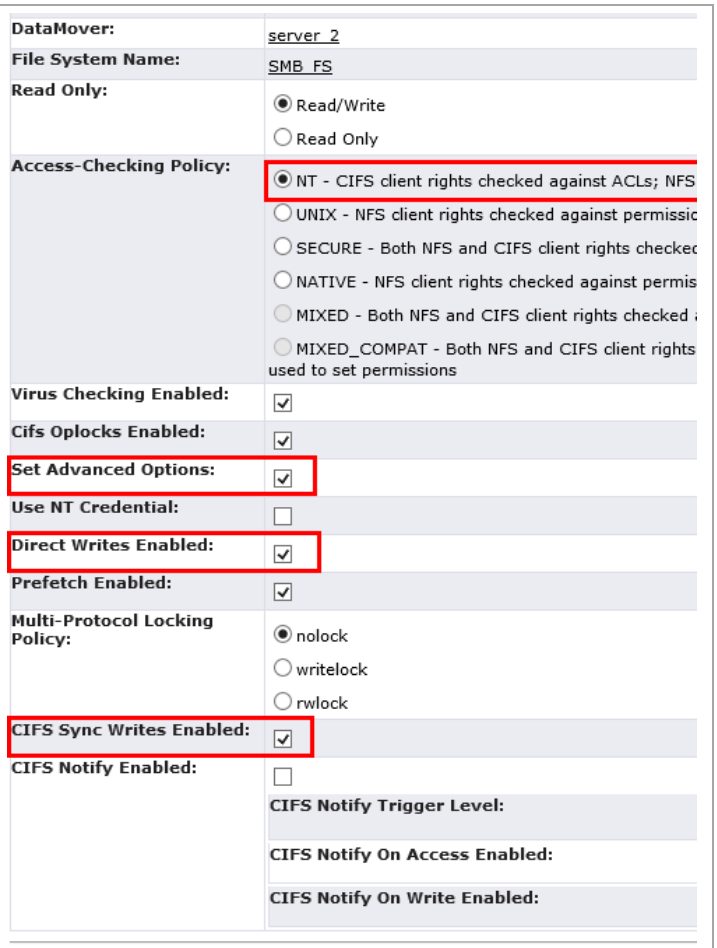


Select the newly created LUN and click **Add to Storage Group**	
Select the **~filestorage** storage group and add it to the **Selected Storage Groups** column Select **OK** Confirm selection with **Yes** Select **OK** following the successful operation.	
In Unisphere, go to **Storage > Storage Configuration > Storage Pools for File** From the **File Storage** side-bar select **Rescan Storage Systems** Select **OK** twice to proceed.	
In Unisphere, go to **System > Monitoring and Alerts > Background Tasks for File** Confirm that the background rescan **Succeeded**.	
Go back to **Storage > Storage Configuration > Storage Pools for File** Confirm a Storage Pool is automatically created using the LUN presented to the ~filestorage storage group **Note:** The automatically created "storage pool for file" will inherit the name of the block storage pool on which the LUN resides.	

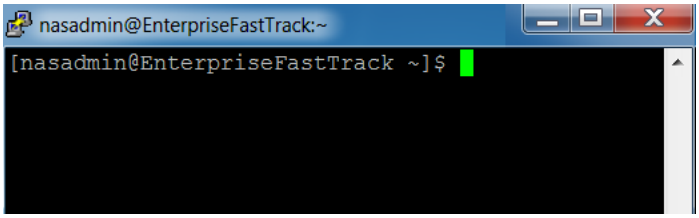
19.5 Configure SMB File Systems and Mounts

In Unisphere, go to **Storage Configuration > File Systems** From the **File Systems** tab select **Create**	
Create the file system by selecting the previously configured **Storage Pool** including the desired size and options. Select **OK.**	
From **Storage Configuration > File Systems go to the Mounts** tab. Select the automatically created mount associated with the newly created File System and click **Properties**	

