FlexPod Datacenter with Microsoft Private Cloud V3 with 7-Mode

Deployment Guide for FlexPod with Microsoft Private Cloud V3 with Data ONTAP 8.1.2 Operating in 7-Mode

June 2013

Table of Contents

1 About the Authors 10

2 About Cisco Validated Design (CVD) Program 11

3 Reference Architecture 12

4 Configuration Guidelines 14

5 Deployment 16

6 Cabling Information 16

7 Cisco Nexus 5548UP Deployment Procedure 22

7.1 Initial Cisco Nexus 5548UP Switch Configuration 22

Nexus 5548 A 22

Nexus 5548 B 23

7.2 Enable Appropriate Cisco Nexus Features 24

Nexus A and Nexus B 24

7.3 Set Global Configurations 24

Nexus A and Nexus B 24

7.4 Create Necessary VLANs 26

Nexus A 26

Nexus B 26

Nexus A and Nexus B 26

7.5 Add Individual Port Descriptions for Troubleshooting 27

Nexus 5548 A 27

Nexus 5548 B 28

7.6 Create Necessary Port Channels 28

Nexus 5548 A 28

Nexus 5548 B 30

7.7 Add Port Channel Configurations 31

Nexus 5548 A 31

Nexus 5548 B 32

7.8 Configure Virtual Port Channels 33

Nexus 5548 A 34

Nexus 5548 B 34

7.9 Configure FCoE Fabric 35

Nexus 5548 A 35

Nexus 5548 B 35

7.10 Link into Existing Network Infrastructure 36

8 NetApp FAS3250A Deployment Procedure 36

8.1 Complete the Configuration Worksheet 36

8.2 Assign Controller Disk Ownership and Initialize Storage 36

Controller A 37

Controller B 39

8.3 Run the Setup Process 40

Controller A 40

Controller B 41

8.4 Upgrade the Service Processor on Each Node to the Latest Release 42

8.5 64-Bit Aggregates 43

Controller A 43

Controller B 43

8.6 Flash Cache 43

Controller A and Controller B 43
8.7 IFGRP LACP 43
Controller A and Controller B 44
8.8 VLAN 44
Controller A and Controller B 44
8.9 IP Config 44
Controller A and Controller B 44
8.10 Cisco Discovery Protocol 44
Controller A and Controller B 44
8.11 Storage Controller Active-Active Configuration 44
Controller A and Controller B 44
Controller A 44
8.12 NTP 45
Controller A and Controller B 45
8.13 Joining a Windows Domain (optional) 45
Controller A and Controller B 45
8.14 iSCSI 45
Controller A and Controller B 45
8.15 FCP 45
Controller A and Controller B 45
8.16 Data ONTAP SecureAdmin 46
Controller A 46
Controller B 46
8.17 Secure Shell 47
Controller A and Controller B 47
8.18 SNMP 47
Controller A and Controller B 47
8.19 SNMPv1 47
Controller A and Controller B 47
8.20 SNMPv3 48
Controller A and Controller B 48
8.21 AutoSupport HTTPS 48
Controller A and Controller B 48
8.22 Security Best Practices 48
Controller A and Controller B 48
8.23 Install Remaining Required Licenses and Enable MultiStore 48
Controller A and Controller B 48
8.24 Enable NDMP 48
Controller A and Controller B 48
8.25 Add Infrastructure Volumes 49
Controller A 49
Controller B 49
8.26 Install SnapManager licenses 49
Controller A and Controller B 49
8.27 NetApp SAN Configuration Create Device Aliases 49
Gather Necessary Information 49
Nexus 5548 A 50
Nexus 5548 B 50
9 Cisco Unified Computing System Deployment Procedure 51
9.1 Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects 51
Cisco UCS 6248 A 51
Cisco UCS 6248 B 51
Log into Cisco UCS Manager 52
9.2 Add a Block of IP Addresses for KVM Access 52

9.3 Synchronize Cisco UCS to NTP 52
9.4 Chassis Discovery Policy 52
9.5 Enable Server and Uplink Ports 53
9.6 Acknowledge the Cisco UCS Chassis 54
9.7 Create Uplink Port Channels to the Cisco Nexus 5548 Switches 55
9.8 Create an Organization 57
9.9 Create a MAC Address Pool 57
9.10 Create WWNN Pools 59
9.11 Create WWPN Pools 60
9.12 Create UUID Suffix Pools 60
9.13 Create Server Pools 61
9.14 Create VLANs 61
9.15 Create VSANs and FCoE Port Channels 66
9.16 Create a FC Adapter Policy for NetApp Storage Arrays 71
9.17 Create Host Firmware Package Policy 72
9.18 Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric 72
9.19 Create a Power Control Policy 74
9.20 Create a Local Disk Configuration Policy 75
9.21 Create a Maintenance Policy 76
9.22 Create a Server Pool Qualification Policy 76
9.23 Create a Server BIOS Policy 76
9.24 Create Dynamic vNIC Connection Policy for VM-FEX (SR-IOV) 79
9.25 Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts 80
9.26 Create a vNIC Template 80
9.27 Create vHBA Templates for Fabric A and B 88
9.28 Create Boot Policies 90
9.29 Create Service Profile Templates 94
Identify the Service Profile Template 95
Networking Section 95
Storage Section 101
Zoning Section 102
vNIC/vHBA Placement Section 103
Server Boot Order Section 104
Maintenance Policy Section 104
Server Assignment Section 105
Operational Policies Section 106
Create the Fabric-B Template. (Optional) 107
9.30 Create VM-FEX Port Profiles and Virtual Switch Clusters 109

10 Create Gold Master Boot LUN 112
10.1 Overview 113
10.2 Creation of Gold Master Boot LUN Workflow 113
Create Gold Master Service Profile 113
Create the GoldMaster Boot LUN 114
Create GoldMaster Zone 114
Prepare the Windows Server 2012 114
Install Windows Server 2012 115
Install Windows Roles and Features 117
Install the Data ONTAP PowerShell Toolkit 117
Install Windows eNIC Drivers 118
10.3 Install NetApp MPIO DSM 119
Sysprep Windows and Clean Up GoldMaster Service Profile 119
10.4 Install NetApp OnCommand Discovery Agent 120
All Hosts 120

11 Deploy Fabric Management Cluster from Gold Master 121

11.1 Create Service Profiles **121**
11.2 Gather Necessary Information **121**
11.3 Create Device Aliases **122**
Nexus 5548 A 122
Nexus 5548 B 122
11.4 Create Zones for Each Service Profile **122**
Nexus 5548 A 122
Nexus 5548 B 123
11.5 FlexClone Boot LUN **123**
11.6 Boot Service Profiles **124**
All Hosts 124
11.7 Configure Windows Networking for FlexPod **125**
All Hosts 125
11.8 Install Cisco Virtual Switch Forwarding Extensions for Hyper-V **127**
All Hosts 127
11.9 Create Hyper-V Virtual Network Switches **128**
All Hosts 128
11.10 Domain Controller Virtual Machines **129**
11.11 Prepare Nodes for Clustering **129**
All Hosts 130
11.12 Install NetApp SnapDrive **130**
Service Account Preparation 130
All Hosts 131
11.13 Install NetApp SnapManager for Hyper-V **132**
Service Account Preparation 132
All Hosts 132
11.14 Install VM-FEX Port Profile Management Utilities in Hyper-V **133**
All Hosts 133
11.15 Create a Cluster **133**
One Server Only 133
11.16 Configure Live Migration Network **133**
One Server Only 133
11.17 Create CSV LUN for VM Storage **134**
One Server Only 134
11.18 Validated the Cluster **135**

12 Create Gold Master Template VM **135**

13 Deploy Fabric Management Virtual Machines **143**
13.1 Automated Creation and Configuration **143**
13.2 Manual Creation and Configuration **144**
Create Fabric Management Virtual Guests 144
Modify Virtual Machine Settings 148
Install Windows Server on the Virtual Machines 150
13.3 Attach VM FEX Port Profile to the Clustered Virtual Machines **150**

14 SQL Server 2012 Failover Cluster Installation **157**
14.1 Overview **157**
14.2 Pre-Requisites **158**
Accounts 159
Groups 159
14.3 Configure the Network Interfaces for the SQL Server Virtual Machine **159**
Install Windows Features in the SQL Server Virtual Machine 163
Install NetApp MPIO DSM 164
Configure Windows Host iSCSI Initiator 169
Install NetApp SnapDrive in the SQL Server Virtual Machines 170

Establish the SQL Server Guest Cluster 177
Create and Map iSCSI LUNs using SnapDrive for SQL Server 182
Change the SQL Server Cluster to Use a Quorum Disk 187
Assign SQL Cluster Disk Names 189
Validated the SQL Server Cluster 190
Create Required User Accounts and Security Groups 192
14.4 Install SQL Server 2012 SP1 198
Install the SQL Server Named Instances on the Guest Cluster (Node 1) 198
Install the SQL Server Named Instances on the Guest Cluster (Node 2) 213
14.5 Post-Installation Tasks 218
Configure Windows Firewall Settings for SQL Named Instances 218
Assign Preferred Owners for SQL Instances in Failover Cluster Manager 233

15 Virtual Machine Manager 236
15.1 Overview 236
15.2 Pre-Requisites 237
Accounts 237
Groups 237
Install the Windows Assessment and Deployment Kit 238
15.3 Install the Pre-Requisite Windows Server Roles and Features 240
Install the SQL Server 2012 SP1 Command Line Utilities 245
Install NetApp MPIO DSM 251
Configure Windows Host iSCSI initiator 256
Install NetApp SnapDrive 257
Create the Cluster 264
Create and Map the LUNs using SnapDrive 267
Change the VMM Server Cluster to Use a Quorum Disk 271
Validated the VMM Server Cluster 273
Create the Virtual Machine Manger Distributed Key Management Container in Active Director Domain Services 275
15.4 Installation 280
Install the Virtual Machine Manager Failover Cluster 280
Creating Virtual Machine Manager Library Share on a Failover Cluster 295
15.5 Add Fabric Management Resources Virtual Machine Manager 308
15.6 Configure Logical Networks 312
15.7 Install the NetApp SCVMM GUI Extension 314
Install the NetApp OnCommand Plug-In GUI Extension 314
Register the NetApp OnCommand Plug-In GUI Extension 316
Configure NetApp OnCommand Plug-In SCVMM GUI Extension 317
15.8 Install Cisco UCS User Interface Extensions for Virtual Machine Manager 318
15.9 Install Cisco UCS PowerTool 321

16 Install and Configure Nexus 1000V for Hyper-V 323
16.1 Intall the Virtual Supervisor Modules Virtual Machine Template 323
16.2 Creat the Virtual Supervisor Modules in the VMS Virtual Machines 327
16.3 Add a Domain Name Service Record for the Virtual Supervisor Module 335
16.4 Configure Virtual Supervisor Modules in the VMS Virtual Machines 336
16.5 Configure Nexus 1000V VSM For Use with Virtual Machine Manager 343
16.6 Configure Virtual Switch Extension Manager in Virtual Machine Manager 343
16.7 Copy Virtual Ethernet Module Installation Packager to the Virtual Machine Manager Virtual Machines 350
16.8 Configure a Logical Switch In Virtual Machine Manager 350
16.9 Creating the Logical Switch on the Hyper-V Hosts 358
16.10 Create a VM Network 361
16.11 Configure the Virtual Machine Manager Virtual Manchine Properties 363
16.12 Configure Virtual Machine Manager Network Interfaces 370

16.13 Rename the New Cluster Network 374
16.14 Configure System Center Application Virtual Machine Network Interfaces 378

17 Install and Configure the SMI-S Provider 382
17.1 Install the SMI-S Provider 382
17.2 Configure the SMI-S Provider 384
17.3 Register SMI-S in SCVMM 384

18 Operations Manger 388
18.1 Overview 388
18.2 Pre-Requisites 389
Accounts 389
Groups 389
Add the .NET Framework 3.5 Feature 390
Install the SQL Server Reporting Services and Analysis Services (Split Configuration) 393
Install Microsoft Report Viewer 2010 SP1 409
Configuration of Operations Manager SQL Server Prerequisites 412
18.3 Installation 415
Install the Operations Manager Management Server 415
Install the Operations Manager Reporting Server 421
18.4 Post-Installation Tasks 426
Register the Required Service Principal Names for the Operations Manager Management Servers 426
Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Server Nodes 428
Install Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server 431
Install Operations Manager Console on the Virtual Machine Manager Management Server 434
Download and Import the Required Prerequisite Management Packs in Operations Manager 438
Install SQL Analysis Management Objects 441
Perform Virtual Machine Manager and Operations Manager Integration 446
18.5 Install NetApp Management Pack 449
Install and Configure SNMP 449
Install NetApp OnCommand Plug-In Management Pack 451
Enable NetApp OnCommand Plug-In Management Pack 455
Configure NetApp OnCommand Plug-In Management Pack 457
18.6 Install the Cisco UCS Management Pack 459
Configuring SCOM to Monitor Cisco Unified Computing System 461
Creating an Administration Account 468
Associating a Run As Account with a Run As Profile 471
Configuring Bidirectional Communication 474

19 Service Manager 478
19.1 Overview 478
19.2 Pre-Requisites 479
Accounts 479
Groups 481
Add the .NET Framework 3.5 Feature on all Server Manager Servers 481
Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers 485
Install SQL Server 2012 Native Client on the on the Management and Data Warehouse Servers 488
Install SQL Server 2012 SP1 Analysis Management Objects 491

Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server 493
Install SharePoint Foundation 2010 Service Pack 1 on the Self-Service Portal Server ... 506
Install .NET Framework 4 on the Self-Service Portal Server 516
Request and Install an SSL Certificate on the Self-Service Portal Server 517
Configuration of Service Manager Environmental Prerequisites 521
19.3 Installation 524
Install the Service Manager Management Server 524
Install the Service Manager Data Warehouse Server 534
Install the Service Manager Self-Service Portal Server 552

20 Orchestrator 560
20.1 Overview 560
20.2 Pre-Requisites 561
Accounts 561
Groups 561
Add the .NET Framework 3.5 Feature 561
Install the Silverlight Runtime 565
20.3 Installation 565
Install the Orchestrator Runbook, Web Service and Designer Server 565
Install an Additional Orchestrator Runbook Server 575
20.4 Install NetApp Integration Pack 583
20.5 Install Cisco UCS Integration Pack 586
20.6 Install Cisco UCS PowerTool 586
20.7 Post-Installation Tasks 589
Install the Virtual Machine Manager Console 589
Install the Microsoft Report Viewer 2010 SP1 592
Install the Operations Manager Console 594
Install System Center 2012 SP1, NetApp, and Cisco UCS Integration Packs 598
Deploy Integration Packs 602

21 App Controller 611
21.1 Overview 613
21.2 Pre-Requisites 613
Accounts 613
Groups 613
Install the .NET Framework 3.5 Feature 614
Install Silverlight Runtime 617
Install the Virtual Machine Manager Console 618
21.3 Installation 622
Install the App Controller Portal Server 622

22 System Center Cloud Services Process Pack 629
22.1 Overview 630
22.2 Pre-Requisites 631
Deploy Chargeback Report Files on the Operations Manager Management Server 631
Deploy Chargeback Report Files on the Service Manager Management Server 632
Create the System Center Operations Manager Connector 634
Create the OrchestratorUsersGroup local group on the Orchestrator Server 636
22.3 Installation 638
Install the Cloud Services Process Pack 638
Install the Cloud Services Process Pack Runbooks 640

23 Deploy App Cluster 644
23.1 Create Service Profiles 644
23.2 Gather Necessary Information 644
23.3 Create Device Aliases 644

Cisco Nexus 5548 A 645
Cisco Nexus 5548 B 645
23.4 Create Zones for Each Service Profile 645
Cisco Nexus 5548 A 645
Cisco Nexus 5548 B 646
23.5 FlexClone Boot LUN 646
23.6 Boot Service Profiles 647
All Hosts 647
23.7 Configure Windows Networking for FlexPod 648
All Hosts 648
23.8 Install Cisco Virtual Switch Forwarding Extensions for Hyper-V 650
All Hosts 650
23.9 Create Hyper-V Virtual Network Switches 651
All Hosts 651
23.10 Prepare Nodes for Clustering 652
All Hosts 652
23.11 Install NetApp SnapDrive 653
Service Account preparation 653
All Hosts 653
23.12 Install NetApp SnapManager for Hyper-V 655
Service Account preparation 655
All Hosts 655
23.13 Install VM-FEX Port Profile Management Utilities in Hyper-V 655
All Hosts 655
23.14 Create a Cluster 656
One Server Only 656
23.15 Configure Live Migration Network 656
One Server Only 656
23.16 Configure Quorum LUN 656
One Server Only 657
23.17 Create CSVs LUN for VM Storage 658
One Server Only 658
23.18 Validated the Cluster 658
23.19 Add the Cluster to SCVMM 659
23.20 Creating the Logical Switch on the Hyper-V Hosts 662

APPENDIX A: Installing Cisco UCS PowerTool 665

APPENDIX B: Installing the Data ONTAP PowerShell Toolkit 668

1 About the Authors

Mike Mankovsky, Technical Leader, Cisco Systems
Mike Mankovsky is a Cisco Unified Computing System architect, focusing on Microsoft solutions with extensive experience in Hyper-V, storage systems, and Microsoft Exchange Server. He has expert product knowledge in Microsoft Windows storage technologies and data protection technologies.

Glenn Sizemore, Technical Marketing Engineer, NetApp
Glenn Sizemore is a Technical Marketing Engineer in the Microsoft Solutions Group at NetApp, where he specializes in Cloud and Automation. Since joining NetApp, Glenn has delivered a variety of Microsoft based solutions ranging from general best practice guidance to co-authoring the NetApp Hyper-V Cloud Fast Track with Cisco reference architecture.

Adam Fazio, Microsoft
Adam Fazio is a Solution Architect in the Worldwide Datacenter and Private Cloud Center of Excellence organization with a passion for evolving customers' IT infrastructure from a cost-center to a key strategic asset. With focus on the broad Core Infrastructure Optimization model, his specialties include: Private & Hybrid Cloud, Datacenter, Virtualization, Management & Operations, Storage, Networking, Security, Directory Services, People & Process. In his 14 years in IT, Adam has successfully led strategic projects for Government, Education Sector, and Fortune 100 organizations. Adam is a lead architect for Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track program. Adam is a course instructor, published writer and regular conference speaker on Microsoft Cloud, Datacenter, and Infrastructure solutions.

Joel Yoker, Microsoft
Joel Yoker is an Architect in the Americas Office of the Chief Technical Officer (OCTO) organization focusing on Private Cloud, Datacenter, Virtualization, Management & Operations, Storage, Networking, Security, Directory Services, Auditing and Compliance. In his 14 years at Microsoft, Joel has successfully led strategic projects for Government, Education Sector, and Fortune 100 organizations. Joel is a lead architect for Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track program and serves as course instructor, published writer and regular conference speaker on Microsoft Private Cloud, virtualization and infrastructure solutions.

Jeff Baker, Microsoft
Jeff Baker is an Architect in the Center of Excellence for Private Cloud at Microsoft Corporation. Jeff has worked with datacenter focused virtualization, management and operations technologies for almost a decade of his 14 plus years in IT. Jeff has IT experience in a broad range of industries including Government, Education, Healthcare, Energy and Fortune 100 companies. Jeff has worked extensively with Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track programs. Jeff is a regular conference speaker on Microsoft Private Cloud, virtualization and infrastructure solutions.

2 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)

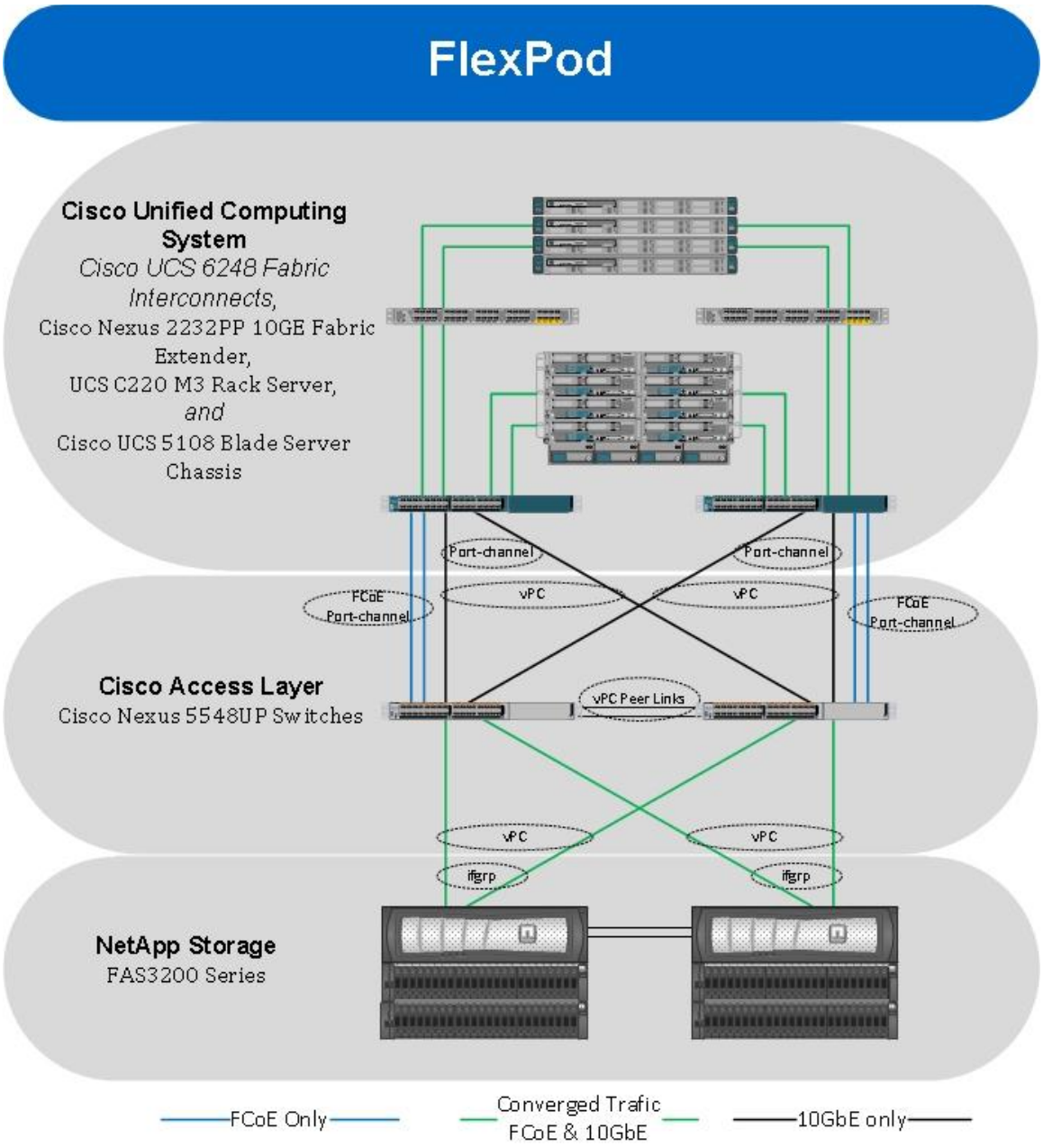
© 2013 Cisco Systems, Inc. All rights reserved

3 Reference Architecture

FlexPod architecture is highly modular, or pod-like. Although each customer's FlexPod unit might vary in its exact configuration, after a FlexPod unit is built, it can easily be scaled as requirements and demands change. This includes both scaling up (adding additional resources within a FlexPod unit) and scaling out (adding additional FlexPod units).

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated foundation for all virtualization solutions. FlexPod with Microsoft Private Cloud validated with Microsoft Private Cloud Fast Track v3 includes NetApp® FAS 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 1 Architecture Overview



The reference configuration shown in Figure 1 includes:

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 6248 fabric interconnects
- Two Cisco Nexus 2232 fabric extenders
- One chassis of Cisco UCS blades with two fabric extenders per chassis
- Four Cisco USC C220 M3 Blade Servers
- One FAS3250A (HA pair)

Storage is provided by a NetApp FAS3250A with accompanying disk shelves. All systems and fabric links feature redundancy and provide end-to-end high availability. For server virtualization, the

deployment includes Hyper-V. Although this is the base design, each of the components can be scaled flexibly to support specific business requirements. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves could be deployed to improve I/O capacity and throughput, or special hardware or software features could be added to introduce new features.

Note: This is a sample bill of materials (BoM) only. This solution is certified for use with any configuration that meets the FlexPod Technical Specification rather than for a specific model. FlexPod and Fast Track programs allow customers to choose from within a model family to make sure that each FlexPod with Microsoft Windows Server 2012 Hyper-V solution meets the customers' requirements.

The remainder of this document guides you through the low-level steps for deploying the base architecture, as shown in Figure 1. This includes everything from physical cabling, to compute and storage configuration, to configuring virtualization with Hyper-V.

4 Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration. Therefore, references are made as to which component is being configured with each step, whether it is A or B. For example, Controller A and Controller B are used to identify the two NetApp 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 similarly configured. Additionally, this document details steps for provisioning multiple Cisco UCS hosts and these are identified sequentially: VMHost-Mgmt-01 and VMHost-Mgmt-02, and so on. Finally, to indicate that the reader should include information pertinent to their environment in a given step, <*italicized text*> appears as part of the command structure. See the following example 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 <management VLAN ID>
```

This document is intended to allow the reader to fully configure the customer environment. In this process, various steps require the reader to insert customer specific naming conventions, IP addresses and VLAN schemes as well as to record appropriate WWPN, WWNN, or MAC addresses.

Table 1 details the list of VLANs necessary for deployment as outlined in this guide. Note that in this document that the VM-Data VLAN is used for virtual machine management interfaces. The VM-Mgmt VLAN is used for management interfaces of the Microsoft Hyper-V hosts. A Layer-3 route must exist between the VM-Mgmt and VM-Data VLANS.

Table 1 Necessary VLANs

VLAN Name	VLAN Purpose	ID Used in this Document
Mgmt	VLAN for management interfaces	805
Native	VLAN to which untagged frames are assigned	2
CSV	VLAN for cluster shared volume	801
iSCSI-A	VLAN for iSCSI traffic for fabric A	802
iSCSI-B	VLAN for iSCSI traffic for fabric B	807
Live Migration	VLAN designated for the movement of VM's from one physical host to another	803
VM Cluster Comm	VLAN for cluster connectivity	806
Database	VLAN for database access	1001
MF-Public	VLAN for application access	1002

5 Deployment

This document details the necessary steps to deploy base infrastructure components as well for provisioning Microsoft Hyper-V as the foundation for virtualized workloads. At the end of these deployment steps, you will be prepared to provision applications on top of a Microsoft Hyper-V virtualized infrastructure.

The FlexPod Validated with Microsoft Private Cloud 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 FlexPod Validated with Microsoft Private Cloud architecture.

6 Cabling Information

The following information is provided as a reference for cabling the physical equipment in a FlexPod 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 FAS3250 running Data ONTAP 8.1.2. This configuration leverages a dual-port 10GbE unified target adapter and the onboard SAS ports for disk shelf connectivity. For any modifications of this prescribed architecture, consult the currently available NetApp Interoperability Matrix Tool (IMT).

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 a FAS3250A system in a different configuration from what is prescribed in the tables in this section. Before starting, be sure the configuration matches what is described in the tables and diagrams in this section

Figure 2 shows a FlexPod cabling diagram. The labels indicate connections to end points rather than port numbers on the physical device. For example, connection 1 is an FCoE target port connected from NetApp controller A to Nexus 5548 A. SAS connections 23, 24, 25, and 26 as well as ACP connections 27 and 28 should be connected to the NetApp storage controller and disk shelves according to best practices for the specific storage controller and disk shelf quantity.

Figure 2 FlexPod Cabling Diagram

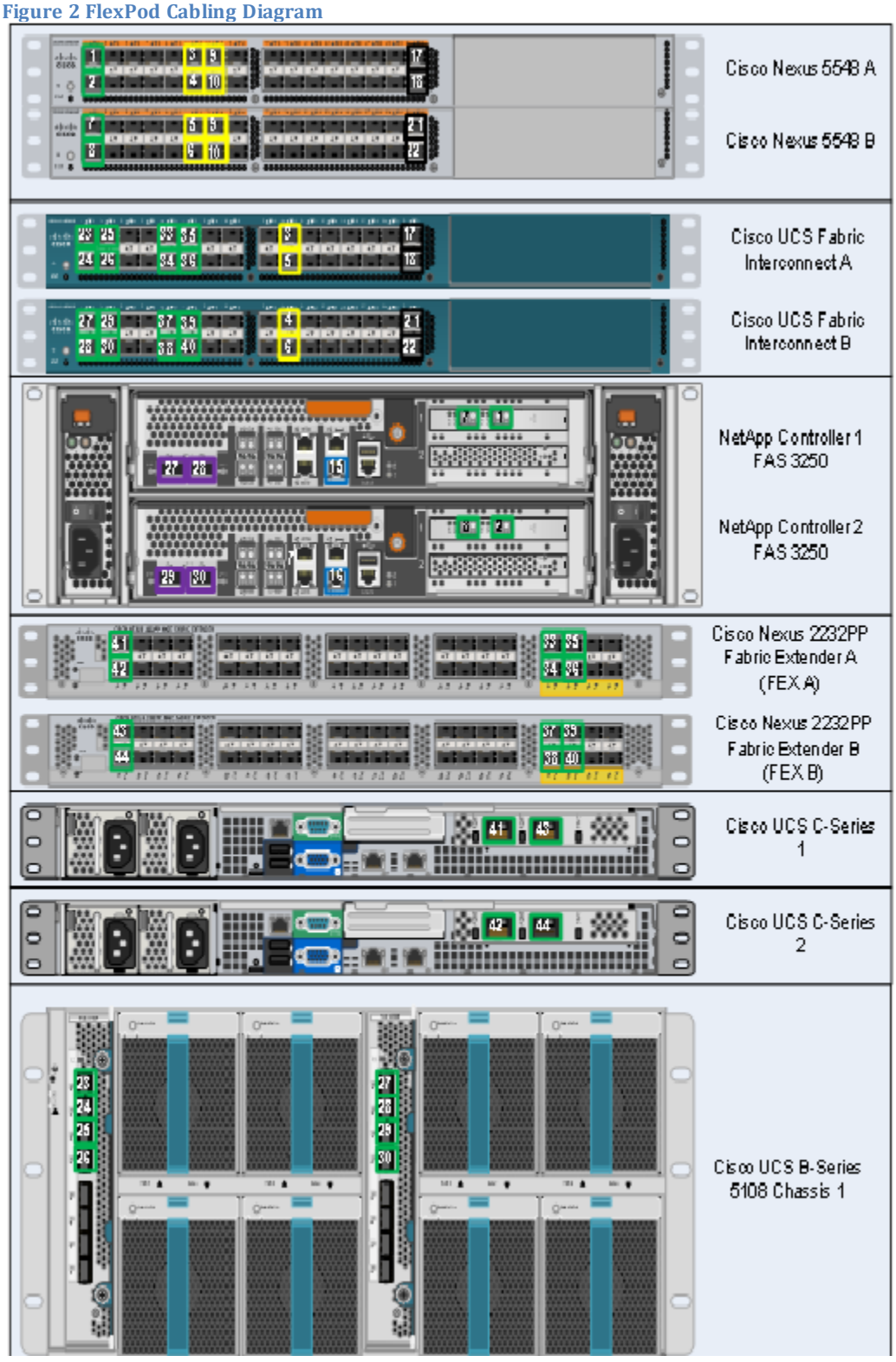


Table 2 Cisco Nexus 5548 A Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	Eth1/1	FCoE/10GbE	NetApp controller A	2a
	Eth1/2	FCoE/10GbE	NetApp controller B	2a
	Eth1/13	10GbE	Cisco Nexus 5548 B	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 B	Eth1/14
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/19
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/19
	Eth1/31	FCoE	Cisco UCS fabric interconnect A	Eth1/31
	Eth1/32	FCoE	Cisco UCS fabric interconnect A	Eth1/32
	MGMT0	100MbE	100MbE management switch	Any

Note: For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Table 3 Cisco Nexus 5548 B Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B	Eth1/1	FCoE/10GbE	NetApp controller A	2b
	Eth1/2	FCoE/10GbE	NetApp controller B	2b
	Eth1/13	10GbE	Cisco Nexus 5548 A	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 A	Eth1/14
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/20
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/20
	Eth1/31	FCoE	Cisco UCS fabric interconnect B	Eth1/31
	Eth1/32	FCoE	Cisco UCS fabric interconnect B	Eth1/32
	MGMT0	100MbE	100MbE management switch	Any

Note: For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Table 4 NetApp controller A Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller A	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	2a	FCoE/10GbE	Cisco Nexus 5548 A	Eth1/1
	2b	FCoE/10GbE	Cisco Nexus 5548 B	Eth1/1

Table 5 NetApp controller B Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller B	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	2a	FCoE/10GbE	Cisco Nexus 5548 A	Eth1/2
	2b	FCoE/10GbE	Cisco Nexus 5548 B	Eth1/2

Table 6 Cisco UCS fabric interconnect A Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/11
	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/11
	Eth1/1	FCoE/10GbE	Chassis 1 FEX 2208 A	Port 1
	Eth1/2	FCoE/10GbE	Chassis 1 FEX 2208 A	Port 2
	Eth1/3	FCoE/10GbE	Chassis 1 FEX 2208 A	Port 3
	Eth1/4	FCoE/10GbE	Chassis 1 FEX 2208 A	Port 4
	Eth1/5	FCoE/10GbE	Chassis 2 FEX 2208A (if required)	Port 1
	Eth1/6	FCoE/10GbE	Chassis 2 FEX 2208 A (if required)	Port 2
	Eth1/7	FCoE/10GbE	Chassis 2 FEX 2208 A (if required)	Port 3
	Eth1/8	FCoE/10GbE	Chassis 2 FEX 2208 A (if required)	Port 4
	Eth1/9	FCoE/10GbE	FEX 2232PP A (if required)	Port 1
	Eth1/10	FCoE/10GbE	FEX 2232PP A (if required)	Port 2
	Eth1/11	FCoE/10GbE	FEX 2232PP A (if required)	Port 3
	Eth1/12	FCoE/10GbE	FEX 2232PP A (if required)	Port 4
	Eth1/31	FCoE	Cisco Nexus 5548 A	Eth1/31
	Eth1/32	FCoE	Cisco Nexus 5548 A	Eth1/32
	MGMT0	1GbE	1GbE management switch	Any
	L1	1GbE	Cisco UCS fabric interconnect B	L1
	L2	1GbE	Cisco UCS fabric interconnect B	L2

Table 7 Cisco UCS fabric interconnect B Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/12
	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/12
	Eth1/1	FCoE/10GbE	Chassis 1 FEX 2208 B	Port 1
	Eth1/2	FCoE/10GbE	Chassis 1 FEX 2208 B	Port 2
	Eth1/3	FCoE/10GbE	Chassis 1 FEX 2208 B	Port 3
	Eth1/4	FCoE/10GbE	Chassis 1 FEX 2208 B	Port 4
	Eth1/5	FCoE/10GbE	Chassis 2 FEX 2208 B (if required)	Port 1
	Eth1/6	FCoE/10GbE	Chassis 2 FEX 2208 B (if required)	Port 2
	Eth1/7	FCoE/10GbE	Chassis 2 FEX 2208 B (if required)	Port 3
	Eth1/8	FCoE/10GbE	Chassis 2 FEX 2208 B (if required)	Port 4
	Eth1/9	FCoE/10GbE	FEX 2232PP B (if required)	Port 1
	Eth1/10	FCoE/10GbE	FEX 2232PP B (if required)	Port 2
	Eth1/11	FCoE/10GbE	FEX 2232PP B (if required)	Port 3
	Eth1/12	FCoE/10GbE	FEX 2232PP B (if required)	Port 4
	Eth1/31	FCoE	Cisco Nexus 5548 B	Eth1/31
	Eth1/32	FCoE	Cisco Nexus 5548 B	Eth1/32
	MGMT0	1GbE	1GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2

Table 8 Cisco Nexus 2232PP Fabric Extender A Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX A	Eth1/1	FCoE/10GbE	Cisco UCS C-Series 1	Port 1
	Eth1/2	FCoE/10GbE	Cisco UCS C-Series 2	Port 1

Table 9 Cisco Nexus 2232PP Fabric Extender B Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX B	Eth1/1	FCoE/10GbE	Cisco UCS C-Series 1	Port 2
	Eth1/2	FCoE/10GbE	Cisco UCS C-Series 2	Port 2

7 Cisco Nexus 5548UP Deployment Procedure

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

Note: The configuration steps detailed in this section provides guidance for configuring the Nexus 5548UP running release 5.2(1)N1(3).

This configuration also leverages the native VLAN on the trunk ports to discard untagged packets, by setting the native VLAN on the Port Channel, but not including this VLAN in the allowed VLANs on the Port Channel.

7.1 Initial Cisco Nexus 5548UP Switch Configuration

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

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.

    Note: Be sure to review the configuration summary before enabling it.

22. Use this configuration and save it? (yes/no) [y]: Enter.
23. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
24. Log in as user admin with the password previously entered.

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.

    Note: Be sure to review the configuration summary before enabling it.

22. Use this configuration and save it? (yes/no) [y]: Enter.
23. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
24. Log in as user `admin` with the password previously entered.

7.2 Enable Appropriate Cisco Nexus Features

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

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`.

7.3 Set Global Configurations

These steps provide details for setting global configurations.

Nexus A and Nexus B

1. From the global configuration mode, type `spanning-tree port type network default` to make sure that, by default, the ports are considered as network ports in regards to spanning-tree.
2. Type `spanning-tree port type edge bpduguard default` to enable bpduguard on all edge ports by default.
3. Type `spanning-tree port type edge bpdufilter default` to enable bpdufilter on all edge ports by default.
4. Type `ip access-list classify_Silver`.
5. Type 10 permit ip <iSCSI-A net address> any

   Note: Where the variable is the network address of the iSCSI-A VLAN in CIDR notation (i.e. 192.168.102.0/24).
6. Type 20 permit ip any <iSCSI-A net address>.
7. Type 30 permit ip <iSCSI-B net address> any.
8. Type 40 permit ip any <iSCSI-B net address>.
9. Type `exit`.
10. Type class-map type qos match-all class-gold.
11. Type `match cos 4`.
12. Type `exit`.
13. Type `class-map type qos match-all class-silver`.
14. Type `match cos 2`.
15. Type `match access-group name classify_Silver`.
16. Type `exit`.
17. Type `class-map type queuing class-gold`.

18. Type `match qos-group 3`.
19. Type `exit`.
20. Type `class-map type queuing class-silver`.
21. Type `match qos-group 4`.
22. Type `exit`.
23. Type `policy-map type qos system_qos_policy`.
24. Type `class class-gold`.
25. Type `set qos-group 3`.
26. Type `class class-silver`.
27. Type `set qos-group 4`.
28. Type `class class-fcoe`.
29. Type `set qos-group 1`.
30. Type `exit`.
31. Type `exit`.
32. Type `policy-map type queuing system_q_in_policy`.
33. Type `class`.
34. Type `queuing class-fcoe`.
35. Type `bandwidth percent 20`.
36. Type `class type queuing class-gold`.
37. Type `bandwidth percent 33`.
38. Type `class type queuing class-silver`.
39. Type `bandwidth percent 29`.
40. Type `class type queuing class-default`.
41. Type `bandwidth percent 18`.
42. Type `exit`.
43. Type `exit`.
44. Type `policy-map type queuing system_q_out_policy`.
45. Type `class type queuing class-fcoe`.
46. Type `bandwidth percent 20`.
47. Type `class type queuing class-gold`.
48. Type `bandwidth percent 33`.
49. Type `class type queuing class-silver`.
50. Type `bandwidth percent 29`.
51. Type `class type queuing class-default`.
52. Type `bandwidth percent 18`.
53. Type `exit`.
54. Type `exit`.
55. Type `class-map type network-qos class-gold`.
56. Type `match qos-group 3`.

57. Type `exit`.
58. Type `class-map type network-qos class-silver`.
59. Type `match qos-group 4`.
60. Type `exit`.
61. Type `policy-map type network-qos system_nq_policy`.
62. Type `class type network-qos class-gold`.
63. Type `set cos 4`.
64. Type `mtu 9000`.
65. Type `class type network-qos class-fcoe`.
66. Type `pause no-drop`.
67. Type `mtu 2158`.
68. Type `class type network-qos class-silver`.
69. Type `set cos 2`.
70. Type `mtu 9000`.
71. Type `class type network-qos class-default`.
72. Type `mtu 9000`.
73. Type `exit`.
74. Type `system qos`.
75. Type `service-policy type qos input system_qos_policy`.
76. Type `service-policy type queuing input system_q_in_policy`.
77. Type `service-policy type queuing output system_q_out_policy`.
78. Type `service-policy type network-qos system_nq_policy`.
79. Type `exit`.
80. Type `copy run start`.

7.4 Create Necessary VLANs

These steps provide details for creating the necessary VLANs.

Nexus A

1. Type `vlan <<Fabric_A_FCoE_VLAN ID>>`.
2. Type `name FCoE_Fabric_A`.
3. Type `exit`.

Nexus B

1. Type `vlan <<Fabric_B_FCoE_VLAN ID>>`.
2. Type `name FCoE_Fabric_B`.
3. Type `exit`.

Nexus A and Nexus B

1. Type `vlan <<Native VLAN ID>>`.
2. Type `name Native-VLAN`.

3. Type `exit`.
4. Type `vlan <<CSV VLAN ID>>`.
5. Type `name CSV-VLAN`.
6. Type `exit`.
7. Type `vlan <<Live Migration VLAN ID>>`.
8. Type `name Live-Migration-VLAN`.
9. Type `exit`.
10. Type `vlan <<iSCSI A VLAN ID>>`.
11. Type `name iSCSI-A-VLAN`.
12. Type `exit`.
13. Type `vlan <<iSCSI B VLAN ID>>`.
14. Type `name iSCSI-B-VLAN`.
15. Type `exit`.
16. Type `vlan <<MGMT VLAN ID>>`.
17. Type `name Mgmt-VLAN`.
18. Type `exit`.
19. Type `vlan <<VM Database VLAN ID>>`.
20. Type `name VM-Database-VLAN`.
21. Type `exit`.
22. Type `vlan <<VM MF-Public VLAN ID>>`.
23. Type `name VM-MF-Public-VLAN`.
24. Type `exit`.
25. Type `vlan <<VM Cluster Comm VLAN ID>>`.
26. Type `name VM-Cluster-Comm-VLAN`.
27. Type `exit`.
28.

7.5 Add Individual Port Descriptions for Troubleshooting

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

Nexus 5548 A

From the global configuration mode.

1. Type `interface Eth1/1`.
2. Type `description <Controller A:e2a>`.
3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description <Controller B:e2a>`.
6. Type `exit`.
7. Type `interface Eth1/11`.

8. Type `description <UCSM A:Eth1/19>`.
9. Type `exit`.
10. Type `interface Eth1/12`.
11. Type `description <UCSM B:Eth1/19>`.
12. Type `exit`.
13. Type `interface Eth1/13`.
14. Type `description <Nexus B:Eth1/13>`.
15. Type `exit`.
16. Type `interface Eth1/14`.
17. Type `description <Nexus B:Eth1/14>`.
18. Type `exit`.

Nexus 5548 B

From the global configuration mode.

1. Type `interface Eth1/1`.
2. Type `description <Controller A:e2b>`.
3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description <Controller B:e2b>`.
6. Type `exit`.
7. Type `interface Eth1/11`.
8. Type `description <UCSM A:Eth1/20>`.
9. Type `exit`.
10. Type `interface Eth1/12`.
11. Type `description <UCSM B:Eth1/20>`.
12. Type `exit`.
13. Type `interface Eth1/13`.
14. Type `description <Nexus A:Eth1/13>`.
15. Type `exit`.
16. Type `interface Eth1/14`.
17. Type `description <Nexus A:Eth1/14>`.
18. Type `exit`.

7.6 Create Necessary Port Channels

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

Nexus 5548 A

From the global configuration mode.

1. Type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.

4. Type `interface Eth1/13-14`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description <`*`Controller A`*`>`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `description <`*`Controller B`*`>`.
17. Type `exit`.
18. Type `interface Eth1/2`.
19. Type `channel-group 12 mode active`.
20. Type `no shutdown`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `description <`*`UCSM A`*`>`.
24. Type `exit`.
25. Type `interface Eth1/11`.
26. Type `channel-group 13 mode active`.
27. Type `no shutdown`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `description <`*`UCSM B`*`>`.
31. Type `exit`.
32. Type `interface Eth1/12`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `interface eth1/31`.
37. Type `switchport description <UCSM A:eth1/31>`.
38. Type `exit`.
39. Type `interface eth1/32`.
40. Type `switchport description <UCSM A:eth1/32>`.
41. Type `exit`.
42. Type `interface Eth1/31-32`.

43. Type `channel-group 15 mode active`.
44. Type `no shutdown`.
45. Type `copy run start`.

Nexus 5548 B

1. From the global configuration mode, type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.
4. Type `interface Eth1/13-14`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description <Controller A>`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `description <Controller B>`.
17. Type `exit`.
18. Type `interface Eth1/2`.
19. Type `channel-group 12 mode active`.
20. Type `no shutdown`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `description <UCSM A>`.
24. Type `exit`.
25. Type `interface Eth1/11`.
26. Type `channel-group 13 mode active`.
27. Type `no shutdown`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `description <UCSM B>`.
31. Type `exit`.
32. Type `interface Eth1/12`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`
35. Type `exit`.

36. Type `interface eth1/31`.
37. Type `switchport description <UCSM B:eth1/31>`.
38. Type `exit`.
39. Type `interface eth1/32`.
40. Type `switchport description <UCSM B:eth1/32>`.
41. Type `exit`.
42. Type `interface eth1/31-32`.
43. Type `channel-group 16 mode active`.
44. Type `no shutdown`.
45. Type `copy run start`.

7.7 Add Port Channel Configurations

These steps provide details for adding Port Channel configurations.

Nexus 5548A

From the global configuration mode.

1. 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>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Databse VLAN ID>>,<<VM MF-Public VLAN ID>>, <<VM Cluster Comm VLAN ID>> <<Fabric A FCoE VLAN ID>>`.
5. Type `spanning-tree port type network`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `switchport mode trunk`.
10. Type `switchport trunk native vlan <<Native VLAN ID>>`.
11. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Fabric A FCoE VLAN ID>>`.
12. Type `spanning-tree port type edge trunk`.
13. Type `no shut`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `switchport mode trunk`.
17. Type `switchport trunk native vlan <<Native VLAN ID>>`.
18. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Fabric A FCoE VLAN ID>>`.
19. Type `spanning-tree port type edge trunk`.
20. Type `no shut`.
21. Type `exit`.

22. Type `interface Po13`.
23. Type `switchport mode trunk`.
24. Type `switchport trunk native vlan <Native VLAN ID>`.
25. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>,<<VM MF-Public VLAN ID>>, <<VM Cluster Comm VLAN ID>> <<Fabric A FCoE VLAN ID>>`.
26. Type `spanning-tree port type edge trunk`.
27. Type `no shut`.
28. Type `exit`.
29. Type `interface Po14`
30. Type `switchport mode trunk`
31. Type `switchport trunk native vlan <Native VLAN ID>`.
32. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Data VLAN ID>>, <<VM Cluster Comm VLAN ID>> <<Fabric A FCoE VLAN ID>>`.
33. Type `spanning-tree port type edge trunk`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `interface Po15`.
37. Type `switchport mode trunk`.
38. Type `switchport trunk allowed vlan <Fabric A FCoE VLAN ID>`
39. Type `no shutdown`
40. Type `exit`.
41. Type `copy run start`.

Nexus 5548 B

From the global configuration mode.

25. Type interface Po10.
26. Type switchport mode trunk.
27. Type `switchport trunk native vlan <<Native VLAN ID>>`.
28. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>,<<VM MF-Public VLAN ID>>, <<Fabric B FCoE VLAN ID>>`.
29. Type `spanning-tree port type network`.
30. Type `no shutdown`.
31. Type `exit`.
32. Type `interface Po11`.
33. Type `switchport mode trunk`.
34. Type `switchport trunk native vlan <<Native VLAN ID>>`.

35. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Fabric B FCoE VLAN ID>>.`
36. Type `spanning-tree port type edge trunk.`
37. Type `no shut.`
38. Type `exit.`
39. Type `interface Po12.`
40. Type `switchport mode trunk.`
41. Type `switchport trunk native vlan <<Native VLAN ID>>.`
42. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Fabric B FCoE VLAN ID>>.`
43. Type `spanning-tree port type edge trunk.`
44. Type `no shut.`
45. Type `exit.`
46. Type `interface Po13.`
47. Type `switchport mode trunk.`
48. Type `switchport trunk native vlan <Native VLAN ID>.`
49. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>,<<VM MF-Public VLAN ID>>, <<Fabric B FCoE VLAN ID>>.` Type `spanning-tree port type edge trunk.`
50. Type `no shut.`
51. Type `exit.`
52. Type `interface Po14.`
53. Type `switchport mode trunk.`
54. Type `switchport trunk native vlan <Native VLAN ID>.`
55. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<iSCSI A VLAN ID>>, <<iSCSI B VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, <<Fabric B FCoE VLAN ID>>.` Type `spanning-tree port type edge trunk.`
56. Type `no shut.`
57. Type `exit.`
58. Type `interface Po16.`
59. Type `switchport mode trunk.`
60. Type `switchport trunk allowed vlan <Fabric B FCoE VLAN ID>`
61. Type `no shutdown.`
62. Type `exit.`
63. Type `copy run start.`

7.8 Configure Virtual Port Channels

These steps provide details for configuring virtual Port Channels (vPCs).

Nexus 5548 A

From the global configuration mode:

1. 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 Po11`.
9. Type `vpc 11`.
10. Type `exit`.
11. Type `interface Po12`.
12. Type `vpc 12`.
13. Type `exit`.
14. Type `interface Po13`.
15. Type `vpc 13`.
16. Type `exit`.
17. Type `interface Po14`.
18. Type `vpc 14`.
19. Type `exit`.
20. Type `copy run start`.

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 Po11`.
9. Type `vpc 11`.
10. Type `exit`.
11. Type `interface Po12`.
12. Type `vpc 12`.
13. Type `exit`
14. Type `interface Po13`.

15. Type `vpc 13`.
16. Type `exit`.
17. Type `interface Po14`.
18. Type `vpc 14`.
19. Type `exit`.
20. Type `copy run start`

7.9 Configure FCoE Fabric

These steps provide details for configuring Fiber Channel over Ethernet Fabric.

Nexus 5548 A

1. Type `interface vfc11`.
2. Type `bind interface po11`.
3. Type `no shutdown`.
4. Type `exit`.
5. Type `interface vfc12`.
6. Type `bind interface po12`.
7. Type `no shutdown`.
8. Type `exit`.
9. Type `interface vfc15`.
10. Type `bind interface po15`.
11. Type `no shutdown`.
12. Type `exit`.
13. Type `vsan database`.
14. Type `vsan <VSAN A ID>`
15. Type `vsan <VSAN B ID> name Fabric_B`.
16. Type `vsan <VSAN A ID> interface vfc11`.
17. Type `vsan <VSAN A ID> interface vfc12`.
18. Type `vsan <VSAN A ID> interface vfc15`.
19. Type `exit`.
20. Type `vlan <<Fabric_A_FCoE_VLAN ID>>`
21. Type `fcoe vsan <VSAN A ID>`.
22. Type `exit`.
23. Type `copy run start`.

Nexus 5548 B

1. Type `interface vfc11`.
2. Type `bind interface po11`.
3. Type `no shutdown`.
4. Type `exit`.

5. Type `interface vfc12`.
6. Type `bind interface po12`.
7. Type `no shutdown`
8. Type `exit`.
9. Type `interface vfc16`
10. Type `bind interface po16`
11. Type `no shutdown`
12. Type `exit`.
13. Type `vsan database`.
14. Type `vsan <VSAN B ID>`
15. Type `vsan <VSAN B ID> name Fabric_B`.
16. Type `vsan <VSAN B ID> interface vfc11`.
17. Type `vsan <VSAN B ID> interface vfc12`.
18. Type `vsan <VSAN B ID> interface vfc16`
19. Type `exit`.
20. Type `vlan <<Fabric_B_FCoE_VLAN ID>>`
21. Type `fcoe vsan <VSAN B ID>`.
22. Type `exit`.
23. Type `copy run start`

7.10 Link into Existing Network Infrastructure

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

8 NetApp FAS3250A Deployment Procedure

8.1 Complete the Configuration Worksheet

Before running the setup script, complete the configuration worksheet from the product manual.

	How to Access the Configuration Worksheet Configuration Guide	Comments
Configuration Worksheet	https://library.netapp.com/ecm/ecm_get_file/ECMM1249829	Requires access to the NetApp Support site.

8.2 Assign Controller Disk Ownership and Initialize Storage

These steps provide details for assigning disk ownership and disk initialization and verification.

Note: Typical best practices should be followed when determining the number of disks to assign to each controller head. You may choose to assign a disproportionate number of disks to a given storage controller in an HA pair, depending on the intended workload.

In this reference architecture, half the total number of disks in the environment is assigned to one controller and the remainder to its partner.

Detail	Detail Value
Controller A MGMT IP	
Controller A netmask	
Controller A gateway	
URL of the Data ONTAP boot software	
Controller B MGMT IP	
Controller B netmask	
Controller B gateway	

Controller A

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, Press Ctrl – C to exit the Autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. If the system is at the LOADER prompt, enter the following command to boot Data ONTAP:

```
autoboot
```

3. During system boot, press Ctrl – C when prompted for the Boot Menu:

```
Press Ctrl-C for Boot Menu…
```

Note: If 8.1.2 is not the version of software being booted, proceed with the steps below to install new software. If 8.1.2 is the version being booted, then proceed with step 14, maintenance mode boot.

4. To install new software first select option 7.

```
7
```

5. Answer `yes` for performing a nondisruptive upgrade.

```
y
```

6. Select e0M for the network port you want to use for the download.

```
e0M
```

7. Select `yes` to reboot now.

```
y
```

8. Enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_controller1_e0m_ip>>
<<var_controller1_mask>>>
<<var_controller1_mgmt_gateway>>.
```

9. Enter the URL where the software can be found.

Note: This Web server must be pingable.

```
<<var_url_boot_software>>
```

10. Press Enter for the username, indicating no user name.

```
Enter
```

11. Enter `yes` to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

12. Enter `yes` to reboot the node.

```
y
```

13. When you see "`Press Ctrl-C for Boot Menu`":

```
Ctrl-C
```

14. To enter Maintenance mode boot, select option 5.

```
5
```

15. When you see the question "`Continue to Boot?`" type `yes`.

```
y
```

16. To verify the HA status of your environment, enter:

```
ha-config show
```

Note: If either component is not in HA mode, use the `ha-config modify` command to put the components in HA mode.

17. To see how many disks are unowned, enter:

```
disk show -a
```

Note: No disks should be owned in this list.

18. Assign disks.

```
disk assign -n <<var_#_of_disks>>
```

Note: This reference architecture allocates half the disks to each controller. However, workload design could dictate different percentages.

19. Reboot the controller.

```
halt
```

20. At the LOADER-A prompt, enter:

```
autoboot
```

21. Press Ctrl – C for Boot Menu when prompted.

```
Ctrl-C
```

22. Select option 4 for Clean configuration and initialize all disks.

```
4
```

23. Answer `yes` to zero disks, reset config and install a new file system.

```
y
```

24. Enter `yes` to erase all the data on the disks.

```
y
```

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots. You can continue to Controller B configuration while the disks for Controller A are zeroing.

Controller B

1. Connect to the storage system console port. You should see a Loader-A prompt. However if the storage system is in a reboot loop, Press Ctrl – C to exit the Autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. If the system is at the LOADER prompt, enter the following command to boot Data ONTAP:

```
autoboot
```

3. During system boot, press Ctrl – C when prompted for the Boot Menu:

```
Press Ctrl-C for Boot Menu…
```

Note: If 8.1.2 is not the version of software being booted, proceed with the steps below to install new software. If 8.1.2 is the version being booted, then proceed with step 14, maintenance mode boot

4. To install new software first select option 7.

```
7
```

5. Enter `yes` for performing a nondisruptive upgrade.

```
y
```

6. Select e0M for the network port you want to use for the download.

```
e0M
```

7. Enter `yes` to reboot now.

```
y
```

8. Enter the IP address, netmask and default gateway for e0M in their respective places.

```
<<var_controller2_e0m_ip>>
<<var_controller2_mask>>
<<var_controller2_mgmt_gateway>>.
```

9. Enter the URL where the software can be found.

Note: This Web server must be pingable.

```
<<var_url_boot_software>>
```

10. Press Enter for the username, indicating no user name.

```
Enter
```

11. Enter `yes` to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

12. Enter `yes` to reboot the node.

```
y
```

13. When you see "`Press Ctrl-C for Boot Menu`":

```
Ctrl-C
```

14. To enter Maintenance mode boot, select option 5:

```
5
```

15. If you see the question "`Continue to Boot?`" type `yes`.

```
y
```

16. To verify the HA status of your environment, enter:

```
ha-config show
```

Note: If either component is not in HA mode, use the `ha-config modify` command to put the components in HA mode.

17. To see how many disks are unowned, enter:

disk show -a

Note: The remaining disks should be shown.

18. Assign disks by entering:

```
disk assign -n <<var_#_of_disks>>
```

Note: This reference architecture allocates half the disks to each controller. However, workload design could dictate different percentages.

19. Reboot the controller.

```
halt
```

20. At the LOADER prompt, enter:

```
autoboot
```

21. Press Ctrl – C for Boot Menu when prompted.

```
Ctrl-C
```

22. Select option 4 for a Clean configuration and initialize all disks.

```
4
```

23. Answer yes to zero disks, reset config and install a new file system.

```
y
```

24. Enter `yes` to erase all the data on the disks.

```
y
```

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots.

8.3 Run the Setup Process

When Data ONTAP is installed on your new storage system, the following files are not populated:

- `/etc/rc`
- `/etc/exports`
- `/etc/hosts`
- `/etc/hosts.equiv`

Controller A

1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.

2. Enter the following information:

```
Please enter the new hostname []:<<var_controller1>>
Do you want to enable IPv6? [n]: Enter

Do you want to configure interface groups? [n]: Enter
```

3. Press Enter to accept the blank IP address.

```
Please enter the IP address for Network Interface e0a []: Enter
Should interface e0a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e0b []:Enter
Should interface e0b take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1a []:Enter
Should interface e1a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1b []:Enter
Should interface e1b take over a partner IP address during failover? [n]: Enter

Please enter the IP address for Network Interface e0M []: <<var_controller1_e0m_ip>>
Please enter the netmaskfor the Network Interface e0M [255.255.255.0]:
<<var_controller1_mask>>

Should interface e0M take over a partner IP address during failover? [n]: y
Please enter the IPv4 address or interface name to be taken over by e0M []: e0M
Please enter flow control for e0M {none, receive, send, full} [full]: Enter
```

4. Enter the following information:

```
Please enter the name or IP address of the IPv4 default gateway:
<<var_controller1_mgmt_gateway>>

The administration host is given root access to the storage system's / etc files for
system administration. To allow /etc root access to all NFS clients enter RETURN below.
Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GTM]: <<var_timezone>>
```

5. Example time zone: America/New_York.

```
Where is the filer located? <<var_location>>
Enter the root directory for HTTP files [home/http]: Enter
Do you want to run DNS resolver? [n]: y
Please enter DNS domain name []: <<var_dns_domain_name>>
Please enter the IP address for first nameserver []: <<var_nameserver_ip>>
Do you want another nameserver? [n]:
```

6. Optionally enter up to three name server IP addresses.

```
Do you want to run NIS client? [n]: Enter
Press the Return key to continue through AutoSupport message
would you like to configure SP LAN interface [y]: Enter
Would you like to enable DHCP on the SP LAN interface [y]: n
Please enter the IP address for the SP: <<var_sp_ip>>
Please enter the netmask for the SP []: <<var_sp_mask>>
Please enter the IP address for the SP gateway: <<var_sp_gateway>>
Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>>
Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>>
New password: <<var_ password>>
Retype new password <<var_ password>>
```

7. Enter the admin password to log in to Controller A.

Controller B

1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.
2. Enter the following information:

```
Please enter the new hostname []:<<var_controller2>>
Do you want to enable IPv6? [n]: Enter

Do you want to configure interface groups? [n]: Enter
```

3. Press Enter to accept the blank IP address.

```
Please enter the IP address for Network Interface e0a []: Enter
Should interface e0a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e0b []:Enter
Should interface e0b take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1a []:Enter
Should interface e1a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1b []:Enter
Should interface e1b take over a partner IP address during failover? [n]: Enter

Please enter the IP address for Network Interface e0M []: <<var_controller2_e0m_ip>>
Please enter the netmaskfor the Network Interface e0M [255.255.255.0]:
<<var_controller2_mask>>

Should interface e0M take over a partner IP address during failover? [n]: y
Please enter the IPv4 address or interface name to be taken over by e0M []: e0M
Please enter flow control for e0M {none, receive, send, full} [full]: Enter
```

4. Enter the following information:

```
Please enter the name or IP address of the IPv4 default gateway:
<<var_controller2_mgmt_gateway>>

The administration host is given root access to the storage system's / etc files for
system administration. To allow /etc root access to all NFS clients enter RETURN below.
Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GTM]: <<var_timezone>>
```

5. Example time zone: America/New_York.

```
Where is the filer located? <<var_location>>
Enter the root directory for HTTP files [home/http]: Enter
Do you want to run DNS resolver? [n]: y
Please enter DNS domain name []: <<var_dns_domain_name>>
Please enter the IP address for first nameserver []: <<var_nameserver_ip>>
Do you want another nameserver? [n]:
```

6. Optionally enter up to three name server IP addresses.

```
Do you want to run NIS client? [n]: Enter
Press the Return key to continue through AutoSupport message
would you like to configure SP LAN interface [y]: Enter
Would you like to enable DHCP on the SP LAN interface [y]: n
Please enter the IP address for the SP: <<var_sp_ip>>
Please enter the netmask for the SP []: <<var_sp_mask>>
Please enter the IP address for the SP gateway: <<var_sp_gateway>>
Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>>
Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>>
New password: <<var_ password>>
Retype new password <<var_ password>>
```

7. Enter the admin password to log in to Controller B.

8.4 Upgrade the Service Processor on Each Node to the Latest Release

With Data ONTAP 8.1.2, you must upgrade to the latest Service Processor (SP) firmware to take advantage of the latest updates available for the remote management device.

1. Using a web browser, connect to http://support.netapp.com/NOW/cgi-bin/fw.

2. Navigate to the Service Process Image for installation from the Data ONTAP prompt page for your storage platform.
3. Proceed to the Download page for the latest release of the SP Firmware for your storage platform.
4. Using the instructions on this page, update the SPs on both controllers. You will need to download the .zip file to a web server that is reachable from the management interfaces of the controllers.

8.5 64-Bit Aggregates

Note: A 64-bit aggregate containing the root volume is created during the Data ONTAP setup process. To create additional 64-bit aggregates, determine the aggregate name, the node on which to create it, and how many disks it will contain. Calculate the RAID group size to allow for roughly balanced (same size) RAID groups of between 12 and 20 disks (for SAS disks) within the aggregate. For example, if 52 disks were being assigned to the aggregate, select a RAID group size of 18. A RAID group size of 18 would yield two 18-disk RAID groups and one 16-disk RAID group. Keep in mind that the default RAID group size is 16 disks, and that the larger the RAID group size, the longer the disk rebuild time in case of a failure.

Controller A

1. Execute the following command to create a new aggregate:

```
aggr create aggr1 -B 64 –r <<var_raidsize>> <<var_num_disks>>
```

Note: Leave at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

Controller B

1. Execute the following command to create a new aggregate:

```
aggr create aggr1 -B 64 –r <<var_raidsize>> <<var_num_disks>>
```

Note: Leave at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

8.6 Flash Cache

Controller A and Controller B

1. Execute the following commands to enable Flash Cache:

```
options flexscale.enable on
options flexscale.lopri_blocks off
options flexscale.normal_data_blocks on
```

Note: For directions on how to configure Flash Cache in metadata mode or low-priority data caching mode, refer to TR-3832: Flash Cache and PAM Best Practices Guide. Before customizing the settings, determine whether the custom settings are required or whether the default settings are sufficient.

8.7 IFGRP LACP

Since this type of interface group requires two or more Ethernet interfaces and a switch that supports LACP, make sure that the switch is configured properly.

Controller A and Controller B

1. Run the following command on the command line and also add it to the `/etc/rc` file, so it is activated upon boot:

```
ifgrp create lacp ifgrp0 -b port e2a e2b
wrfile -a /etc/rc "ifgrp create lacp ifgrp0 -b ip e2a e2b"
```

Note: All interfaces must be in `down` status before being added to an interface group.

8.8 VLAN

Controller A and Controller B

1. Follow the steps below to create a VLAN interface for iSCSI data traffic.

```
vlan create ifgrp0 <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
wrfile -a /etc/rc "vlan create ifgrp0 <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>"
```

8.9 IP Config

Controller A and Controller B

1. Run the following commands on the command line.

```
ifconfig ifgrp0-<<var_iscsi_a_vlan_id>> <<var_iscsi_a_ip>> netmask <<var_iscsi_a_mask>>
mtusize 9000 partner ifgrp0-<<var_iscsi_a_vlan_id>>
ifconfig ifgrp0-<<var_iscsi_b_vlan_id>> <<var_iscsi_b_ip>> netmask <<var_iscsi_b_mask>>
mtusize 9000 partner ifgrp0-<<var_iscsi_b_vlan_id>>
wrfile -a /etc/rc "ifconfig ifgrp0-<<var_iscsi_a_vlan_id>> <<var_iscsi_a_ip>> netmask
<<var_iscsi_a_mask>> mtusize 9000 partner ifgrp0-<<var_iscsi_a_vlan_id>>"
wrfile -a /etc/rc "ifconfig ifgrp0-<<var_iscsi_b_vlan_id>> <<var_iscsi_b_ip>> netmask
<<var_iscsi_b_mask>> mtusize 9000 partner ifgrp0-<<var_iscsi_b_vlan_id>>"
```

8.10 Cisco Discovery Protocol

Controller A and Controller B

Follow these steps to enable Cisco Discovery Protocol (CDP) on controller 1 and controller 2.

1. Enable CDP.

```
options cdpd.enable on
```

8.11 Storage Controller Active-Active Configuration

Controller A and Controller B

Enable two storage controllers to an active-active configuration.

1. Enter the cluster license on both nodes.

```
license add <<var_cf_license>>
```

2. Reboot each storage controller.

```
reboot
```

3. Log back in to both controllers.

Controller A

1. Enable failover on Controller A, if it is not enabled already.

```
cf enable
```

8.12 NTP

The following commands configure and enable time synchronization on the storage controller. You must have either a publically available IP address or your company's standard NTP server name or IP address.

Controller A and Controller B

1. Run the following commands to configure and enable the NTP server:

```
date <<var_date>>
```

2. Enter the current date in the format of [[[[CC]yy]mm]dd]hhmm[.ss]].

For example: `date 201208311436`; would set the date to August 31st 2012 at 14:36.

```
options timed.servers <<var_global_ntp_server_ip>>
options timed.enable on
```

8.13 Joining a Windows Domain (optional)

The following commands should be used to allow the NetApp controllers to join the existing Domain.

Controller A and Controller B

24. Add the controller to the domain by running cifs setup.

```
CIFS setup
Do you want to make the system visible via WINS? [N] n
Choose (2) NTFS-only filer [2] 2
Enter the password for the root user []: <<var_root_password>>
Reenter the password: <<var_root_password>>
Would you like the change this name? [n]: Enter
Choose (1) Active Directory Domain Authentication : 1 Enter
Configure the DNS Resolver Service ?[y]: y
What is the filers DSN Domain name? []: <<var_dnsdomain>>
What the IPv4 Addresses of your Authoritative DNS servers? []:  <<var_ip_DNSserver>>
What is the name of the Active Directory Domain Controller? : <<var_dnsdomain>>
Would you like to configure time services? [y]: [Enter]
Enter the time server host []:<<var_dnsdomain>>
Enter the ame of the windows user [administrator@<<var_fas3240_dnsdomain>>] [Enter]
Password for <<var_domainAccountUsed>>: <<password>>
Choose (1) Create the filers machine account in the "computers" container: 1
Do you want to configure a <<var_ntap_hostname>>/administrator account [Y]: [Enter]
Password for the <<var_ntap_hostname>>/Administrator <<var_password>> [Enter]
Would you like to specify a user or group that can administer CIFS [n]: [Enter]
```

8.14 iSCSI

Controller A and Controller B

1. Add a license for iSCSI.

```
license add <<var_iscsi_license>>
```

2. Start iSCSI

```
iscsi start
```

8.15 FCP

Controller A and Controller B

1. License FCP.

```
license add <<var_fc_license>>
```

2. Start the FCP service.

```
fcp start
```

3. Record the WWPN or FC port name for later use.

```
fcp show adapters
```

4. If using FC instead of FCoE between storage and the network, if necessary execute the following commands to make ports 0c and 0d target ports.

```
fcadmin config
```

5. Make an FC port into a target.
6. Only FC ports that are configured as targets can be used to connect to initiator hosts on the SAN.
7. For example, make a port called <<var_fctarget01>> into a target port by running the following command:

```
fcadmin config -t target <<var_fctarget01>>
```

25. If an initiator port is made into a target port, a reboot is required. NetApp recommends rebooting after completing the entire configuration because other configuration steps might also require a reboot.

8.16 Data ONTAP SecureAdmin

Secure API access to the storage controller must be configured.

Controller A

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup ssl
SSL Setup has already been done before. Do you want to proceed? [no] y
Country Name (2 letter code) [US]: <<var_country_code>>
State or Province Name (full name) [California]: <<var_state>>
Locality Name (city, town, etc.) [Santa Clara]: <<var_city>>
Organization Name (company) [Your Company]: <<var_org>>
Organization Unit Name (division): <<var_unit>>
Common Name (fully qualified domain name) [<<var_controller1_fqdn>>]: Enter
Administrator email: <<var_admin_email>>
Days until expires [5475] : Enter
Key length (bits) [512] : <<var_key_length>>
```

Note: We recommend that your key length be 1024.

26. After the initialization, the CSR is available in the file /etc/keymgr/csr/secureadmin_tmp.pem.
27. Configure and enable SSL and HTTPS for API access using the following options.

```
options httpd.access none
options httpd.admin.enable off
options httpd.admin.ssl.enable on
options ssl.enable on
```

Controller B

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup ssl
SSL Setup has already been done before. Do you want to proceed? [no] y
```

```
Country Name (2 letter code) [US]: <<var_country_code>>
State or Province Name (full name) [California]: <<var_state>>
Locality Name (city, town, etc.) [Santa Clara]: <<var_city>>
Organization Name (company) [Your Company]: <<var_org>>
Organization Unit Name (division): <<var_unit>>
Common Name (fully qualified domain name) [<<var_controller2_fqdn>>]: Enter
Administrator email: <<var_admin_email>>
Days until expires [5475] : Enter
Key length (bits) [512] : <<var_key_length>>
```

2. NetApp recommends that your key length be 1024.
3. After the initialization, the CSR is available in the file `/etc/keymgr/csr/secureadmin_tmp.pem`.
4. Configure and enable SSL and HTTPS for API access using the following options.

```
options httpd.access none
options httpd.admin.enable off
options httpd.admin.ssl.enable on
options ssl.enable on
```

8.17 Secure Shell

SSH must be configured and enabled.

Controller A and Controller B

1. Use the following one-time command to generate host keys.

```
secureadmin disable ssh
secureadmin setup -f -q ssh 768 512 1024
```

2. Use the following options to configure and enable SSH.

```
options ssh.idle.timeout 60
options autologout.telnet.timeout 5
```

8.18 SNMP

Controller A and Controller B

1. Run the following commands to configure SNMP basics, such as the local and contact information. When polled, this information displays as the `sysLocation` and `sysContact` variables in SNMP.

```
snmp contact "<<var_admin_email>>"
snmp location "<<var_location>>"
snmp init 1
options snmp.enable on
```

2. Configure SNMP traps to send them to remote hosts, such as a DFM server or another fault management system.

```
snmp traphost add <<var_oncommand_server_fqdn>>
```

8.19 SNMPv1

Controller A and Controller B

1. Set the shared secret plain-text password, which is called a community.

```
snmp community delete all
snmp community add ro <<var_snmp_community>>
```

Note: Use the `delete all` command with caution. If community strings are used for other monitoring products, the `delete all` command will remove them.

8.20 SNMPv3

SNMPv3 requires a user to be defined and configured for authentication.

Controller A and Controller B

Note: Create a user called `snmpv3user`.

```
useradmin role add snmp_requests -a login-snmp
useradmin group add snmp_managers -r snmp_requests
useradmin user add snmpv3user -g snmp_managers
New Password: <<var_ password>>
Retype new password: <<var_ password>>
```

8.21 AutoSupport HTTPS

AutoSupport™ sends support summary information to NetApp through HTTPS.

Controller A and Controller B

Note: Execute the following commands to configure AutoSupport:

```
options autosupport.noteto <<var_admin_email>>
```

8.22 Security Best Practices

Apply the following commands according to local security policies.

Controller A and Controller B

1. Run the following commands to enhance security on the storage controller:

```
options rsh.access none
options webdav.enable off
options security.passwd.rules.maximum 14
options security.passwd.rules.minimum.symbol 1
options security.passwd.lockout.numtries 6
options autologout.console.timeout 5
```

8.23 Install Remaining Required Licenses and Enable MultiStore

Controller A and Controller B

1. Install the following licenses to enable SnapRestore® and FlexClone®.

```
license add <<var_snaprestore_license>>
license add <<var_flex_clone_license>>
options licensed_feature.multistore.enable on
```

8.24 Enable NDMP

Run the following commands to enable NDMP.

Controller A and Controller B

```
options ndmpd.enable on
```

8.25 Add Infrastructure Volumes

Controller A

1. Create a FlexVol® volume in Aggr1 to host the UCS boot LUNs, and Cluster Quorum.

```
vol create ucs_boot -s none aggr1 500g
vol create quorum -s none aggr1 10g
```

2. Configure volume dedupe.

```
sis config -s auto /vol/ucs_boot
sis config -s auto /vol/quorum
sis on /vol/ucs_boot
sis on /vol/hyperv_quorum
sis start -s /vol/ucs_boot
sis start -s /vol/hyperv_quorum
```

Controller B

1. Create a 1.5TB FlexVol volume in Aggr1 to host the management infrastructure virtual machines.

```
vol create fabric_mgmt_csv -s none aggr1 1.5t
```

2. Configure dedupe.

```
sis config -s auto /vol/fabric_mgmt_csv
sis config -s auto /vol/ucs_boot
sis on /vol/ucs_boot
sis on /vol/fabric_mgmt_csv
sis start -s /vol/ucs_boot
sis start -s /vol/fabric_mgmt_csv
```

8.26 Install SnapManager licenses

Controller A and Controller B

1. Add a license for SnapManger for Hyper-V.

```
license add <<var_snapmanager_hyperv_license>>
```

2. Add a license for SnapDrive for Windows.

```
license add <<var_snapdrive_windows_license>>
```

8.27 NetApp SAN Configuration Create Device Aliases

These steps provide details for configuring device aliases and zones for the primary boot path. Instructions are given for all target ports, however, the redundant path is enabled following operating system installation.

Gather Necessary Information

To proceed with the FlexPod deployment, specific information must be gathered from the NetApp controllers. Insert the required information in the table below.

Table 9 FC Port Names for Storage Controllers 1 and 2

NetApp Controller	FC Port	FC Portname
Controller A	2a	
	2b	
Controller B	2a	
	2b	

Note: To gather the information in the table above, run `fcp portname show`.

Nexus 5548 A

1. Create device alias.
2. Type `device-alias database`.
3. Type `device-alias name controller_A_2a pwwn <Controller A 2a WWPN>`.
4. Type `device-alias name controller_B_2a pwwn <Controller B 2a WWPN>`.
5. type `exit`.
6. Type `device-alias commit`.
7. Type copy running-config startup-config

Nexus 5548 B

1. Using the information in Table 10, create device alias.
2. Type `device-alias database`.
3. Type `device-alias name controller_A_2b pwwn <Controller A 2b WWPN>`.
4. Type `device-alias name controller_B_2b pwwn <Controller B 2b WWPN>`.
5. type `exit`.
6. Type `device-alias commit`.

9 Cisco Unified Computing System Deployment Procedure

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

Note: Cisco UCS Firmware 2.1(1b) is the minimum required Cisco UCS ferimware version. See the FlexPod with Microsoft Private Cloud v3 Design Guide for details.

9.1 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 make sure 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.

1. Open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.
2. Select the Launch link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter `admin` for the username and enter the administrative password and click `Login` to log in to the Cisco UCS Manager software.

9.2 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.

1. Select the `Admin` tab at the top of the left window.
2. Select `All > Communication Management`.
3. Right-click `Management IP Pool`.
4. Select `Create Block of IP Addresses`.
5. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
6. Click `OK` to create the IP block.
7. Click `OK` in the message box.