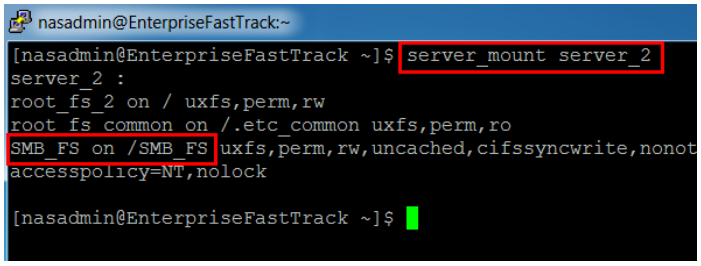
From the mount properties ensure the following settings:
Access-Checking Policy = NT – CIFS…
Set Advanced Options:
Direct Writes Enabled = Yes
CIFS Sync Writes Enabled = Yes
Select **OK** to apply the changes



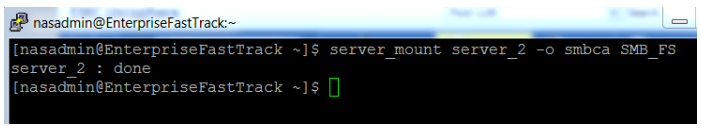
The Continuous Availability option should be enabled for file shares targeted for Hyper-V or SQL Server use.
To enable Continuous Availability, using an SSH client (like PuTTY) connect to the VNX control station as nasadmin.

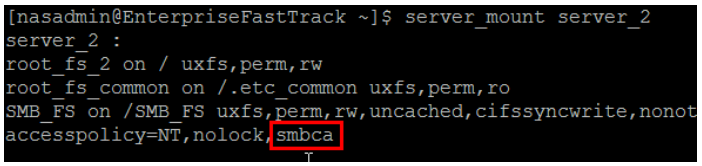


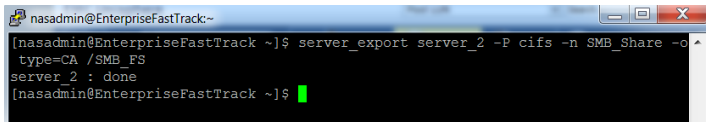
Run the 'server_mount' command against the primary datamover owning the newly created file system. For example:
`server_mount server_2`
Note the file system and path name, SMB_FS and /SMB_FS for this example

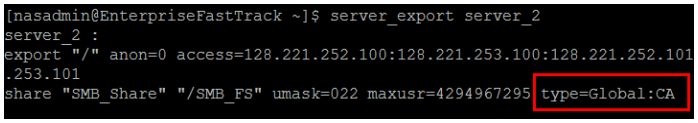


Run the following command to mount the file system with the Continuous Availability option:
`server_mount server_2 -o smbca SMB_FS`