9.3 Synchronize Cisco UCS to NTP

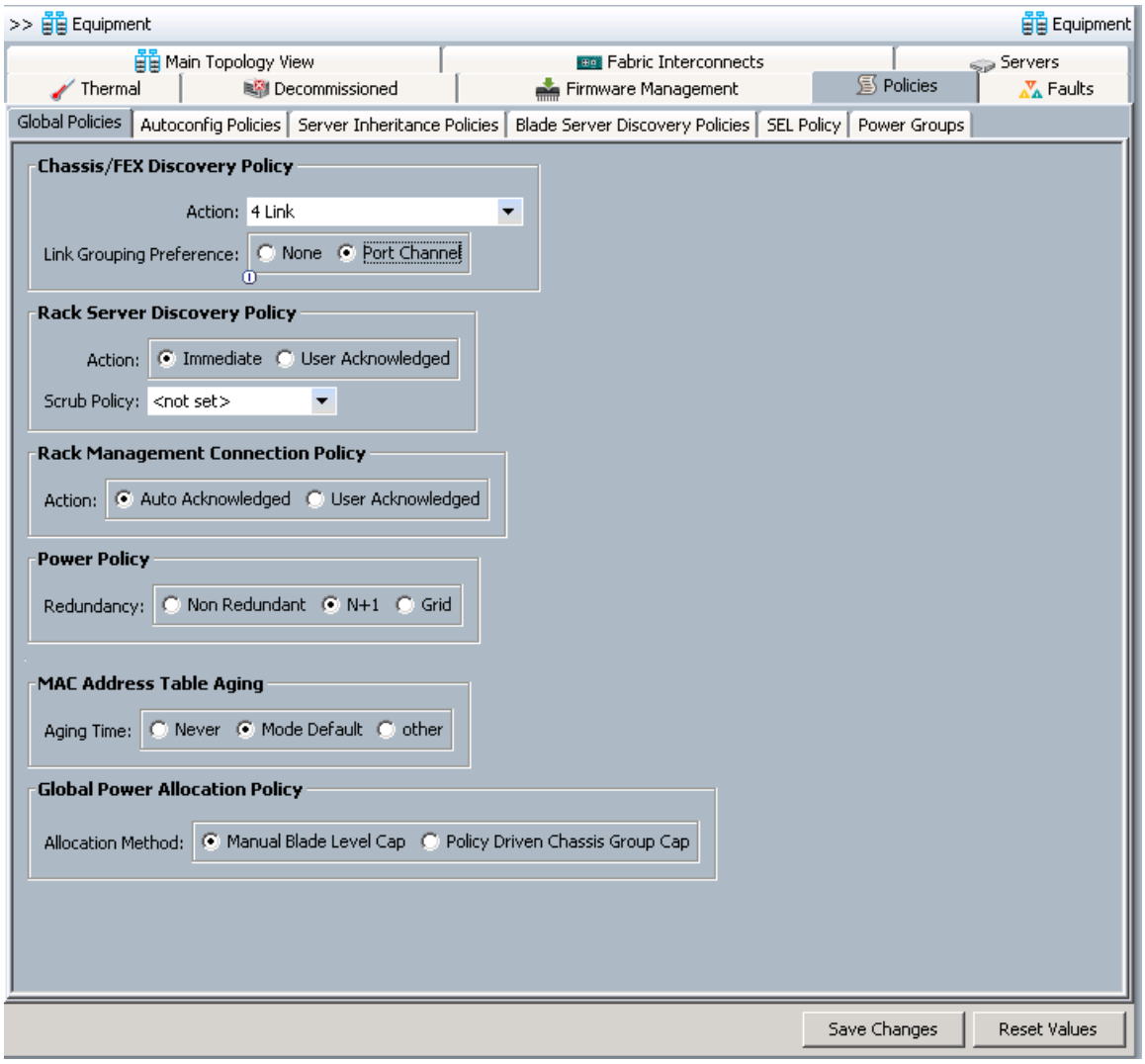
These steps provide details for synchronizing the Cisco UCS environment to the NTP server.

1. Select the `Admin` tab at the top of the left window.
8. Select `All > Timezone Management`.
9. Right-click `Timezone Management`.
10. In the right pane, select the appropriate timezone in the `Timezone` drop-down menu.
11. Click `Save Changes` and then `OK`.
12. Click `Add NTP Server`.
13. Input the NTP server IP and click `OK`.

9.4 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.

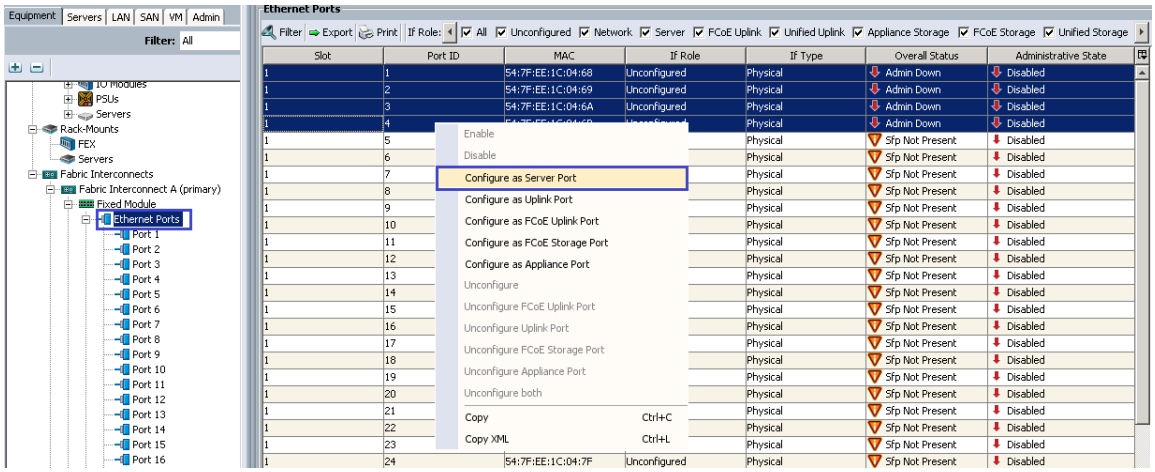
1. Navigate to the Equipment tab in the left pane and select the Equipment top-node object.
2. In the right pane, click the Policies tab.
3. Under Global Policies, change the Chassis Discovery Policy to 4-link or set it to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Keep Link Grouping Preference set to Port Channel
5. Click Save Changes in the bottom right corner.



9.5 Enable Server and Uplink Ports

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

1. Select the `Equipment` tab on the top left of the window.
2. Select `Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module`.
3. Expand the `Ethernet Ports` object.
4. Select the ports that are connected to the chassis or to the Cisco 2232 FEX (four per FEX), right-click them, and select Configure as Server Port.
5. Click Yes to confirm the server ports, and then click OK.
6. The ports connected to the chassis or to the Cisco 2232 FEX are now configured as server ports.

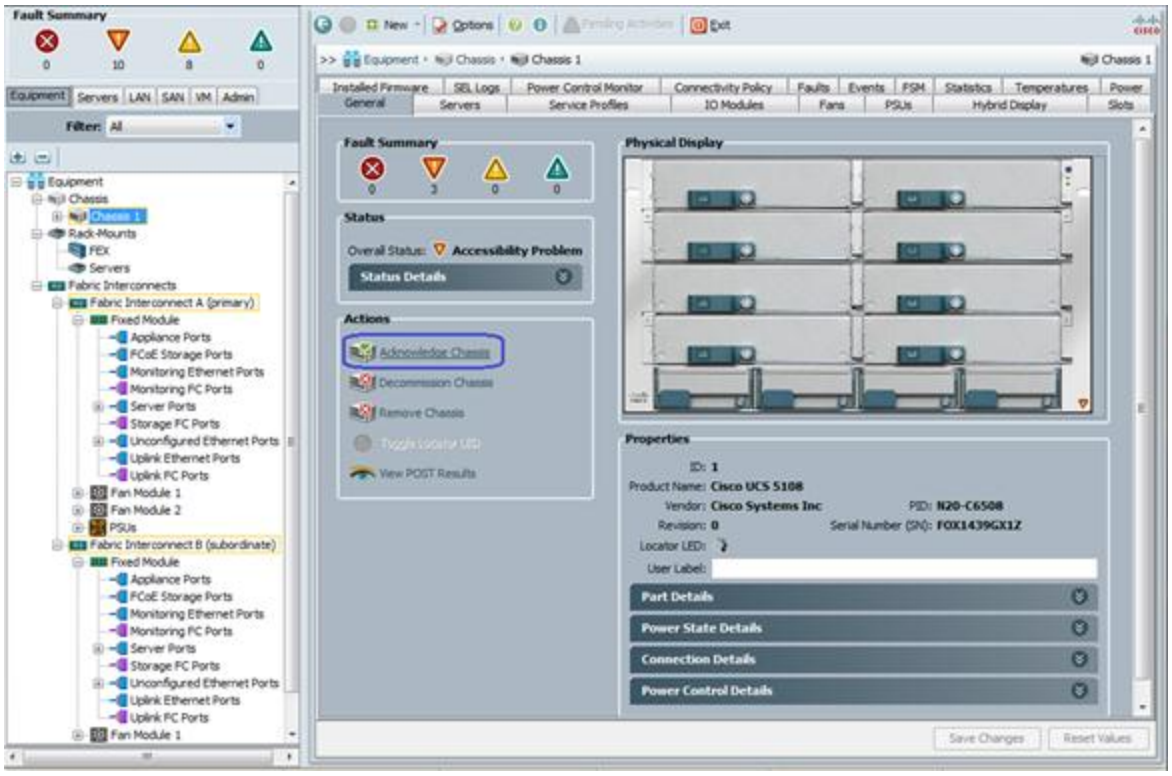


7. A prompt displays asking if this is what you want to do. Click `Yes`, then `OK` to continue.
8. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select `Configure as Uplink Port`.
9. A prompt displays asking if this is what you want to do. Click `Yes`, then `OK` to continue.
10. Select `Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module`.
11. Expand the `Ethernet Ports` object.
12. Select ports the number of ports that are connected to the Cisco UCS chassis (4 per chassis), right-click them, and select `Configure as Server Port`.
13. A prompt displays asking if this is what you want to do. Click `Yes`, then `OK` to continue.
14. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select `Configure as Uplink Port`.
15. A prompt displays asking if this is what you want to do. Click `Yes`, then `OK` to continue.
16. At the prompt, click Yes to confirm the uplink ports, and then click OK.

9.6 Acknowledge the Cisco UCS Chassis

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

1. Select `Chassis 1` in the left pane.
2. Click Acknowledge Chassis.



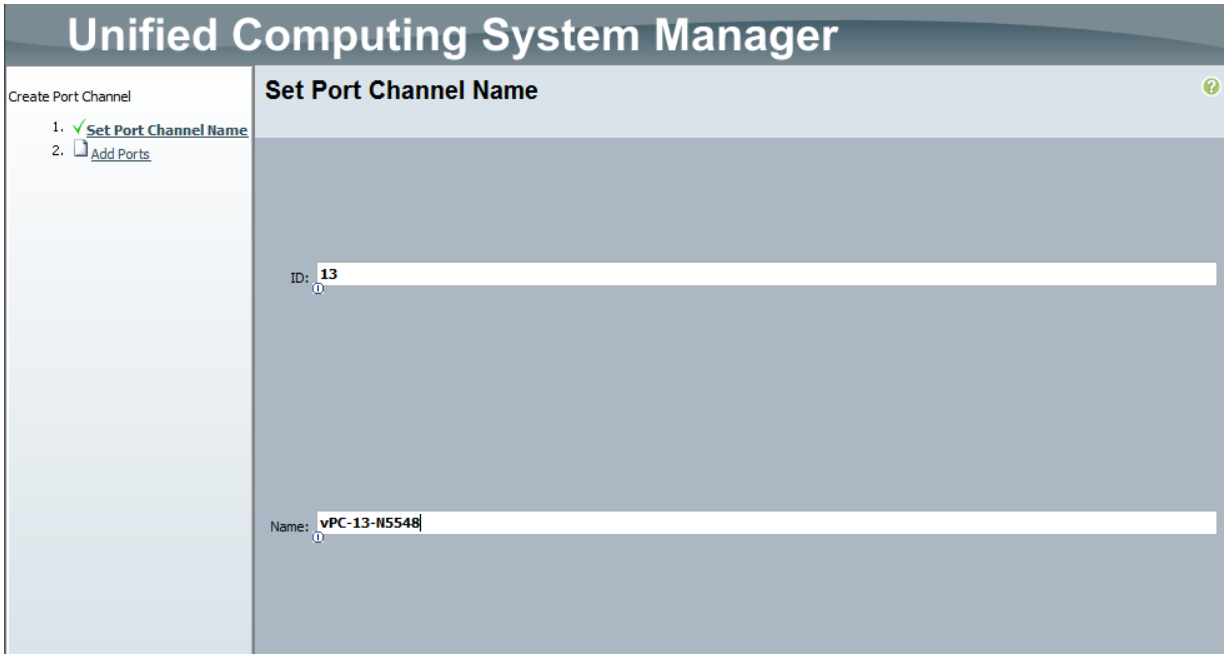
9.7 Create Uplink Port Channels to the Cisco Nexus 5548 Switches

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

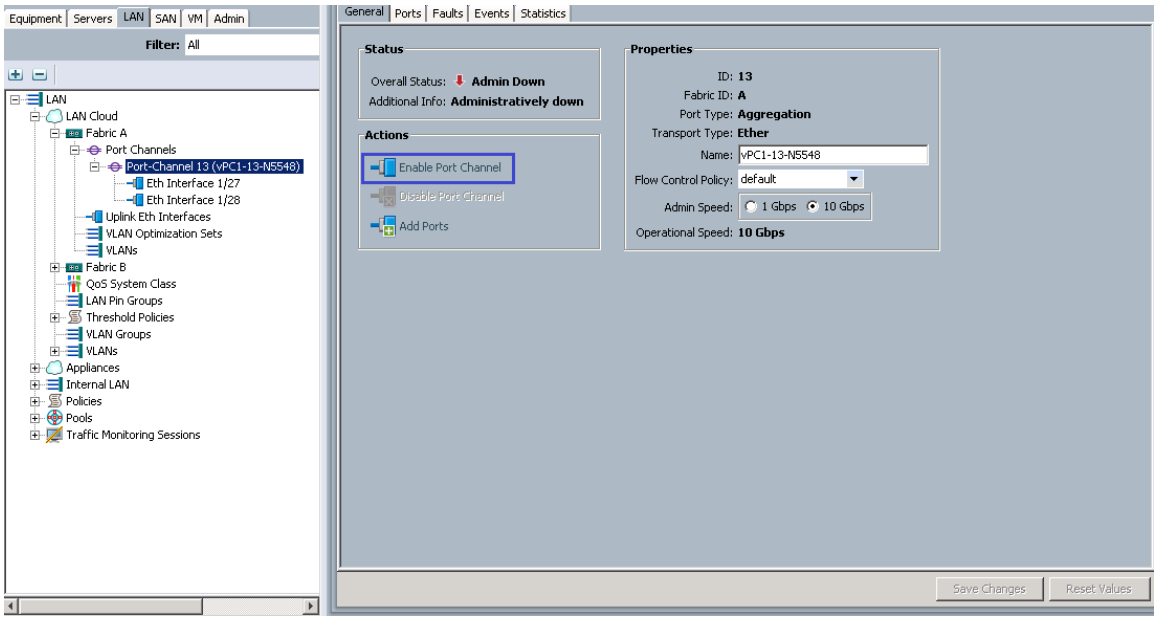
1. Select the `LAN` tab on the left of the window.

Note: Two Port Channels are created, one from fabric A to both Cisco Nexus 5548 switches and one from fabric B to both Cisco Nexus 5548 switches.

2. Under `LAN Cloud`, expand the `Fabric A` tree.
3. Right-click `Port Channels`.
4. Select `Create Port Channel`.
5. Enter `13` as the unique ID of the Port Channel.
6. Enter `vPC-13-N5548` as the name of the Port Channel.
7. Click `Next`.



8. Select the port with slot ID: `1` and port: `19` and also the port with slot ID: `1` and port `20` to be added to the Port Channel.
9. Click >> to add the ports to the Port Channel.
10. Click `Finish` to create the Port Channel.
11. Select the check box for `Show navigator for Port-Channel 13 (Fabric A)`
12. Click `OK` to continue.
13. Under `Actions`, select `Enable Port Channel`.
14. In the pop-up box, click `Yes`, then `OK` to enable.



15. Wait until the overall status of the Port Channel is up.

16. Click OK to close the Navigator.
17. Under LAN Cloud, expand the Fabric B tree.
18. Right-click Port Channels.
19. Select Create Port Channel.
20. Enter 14 as the unique ID of the Port Channel.
21. Enter vPC-14-N5548 as the name of the Port Channel.
22. Click Next.
23. Select the port with slot ID: 1 and port: 19 and also the port with slot ID: 1 and port 20 to be added to the Port Channel.
24. Click >> to add the ports to the Port Channel.
25. Click Finish to create the Port Channel.
26. Select Check box for Show navigator for Port-Channel 14 (Fabric B).
27. Click OK to continue.
28. Under Actions, select Enable Port Channel.
29. In the pop-up box, click Yes, then OK to enable.
30. Wait until the overall status of the Port Channel is up
31. Click OK to close the Navigator.

9.8 Create an Organization

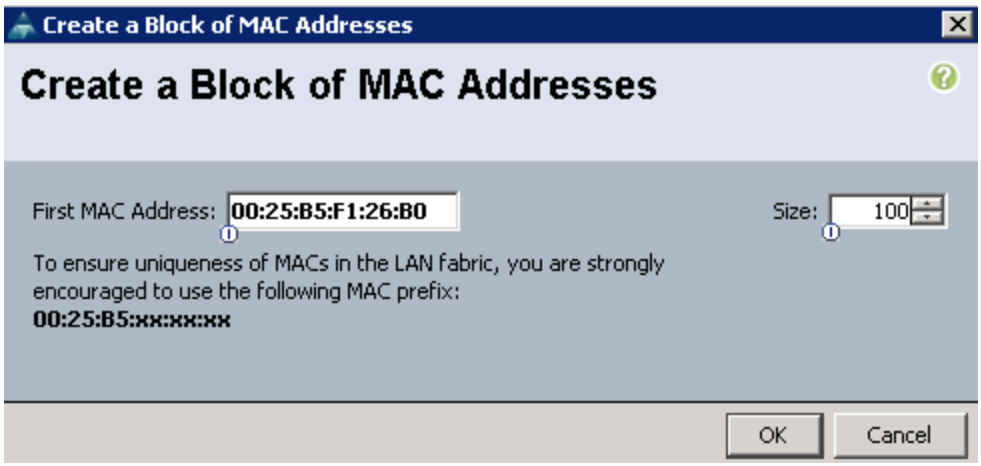
These steps provide details for configuring an organization in the Cisco UCS environment. Organizations are used as a means to organize and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources. This document does not assume the use of Organizations; however the necessary steps are included below.

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

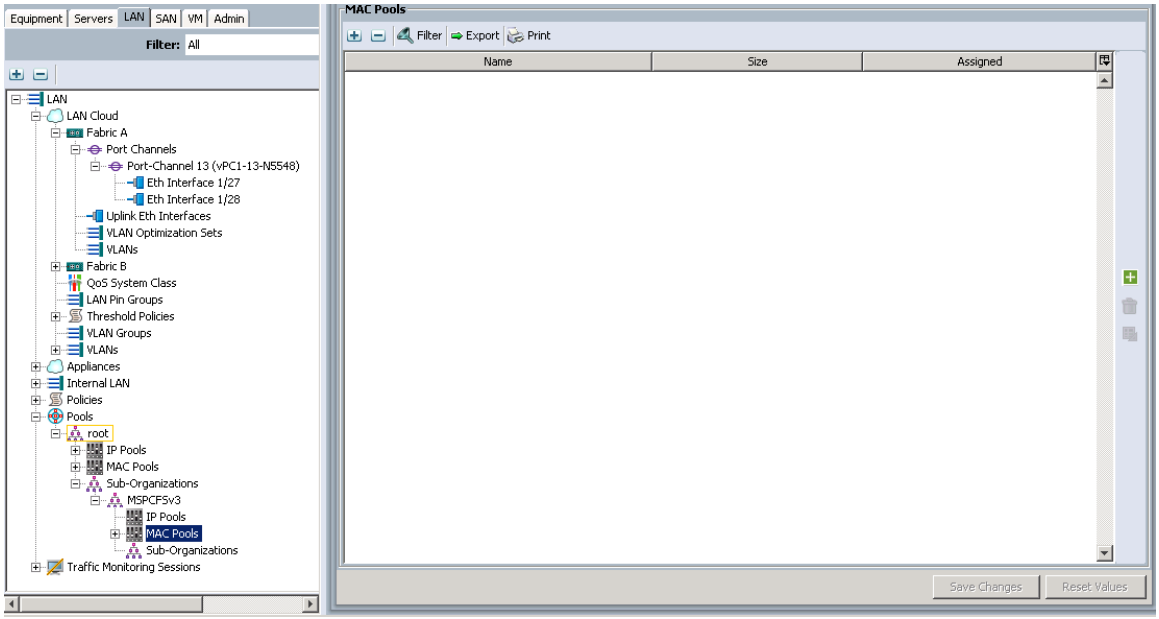
9.9 Create a MAC Address Pool

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

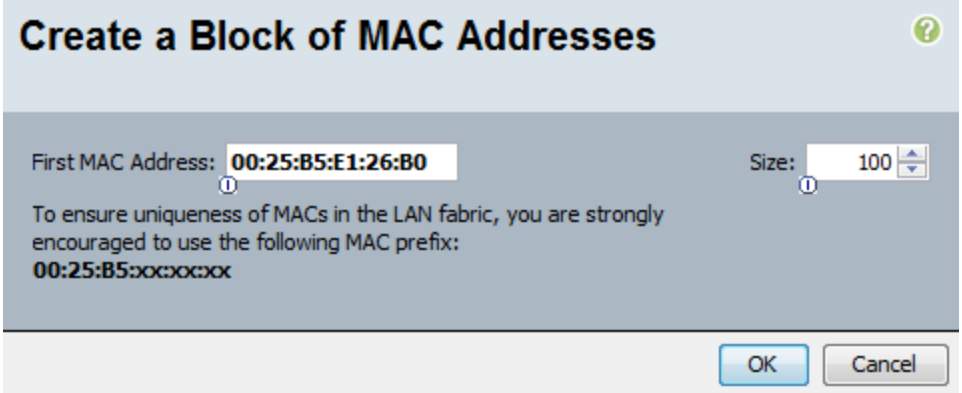
1. Select the LAN tab on the left of the window.
2. Select Pools > root > MAC Pools > MAC Pool default
3. In the right pane click Create a Block of MAC Addresses.
4. Specify a starting MAC address.
5. Specify a size of the MAC address pool sufficient to support the available blade resources.



6. Select Pools > Sub Organizations.



7. Right-click MAC Pools under the organization previously created.
8. Select Create MAC Pool to create the MAC address pool.
9. Enter MAC_Pool for the name of the MAC pool.
10. (Optional) Enter a description of the MAC pool.
11. Select Default assignment order.tesr
12. Click Next.
13. Click Add.
14. Specify a starting MAC address.
15. Specify a size of the MAC address pool sufficient to support the available blade resources.



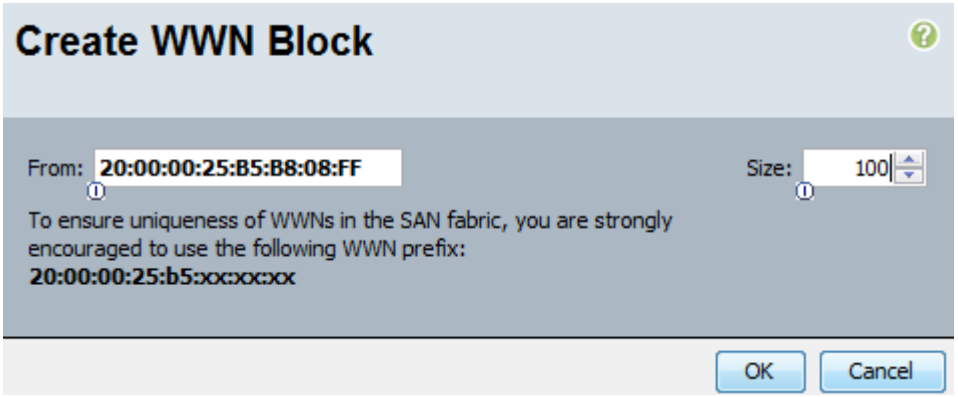
16. Click `OK`.
17. Click `Finish`.
18. In the message box that displays, click `OK`.

9.10 Create WWNN Pools

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

1. Select the `SAN` tab at the top left of the window.
2. Select `Pools > root`.
3. Right-click `WWNN Pools`
4. Select `Create WWNN Pool`.
5. Enter `WWNN_Pool` as the name of the WWNN pool.
6. (Optional) Add a description for the WWNN pool.
7. Click `Next` to continue.
8. Click `Add` to add a block of WWNN's.

   Note: The default is appropriate for most configurations, modify if necessary.
9. Specify a size of the WWNN block sufficient to support the available blade resources.

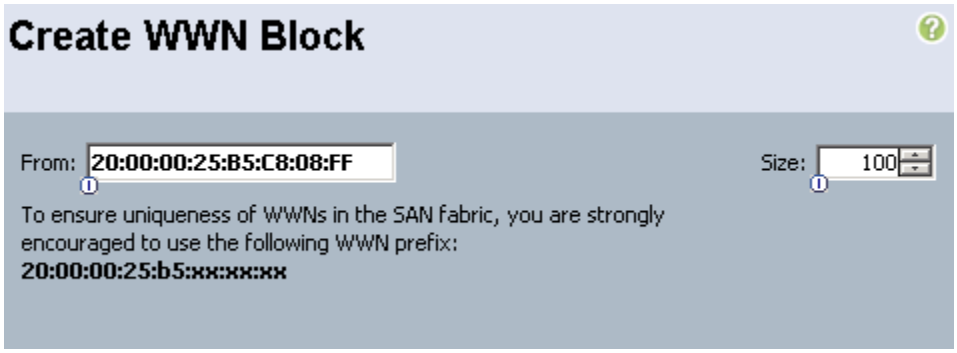


10. Click `OK` to proceed.
11. Click `Finish` to proceed.
12. Click `OK` to finish.

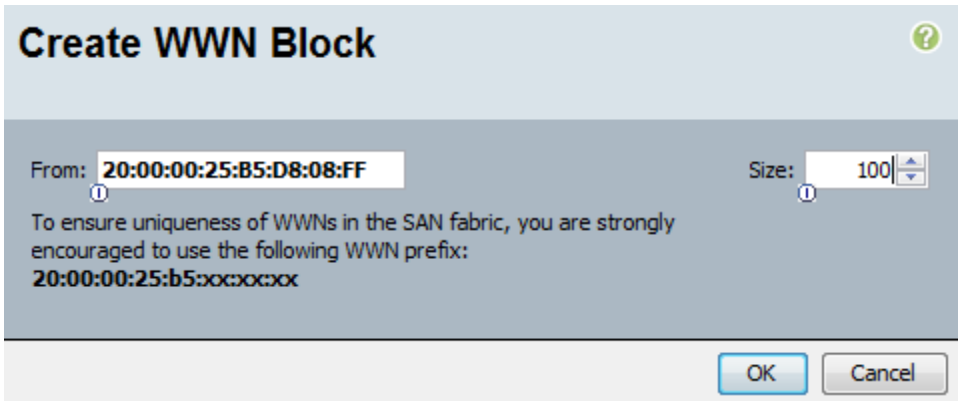
9.11 Create WWPN Pools

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

1. Select the SAN tab at the top left of the window.
2. Select Pools > root.
3. Select WWPN Pool default.
4. In the right pane click Create WWN Block.
5. Enter the starting WWPN in the From field.
6. Specify a size of the WWPN block sufficient to support the available server resources.



7. Select Pools > root > and the previously created sub organization.
8. In the right pane click Create WWN Block.
9. Enter the starting WWPN in the From field.
10. Specify a size of the WWPN block sufficient to support the available server resources.



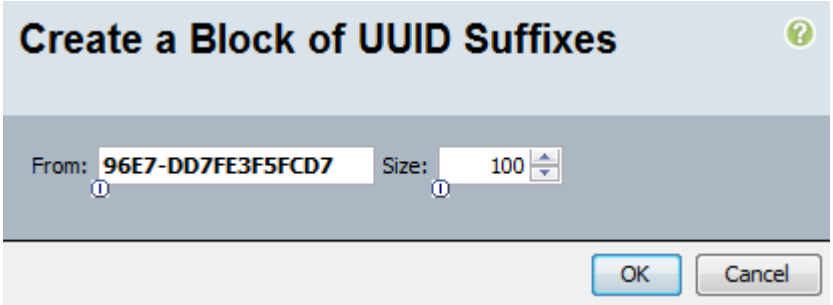
11. Click OK.
12. Click Finish to create the WWPN pool.
13. Click OK.

9.12 Create UUID Suffix Pools

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

1. Select the Servers tab on the top left of the window.
2. Select Pools > root.

3. Right-click `UUID Suffix Pools`
4. Select `Create UUID Suffix Pool`.
5. Name the UUID suffix pool UUID_Pool.
6. (Optional) Give the UUID suffix pool a description.
7. Leave the prefix at the derived option.
8. Click `Next` to continue.
9. Click `Add` to add a block of UUID's
10. The From field is fine at the default setting.
11. Specify a size of the UUID block sufficient to support the available blade resources.



12. Click `OK`.
13. Click `Finish` to proceed.
14. Click `OK` to finish.

9.13 Create Server Pools

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

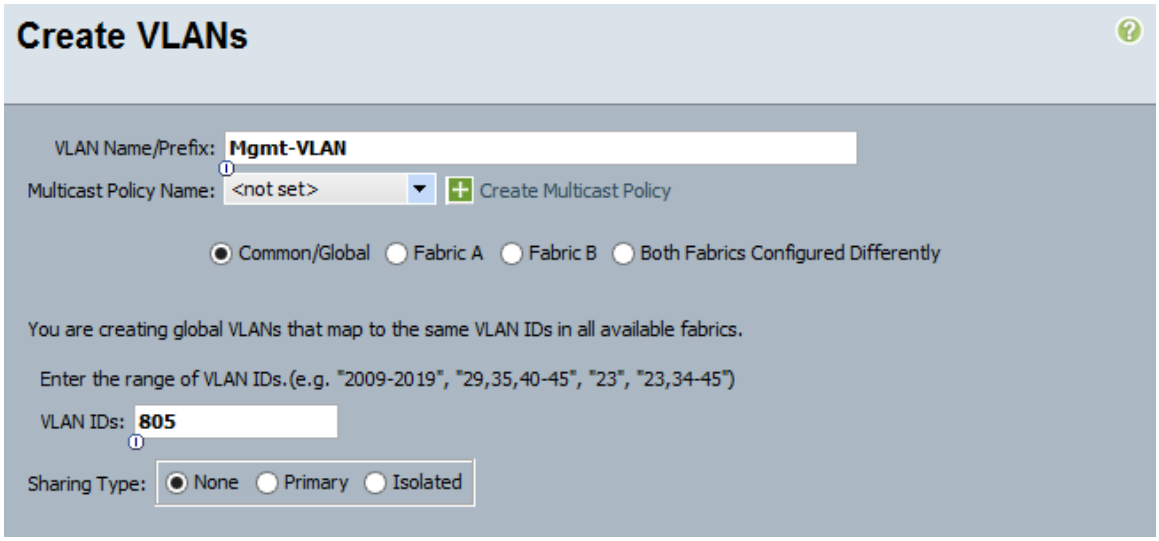
1. Select the `Servers` tab at the top left of the window.
2. Select `Pools > root`.
3. Right-click `Server Pools`.
4. Select `Create Server Pool`.
5. Name the server pool `Infra_Pool`.
6. (Optional) Give the server pool a description.
7. Click `Next` to continue to add servers.
8. Select two server to be used for the infrastructure cluster and Click `>>` to add them to the pool.
9. Click `Finish`.
10. Select `OK` to finish.

9.14 Create VLANs

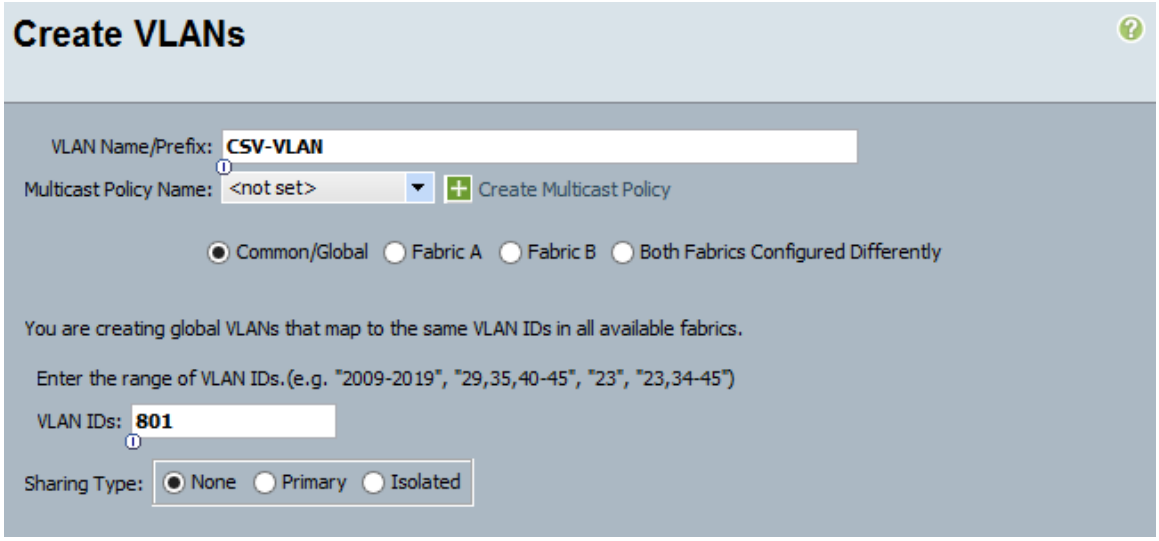
These steps provide details for configuring the necessary VLANs for the Cisco UCS environment.

1. Select the `LAN` tab on the left of the window. Eight VLANs are created.
2. Select `LAN Cloud`.
3. Right-click `VLANs`.

4. Select `Create VLANs`.
5. Enter `MGMT-VLAN` as the name of the VLAN to be used for management traffic.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter the VLAN ID for the management VLAN. Keep the sharing type as `none`.
8. Click `OK`.

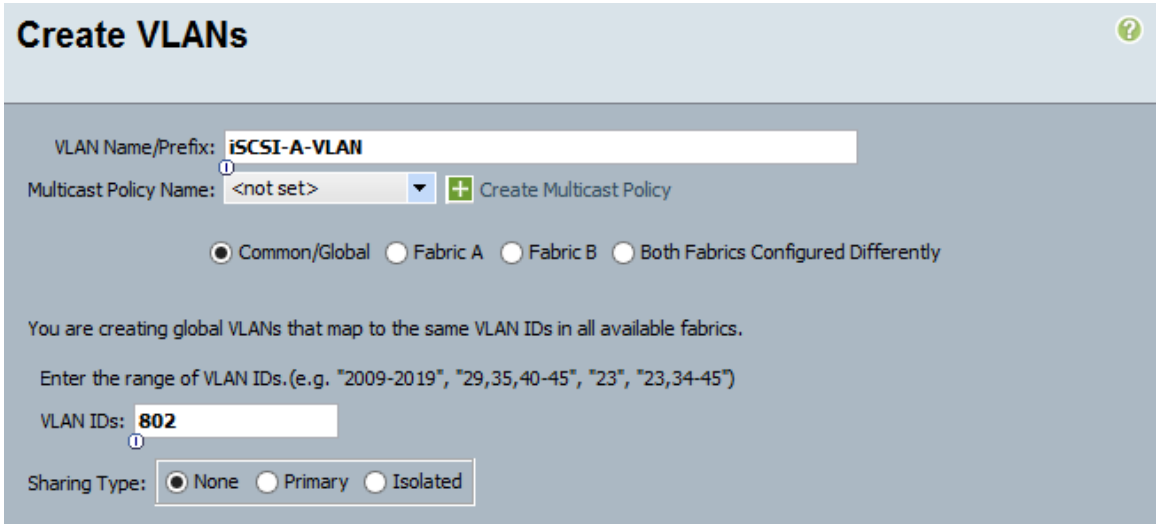


9. Right-click `VLANs`.
10. Select `Create VLANs`.
11. Enter `CSV-VLAN` as the name of the VLAN to be used for the CSV VLAN.
12. Keep the `Common/Global` option selected for the scope of the VLAN.
13. Enter the VLAN ID for the CSV VLAN.
14. Click `OK`.

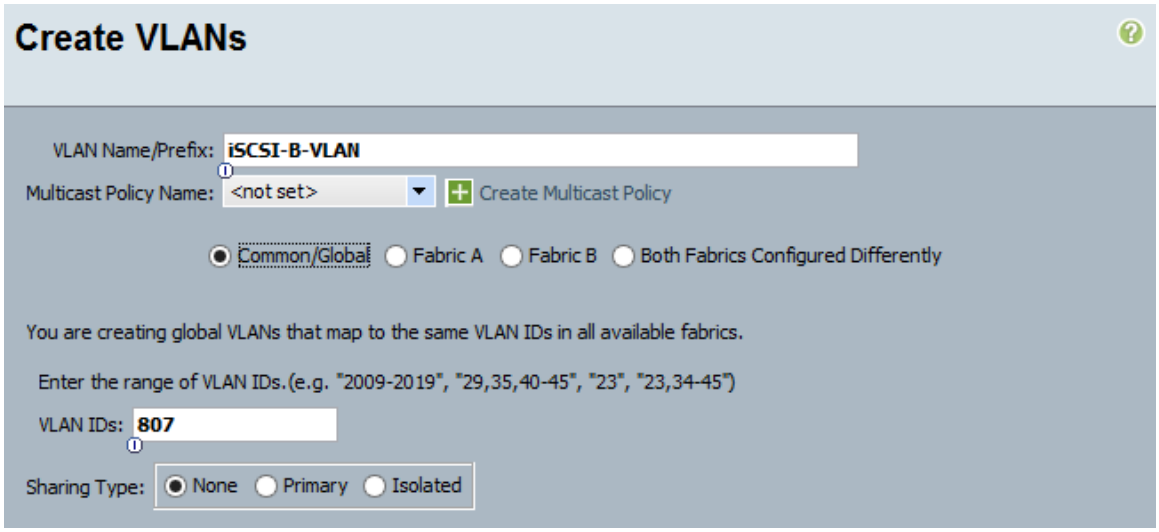


15. Right-click `VLANs`.
16. Select `Create VLANs`.
17. Enter `iSCSI-A-VLAN` as the name of the VLAN to be used for the first iSCSI VLAN.

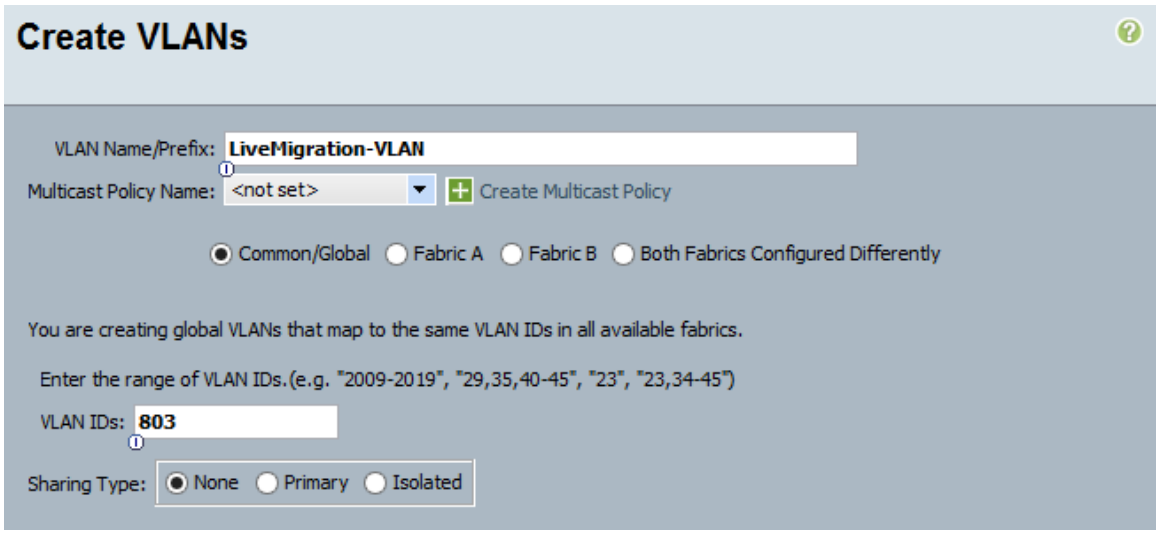
18. Keep the `Common/Global` option selected for the scope of the VLAN.
19. Enter the VLAN ID for the first iSCSI VLAN.
20. Click `OK`.



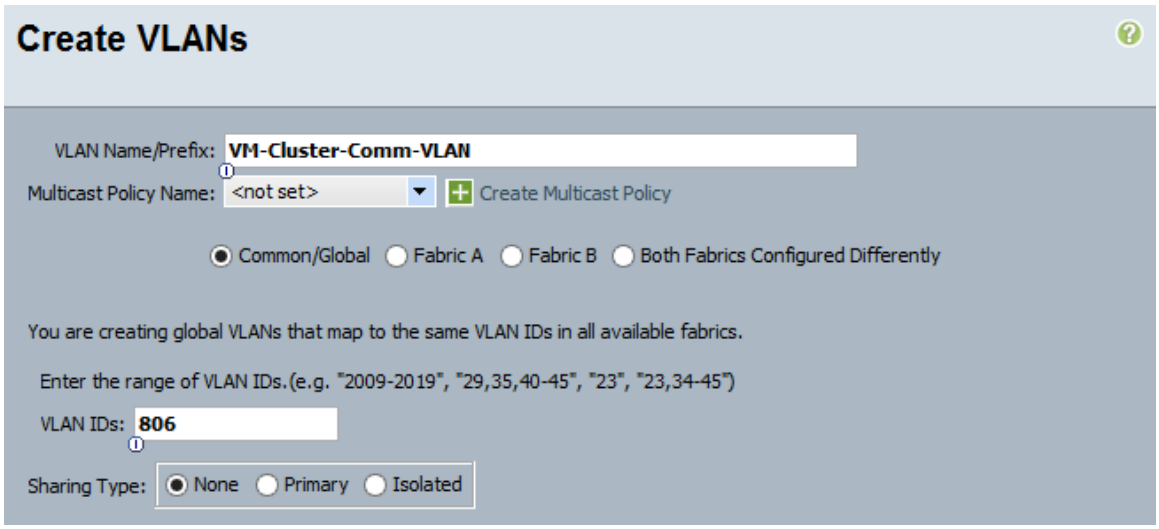
21. Right-click `VLANs`.
22. Select `Create VLANs`.
23. Enter `iSCSI-VLAN-B` as the name of the VLAN to be used for the second iSCSI VLAN.
24. Keep the `Common/Global` option selected for the scope of the VLAN.
25. Enter the VLAN ID for the second iSCSI VLAN.
26. Click `OK`.



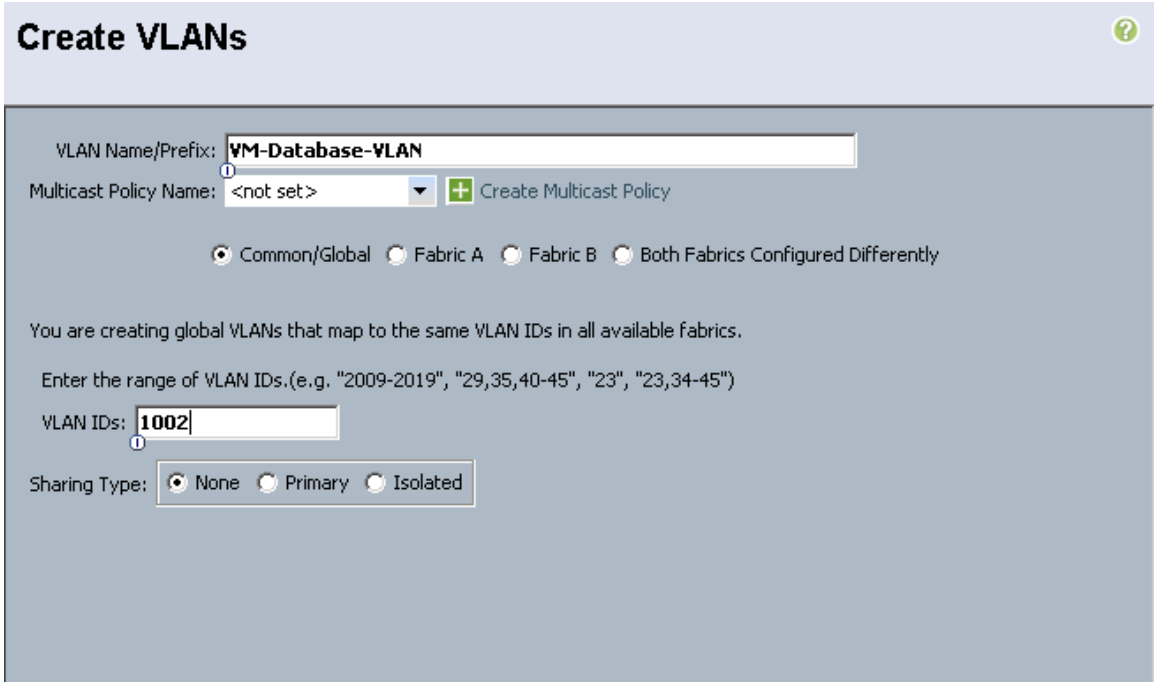
27. Right-click VLANs.
28. Select `Create VLANs`.
29. Enter `Live Migration-VLAN` as the name of the VLAN to be used for the live migration VLAN.
30. Keep the `Common/Global` option selected for the scope of the VLAN.
31. Enter the VLAN ID for the live migration VLAN.
32. Click `OK`,



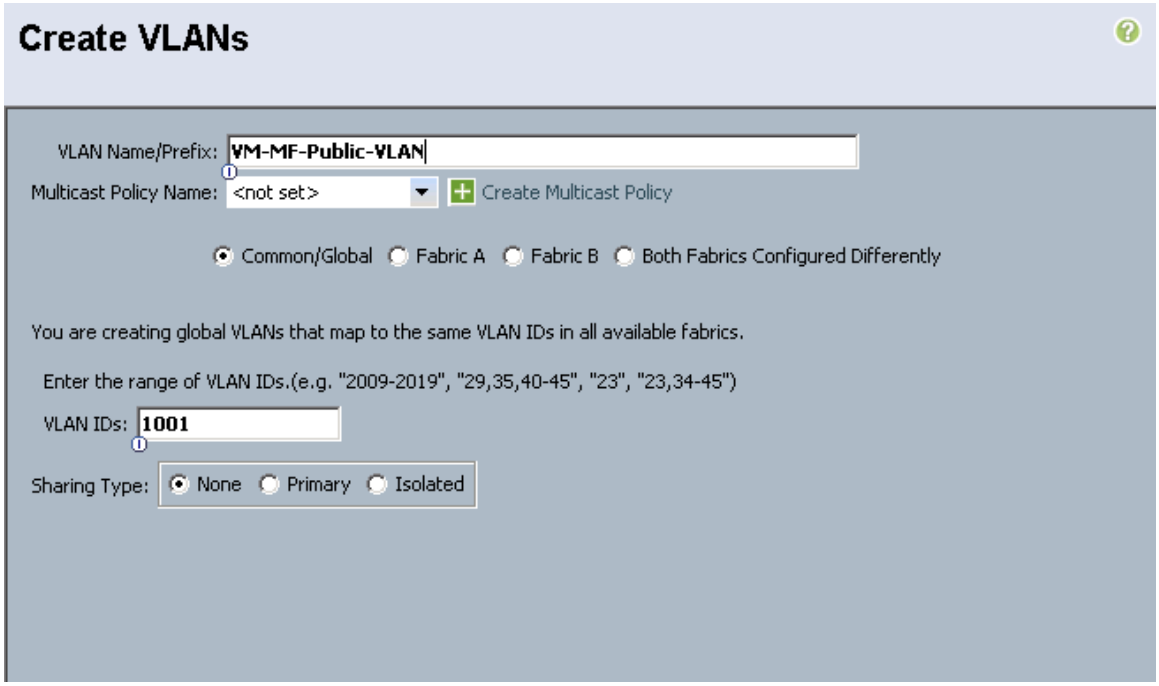
33. Right clisk VLANs
34. Select `Create VLANs`.
35. Enter `VM-Cluster-Comm-VLAN` as the name of the VLAN to be used for the VM Cluster VLAN.
36. Keep the `Common/Global` option selected for the scope of the VLAN.
37. Enter the VLAN ID for the VM Cluster VLAN.
38. Click `OK`.



39. Right-click `VLANs`.
40. Select `Create VLANs`.
41. Enter VM-Database-VLAN as the name of the VLAN to be used for the VM data VLAN.
42. Keep the `Common/Global` option selected for the scope of the VLAN.
43. Enter the VLAN ID for the VM data VLAN.
44. Click `OK`.

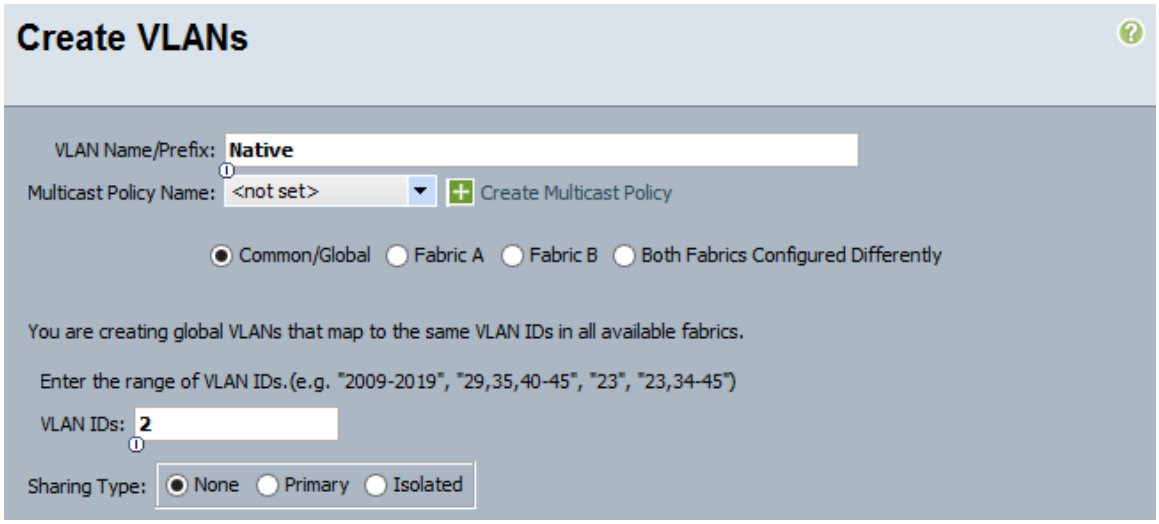


45. Right-click `VLANs`.
46. Select `Create VLANs`.
47. Enter VM-MF-Public-VLAN as the name of the VLAN to be used for the VM data VLAN.
48. Keep the `Common/Global` option selected for the scope of the VLAN.
49. Enter the VLAN ID for the VM data VLAN.
50. Click `OK`.



51. Right-click `VLANs`.

52. Select `Create VLANs`.
53. Enter `Native-VLAN` as the name of the VLAN to be used for the Native VLAN.
54. Keep the `Common/Global` option selected for the scope of the VLAN.
55. Enter the VLAN ID for the Native VLAN.
56. Click `OK`.

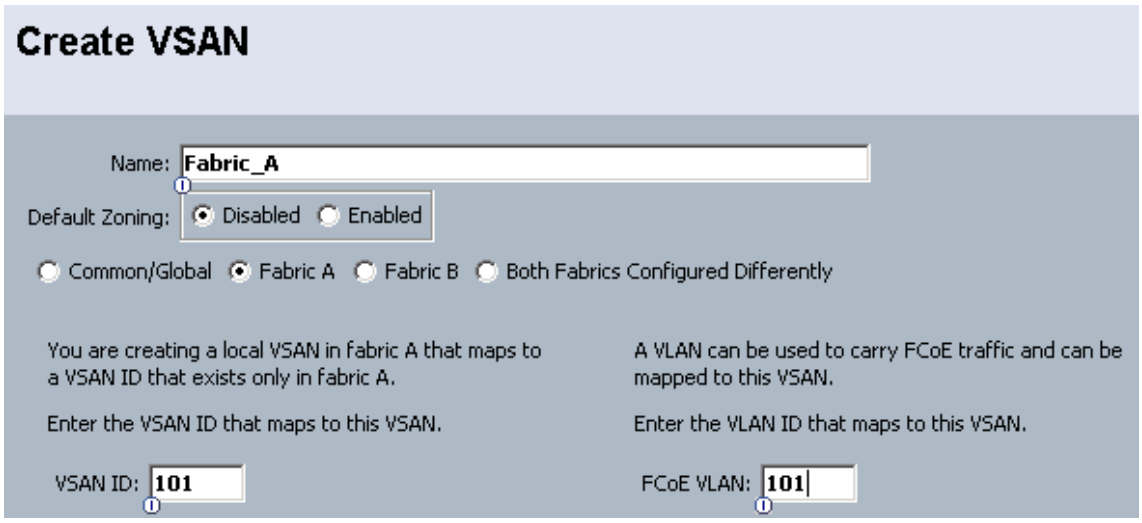


57. In the list of VLANs in the left pane, right-click the newly created Native-VLAN and select `Set as Native VLAN`.
58. Click `Yes` and `OK`.

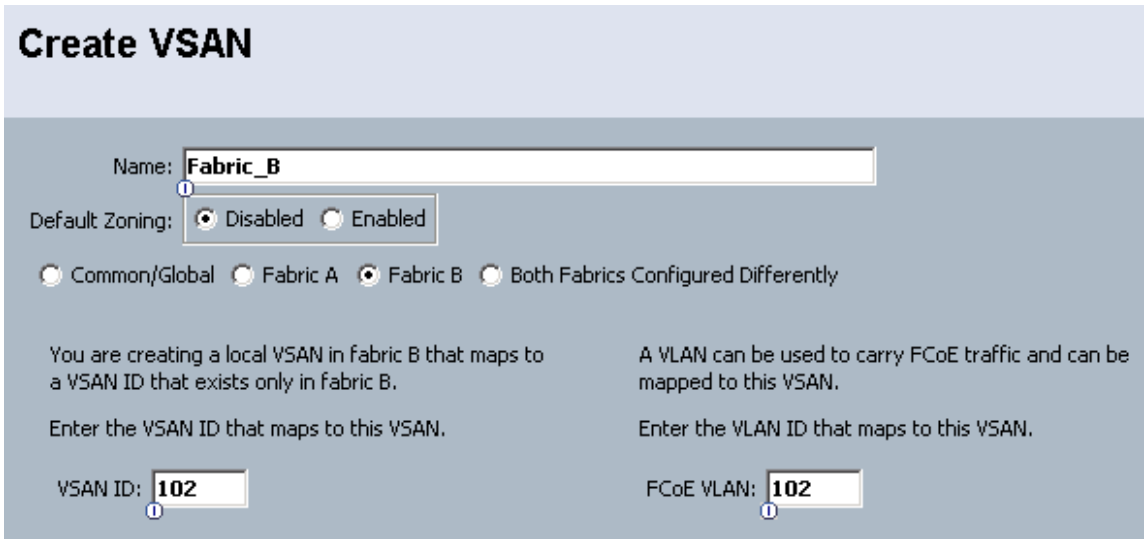
9.15 Create VSANs and FCoE Port Channels

These steps provide details for configuring the necessary VSANs and FCoE Port Channels for the Cisco UCS environment.

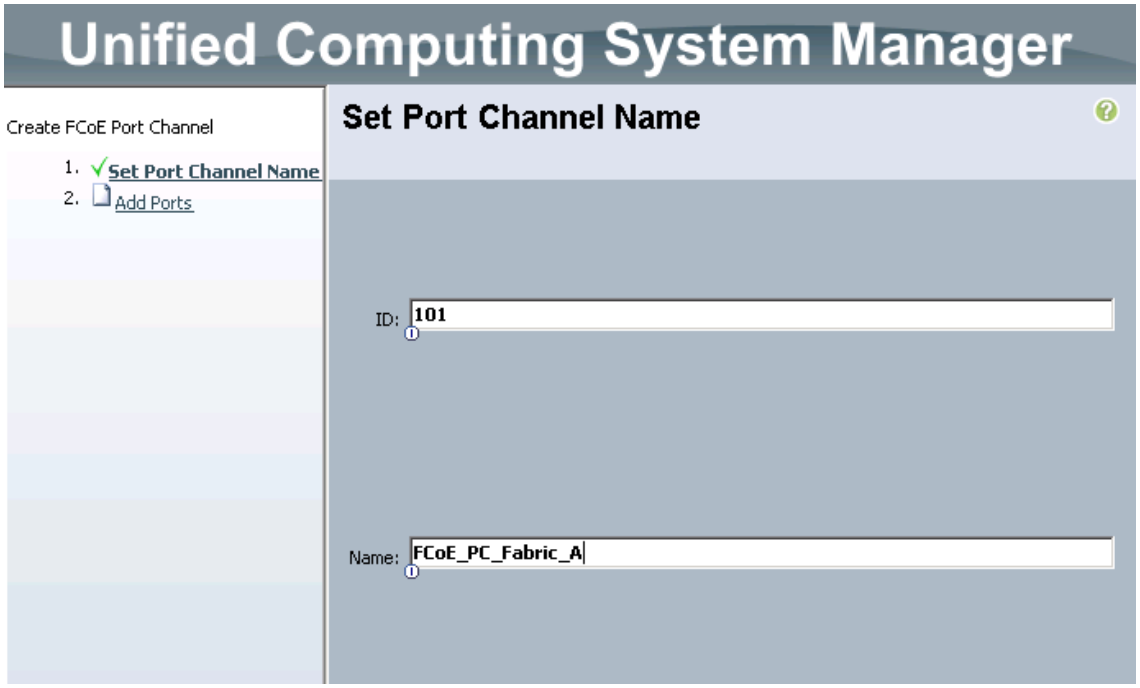
1. Select the `SAN` tab at the top left of the window.
2. Expand the `SAN Cloud` tree.
3. Right-click VSANs
4. Select `Create VSAN`.
5. Enter `VSAN_A` as the VSAN name for fabric A.
6. Keep the `Disabled` option selected for the Default Zoning
7. Select `Fabric A`.
8. Enter the VSAN ID for fabric A.
9. Enter the FCoE VLAN ID for fabric A.
10. Click `OK` and then `OK` to create the VSAN.



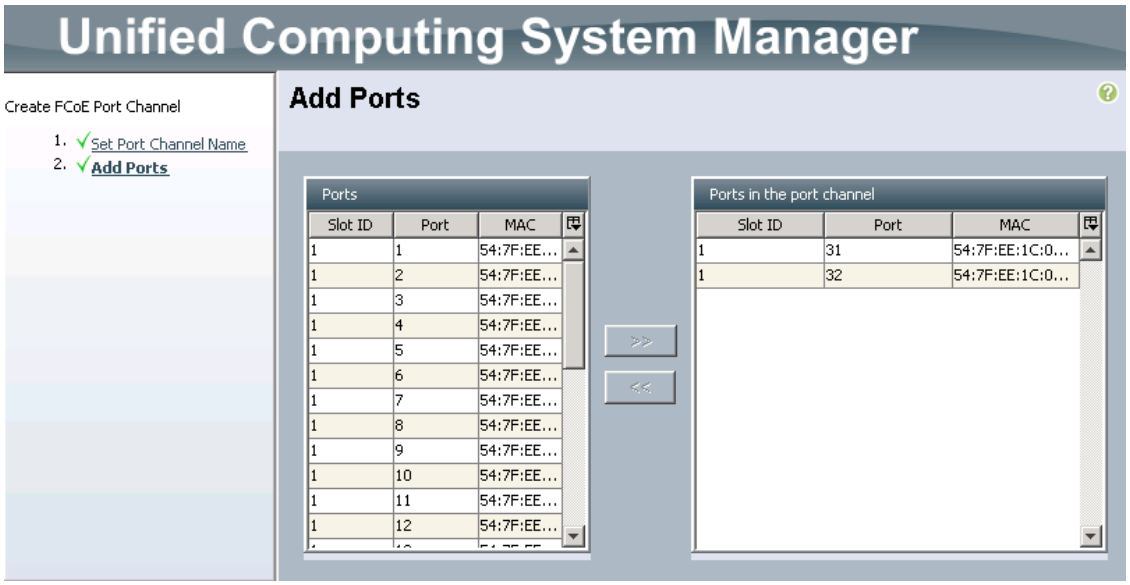
11. Right-click `VSANs`.
12. Select `Create VSAN`.
13. Enter `VSAN_B` as the VSAN name for fabric B.
14. Keep the `Disabled` option selected for the Default Zoning
15. Select `Fabric B`.
16. Enter the `VSAN ID` for fabric B.
17. Enter the FCoE VLAN ID for fabric B.
18. Click `OK` and then `OK` to create the VSAN.



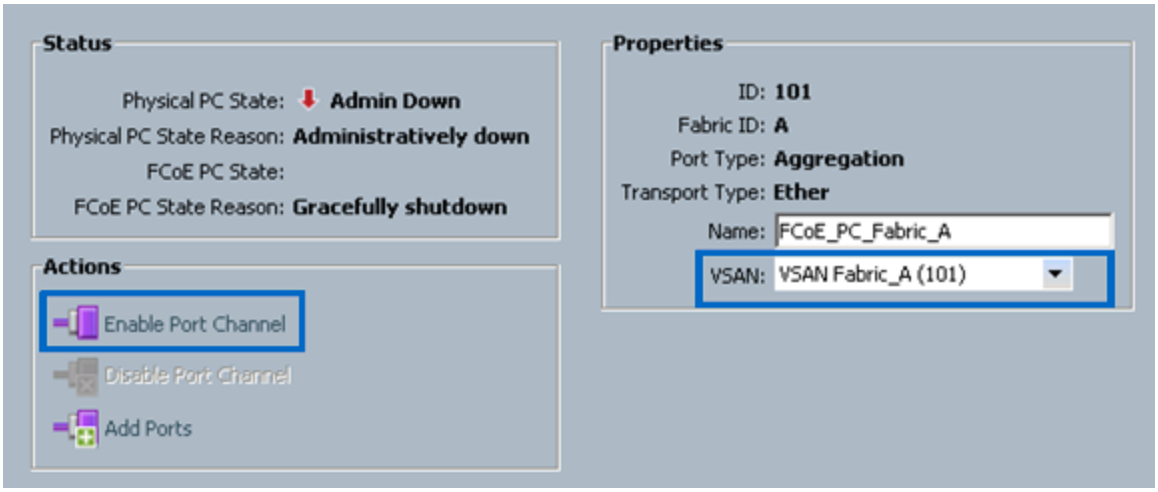
19. Under `SAN Cloud`, expand the `Fabric A` tree.
20. Right-click `FCoE Port Channels`
21. Select `Create FCoE Port Channel`.
22. Click `Yes` and then enter `101` for the Port Channel ID and `FCoE_PC_Fabric-A` for the Port Channel name.
23. Click `Next`.



24. Select ports `31` and `32` and click >> to add the ports to the Port Channel.
25. Click `Finish`.

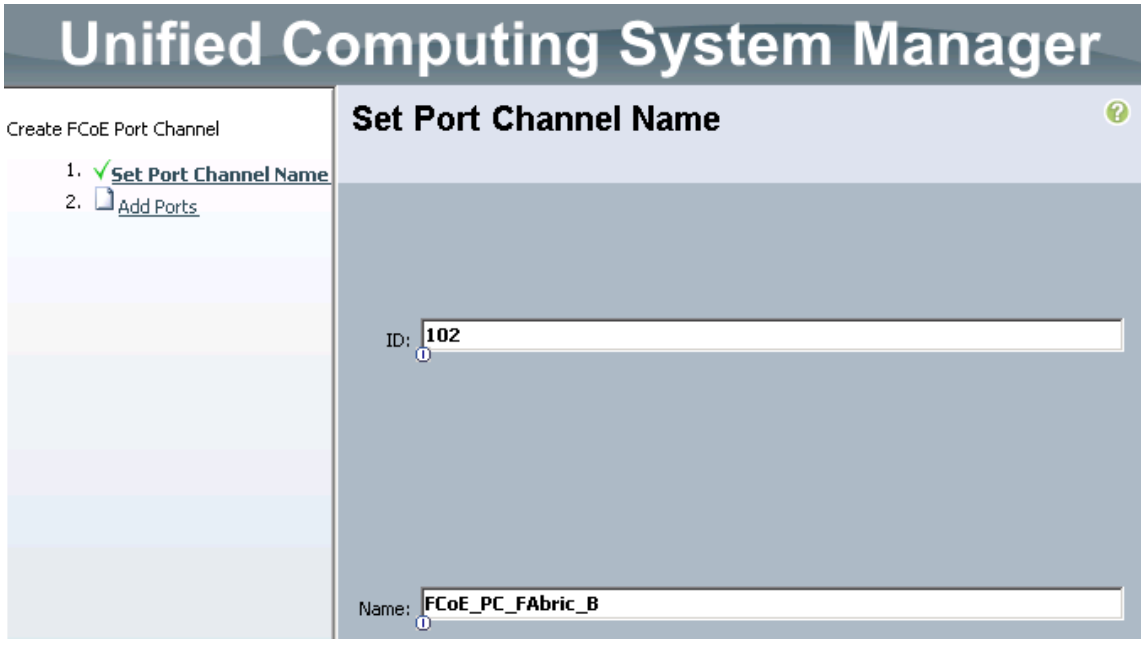


26. Select the Check box for `Show navigator for FCoE Port-Channel 101 (Fabric A)`
27. Click `OK` to complete creating the FCoE Port Channel.
28. In the VSAN pull-down under Properties select the `vsan VSAN_A for fabric A`.
29. Click `Apply`, then click `OK`.
30. Under `Actions`, click `Enable Port Channel`.
31. Click `Yes` and then `OK` to enable the Port Channel. This action also enables the two FCoE ports in the Port Channel.

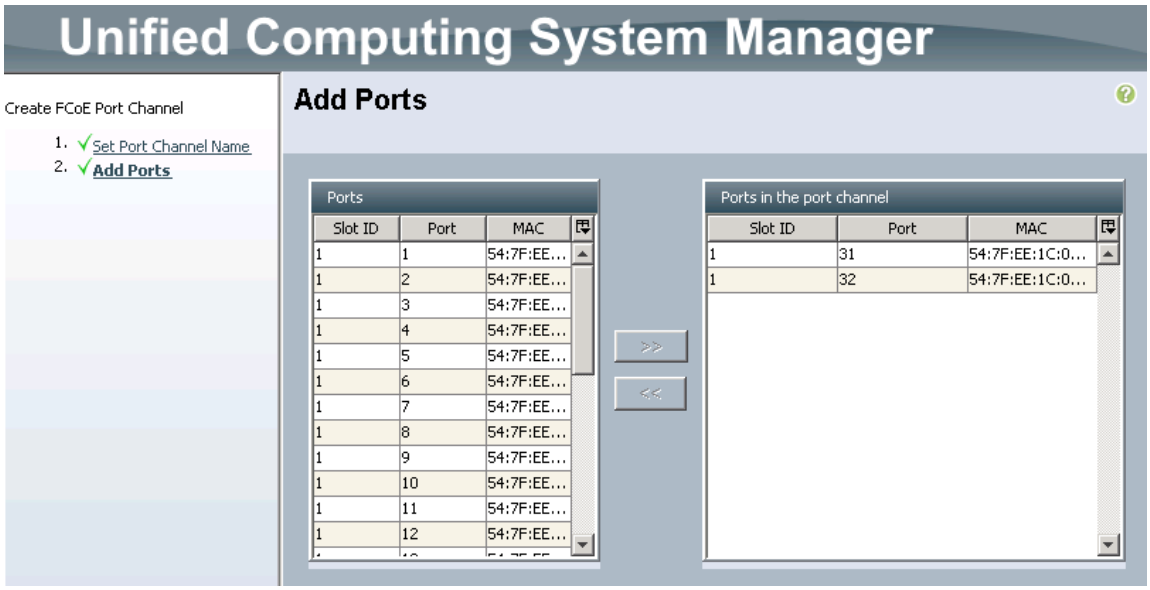


32. Click `OK` to Close the Navigator.
    Note: The FCoE Port Channel may take a few seconds to come up. The operational speed will be displayed when the link speed is negotiated. This may take approximately 30 seconds.

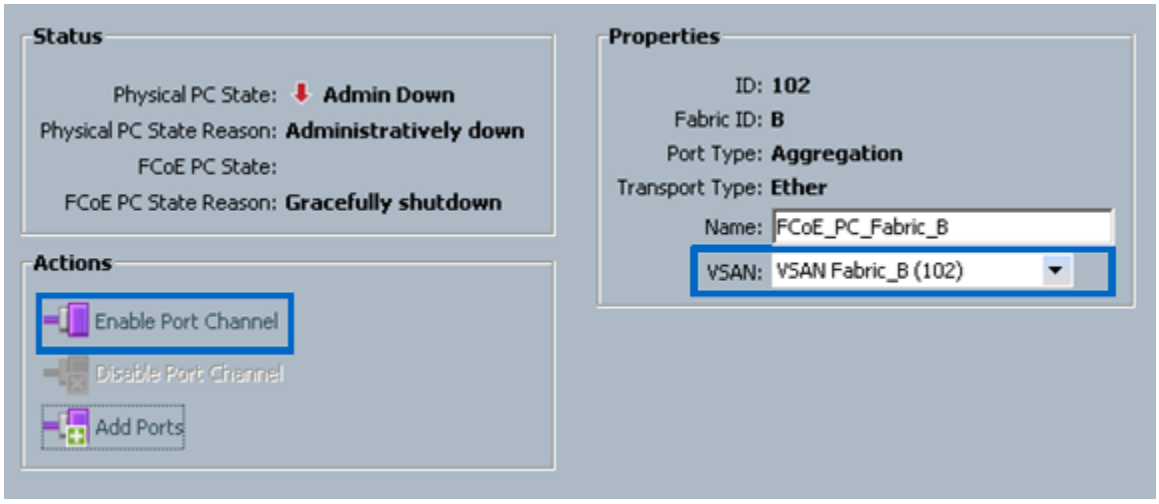
    Note: If the Overall State results in an error condition and does not clear after 30 seconds the FC uplink ports on the Nexus 5548UP will need to shut down and brought back up in order to establish the link.
33. Under `SAN Cloud`, expand the `Fabric B` tree.
34. Right-click `FCoE Port Channels`
35. Select `Create FcoE Port Channel`.
36. Click `Yes`, and then enter `102` for the Port Channel ID and `FCoE_PC_Fabric_B` for the Port Channel name.
37. Click `Next`.



38. Select ports `31` and `32` and click >> to add the ports to the Port Channel.
39. Click `Finish`.



40. Select Check box for `Show navigator for FCoE Port-Channel 102 (Fabric B)`
41. Click `OK` to complete creating the Port Channel.
42. In the VSAN pull-down under Properties, select `VSAN_B` for fabric B.
43. Click `Apply`, then click `OK`.
44. Under Actions, click `Enable Port Channel`.
45. Click `Yes`, then `OK` to enable the Port Channel. This action also enables the two FC ports in the Port Channel.



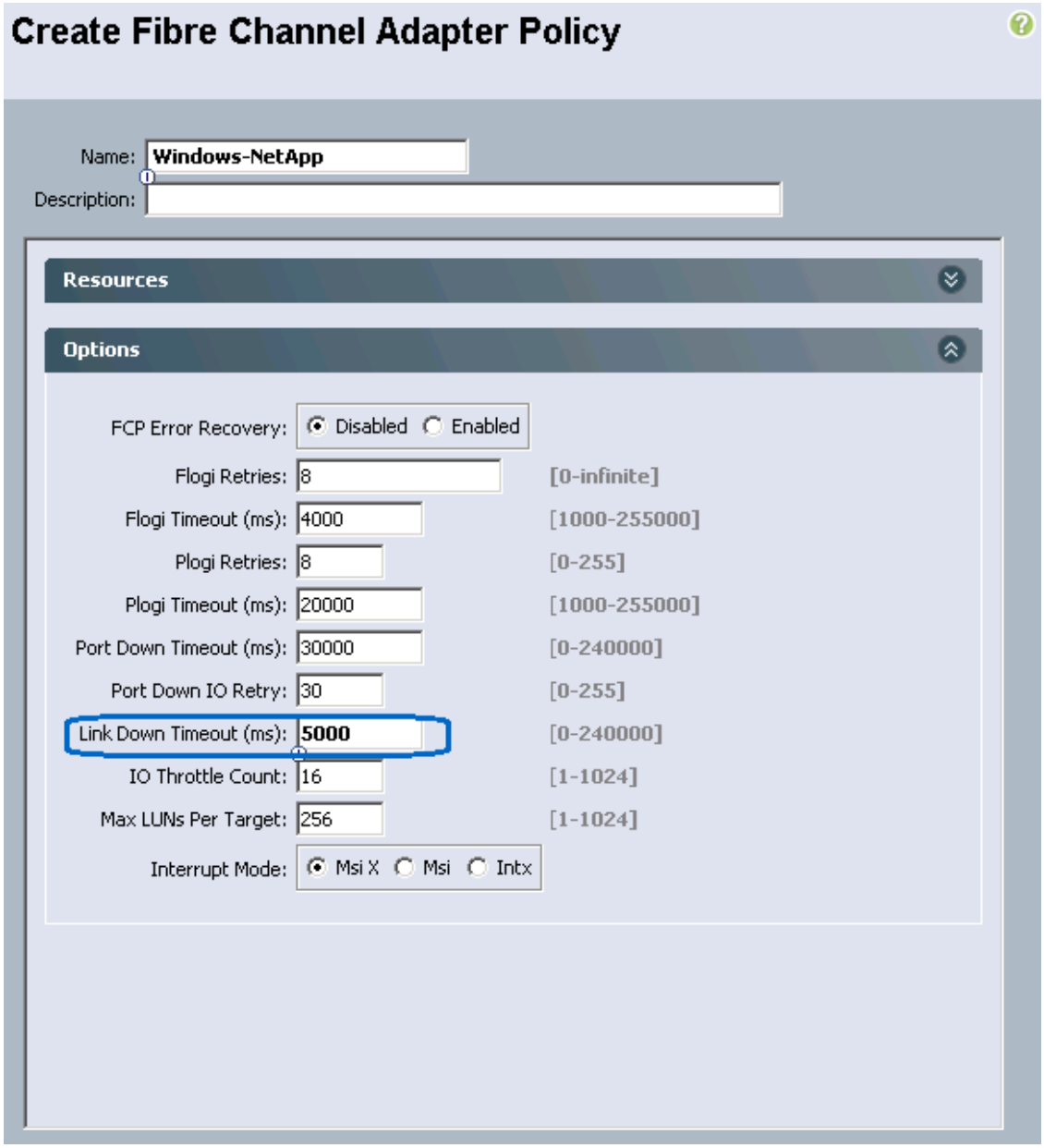
46. Click `OK` to Close the Navigator.
    Note: The FC Port Channel may take a few seconds to come up. The operational speed will be displayed when the link speed is negotiated. This may take approximately 30 seconds.

    Note: If the Overall State results in an error condition and does not clear after 30 seconds the FC uplink ports on the Nexus 5548UP will need to shut down and brought back up in order to establish the link.

9.16 Create a FC Adapter Policy for NetApp Storage Arrays

These steps provide details for a FC adapter policy for NetApp storage arrays.

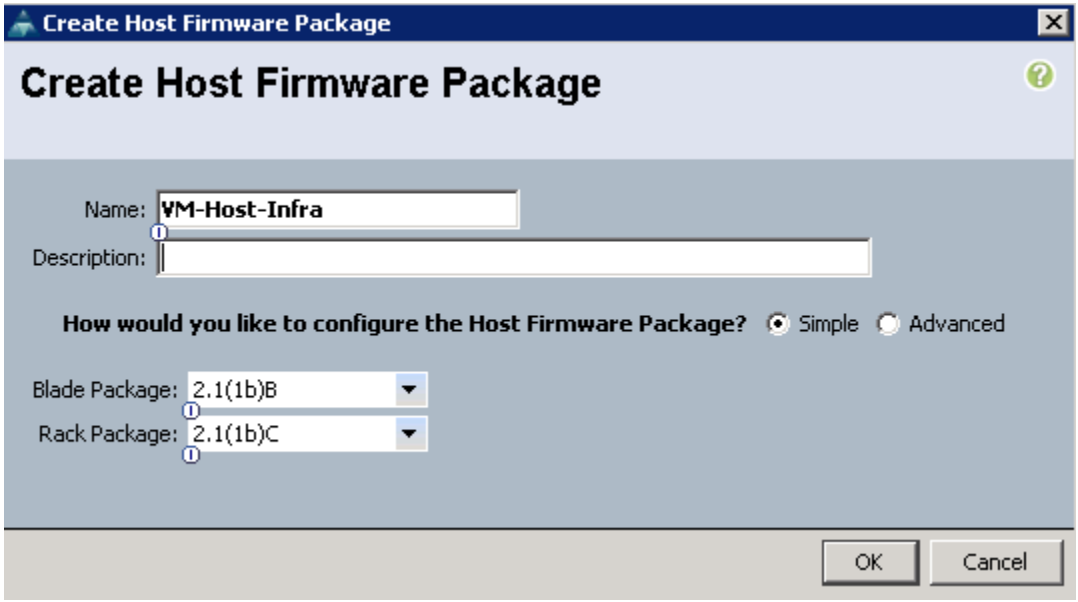
1. Select to the SAN tab at the top of the left window.
2. Go to `SAN > Policies > root`.
3. Right-click `Fibre Channel Adapter Policies` and click Create New Fibre Channel Adapter Policy.
4. Use `Windows-NetApp` as the name of the Fibre Channel Adapter Policy.
5. The default values are appropriate for most configurable items. Expand the `Options` dropdown. and set the `Link Down Timeout (MS)` option to `5000`.
6. Click `OK` to complete creating the FC adapter policy.
7. Click `OK`.



9.17 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.