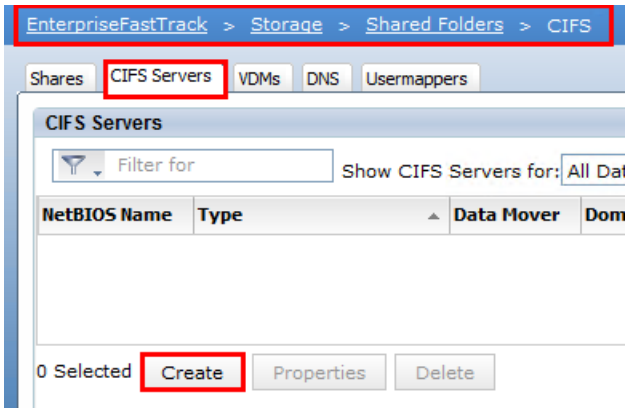


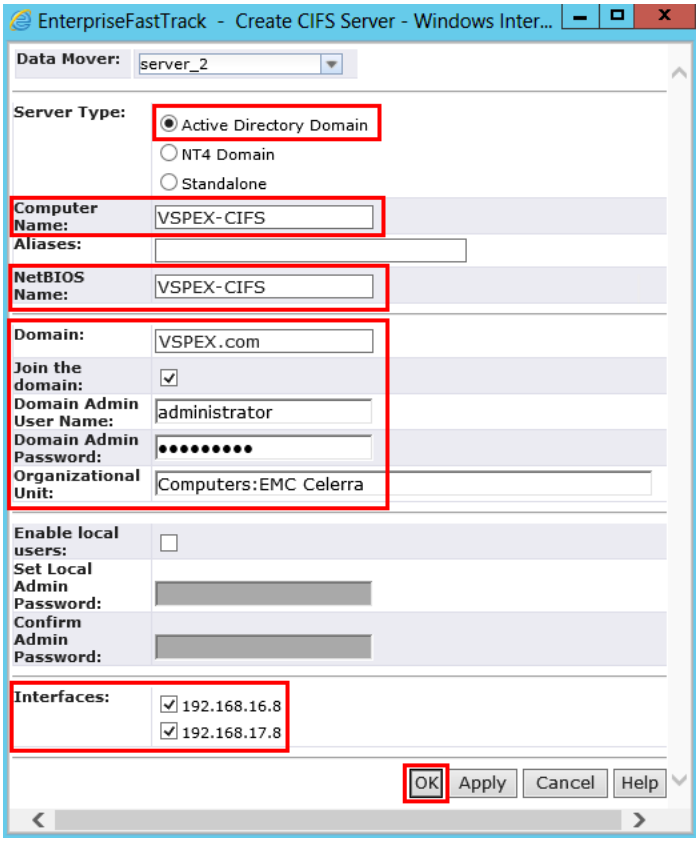
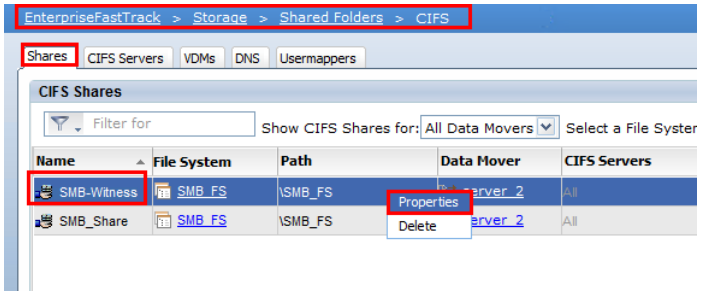
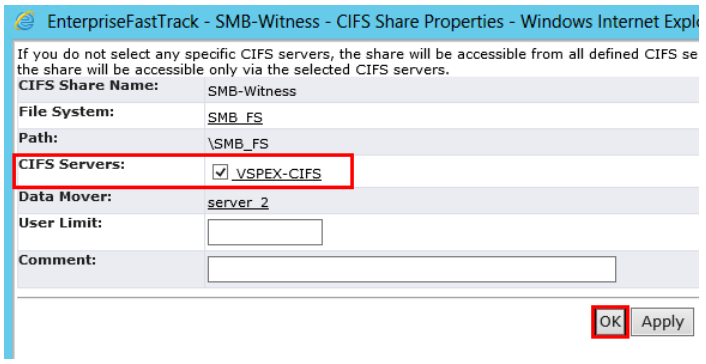
Run the `server_mount server_2` command to confirm the 'smbca' option is set.	

Run the following command to create a "share" and export the share with the CA option:
`server_export <server_number> -P cifs -n <share_name> -o type=CA <mount_path>`
For example:
`server_export server_2 -P cifs -n SMB_Share -o type=CA /SMB_FS`
Repeat this command if multiple shares are desired.
	

Run the `server_export server_2` command to confirm the CA option is set	

19.6 Configure VNX CIFS Servers and Associated Shares

In Unisphere, go to **Storage > Shared Folders > CIFS** Select the **CIFS Servers** tab and click **Create**	

Enter the desired options for **Computer Name, NetBIOS Name.** Enter the **Domain** to which to join the server with the appropriate credentials. Also select the previously configured interfaces to assign to the server. Click **OK**	
In Unisphere, go to **Storage > Shared Folders > CIFS** Select the **Shares** tab Right click on the appropriate shares to assign to the newly created CIFS server and select **Properties**	
Check off the CIFS Server and click **OK**	