1. Select the `Servers` tab at the top left of the window.
2. Select `Policies > root or a suborganization`.
3. Right Click `Host Firmware Packages`.
4. Select `Create Host Firmware Package`.
5. Enter the name of the host firmware package for the corresponding server configuration and an optional description.
6. Two typs of host firmware package are available. The simple option specifies all firmware based on a firmware verstion boundle. The Adavnced option allows granular control of the firmware version for each device type. **Select the Simple option** unless granular firmware version control is required.
7. The Blade package is for blade serves and the Rack Package is for rack serves. Select the Blade Package and Rack Package in the dropdown text boxes.
8. Click OK to create the host firmware package.

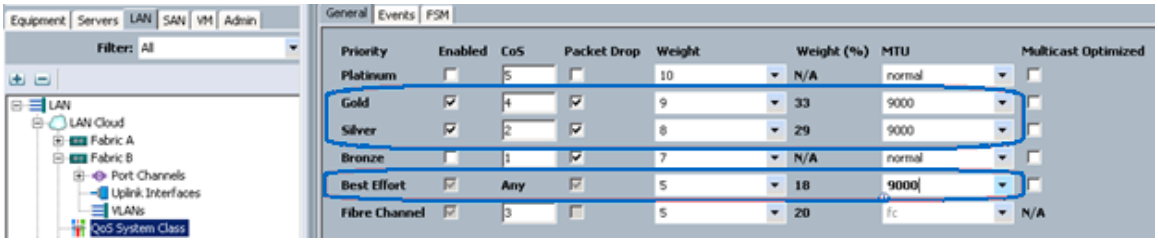


9.18 Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric

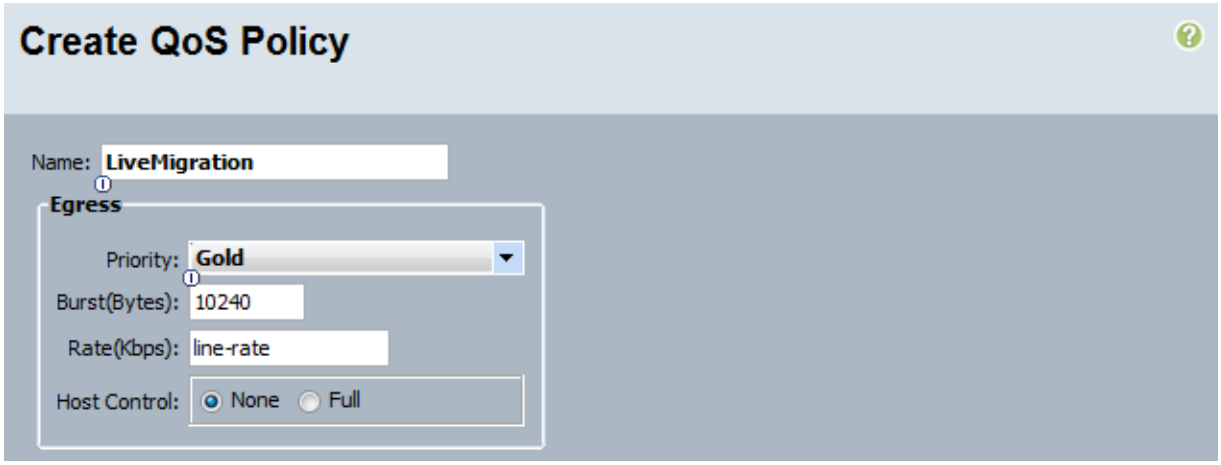
These steps provide details for setting Jumbo frames and enabling the quality of server in the Cisco UCS Fabric.

1. Select the `LAN` tab at the top left of the window.
2. Go to `LAN Cloud > QoS System Class`.
3. In the right pane, click the `General` tab
4. On the `Gold and Silver Priority, and Best Efforts row`, type `9000` in the `MTU` boxes.
5. Click `Save Changes` in the bottom right corner.

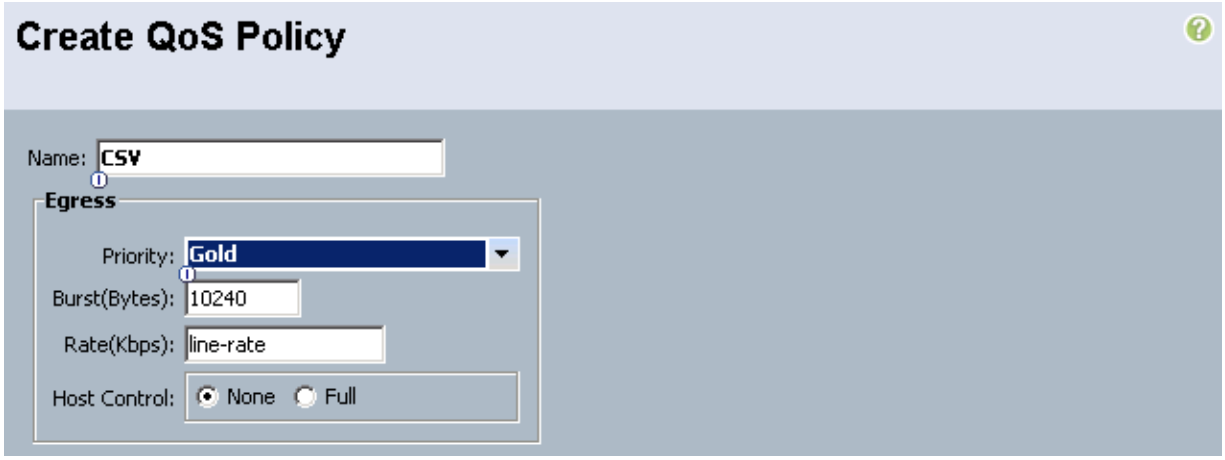
6. Click OK to continue.



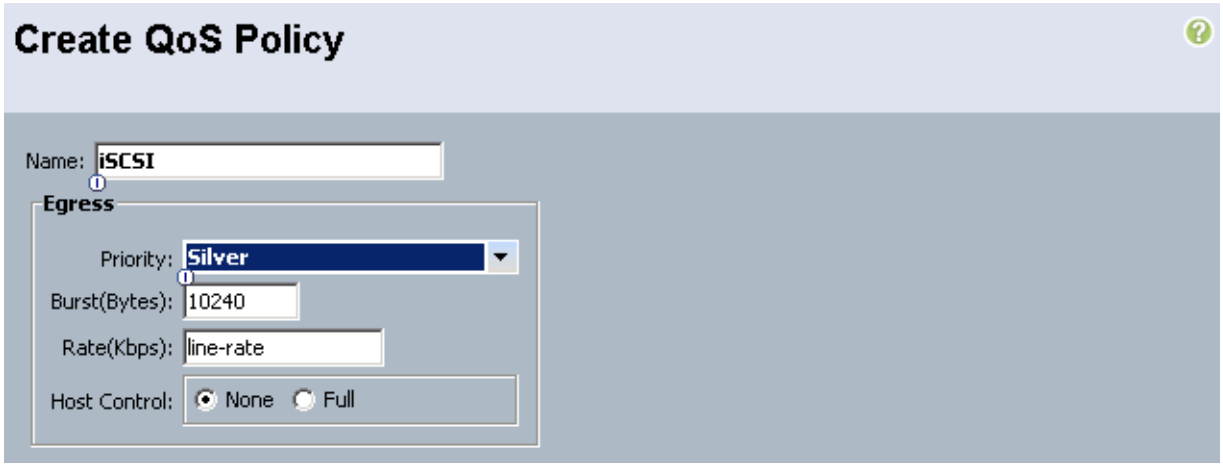
7. Select the LAN tab on the left of the window.
8. Go to LAN > Policies > Root >.
9. Right-click QoS Policies.
10. Select Create QoS Policy.
11. Enter LiveMigration as the QoS Policy name.
12. Change the Priority to Gold. Leave Burst(Bytes) set to 10240. Leave Rate(Kbps) set to line-rate. Leave Host Control set to None.
13. Click OK in the bottom right corner.



14. Right-click QoS Policies.
15. Select Create QoS Policy.
16. Enter CSV as the QoS Policy name.
17. Change the Priority to Gold. Leave Burst(Bytes) set to 10240. Leave Rate(Kbps) set to line-rate. Leave Host Control set to None.
18. Click OK in the bottom right corner.



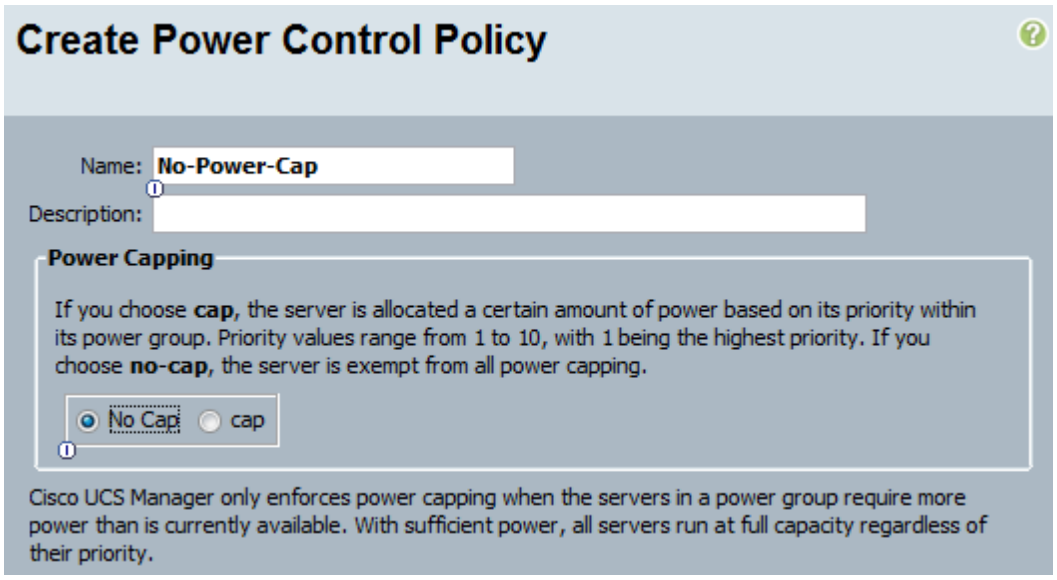
19. Right-click `QoS Policies`.
20. Select `Create QoS Policy`.
21. Enter `iSCSI` as the QoS Policy name.
22. Change the `Priority` to `Silver`. Leave `Burst(Bytes)` set to `10240`. Leave `Rate(Kbps)` set to `line-rate`. Leave `Host Control` set to `None`.
23. Click `OK` in the bottom right corner.



9.19 Create a Power Control Policy

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

1. Select the `Servers` tab at the top left of the window.
2. Go to `Policies > root`.
3. Right-click `Power Controller Policies`.
4. Select `Create Power Control Policy`.
5. Enter `No-Power-Cap` as the power control policy name.
6. Change the `Power Capping` to `No Cap`.
7. Click `OK` to complete creating the host firmware package.
8. Click `OK`.

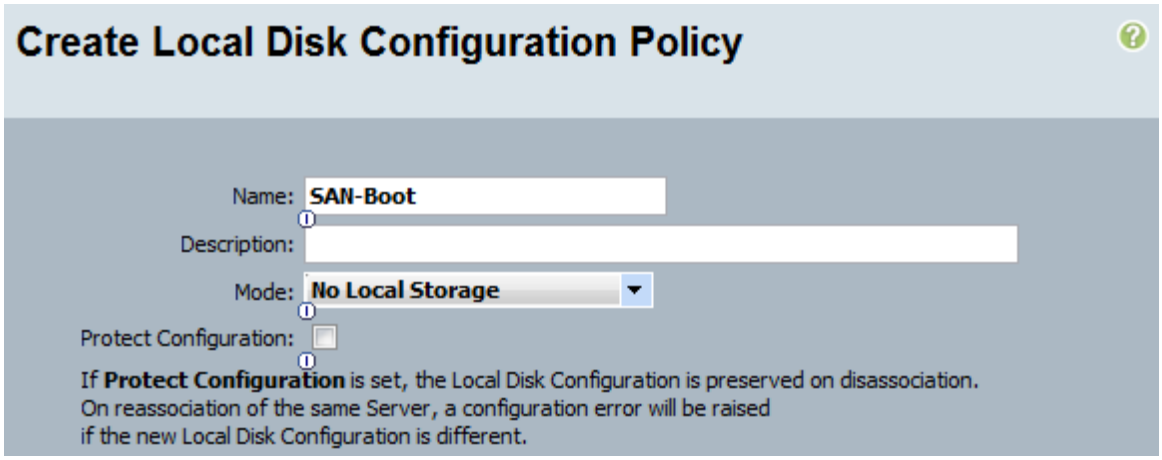


9.20 Create a Local Disk Configuration Policy

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 should not be used on blades that contain local disks.

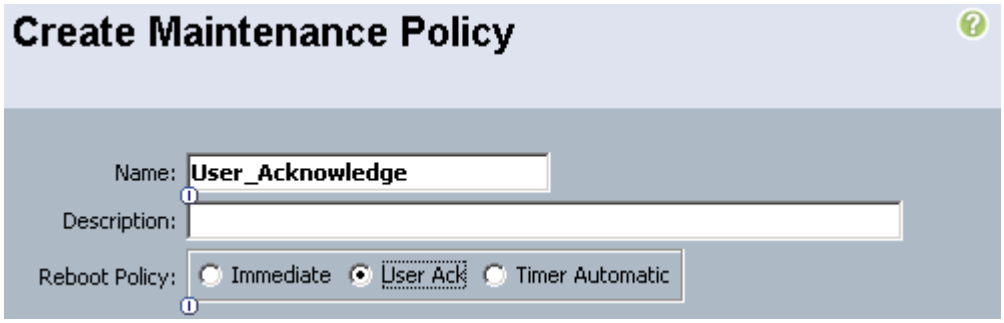
1. Select the `Servers` tab on the left of the window.
2. Go to `Policies > root`.
3. Right-click `Local Disk Config Policies`.
4. Select `Create Local Disk Configuration Policy`.
5. Enter `SAN Boot` as the local disk configuration policy name.
6. Change the `Mode` to `No Local Storage`. Uncheck the `Protect Configuration` box.
7. Click `OK` to complete creating the host firmware package.
8. Click `OK`.



9.21 Create a Maintenance Policy

These steps provide details for creating a maintenance policy. The maintenance policy controls the timing of a server reboot after an update has been made that requires the server to reboot prior to the update taking affect.

1. Select the Servers tab on the left of the window.
2. Go to Policies > root or sub-organization
3. Right click Maintenance Policy and select Create Maintenance Policy.
4. Name the policy User_Acknowledge
5. Select the User Ack option.
6. Click OK to create the policy.



9.22 Create a Server Pool Qualification Policy

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

1. Select the Servers tab on the left of the window
2. Go to Policies > root.
3. Right-click Server Pool Qualification Policies.
4. Select Create Server Pool Policy Qualification.
5. Select Server Model Qualifications.
6. Enter B200 M3 or C220 M3 as the Model(RegEx).
7. Click OK to complete creating the host firmware package.
8. Click OK.

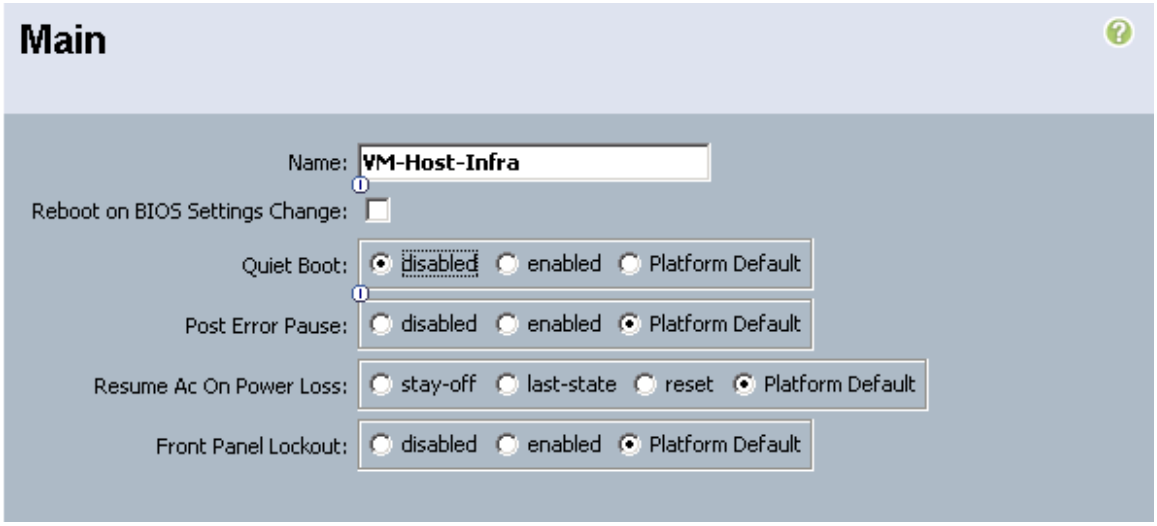
9.23 Create a Server BIOS Policy

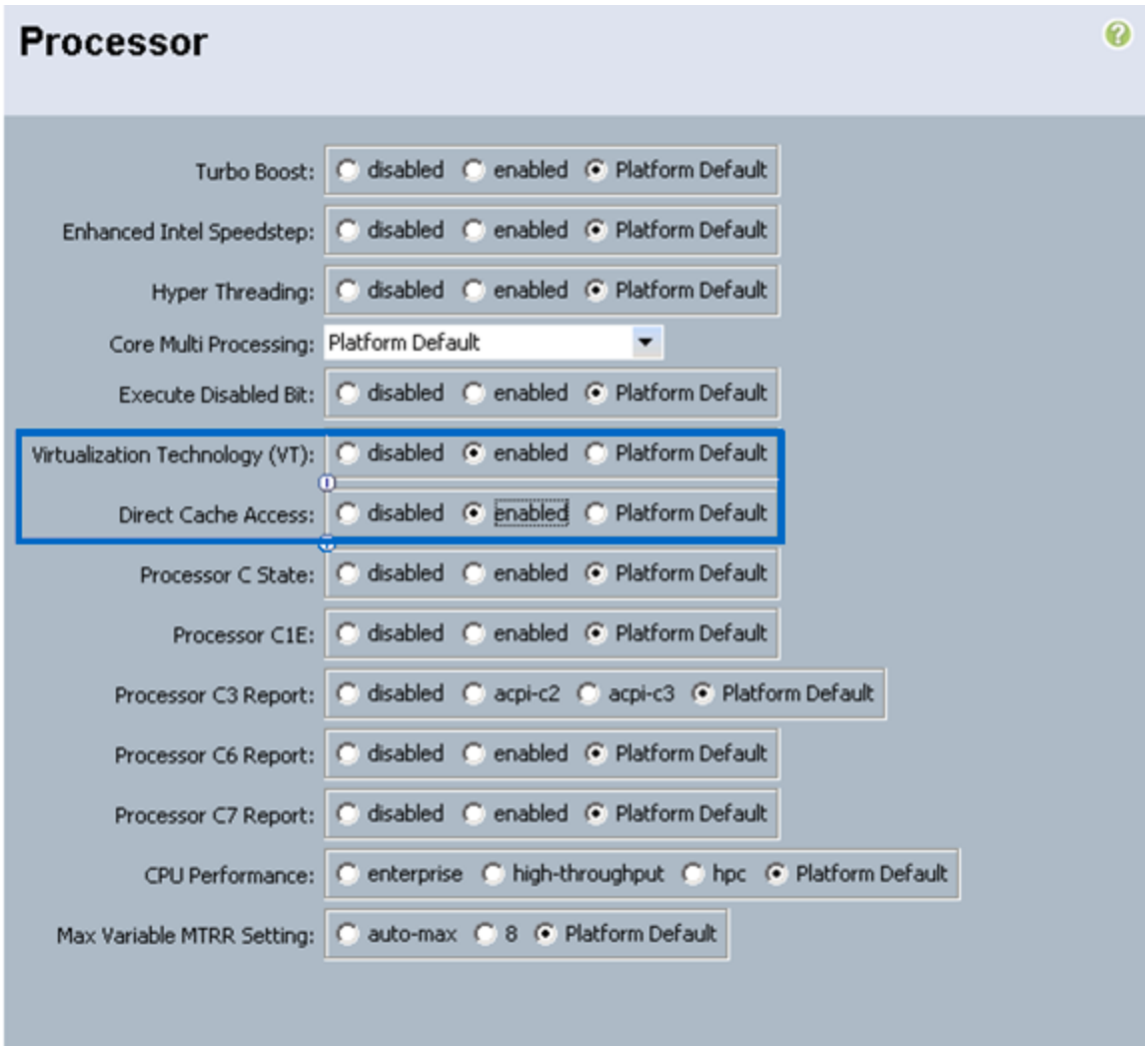
These steps provide details for creating a server BIOS policy for the Cisco UCS environment.

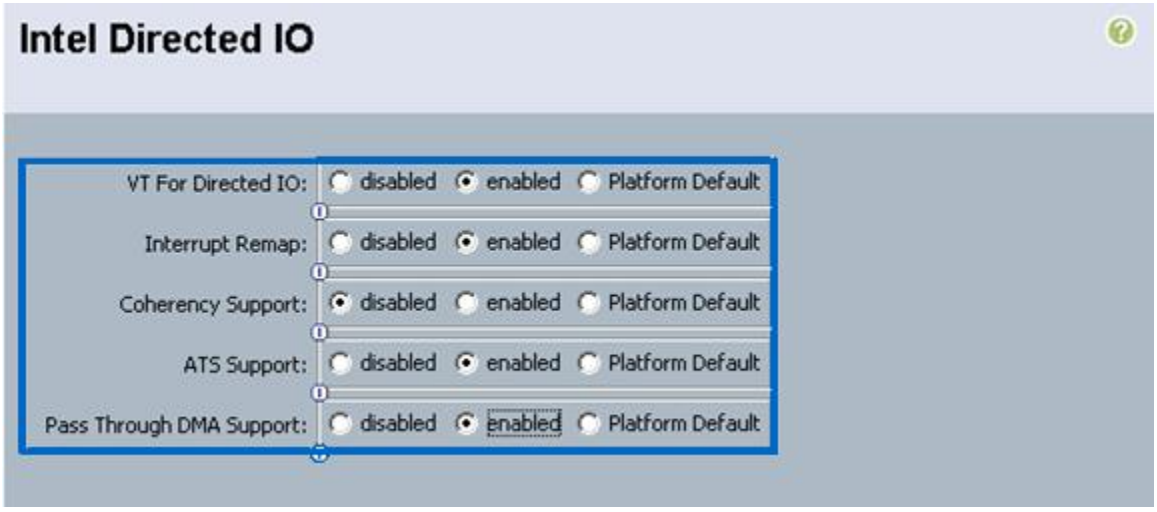
1. Select the Servers tab on the left of the window.

2. Go to `Policies > root`.
3. Right-click `BIOS Policies`.
4. Select `Create BIOS Policy`.
5. Enter `VMHost-Mgmt` as the BIOS policy name.
6. Make the following changes to support VM-FEX (SR-IOV):

Property	Setting
Quiet Boot	Disabled
Virtual Technology (VT)	Enabled
VT Fort Direct IO	Enabled
Interrupt Remap	Enabled
Coherency Support	Disabled
ATS Support	Enabled
Pass Through DMA Support	Enabled







7. Click `Finish` to complete creating the BIOS policy.
8. Click `OK`.

9.24 Create Dynamic vNIC Connection Policy for VM-FEX (SR-IOV)

These steps provide details for creating the vNIC Connection Policy for use with VM-FEX (SR-IOV).

Note: The maximum number of dynamic vNICs for C-Series servers is determined with a Cisco VIC 1225 is determined by the following formula.

Maximum Number of Dynamic vNICs = (((15 * n) – 3) – e) – f

n = the number of uplinks connecting the fabric extender to the Cisco UCS fabric interconnect.

e = the number of eNIC (static Ethernet NICs)

f = the number of fNIC (HBAs)

Note: The maximum number of dynamic vNICs for B-Series servers is determined with a Cisco VIC 1240 is determined by the following formula.

Maximum Number of Dynamic vNICs = (((63 * n) – 2) – e) – f

n = the number of uplinks connecting the fabric extender to the Cisco UCS fabric interconnect.

e = the number of eNIC (static Ethernet NICs)

f = the number of fNIC (HBAs)

1. Select the `LAN` tab on the left of the window.
2. Go to `Policies > root`.
3. Right-click Dynamic vNIC Connection Policy and select `create`.
4. Enter the name `VF-iSCSI-A`
5. Enter `20` for the Dynamic vNIC value.

Note: The number of Dynamic vNICs may need to be reduced depending on the adapter version and the number of uplinks between the IOM or FEX and the fabric interconnect. The service profile will fail to associate with the blade or rack server if there are too many Dynamic vNICs specified.

6. Select `Windows` adapter policy from the dropdown box.
7. Select `Protected Perf A` protection policy.
8. Click `OK` to create the dynamic vNIC policy for the iSCS-A virtual function.

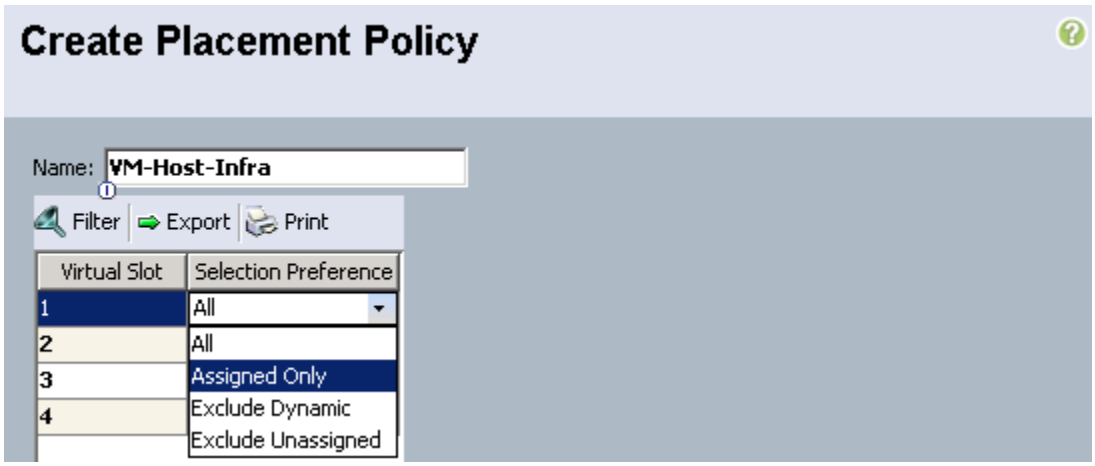
9. Right-click Dynamic vNIC Connection Policy and select `create`.
10. Enter the name `VF-iSCSI-B`
11. Enter `20` for the Dynamic vNIC value.

Note: The number of Dynamic vNICs may need to be reduced depending on the adapter version and the number of uplinks between the IOM or FEX and the fabric interconnect. The service profile will fail to associate with the blade or rack server if there are too many Dynamic vNICs specified.

12. Select `Windows` adapter policy from the dropdown box.
13. Select `Protected Perf B` protection policy.
14. Click `OK` to create the dynamic vNIC policy for the iSCS-A virtual function.

9.25 Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts

1. Right-click vNIC/HBA Placement policy and select `create`.
2. Enter the name `VMHost-Mgmt`.
3. Click `1` and select `Assign Only`.
4. Click `OK`.

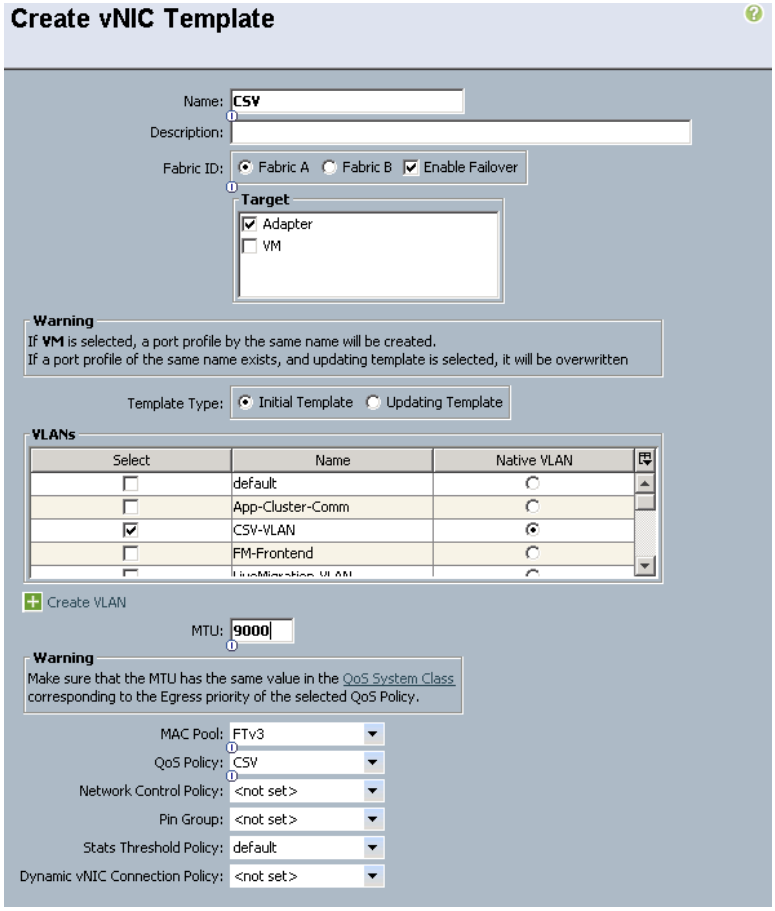


9.26 Create a vNIC Template

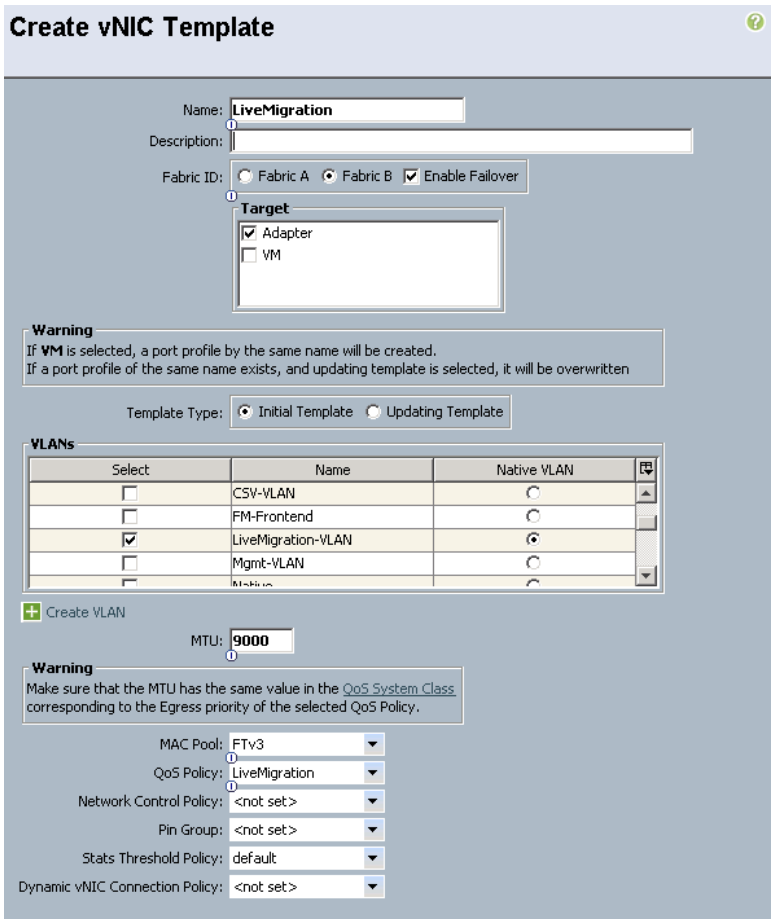
These steps provide details for creating multiple vNIC templates for the Cisco UCS environment.

1. Select the `LAN` tab on the left of the window.
2. Go to `Policies > root`.
3. Right-click `vNIC Templates`.
4. Select `Create vNIC Template`.
5. Enter `CSV` as the vNIC template name.

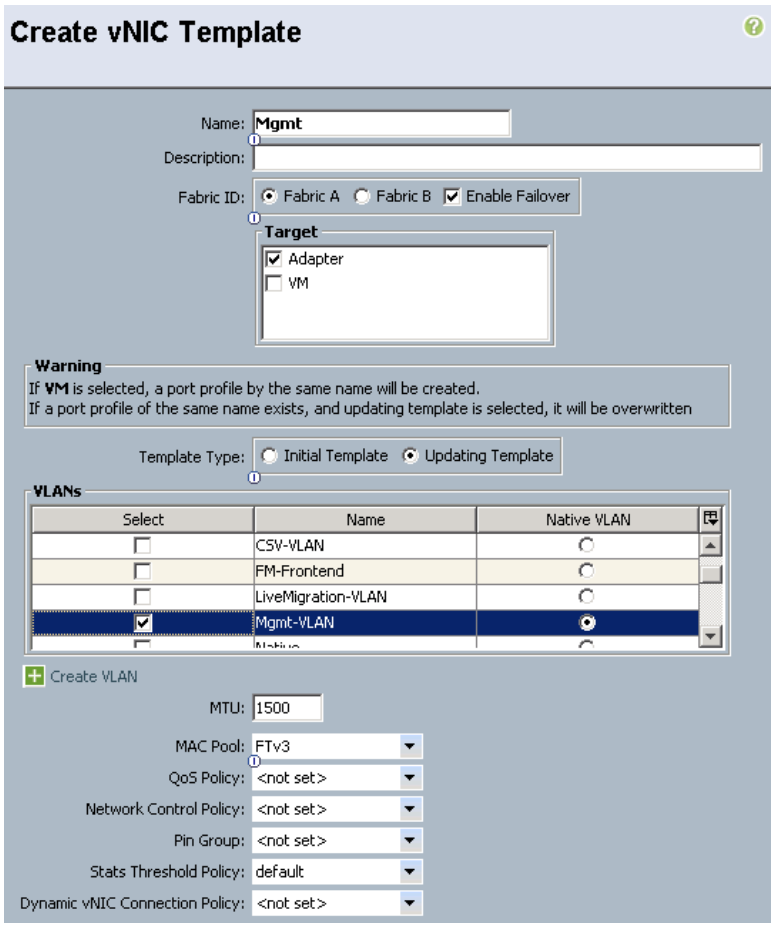
6. Leave Fabric A checked. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select CSV VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool:, select the MAC pool created earlier. Under QOS Policy: select CSV.
7. Click OK to complete creating the vNIC template.
8. Click OK.



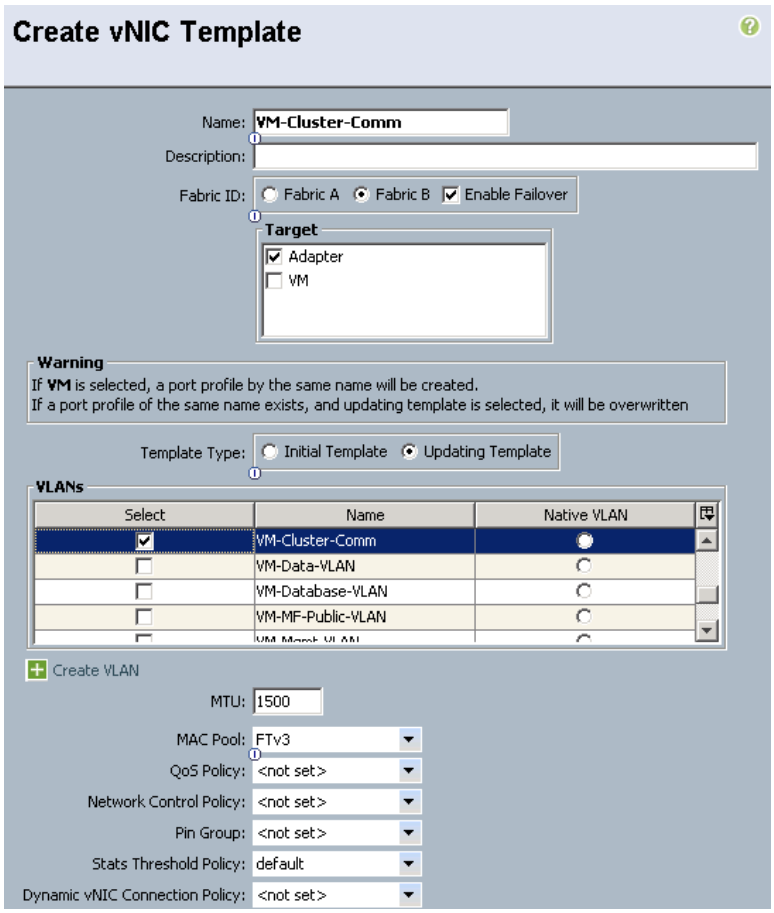
9. Select the LAN tab on the left of the window.
10. Go to Policies > root.
11. Right-click vNIC Templates.
12. Select Create vNIC Template.
13. Enter LiveMigration as the vNIC template name.
14. Check Fabric B. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select Live-Migration-VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool:, select the MAC pool created earlier. Under QoS Policy, select Live-Migration.
15. Click OK to complete creating the vNIC template.
16. Click OK.



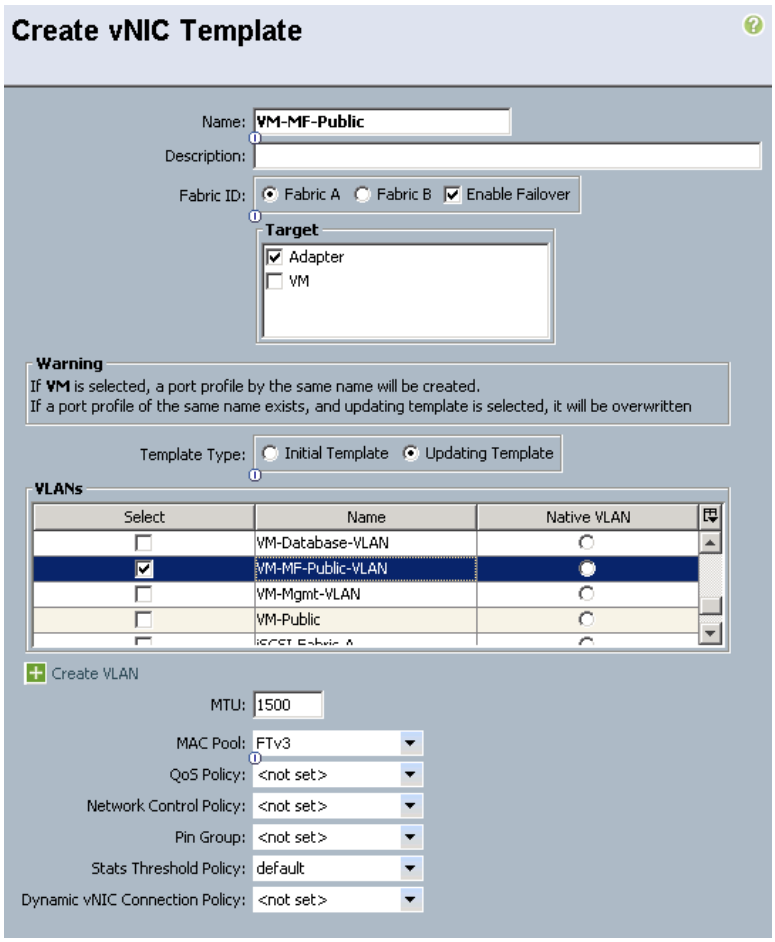
17. Select the LAN tab on the left of the window.
18. Go to Policies > root.
19. Right-click vNIC Templates.
20. Select Create vNIC Template.
21. Enter Mgmt as the vNIC template name.
22. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select MGMT-VLAN. Set as Native VLAN. Under MAC Pool: select the MAC pool created earlier.
23. Click OK to complete creating the vNIC template.
24. Click OK.



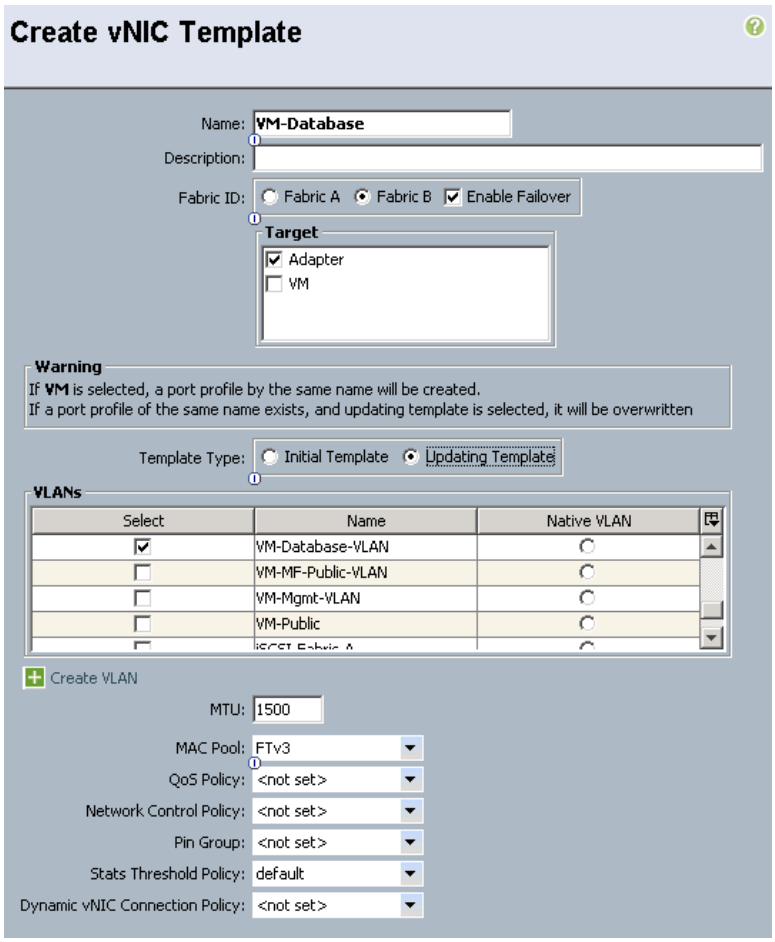
25. Select the `LAN` tab on the left of the window.
26. Go to `Policies > root.`
27. Right-click `vNIC Templates.`
28. Select `Create vNIC Template.`
29. Enter `VM-Cluster-Comm` as the vNIC template name.
30. Check `Fabric B.` Check the `Enable Failover` box. Under target, unselect the `VM` box. Select `Updating Template` as the `Template Type.` Under `VLANs,` select `VM-Cluster-Comm. Do not set a Native VLAN. Under MTU, enter 1500.` Under `MAC Pool,` select `the MAC pool created earlier.`
31. Click `OK` to complete creating the vNIC template.
32. Click `OK.`



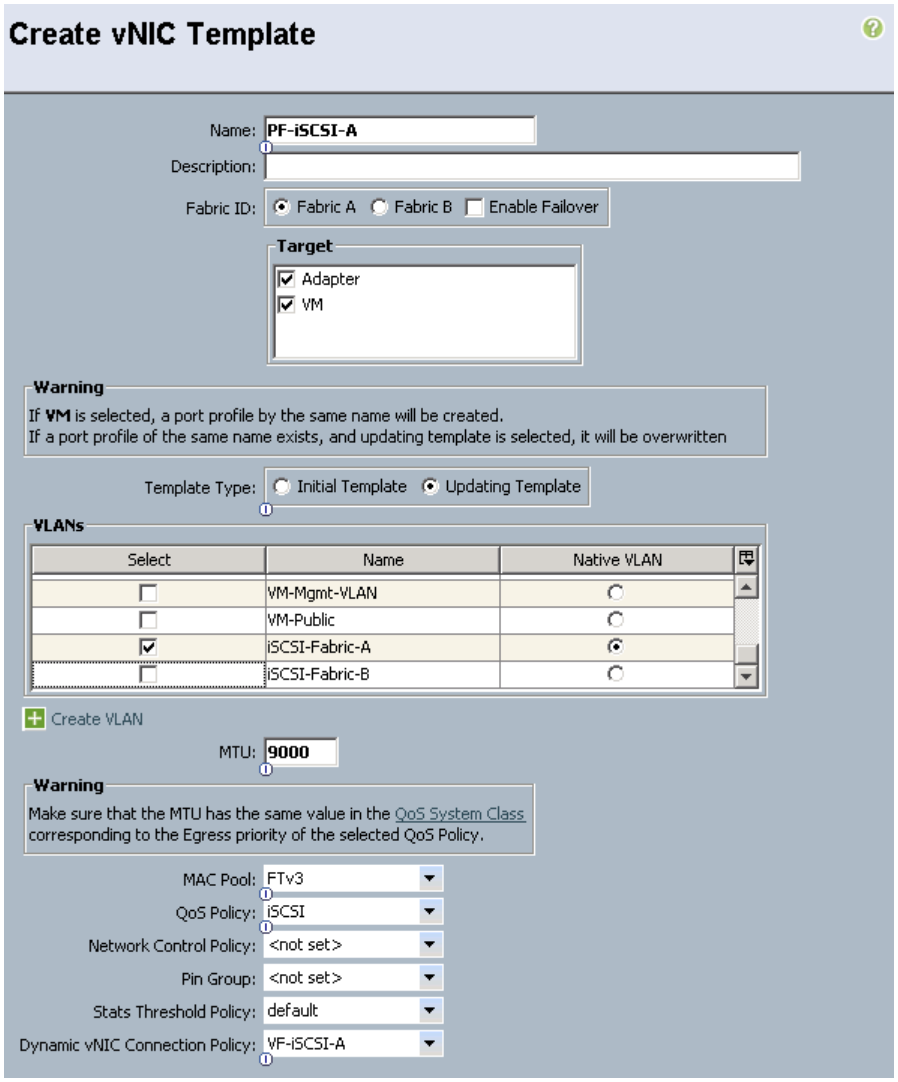
33. Select the LAN tab on the left of the window.
34. Go to Policies > root.
35. Right-click vNIC Templates.
36. Select Create vNIC Template.
37. Enter VM-MF-Public as the vNIC template name.
38. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select VM-MF-Public. Do not set a Native VLAN. Under MAC Pool, select the MAC pool created earlier.
39. Click OK to complete creating the vNIC template.
40. Click OK.



41. Select the LAN tab on the left of the window.
42. Go to Policies > root.
43. Right-click vNIC Templates.
44. Select Create vNIC Template.
45. Enter VM-Database as the vNIC template name.
46. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select VM-Database. Do not set a Native VLAN. Under MAC Pool, select the MAC pool created earlier.
47. Click OK to complete creating the vNIC template.
48. Click OK.

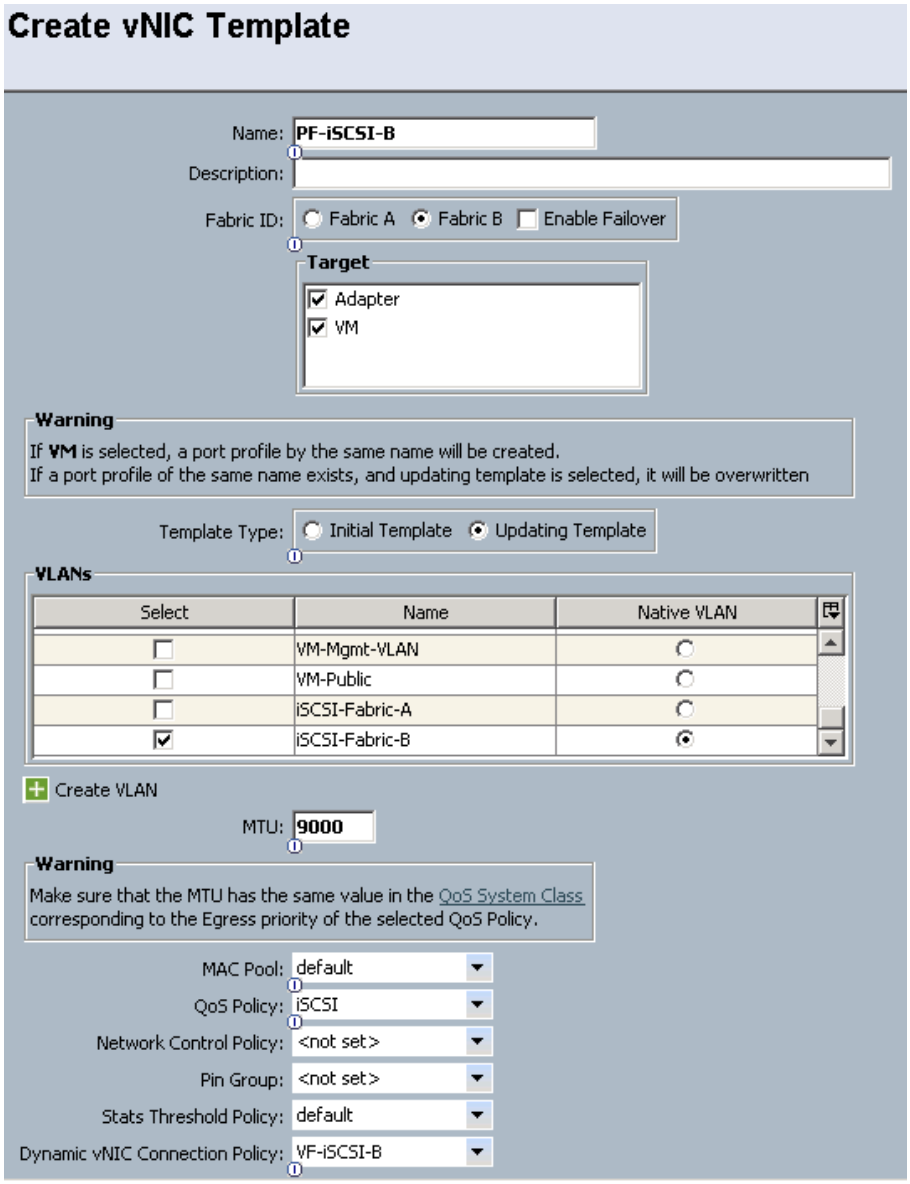


49. Select the LAN tab on the left of the window.
50. Go to Policies > root.
51. Right-click vNIC Templates.
52. Select Create vNIC Template.
53. Enter PF-iSCSI-A as the vNIC template name.
54. Check Fabric A. Uncheck the Enable Failover box. Under target, select Adapter and VM box. Select Updating Template as the Template Type. Under VLANs, select iSCSI-VLAN-A and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool, select the MAC pool created earlier. Under QoS Policy, select iSCSI. Under Dynamic vNIC Connection Policy, select VF-iSCSI-A.
55. Click OK to complete creating the vNIC template.
56. Click OK.



Note: A Port profile is automatically created when creating a vNIC template and checking the VM check box.

57. Select the LAN tab on the left of the window.
58. Go to Policies > root or sub-organiztion.
59. Right-click vNIC Templates.
60. Select Create vNIC Template.
61. Enter PF-iSCSI-B as the vNIC template name.
62. Check Fabric B. Uncheck the Enable Failover box. Under target, select Adapter and VM box. Select Updating Template as the Template Type. Under VLANs, select iSCSI-VLAN-B and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool, select the MAC pool created earlier. Under QoS Policy, select iSCSI. Under Dynamic vNIC Connection Policy, select VF-iSCSI-B. Click OK to complete creating the vNIC template.
63. Click OK.



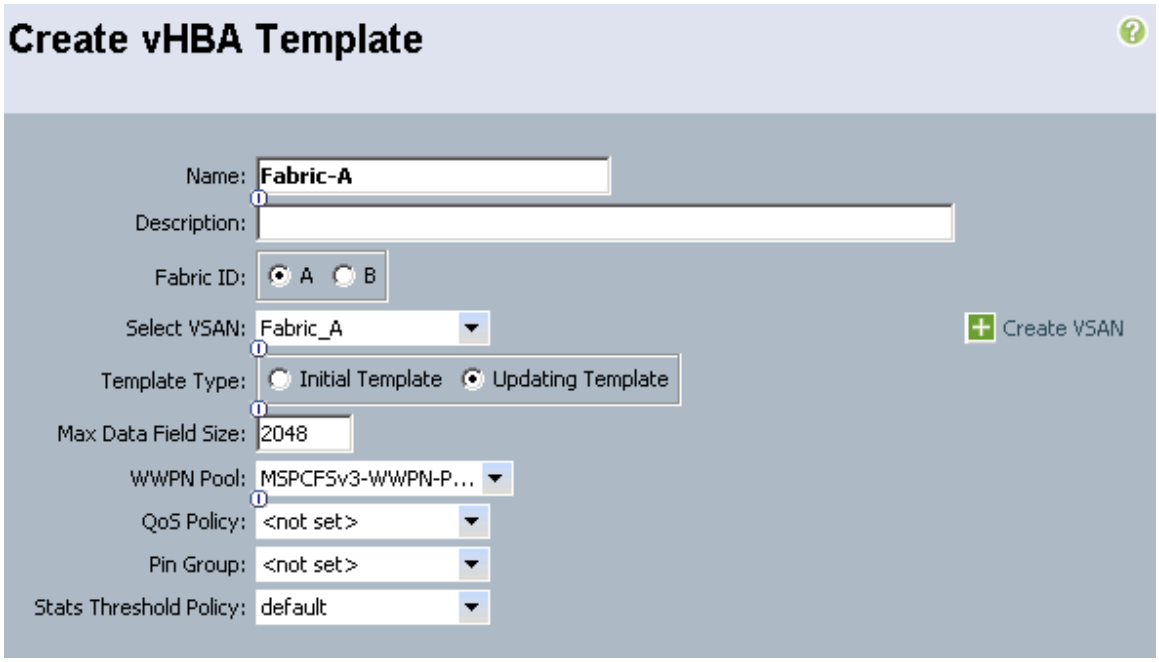
Note: A Port profile is automatically created when creating a vNIC template and checking the VM check box

9.27 Create vHBA Templates for Fabric A and B

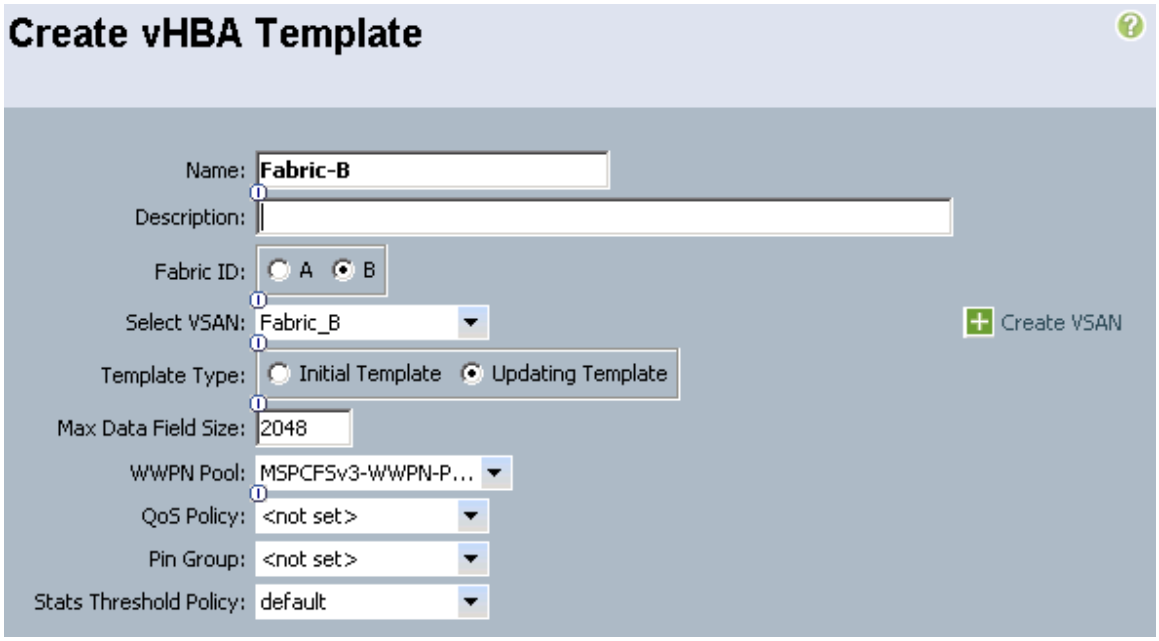
These steps provide details for creating multiple vHBA templates for the Cisco UCS environment.

1. Select the `VSAN` tab on the left of the window.
2. Go to `Policies > root.`
3. Right-click `vHBA Templates.`
4. Select `Create vNIC Template.`
5. Enter `Fabric-A` as the vHBA template name.
6. Select `Fabric A.` Under `Select VSAN`, select `VSAN_A.` Under `WWN Pool`, select the previously created `WWN pool.`
7. Click `OK` to complete creating the vHBA template.

8. Click OK.



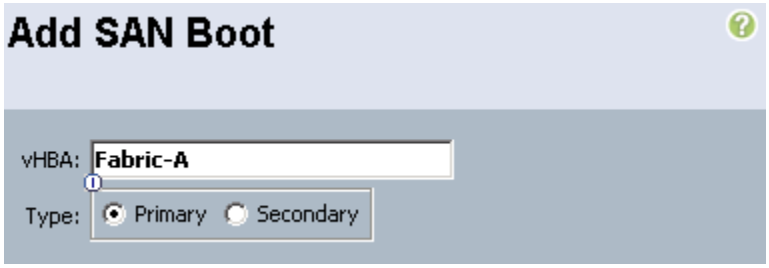
9. Select the VSAN tab on the left of the window.
10. Go to Policies > root.
11. Right-click vHBA Templates.
12. Select Create vHBA Template.
13. Enter Fabric-B as the vHBA template name.
14. Select Fabric B. Under Select VSAN, select VSAN_B. Under WWN Pool, select the previously created WWN pool.
15. Click OK to complete creating the vHBA template.
16. Click OK.



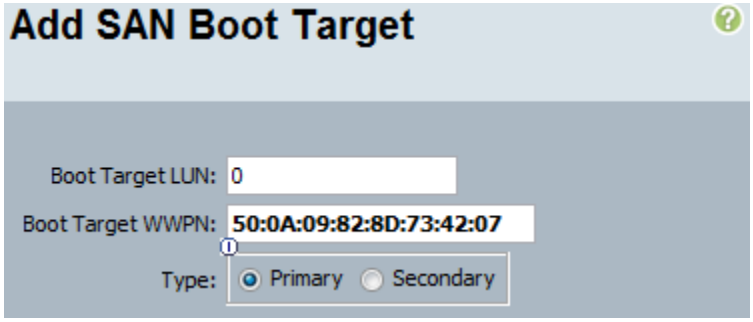
9.28 Create Boot Policies

These steps provide details for creating boot policies for the Cisco UCS environment. These directions apply to an environment in which each storage Controller B-a port is connected to fabric A and each storage Controller B-b port is connected to fabric B. In these steps, 2 boot policies will be configured. The first policy will configure the primary target to be controller A port 2-a and the second boot policy primary target will be controller B port 2b.

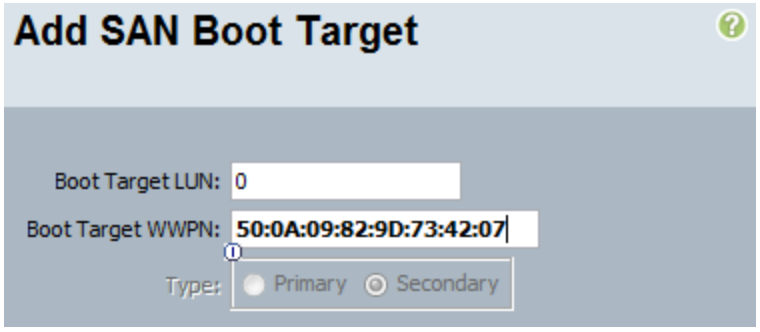
1. Select the `Servers` tab at the top left of the window.
2. Go to `Policies > root`.
3. Right-click `Boot Policies`.
4. Select `Create Boot Policy`.
5. Name the boot policy Boot-FAS01-A.
6. (Optional) Give the boot policy a description.
7. Leave `Reboot on Boot Order Change and Enforce vNIC/vHBA Name` 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-A` in the vHBA field in the Add SAN Boot window that displays.
11. Make sure 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 FCoE adapter interface `2a` of controller A. To obtain this information, log in to controller A and run the `fcp show adapters` command.
15. Be sure to use the FC portname for 2a and not the FC node name.
16. Keep the type as `Primary`.
17. Click `OK` to add the SAN boot target.



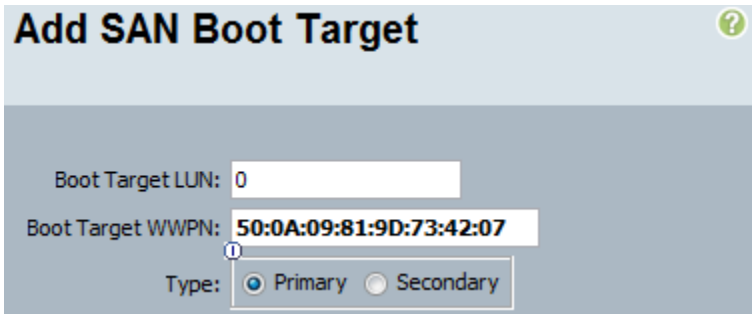
18. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as `0`.
19. Enter the WWPN for the primary FCoE adapter interface `2a` of controller B. To obtain this information, log in to the controller B and run the `fcp show adapters` command.
20. Be sure to use the FC portname for port 2a and not the FC node name.
21. Click `OK` to add the SAN boot target.



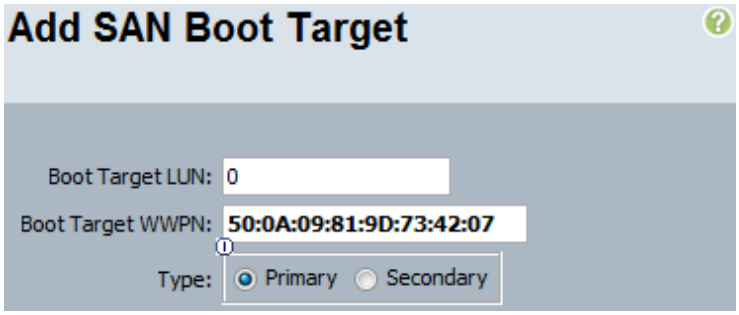
22. Select `Add SAN Boot` under the vHBA drop-down menu.
23. Enter `Fabric-B` in the vHBA field in the Add SAN Boot window that displays.
24. The type should automatically be set to `Secondary` and it should be grayed out. This is fine.
25. Click `OK` to add the SAN boot target.

26. Select `Add SAN Boot Target` under the vHBA drop-down menu.
27. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as `0`.

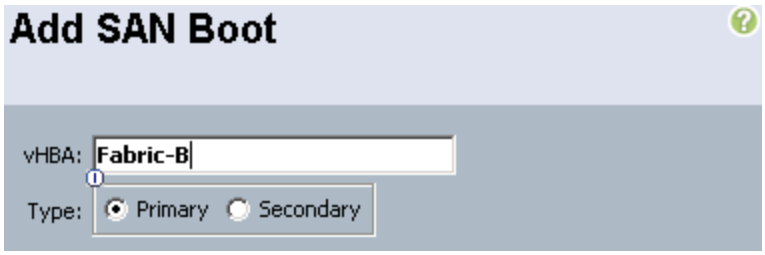
28. Enter the WWPN for the primary FCoE adapter interface 2b of the controller A. To obtain this information, log in to controller B and run the `fcp show adapters` command.
29. Be sure to use the FC portname for port 2b and not the FC node name.
30. Keep the type as Primary.
31. Click `OK` to add the SAN boot target.



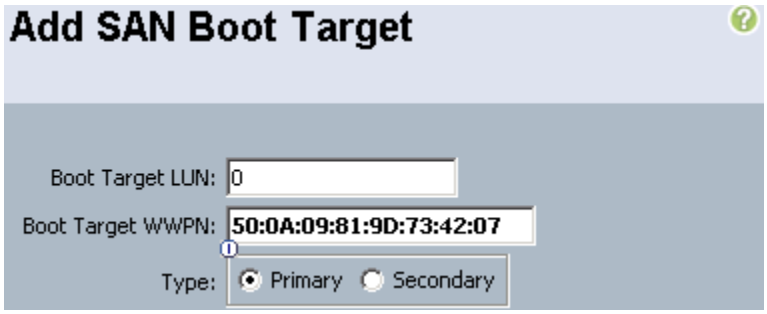
32. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as `0`.
33. Enter the WWPN for the primary FCoE adapter interface `2b` of controller B. To obtain this information, log in to controller A and run the `fcp show adapters` command.
34. Be sure to use the FC portname for port 2b and not the FC node name.
35. Click `OK` to add the SAN boot target.



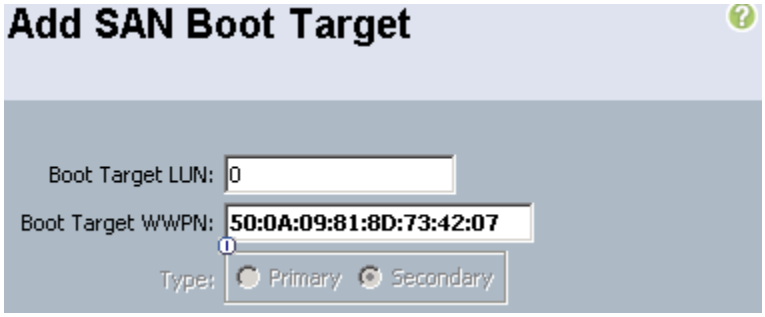
36. Right-click `Boot Policies again`.
37. Select Create Boot Policy.
38. Name the boot policy Boot-FAS01-B.
39. (Optional) Give the boot policy a description.
40. Leave `Reboot on Boot Order Change and Enforce vNIC/vHBA Name` unchecked.
41. Expand the Local Devices drop-down menu and select `Add CD-ROM`.
42. Click the vHBA drop-down menu and select `Add SAN Boot`.
43. Enter `Fabric-B` in the vHBA field in the Add SAN Boot window that displays.
44. Make sure that `Primary` is selected as the type.
45. Click `OK` to add the SAN boot target.



46. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as `0`.
47. Enter the WWPN for the primary FCoE adapter interface `2b` of controller B. To obtain this information, log in to controller B and run the `fcp show adapters` command.
48. Be sure to use the FC portname for port `2b` and not the FC node name.
49. Keep the type as `Primary`.
50. Click `OK` to add the SAN boot target.

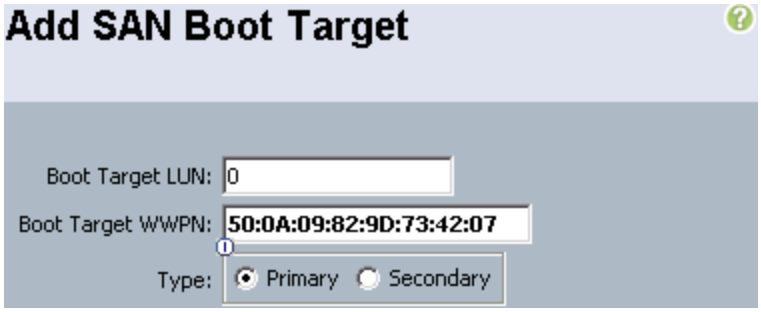


51. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
52. Enter the WWPN for the primary FCoE adapter interface `2b` of controller A. To obtain this information, log in to controller A and run the `fcp show adapters` command.
53. Be sure to use the FC portname for port `2b` and not the FC node name.
54. Click `OK` to add the SAN boot target.

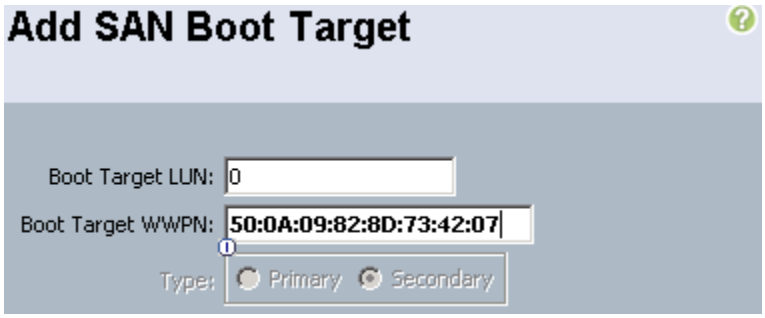


55. Select `Add SAN Boot` under the vHBA drop-down menu.
56. Enter `Fabric-A` in the vHBA field in the Add SAN Boot window that displays.
57. The type should automatically be set to `Secondary` and it should be grayed out. This is fine.
58. Click `OK` to add the SAN boot target.

59. Select `Add SAN Boot Target` under the vHBA drop-down menu.
60. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as `0`.
61. Enter the WWPN for the primary FCoE adapter interface `2a` of controller B. To obtain this information, log in to controller A and run the `fcp show adapters` command.
62. Be sure to use the FC portname for port 2a and not the FC node name.
63. Keep the type as `Primary`.
64. Click `OK` to add the SAN boot target.



65. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as `0`.
66. Enter the WWPN for the primary FCoE adapter interface `2a` of controller A. To obtain this information, log in to controller B and run the `fcp show adapters` command.
67. Be sure to use the FC portname for port 2a and not the FC node name.
68. Click `OK` to add the SAN boot target.



69. Click `OK` to create the boot policy in the Create Boot Policy pop-up window.

9.29 Create Service Profile Templates

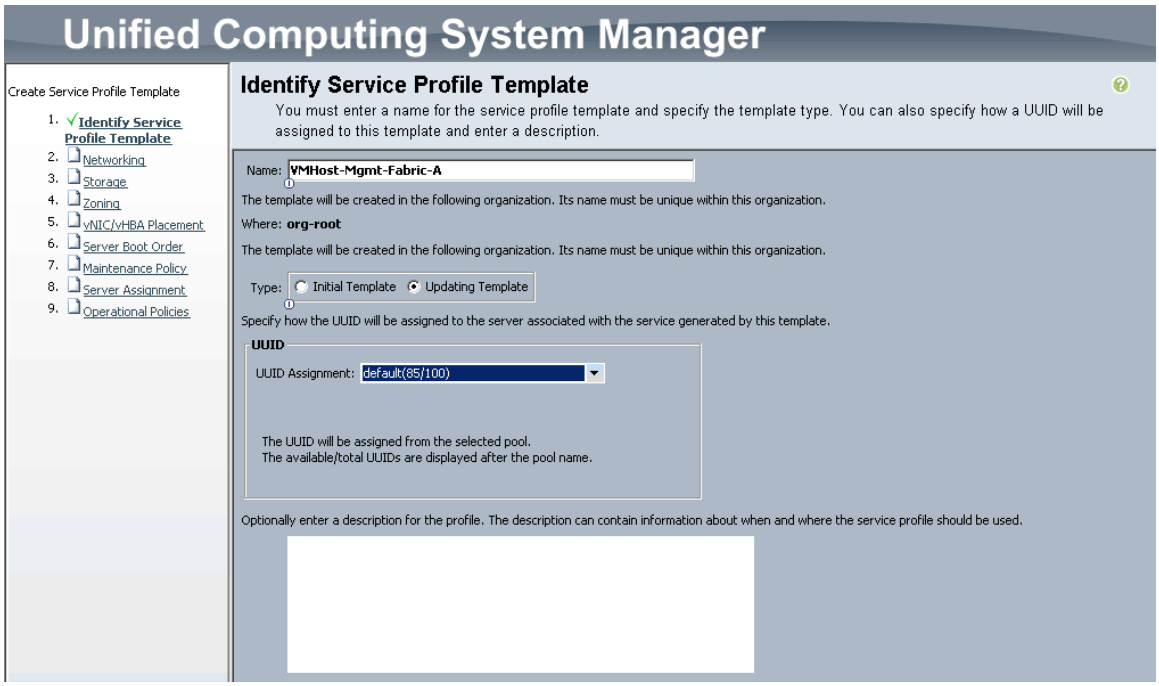
This section details the creation of two service profile templates: one for fabric A and one for fabric B. The first profile is created and then cloned and modified for the second host.

1. Select the `Servers` tab at the top left of the window.
2. Go to `Service Profile Templates > root or sub-organization.`

3. Right-click `root or sub-organization`.
4. Select `Create Service Profile Template`.
5. The Create Service Profile Template window displays.

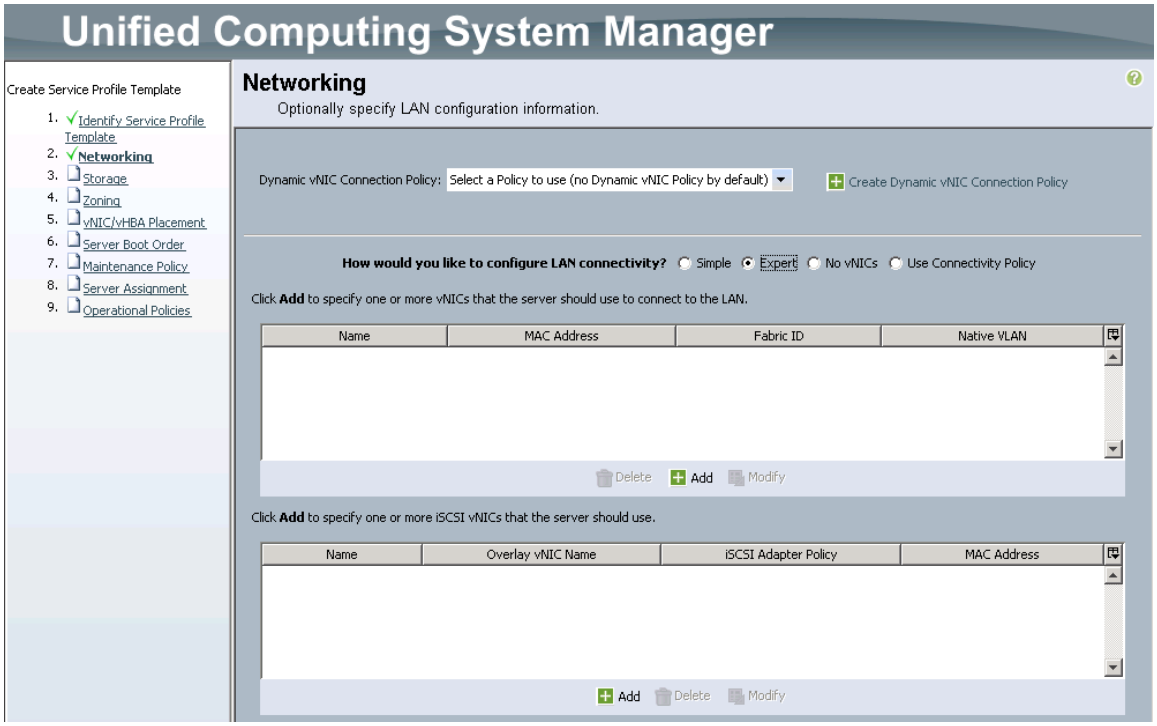
Identify the Service Profile Template

1. These steps detail configuration info for the `Identify the Service Profile Template` Section.
2. Name the service profile template `VMHost-Mgmt-Fabric-A`. This service profile template is configured to boot from controller a on fabric A.
3. Select `Updating Template`.
4. In the `UUID section`, select `UUID_Pool` as the UUID pool.
5. Click `Next` to continue to the next section.



Networking Section

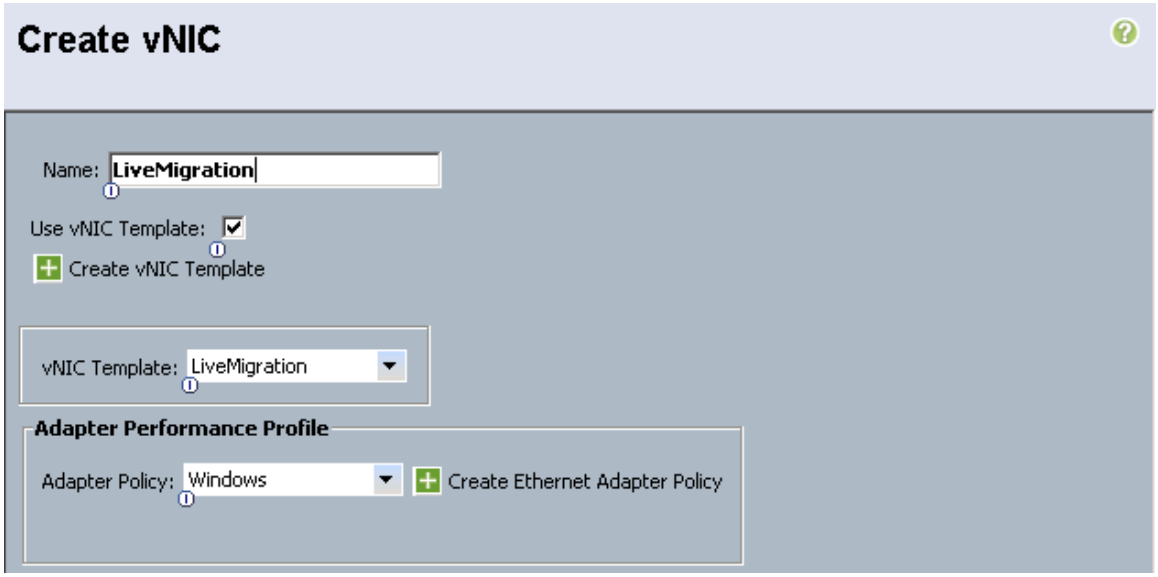
1. Leave the `Dynamic vNIC Connection Policy` field at the default.
2. Select `Expert` for the `How would you like to configure LAN connectivity?` option.