20 Appendix D: Sample SMB Cluster Configuration

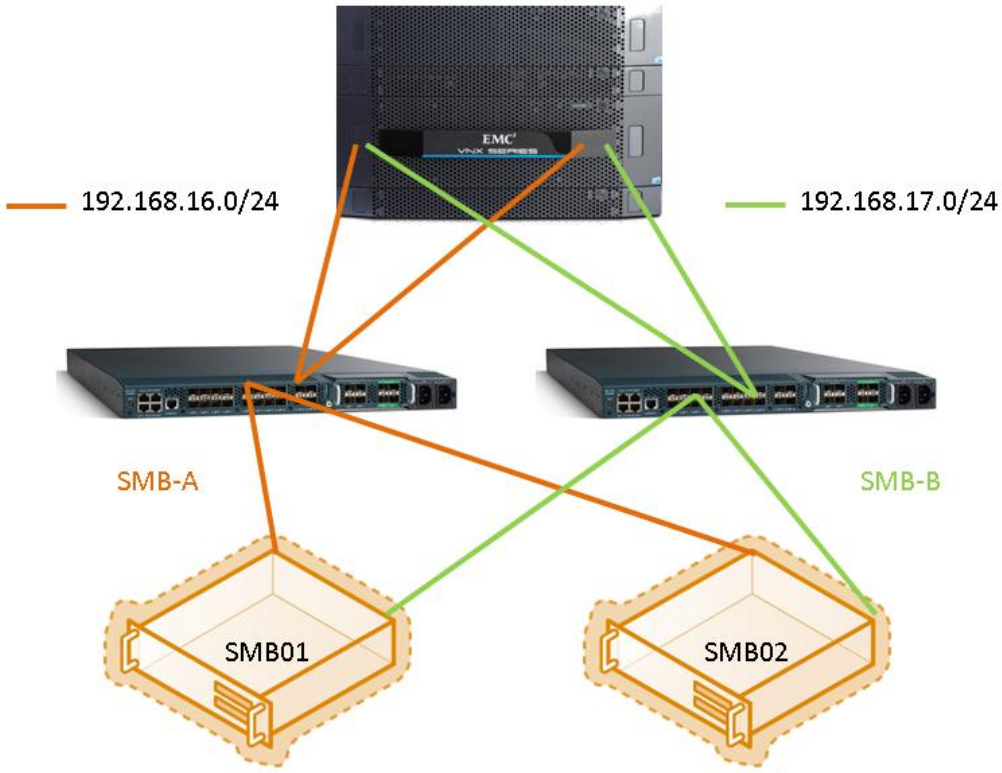
These steps detail the steps needed to create an SMB cluster using virtual machines. It assumes that the virtual machines have been configured with the Failover Clustering feature already added and are members of an Active Directory domain. This is an example to demonstrate what needs to be done. No specific cluster role has been added, but once the basic cluster is configured, it could readily for any clustered role that supports its storage on SMB shares.

20.1 Overview

One of the benefits of SMB 3.0 storage for clusters is the simplicity of configuring it for cluster storage. Windows Server will automatically use any network it finds that is connecting the servers to the SMB 3.0 storage. This is known as 'multi-channel' IO. It does not require any configuration; it is just used. This contrasts with setting up either Fibre Channel or iSCSI storage. To set up that storage requires defining the paths to the storage and then installing and configuring the paths to support multipath IO, either with Microsoft's built-in MPIO software, or with EMC's PowerPath software.

The virtual machines used in this example each contain two NICs, labeled SMB-A and SMB-B. Each is on a separate network. The A network is 192.168.16.0/24, and the B network is 192.168.17.0/24. Similarly, the VNX5500 is configured with two NICs. One presents access to the SMB share via the 192.168.16.0/24 network, and the other presents the SMB share via the 192.168.17.0/24 network. The following figure provides a conceptual picture of this example configuration.

Figure 14 Example SMB 3.0 Failover Cluster



The VNX5500 SMB Datamover has an A side controller and a B side controller. Each side has two NICs. To provide high availability, a connection from each IP subnet is connected to each side. The connection is made directly from the Cisco UCS 6248 switches with a 10 GE fibre cable to ensure maximum throughput. With this configuration, the failure of any single component will not prevent

data access from continuing. When all components are running on 10 GE connections, the potential throughput is up to 20 Gbps to both VMs.

In addition to the two networks used for data communications, there are one or more networks used for the cluster. These networks could include a public network for accessing the role being clustered, a cluster communication network, and possibly more, depending on the configuration of the role. For simplicity in this example, only a single public network is configured, but it is not shown in the figure. Both public access and cluster communication will run on this single network. The following table shows the IP configuration for this example.