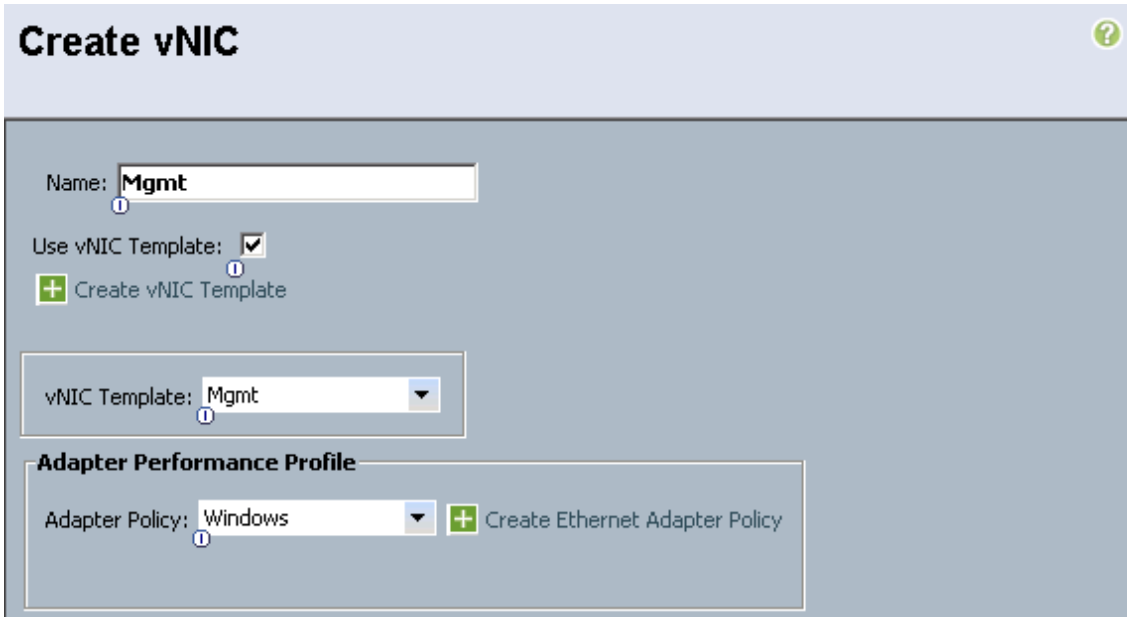
3. Click `Add` to add a vNIC to the template.
4. The `Create vNIC window` displays. Name the vNIC `CSV`.
5. Check the `Use vNIC Template` checkbox.
6. Select `CSV` for the vNIC Template field.
7. Select `Windows` in the Adapter Policy field.
8. Click `OK` to add the vNIC to the template.

9. Click `Add` to add a vNIC to the template.
10. The `Create vNIC window` displays. Name the vNIC `LiveMigration`.

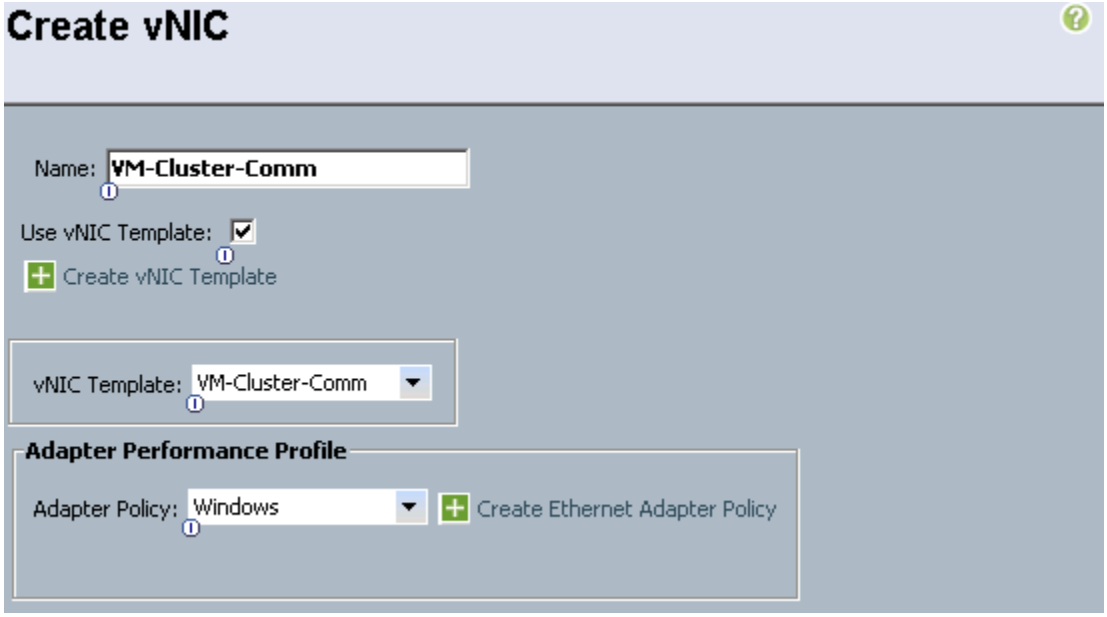
11. Check the `Use LAN Connectivity Template` checkbox.
12. Select `LiveMigration` for the vNIC Template field.
13. Select `Windows` in the Adapter Policy field.
14. Click `OK` to add the vNIC to the template.



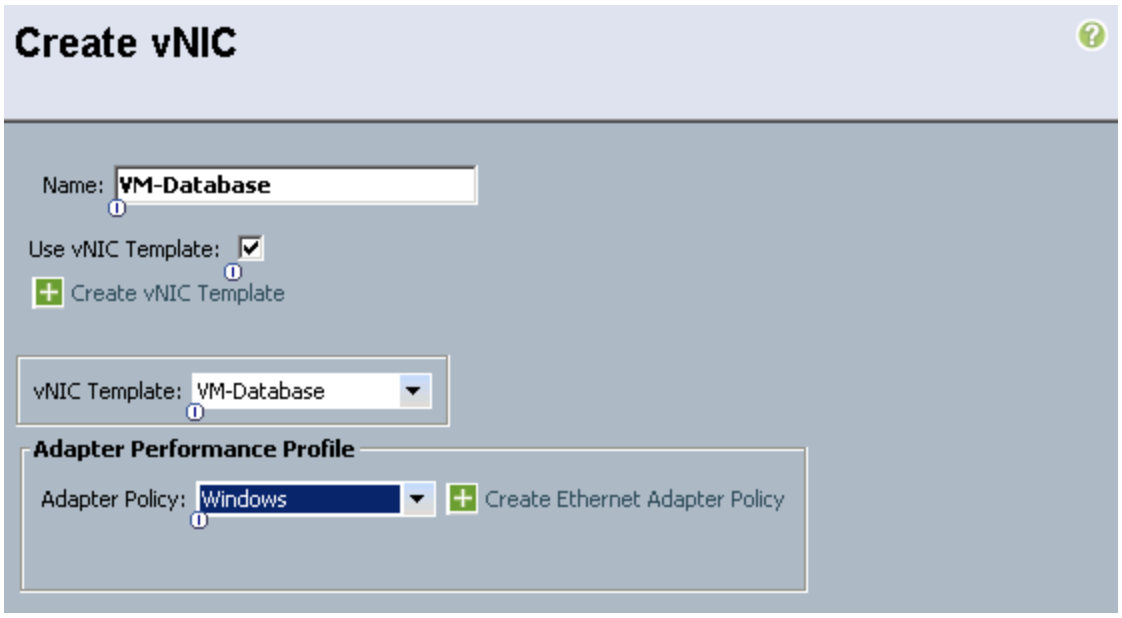
15. Click `Add` to add a vNIC to the template.
16. The `Create vNIC window` displays. Name the vNIC `Mgmt`.
17. Check the `Use LAN Connectivity Template` checkbox.
18. Select `Mgmt` for the vNIC Template field.
19. Select `Windows` in the Adapter Policy field.
20. Click `OK` to add the vNIC to the template.



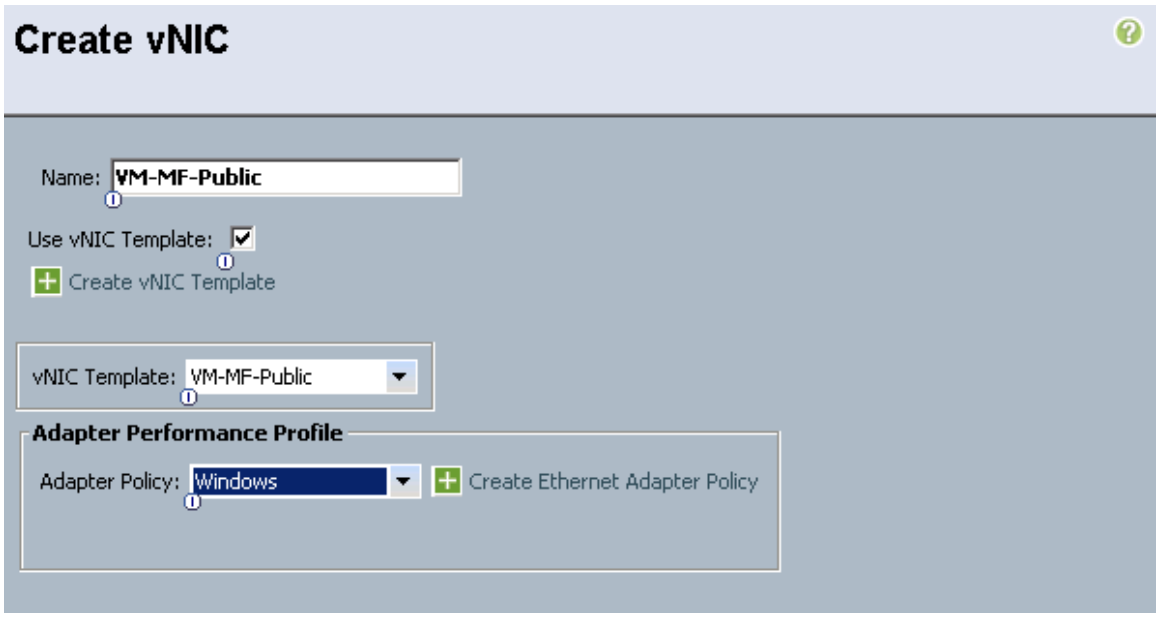
21. Click `Add` to add a vNIC to the template.
22. The `Create vNIC window` displays. Name the vNIC `VM-Cluster-Comm`.
23. Check the `Use LAN Connectivity Template` checkbox.
24. Select `VM-Cluster-Comm` for the vNIC Template field.
25. Select `Windows` in the Adapter Policy field.
26. Click `OK` to add the vNIC to the template.



27. Click `Add` to add a vNIC to the template.
28. The `Create vNIC window` displays. Name the vNIC `VM-Database`.
29. Check the `Use LAN Connectivity Template` checkbox.
30. Select `VM-Database` for the vNIC Template field.
31. Select `Windows` in the Adapter Policy field.
32. Click `OK` to add the vNIC to the template.

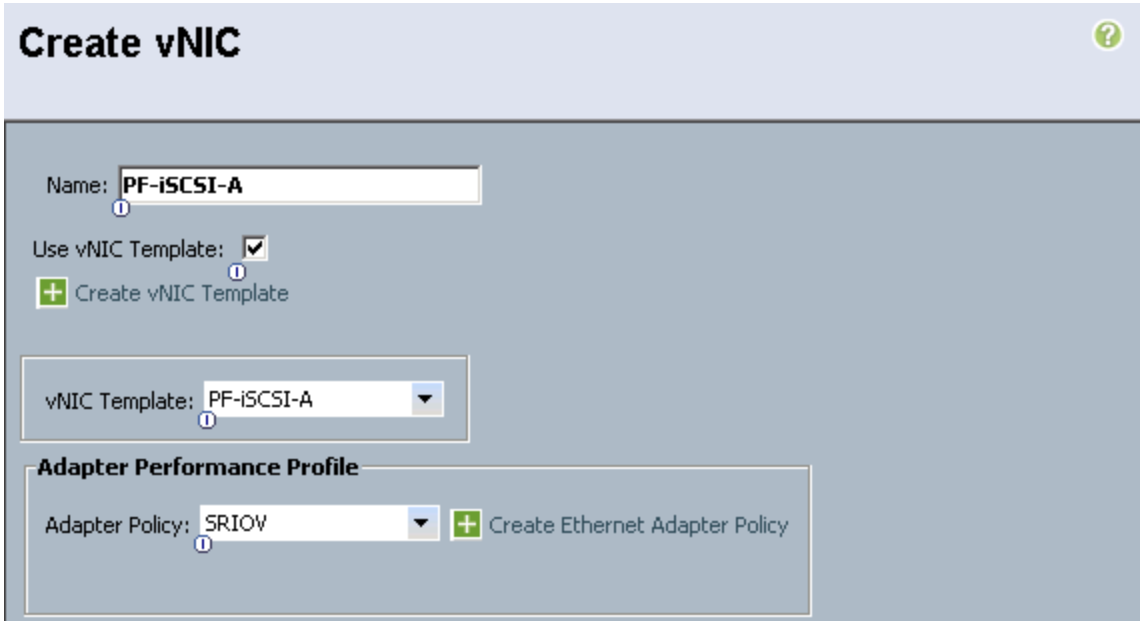


33. Click `Add` to add a vNIC to the template.
34. The `Create vNIC window` displays. Name the vNIC `VM-MF-Public`.
35. Check the `Use LAN Connectivity Template` checkbox.
36. Select `VM-MF-Public` for the vNIC Template field.
37. Select `Windows` in the Adapter Policy field.
38. Click `OK` to add the vNIC to the template.

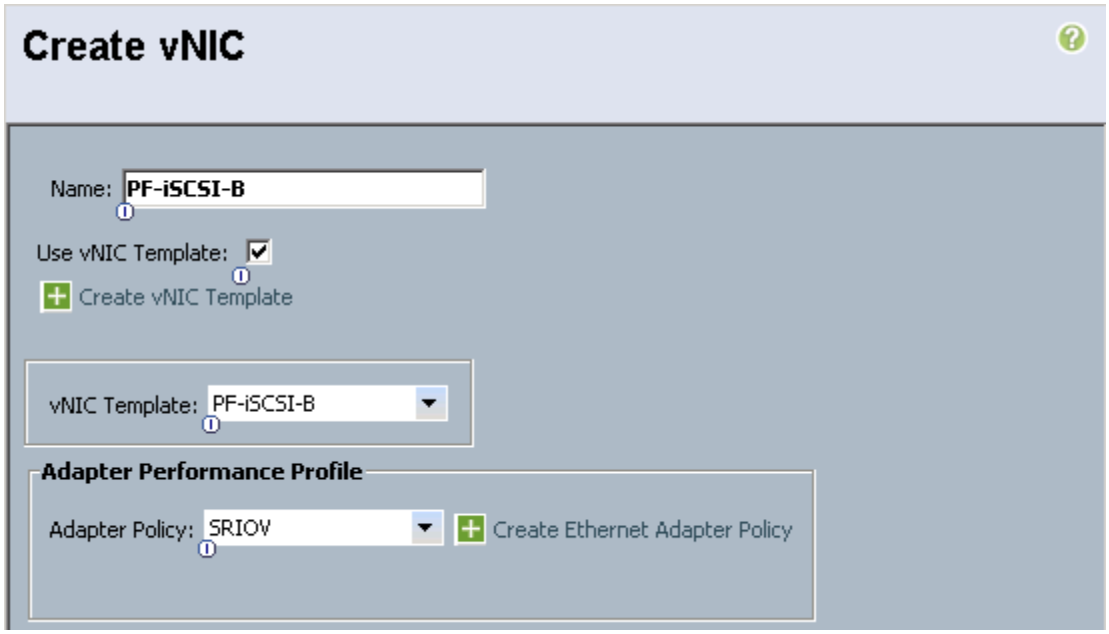


39. Click `Add` to add a vNIC to the template.
40. The `Create vNIC window` displays. Name the vNIC PF-`iSCSI-A`.
41. Check the `Use LAN Connectivity Template` checkbox.

42. Select PF-iSCSI-A for the vNIC Template field.
43. Select SRIOV in the Adapter Policy field.
44. Click OK to add the vNIC to the template.



45. Click Add to add a vNIC to the template.
46. Check the Use LAN Connectivity Template checkbox.
47. Select PF-iSCSI-B for the vNIC Template field.
48. Select SRIOV in the Adapter Policy field.
49. Click OK to add the vNIC to the template.

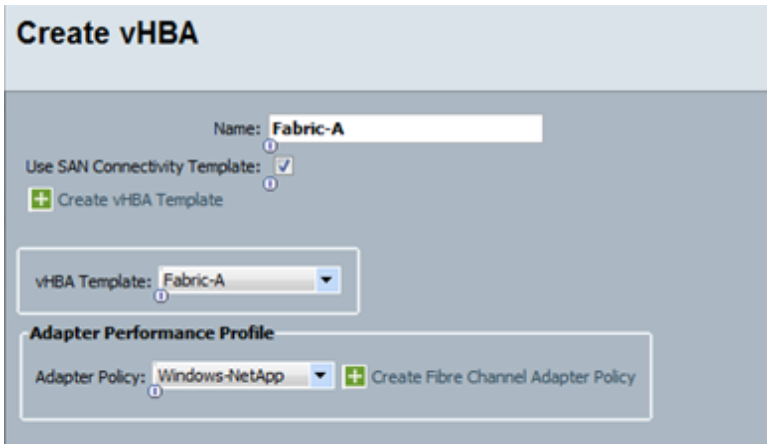


50. Verify: Review the table to make sure that all of the vNICs were created.

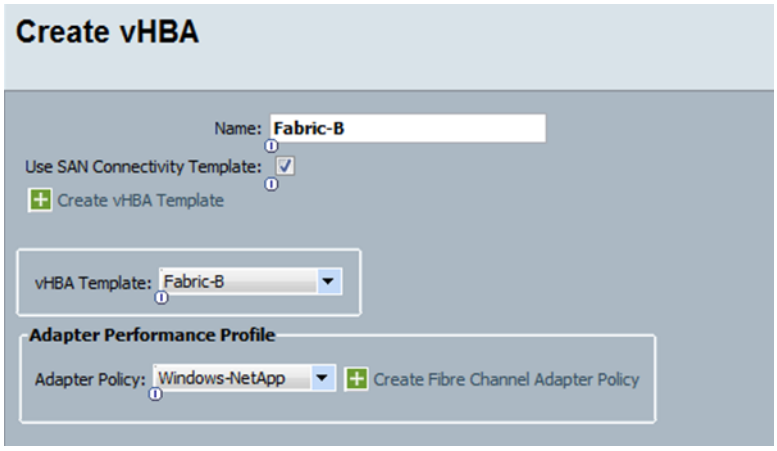
51. Click Next to continue to the next section.

Storage Section

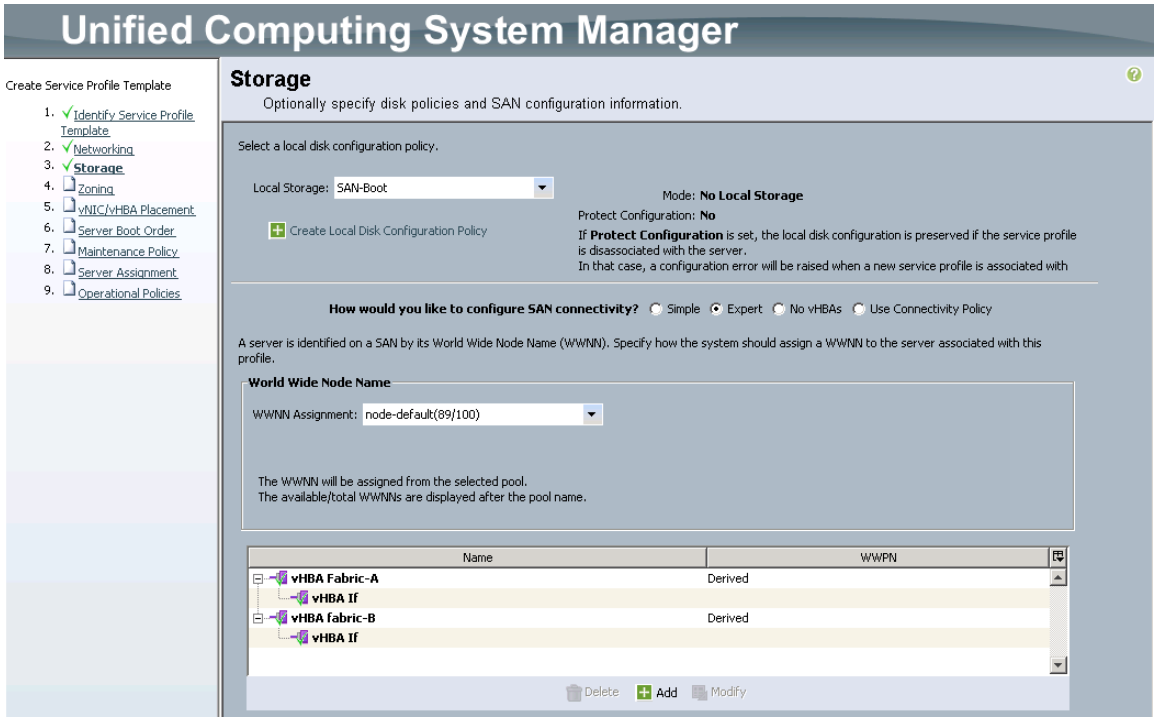
1. Select Default for the Local Storage field.
2. Select the appropriate local storage policy if the server in question does not have local disk.
3. Select SAN-Boot for the local disk configuration policy.
4. Select the Expert option for the How would you like to configure SAN connectivity field.
5. In the WWNN Assignment field, select WWNN_Pool.
6. Click the Add button at the bottom of the window to add vHBAs to the template.
7. The Create vHBA window displays. Name the vHBA Fabric-A.
8. Check the box for Use SAN Connectivity Template.
9. Select Fabric-A in the vHBA Template field.
10. Select Windows-NetApp in the Adapter Policy field.
11. Click OK to add the vHBA to the template.



12. Click the Add button at the bottom of the window to add vHBAs to the template.
13. The Create vHBA window displays. Name the vHBA Fabric-B.
14. Check the box for Use SAN Connectivity Template.
15. Select Fabric-B in the vHBA Template field.
16. Select Windows-NetApp in the Adapter Policy field.
17. Click OK to add the vHBA to the template.



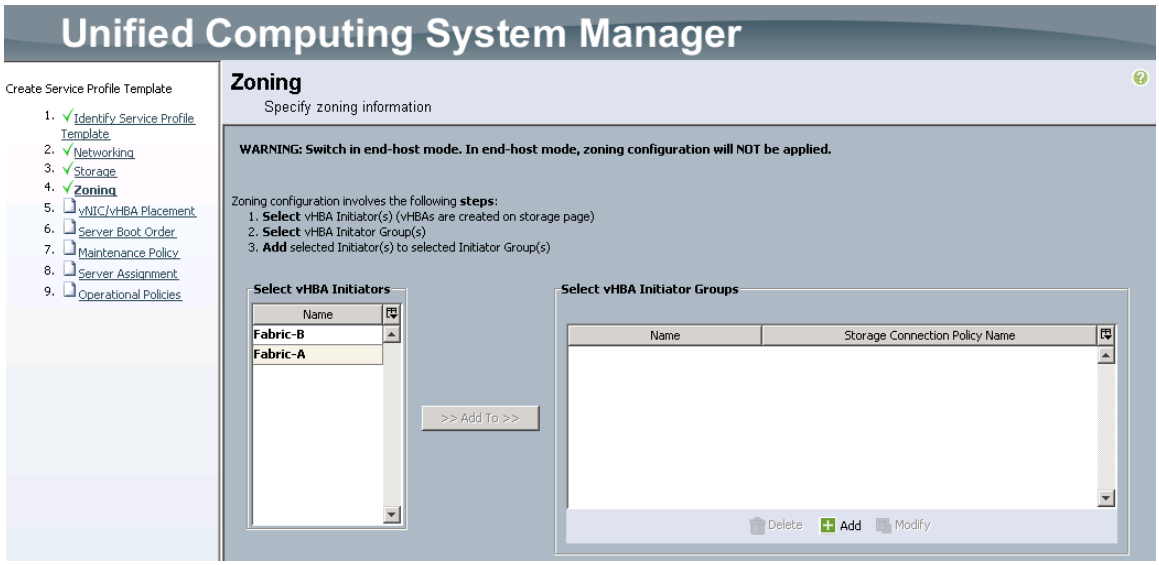
18. Verify – Review the table to make sure that both of the vHBAs were created.



19. Click `Next` to continue to the next section.

Zoning Section

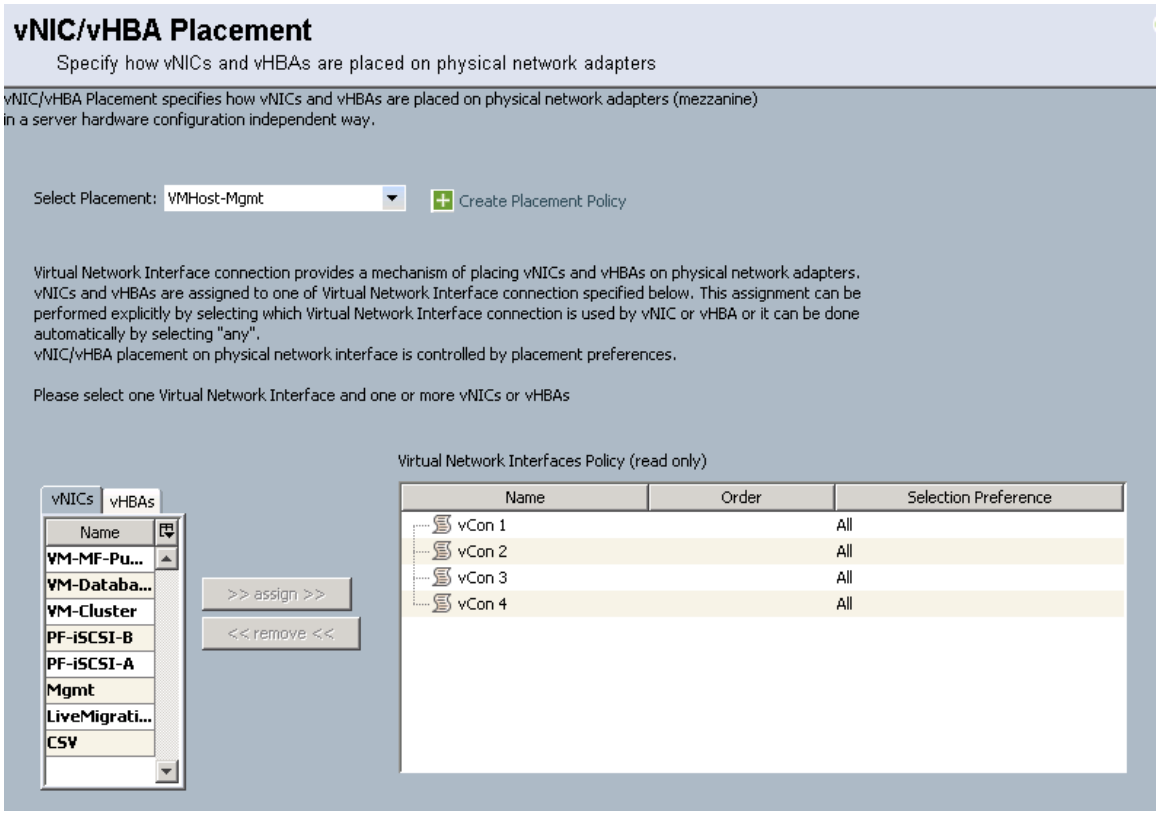
Note: Zoning configuration in this section is not required because the Fabric Interconnects are in End-Host mode and zoning is configured on the Cisco Nexus 5548 switches.



20. Click Next to continue the next section.

vNIC/vHBA Placement Section

1. Select the `VMHost-Mgmt` Placement Policy in the `Select Placement` field.



2. Select vCon1 assign the vNICs in the following order:

- Mgmt
- LiveMigration
- CSV

- VM-Database
- VM-MF-Public
- VM-Cluster-Comm
- PF-iSCSI-A
- PF-iSCSI-B

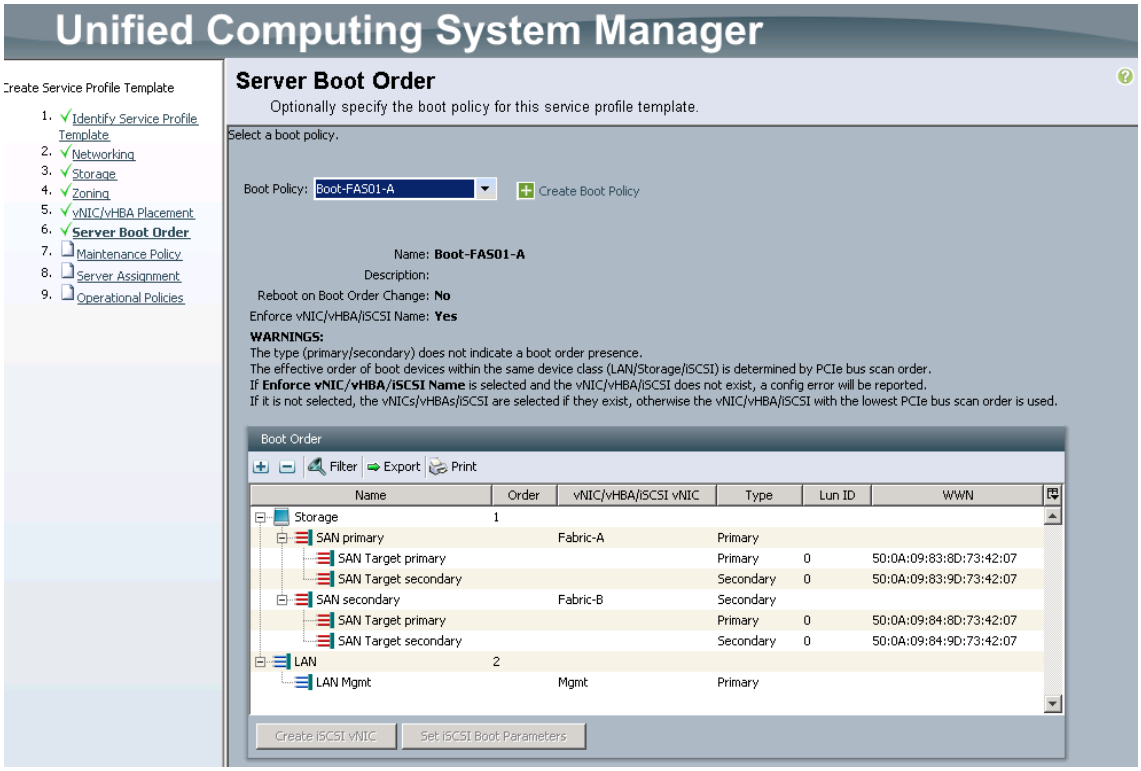
3. Click the vHBA tab and add the vHBAs in the following order:

- Fabric-A
- Fabric-B

4. Verify: Review the table to make sure that all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not important.
5. Click `Next` to continue to the next section.

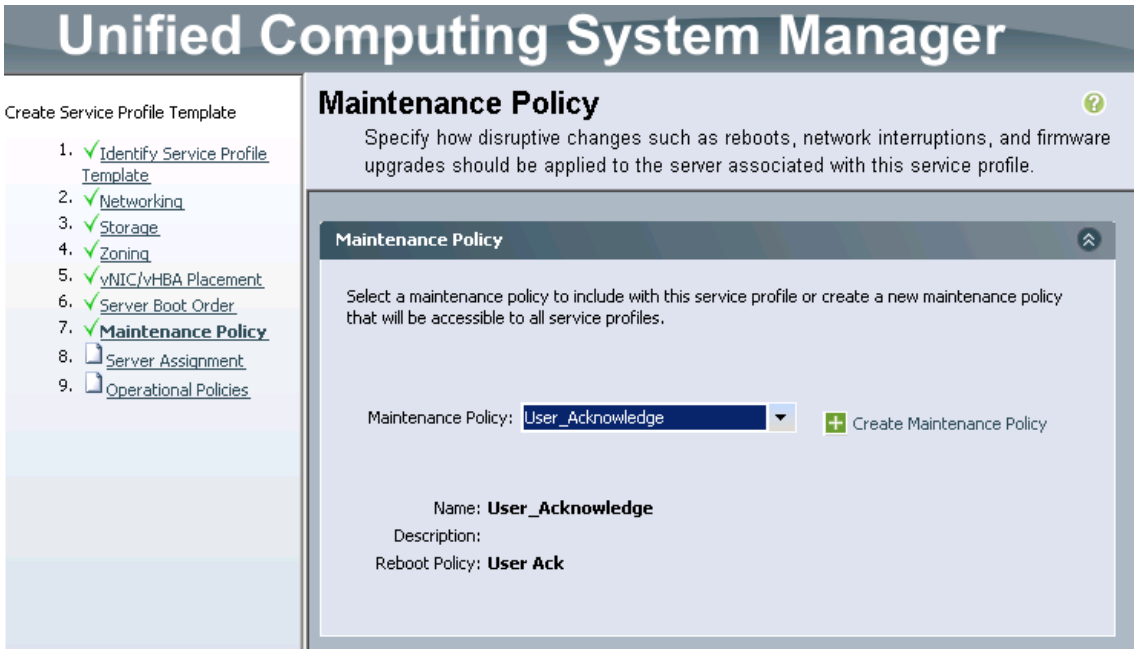
Server Boot Order Section

1. Select `Boot-FAS01-A` in the Boot Policy field.
2. Verify: Review the table to make sure that all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
3. Click `Next` to continue to the next section.



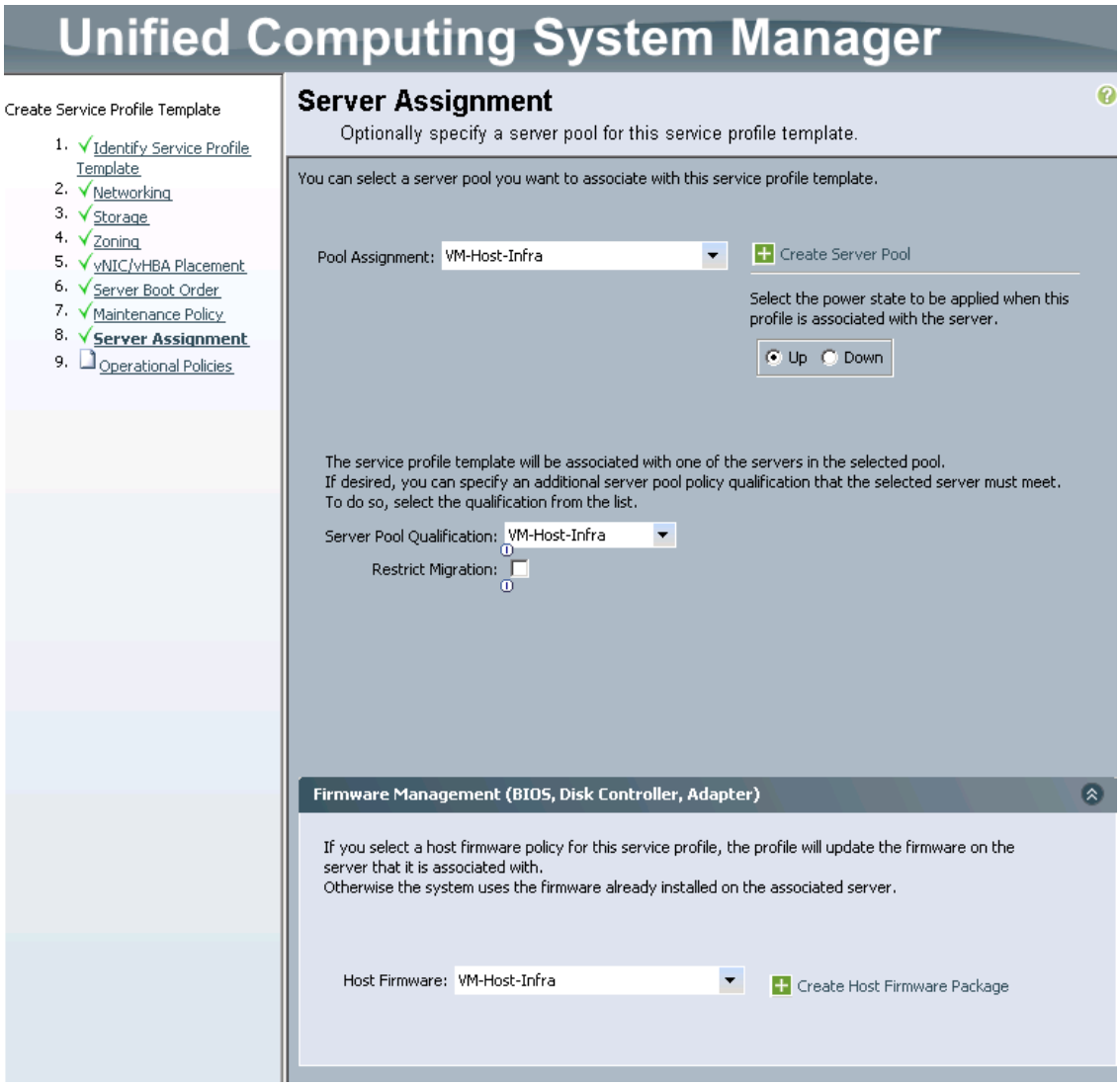
Maintenance Policy Section

1. Select the previously created policy User_Acknowledge.
2. Click `Next` to continue to the next section.



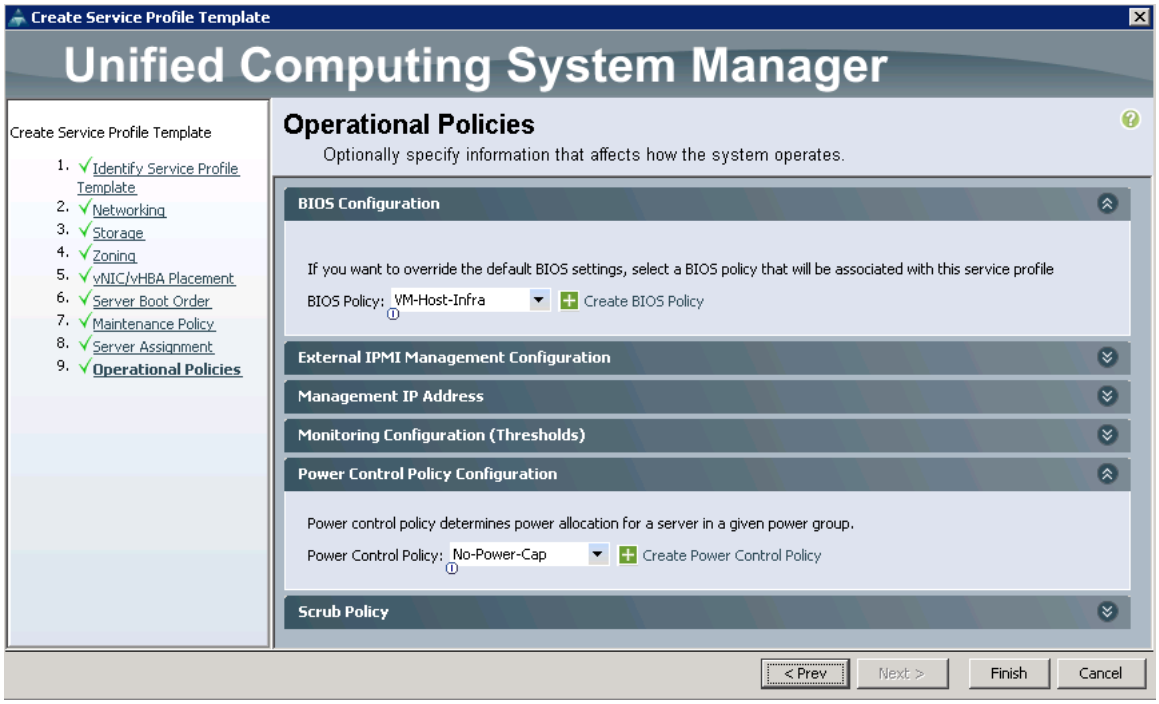
Server Assignment Section

1. Select `VMHost-Mgmt` in the `Pool Assignment` field.
2. Select `VMHost-Mgmt` for the Server Pool Qualification field.
3. Select `Up` for the power state.
4. Select `VMHost-Mgmt` in the `Host Firmware` field.
5. Click `Next` to continue to the next section.