Table 38 IP Configuration

Server	Role	Public	SMB-A	SMB-B
VNX-A	SMB3 Server		192.168.16.8/24	192.168.17.8/24
VNX-B	SMB3 Server		192.168.16.9/24	192.168.17.9/24
SMB01	Node 1	10.29.130.81/24	192.168.16.81/24	192.168.17.81/24
SMB02	Node 2	10.29.130.82/24	192.168.16.82/24	192.168.17.82/24
SMBClus	Cluster	10.29.130.80/24		

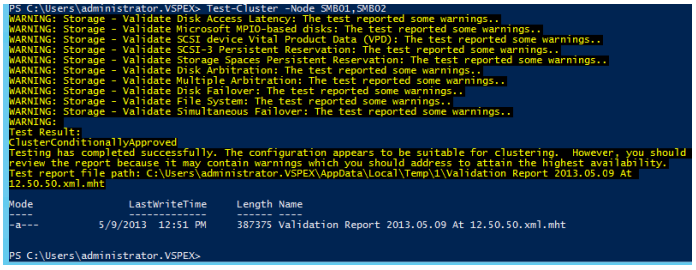
20.2 Create the Cluster

The first thing that needs to be done is to form the cluster with no storage. This will create the computer account for the cluster which is needed before adding storage to the cluster.

From a PowerShell window on one of the servers to be used to form the cluster, issue the following PowerShell command:

`Test-Cluster –Node SMB01,SMB02`

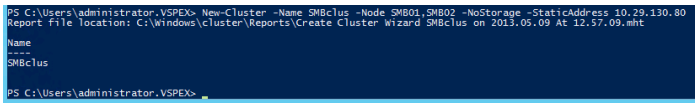
You will receive warning messages because there is no storage yet being presented to the cluster. You should view the report shown in the last line of the display to ensure there are no other errors or warnings that should be resolved before proceeding.



Once you are satisfied there are no more issues to be resolved, form the cluster with the following PowerShell command:

`New-Cluster –Name SMBClus –Node SMB01,SMB02 –NoStorage –StaticAddress 10.29.130.80`

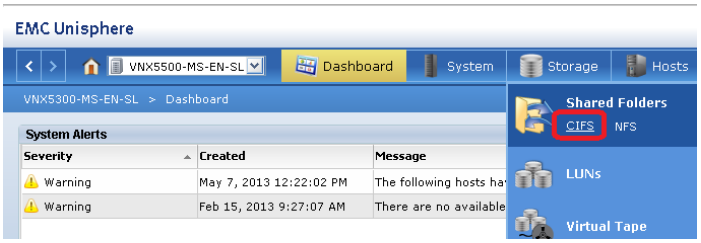
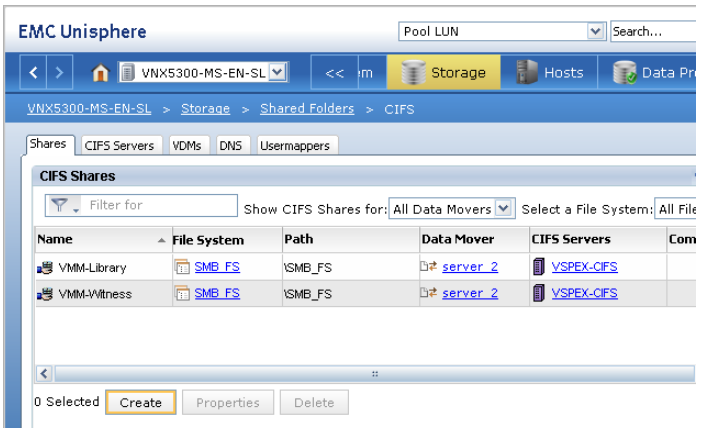
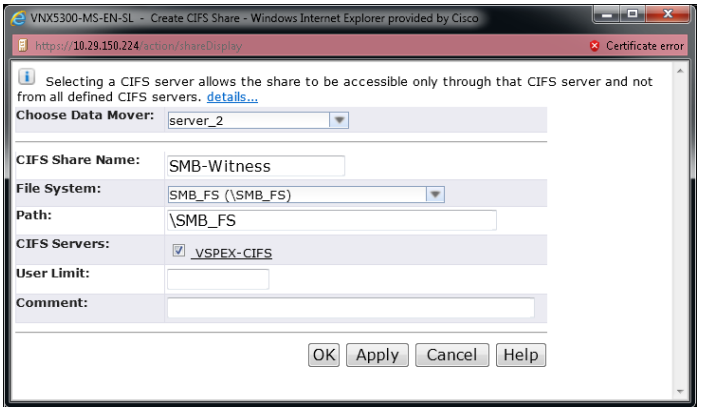
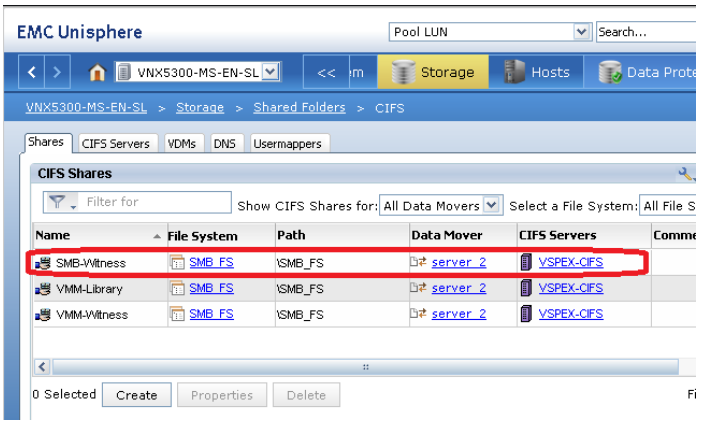
In this example, static IP addresses are being used. If DHCP addresses are being used, you would not include the –StaticAddress parameter.



20.3 VNX5500 Share Preparation

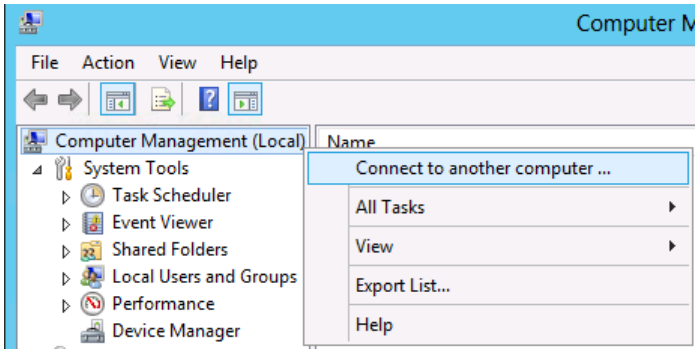
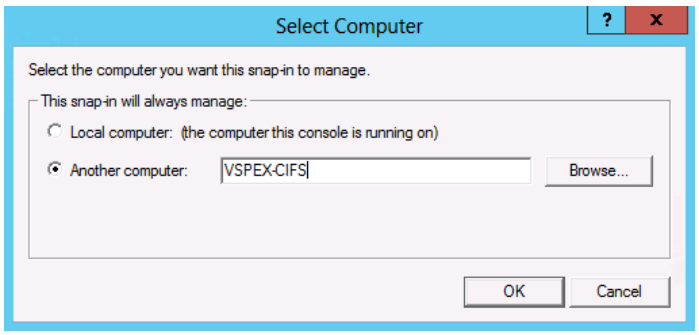
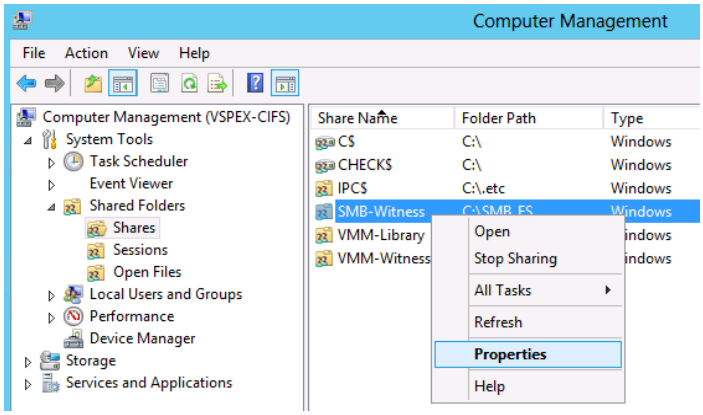
This sample assumes that the physical VNX5500 has been installed and provisioned for SMB 3.0.

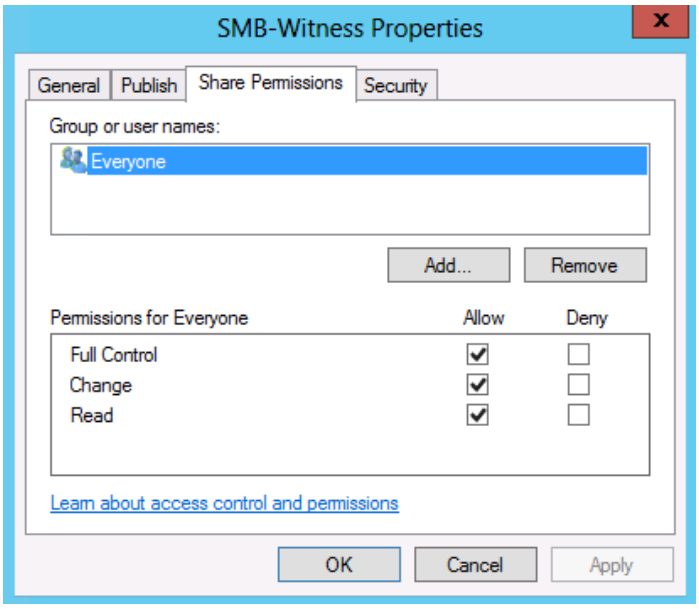
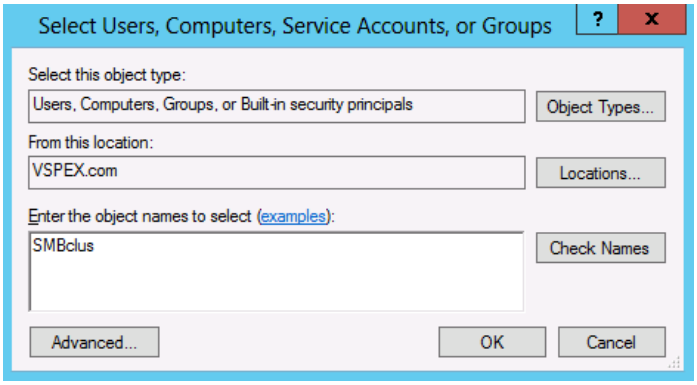
A cluster requires a quorum model of some sort. A File Share Witness is one of the options for configuring the quorum. These steps will demonstrate how to provision a File Share Witness for a Failover Cluster.

In the Unisphere console, select **Storage > Shared Folders > CIFS**.	
Click **Create** in the lower left-hand corner to create a new SMB share.	
In the **Create CIFS Share** window, enter a name for the share in the **CIFS Share Name** field. Check the box by the name of the **CIFS Server** that you want to use. Click **OK** to continue.	
The newly created share shows in the Storage > Shared Folders > CIFS window. This is all the configuration that is necessary from the Unisphere console.	

20.4 Set Share Permissions

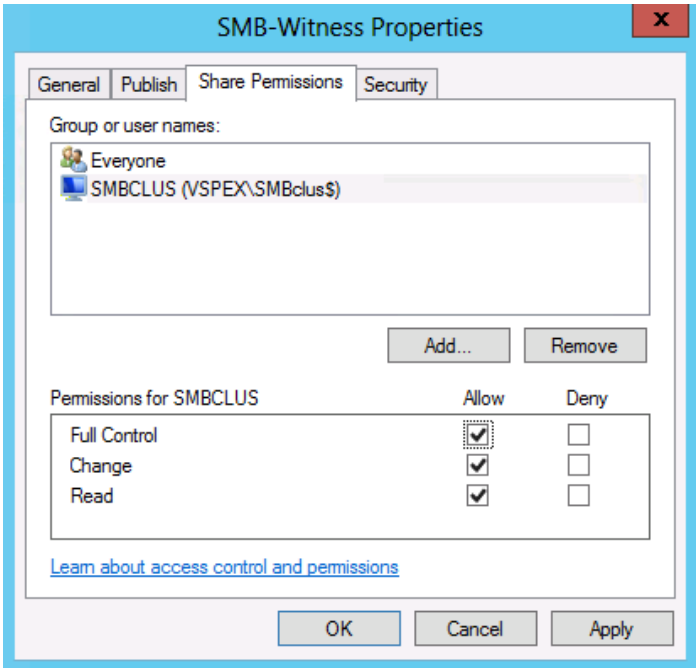
When the share is created through the Unisphere console, move to one of the servers that will be used for creating the cluster. (Actually, any Windows Server host will work.) Permissions for the share need to be set to full access.

From **Server Manager** select the **Tools** menu and select **Computer Management**. Right-click on **Computer Management (Local)** and select **Connect to another computer…** from the drop-down menu.	
Enter the name of the VNX5500 CIFS server. This is registered in Active Directory when joined to the domain. Click **OK** to continue.	
Back in **Computer Management**, expand **System Tools** and **Shared Folders**. Click on **Shares** under Shared Folders. In the center pane, right-click on the name of the share you just created and select **Properties**.	

In the share **Properties** window, click the **Add...** button to add additional access identities.	
Full access permissions must be granted to the domain administrator and the computer accounts of each node in the cluster as well as the cluster computer account. In the Selection window, ensure that Computers are one of the **Object Types** to be searched. Enter the cluster computer account name, and click **OK**.	

Click the check box for **Full Control** and click **OK**. Repeat for the node computer accounts and the domain administrator.

Note: Depending on the role being clustered, there may be additional security principals that need to be added. For example, when clustering SQL Server, the SQL Server service account must also be granted full permissions.



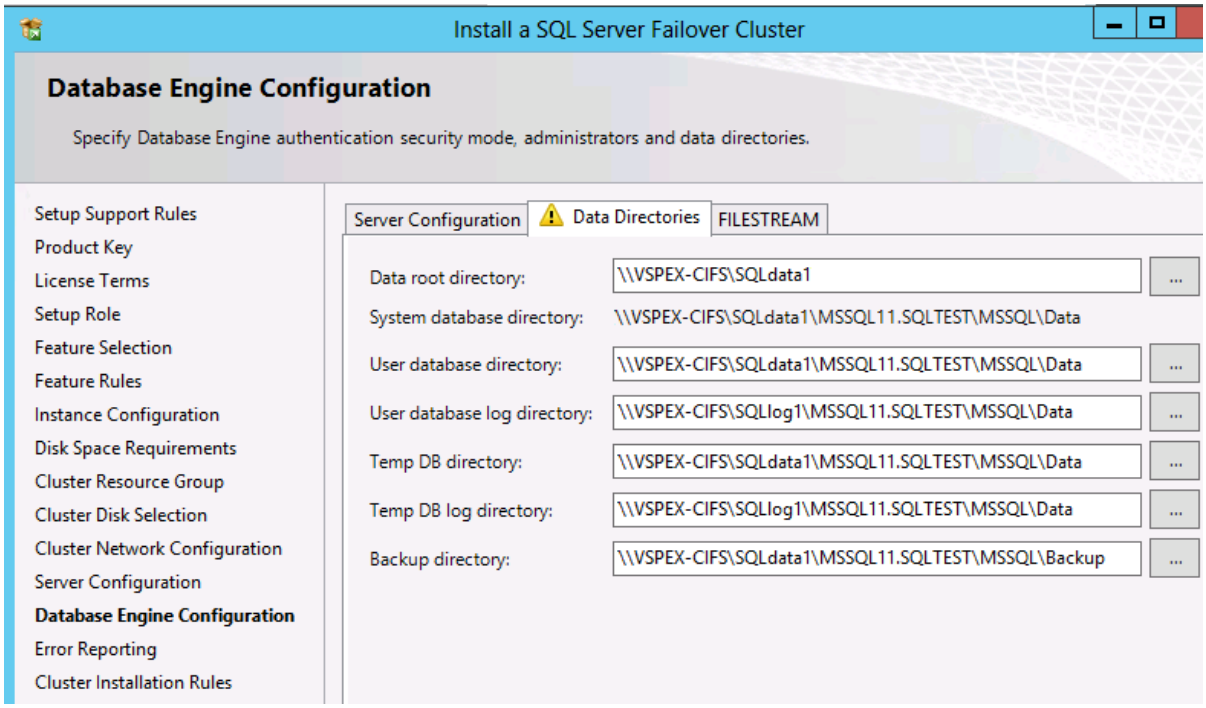
20.5 Complete the Cluster

You are now ready to add this share to the cluster as the File Share witness. Enter the following PowerShell comand to add the share.

```
Set-ClusterQuorum -NodeAndFileShareMajority '\\VSPEX-CIFS\SMB-Witness' -Cluster SMBclus
```

Follow the steps above to provision and set the protection for any other VNX SMB 3.0 share that will be used in the cluster. Roles that can make use of this storage are those roles that can use SMB shares as their storage. The additional shares are not actually added to the cluster; the roles simply point to the created shares when they are provisioning their storage. For example, when SQL Server is defining its data paths for data and logs, it looks something like the following figure:

Figure 15 Example SQL Server Storage with CIFS/SMB 3.0



In this example, two shares were created on the VNX5500 – SQLdata1 and SQLlog1.