Operational Policies Section

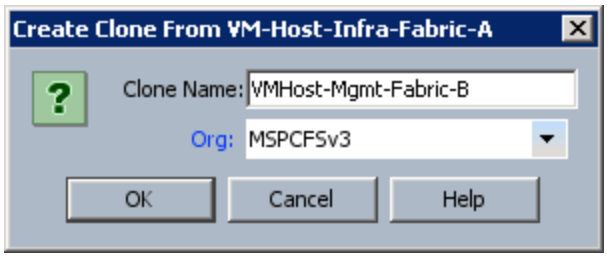
1. Select `VMHost-Mgmt` in the `BIOS Policy` field.
2. Expand `Power Control Policy Configuration`.
3. Select `No-Power-Cap` in the `Power Control Policy` field.
4. Click `Finish` to create the Service Profile template.



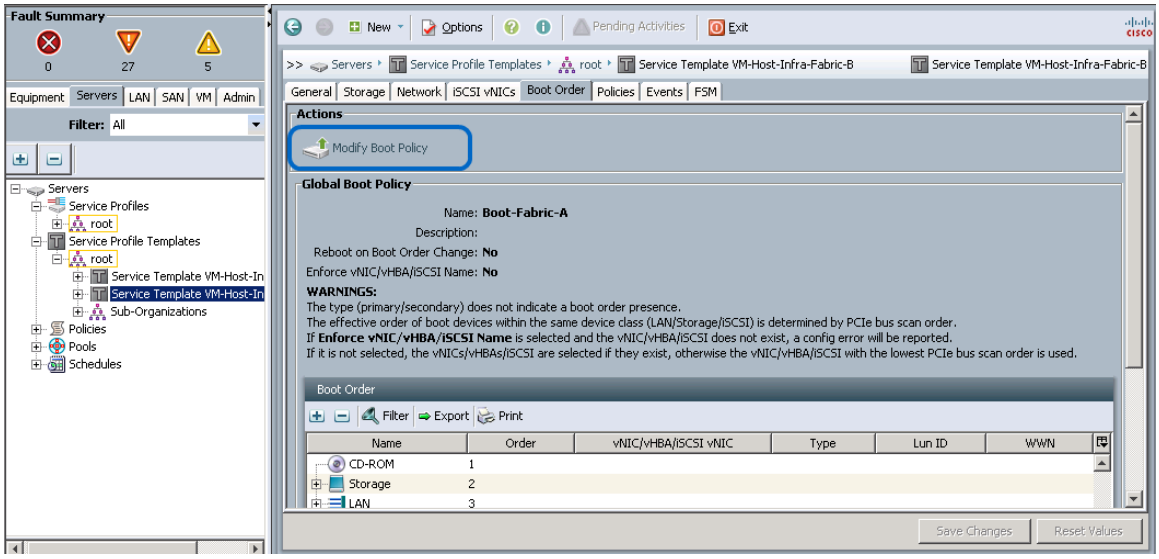
5. Click `OK` in the pop-up window to proceed.

Create the Fabric-B Template. (Optional)

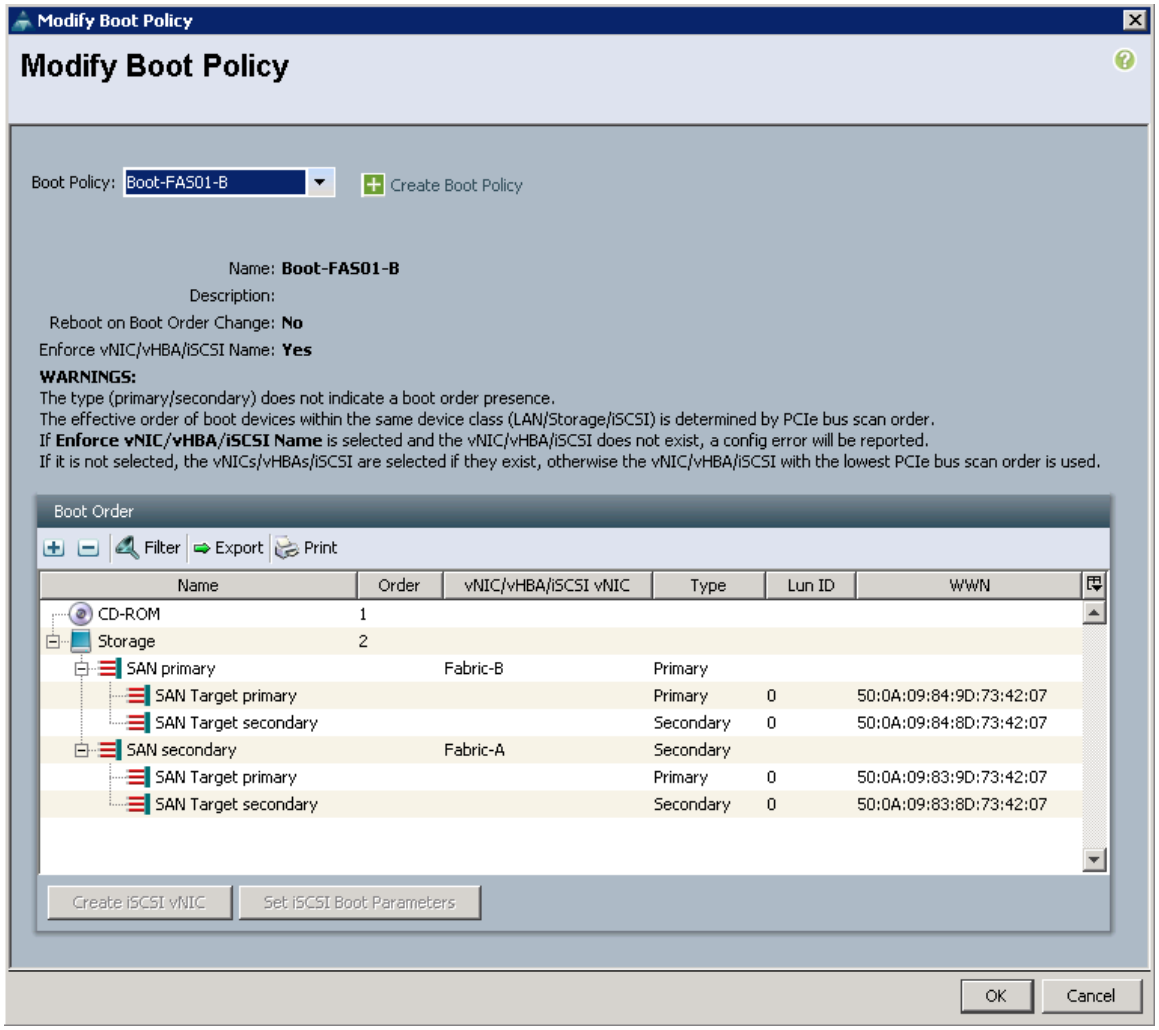
1. Select the `Servers` tab at the top left of the window.
2. Go to `Service Profile Templates > root or a sub-organization.`
3. Select the previously created `VMHost-Mgmt-Fabric-A` template
4. Click Create a Clone.
5. Enter `VMHost-Mgmt-Fabric-B` in the Clone Name field and click `OK`.



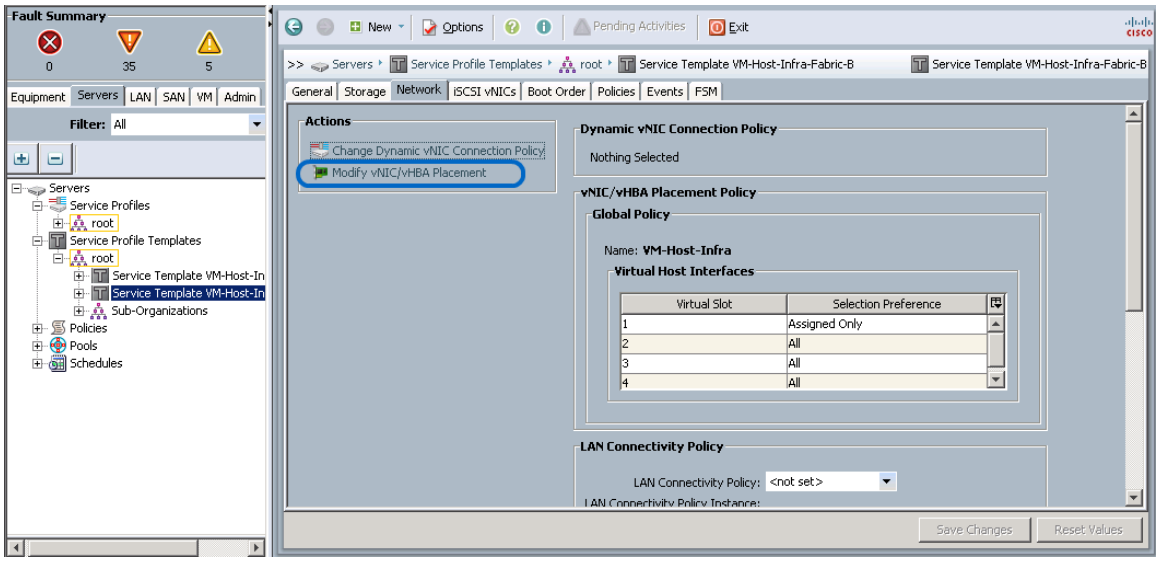
6. Select the newly created service profile template and select the `Boot Order` tab.
7. Click Modify Boot Policy.



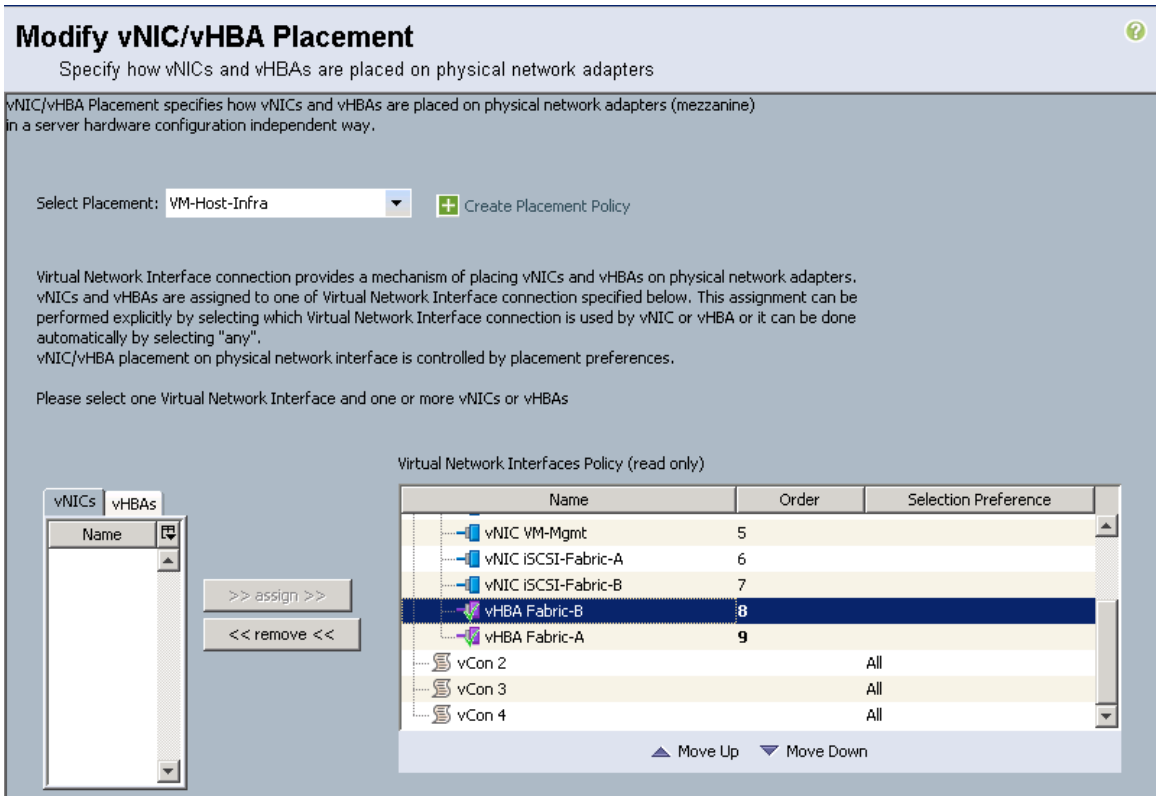
8. Select `Boot-FAS01-B` Boot Policy and click `OK`.



9. Select the Network tab and click Modify vNIC/HBA Placement Policy.



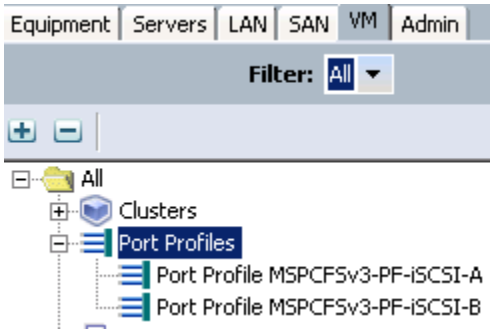
10. Move vHBA `Fabric-B` ahead of vHBA `Fabric-A` in the placement order and click `OK`.



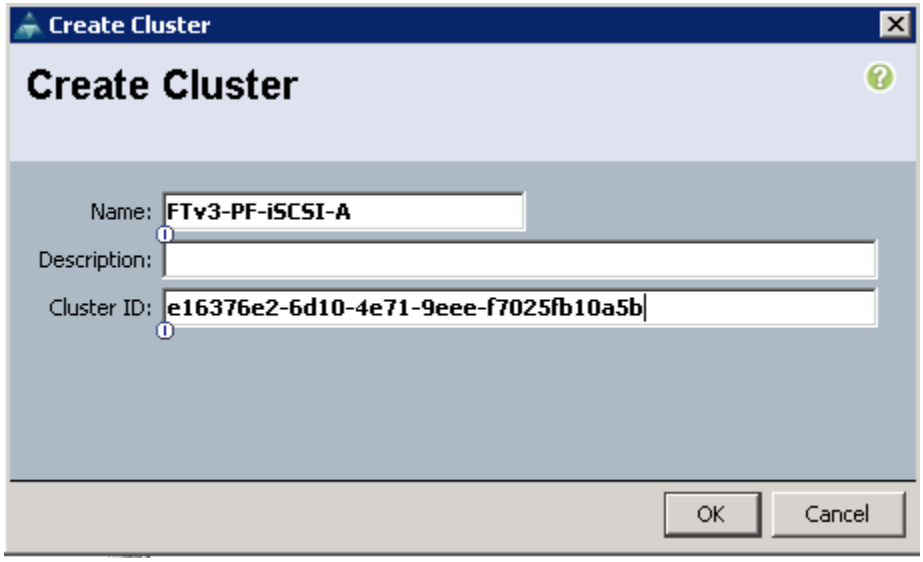
9.30 Create VM-FEX Port Profiles and Virtual Switch Clusters

These steps provide details for verifying that the port profiles and creating virtual Switch Clusters which will be used by the SR-IOV physical and virtual functions.

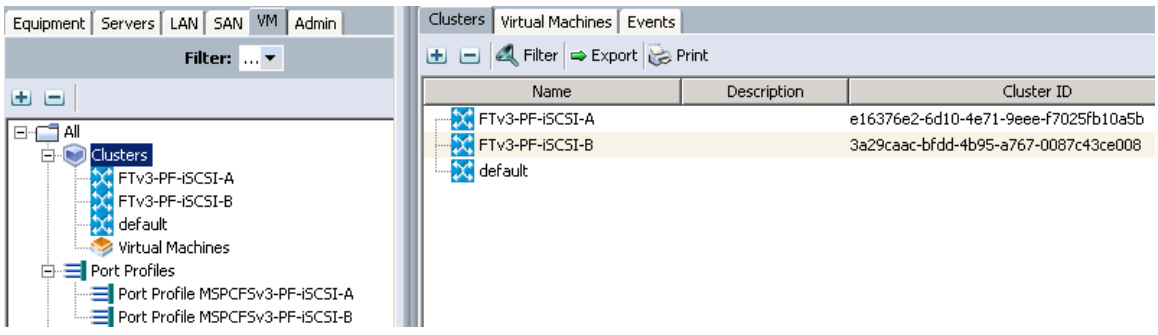
1. Select the VM tab at the top left of the window.
2. Note that the PF-iSCSI-A and PF-iSCSI-B port profiles have automatically been created because the VM option was selected in the vNIC Template creation step.



3. Right-click `the cluster object` and select `Create Cluster`.
4. Enter the iSCSI-A fabric cluster name.
5. Open a PowerShell window and type the following command to generate a GUID.
   `[system.guid]::NewGuid()`
6. Copy the GUID generated in the previous step and past it Cluster ID text box.

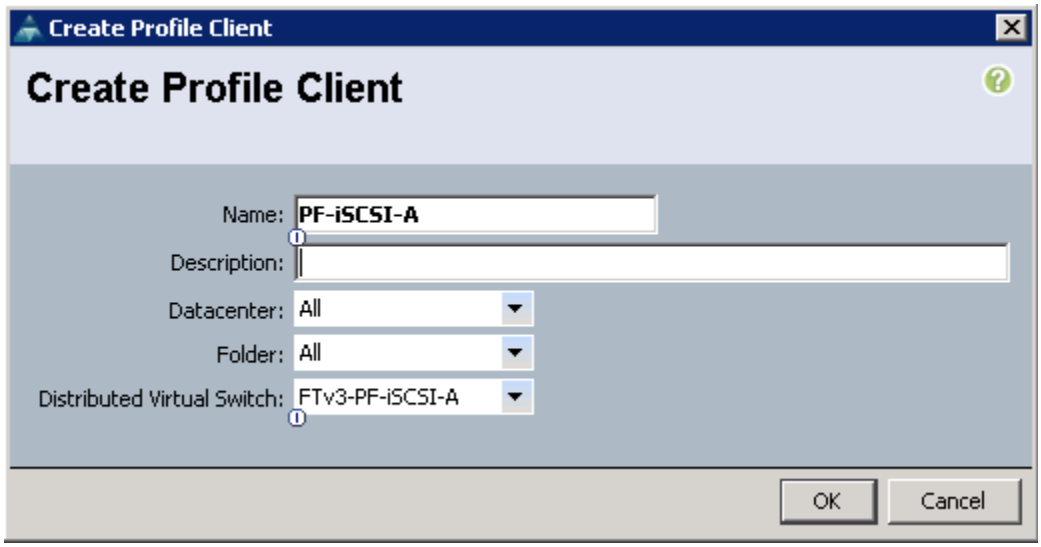


7. Click `OK` to create the cluster.
8. Repeat steps 3 through 7 to create the cluster for iSCSI-B fabric.

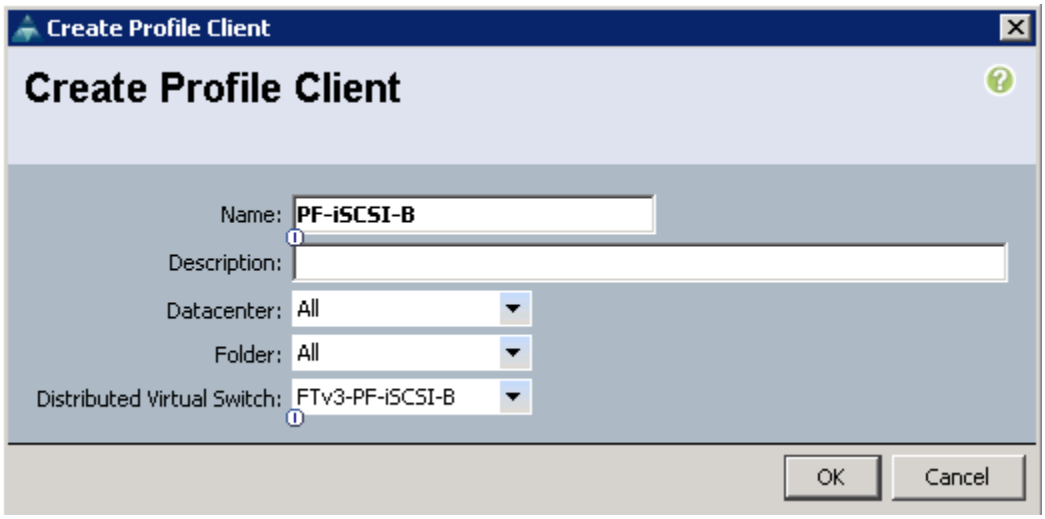


9. Right-Click on the PF-iSCSI-A Port Profile created in the previous step and select `Create Profile Client.`

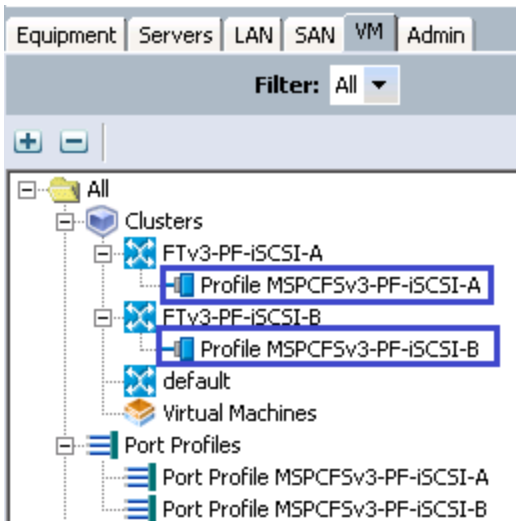
10. Enter the name `PF-iSCSI-A`.
11. Leave the default setting All for the Datacenter and Folder option.
12. Select the previously created virtual switch cluster FT-v3-PF-iSCSI-A for the distributed virtual switch option.



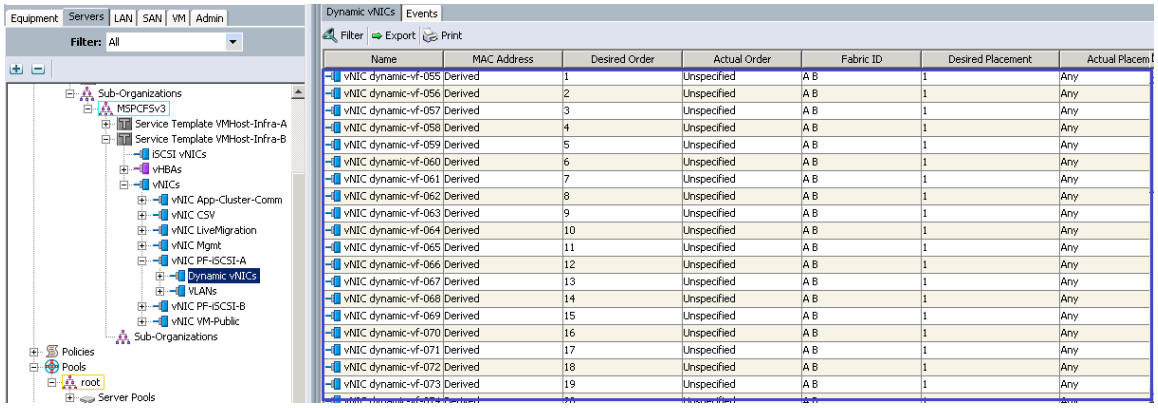
13. Click `OK` to create the port profile client.
14. Right-Click on the PF-iSCSI-B Port Profile created in the previous step and select `Create Profile Client`.
15. Enter the name `PF-iSCSI-B`.
16. Leave the default setting All for the Datacenter and Folder option.
17. Select the previously created virtual switch cluster `FT-v3-PF-iSCSI-B` for the distributed virtual switch option.



18. Click `OK` to create the port profile client.
19. Verify that the new port profile clients appear under each virtual switch cluster.



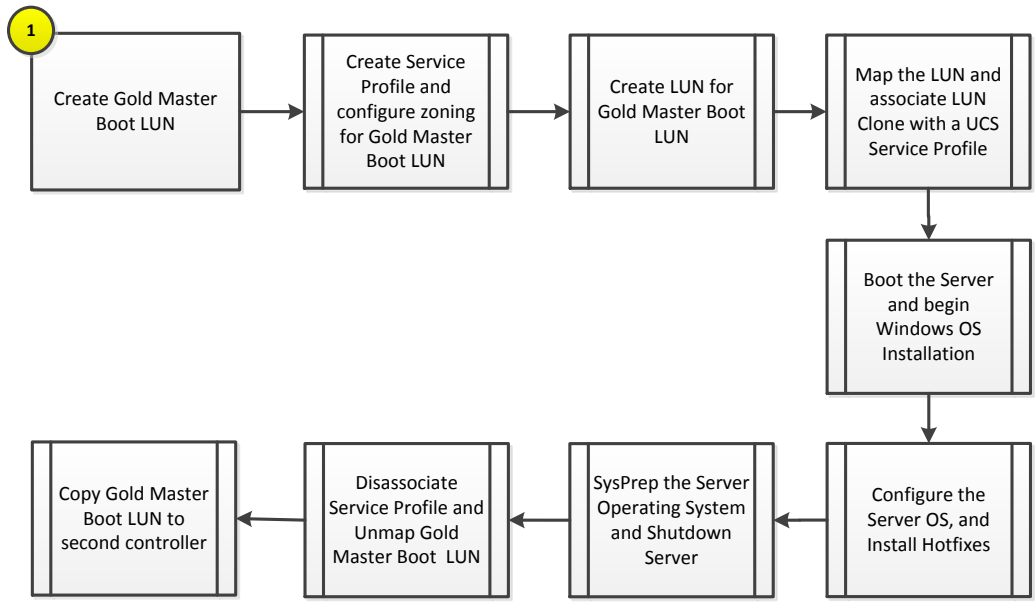
20. Select the Servers tab.
21. Find the service profile template created in the previous section and expand the vNICs object.
22. Expand the vNIC PF-iSCSI-A object and select Dynamic vNICs in the left tree view.
23. Verify that multiple vNICs appear in the right pane.



24. Repeat steps 22 and 23 for the vNIC PF-iSCSI-B.

10 Create Gold Master Boot LUN

The process to create a Gold Master Boot LUN is comprised of the following high-level steps:



10.1 Overview

Instead of using Windows Deployment Services to automate the provisioning of Hyper-V hosts, the deployment process of the Hyper-V hosts takes advantage of the built-in LUN cloning capabilities of the NetApp storage.

This section provides high-level walkthrough on how to create the Gold Master Boot LUN for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- NetApp PowerShell Toolkit 1.7 or higher installed on an administrative host
- Access to Windows 2012 installation ISO image
- Access to Cisco UCS FCoE driver installation ISO image
- Access to Cisco UCS Ethernet driver installation ISO image

10.2 Creation of Gold Master Boot LUN Workflow

The following workflow will explain how to build the gold master lun that will be used to provision the remaining Server 2012 hosts.

Create Gold Master Service Profile

Perform the following steps to buld the Gold Master service profile that will be used to create the boot LUN.

1. Open the Cisco UCS Manager and select the Servers tab at the top left of the window.
2. Select and expand the Service Profile Templates > root object.
3. Right-click VMHost-Mgmt-Fabric-A and select the action “Create Service Profiles From Template”.
4. Enter GoldMaster for the service profile suffix.

5. Enter 1 for the number of service profiles to create.
6. Select GoldMaster for the Service Profile Template field. It should be under Organizations > root.
7. Click OK to create the service profile, and OK again to acknowledge the creation.
8. Select the newly created service profile, from the left hand management pane expand vHBA vHBA_Fabric-A and write down the WWPN.

Create the GoldMaster Boot LUN

Perform the following steps to configure the NetApp storage needed for the Gold Master Boot LUN:

1. Start a Windows PowerShell session on the administrative host and import the Data ONTAP PowerShell Toolkit module.

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NaController <<var_ntap_A_hostname>> -credential root
```

3. Create a new Qtree to hold the boot LUN.

```
New-NaQtree /vol/ucs_boot/goldmaster
```

4. Create the NetApp LUN for the Gold Master Boot LUN.

```
New-NaLun /vol/ucs_boot/goldmaster/goldmaster.lun 200g –type windows_2008 -unreserved
```

5. Create the NetApp igroup for the Gold Master Boot LUN.

```
New-NaIgroup -Name goldmaster -Protocol fcp -Type windows
```

6. Add the WWPN from the <<vHBA_A>> vHBA in the Goldmaster service profile to the Gold Master Boot LUN igroup.

```
Add-NaIgroupInitiator –Igroup goldmaster –Initiator <vHBA_A WWPN>
```

7. Map the igroup to the Gold Master Boot LUN.

```
Add-NaLunMap /vol/ucs_boot/goldmaster/goldmaster.lun goldmaster
```

Create GoldMaster Zone

Perfrom the following setps to zone the GoldMaster service profile.

1. Create a temporary zone for the goldmaster service profile.

```
zone name goldmaster_A vsan <Fabric A VSAN ID>
  member device-alias controller_A_2a
  member pwwn <Fabric-A WWPN>
exit
```

2. Add the new zone to the zoneset.

```
zoneset name Flexpod vsan <Fabric A VSAN ID>.
  member goldmaster_A
exit
```

3. Activate the zoneset.

```
zoneset name Flexpod vsan <Fabric A VSAN ID>.
exit
copy run start
```

Prepare the Windows Server 2012

This section details the steps required to prepare the server for OS installation.

1. Right-Click on the VM-Host service profile and select KVM Console.

2. From the virtual KVM Console, select the Virtual Media tab.
3. Select Add Image in the right pane.
4. Browse to the Windows Server 2012 installation ISO image file and click Open.
5. Map the image that you just added by selecting Mapped.
6. To boot the server, select the KVM tab.
7. Select Power On Server in the KVM interface Summary tab, and then click OK.

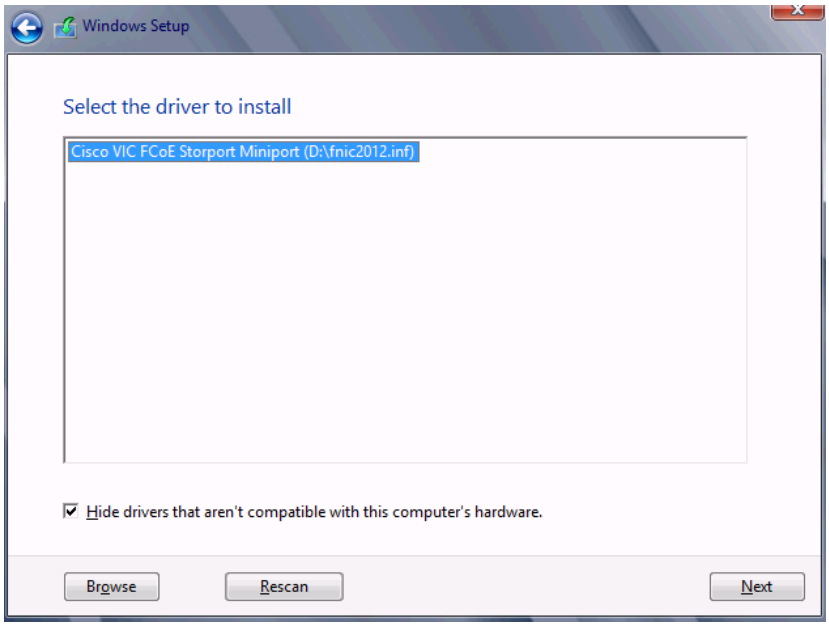
Install Windows Server 2012

The following steps describe the installation of Windows Server 2012 to each host.

1. On boot, the machine detects the presence of the Windows installation media.
2. After the installer is finished loading, enter the relevant region information and click **Next**.
3. Click Install now.
4. Enter the **Product Key** and click **Next**.
5. Select Windows Server 2012 Datacenter (Server with a GUI) and click Next.

Note: You may optionally remove the GUI after the server is operational.

6. After reviewing the EULA, Check the **I accept the license terms**, and click **Next**.
7. Select Custom (advanced) installation.
8. Chage the ISO in the Virtual Media Session manager by unchecking the Mapped checkbox for the Windows ISO and select yes when it asks you to confirm the action.
9. Click Add Image.
10. **Browse** to the Cisco fNIC driver ISO, click **Open**.
11. Select the **Mapped** checkbox next to the Cisco fNIC Driver ISO.
12. Back in the KVM Console, click the "**Load Driver**" option, and select **OK**.
13. The Cisco VIC FCoE Storport Miniport driver should autodetected, Click **Next**.

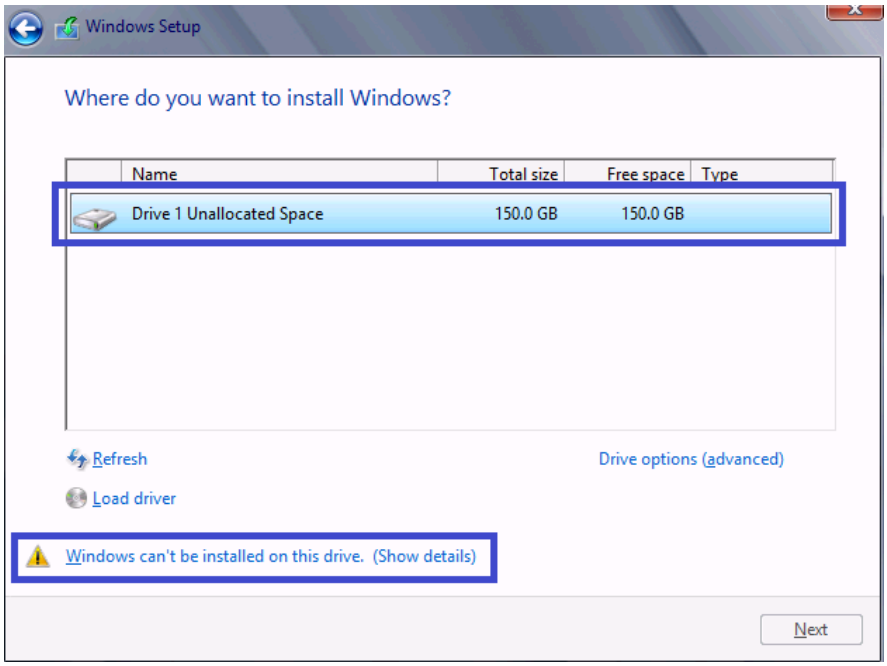


14. You should see a LUN listed in the drive selection screen.

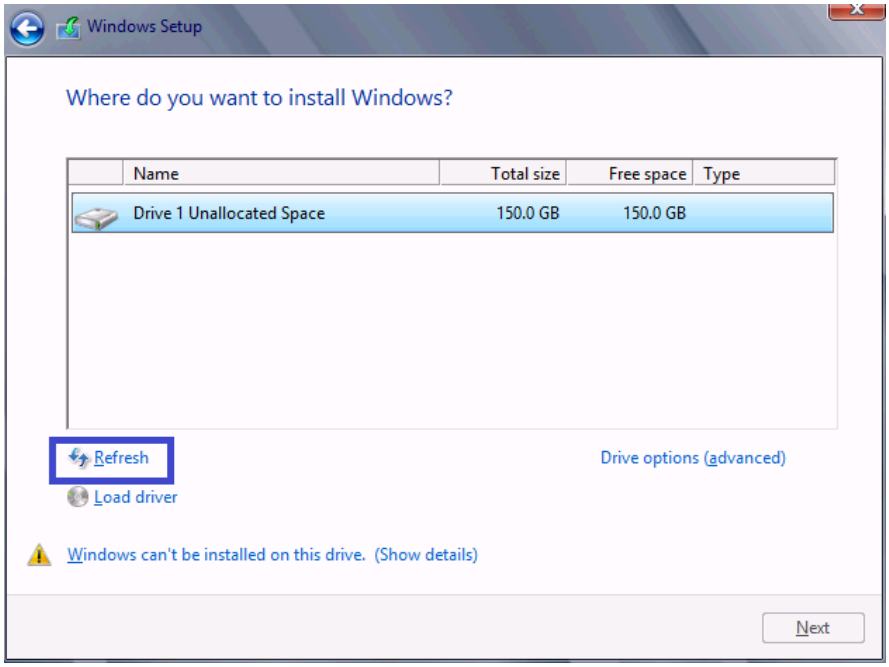
Note: Only a single LUN instance should be displayed. Multiple instance of the same LUN indicated that there are multiple paths to the installation LUN. Verify that the SAN zoning is correct and restart the installation.

Note: The message "Windows Can't be installed on this drive" appears because the Windows installation ISO image is not mapped at this time.

Note: The Cisco eNIC driver can be loaded at this point in the same way as the fNIC driver. Loading the eNIC driver at this time bypasses the need to load the eNIC driver in the section titled "Installing Windows eNIC Driver".



15. In the Virtual Media Session manager clear the Mapped checkbox for the Cisco Driver ISO that you recently added (fNIC driver) and choose yes to acknowledge.
16. Select the **Mapped** checkbox for the Windows ISO in the virtual media session manager.
17. Back in the KVM console click **Refresh** to update the cdrom drive status.



18. Select the new LUN, and click the Windows cannot be installed to this disk link.
19. Click **OK** to online the LUN.
20. Select the LUN, and click **Next** continue with the install.
21. When Windows is finished installing enter an Administrator password on the settings page and click **Finish**.

Install Windows Roles and Features

The following steps describe how to install all required roles and features from Windows Server 2012 Installation media. If you unmapped the installation ISO you will need to remap it now.

1. Log into Windows with the Administrator password previously entered during installation.
2. Verify that the Windows installation disk is mapped to E: drive.
3. Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.
4. Add the Net 3.5 feature by entering the following command:

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

5. Add MPIO, and DCB by entering the following command:

```
Add-WindowsFeature Multipath-IO, Data-Center-Bridging -IncludeManagementTools -Restart
```

Install the Data ONTAP PowerShell Toolkit.

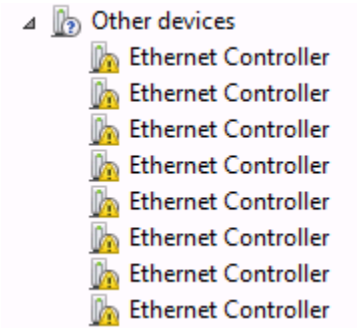
The following steps describe who to install the NetApp Data ONTAP PowerShell toolkit.

1. Download the DataONTAP PowerShell toolkit from the NetApp Communities https://communities.netapp.com/community/products_and_solutions/microsoft/powershell
2. Run DataONTAP windows installation package.
3. Click **Next** on the welcome page.
4. Accept the ELUA and click next.
5. Validate the Installation path and click **Next**.
6. Click **Install**.

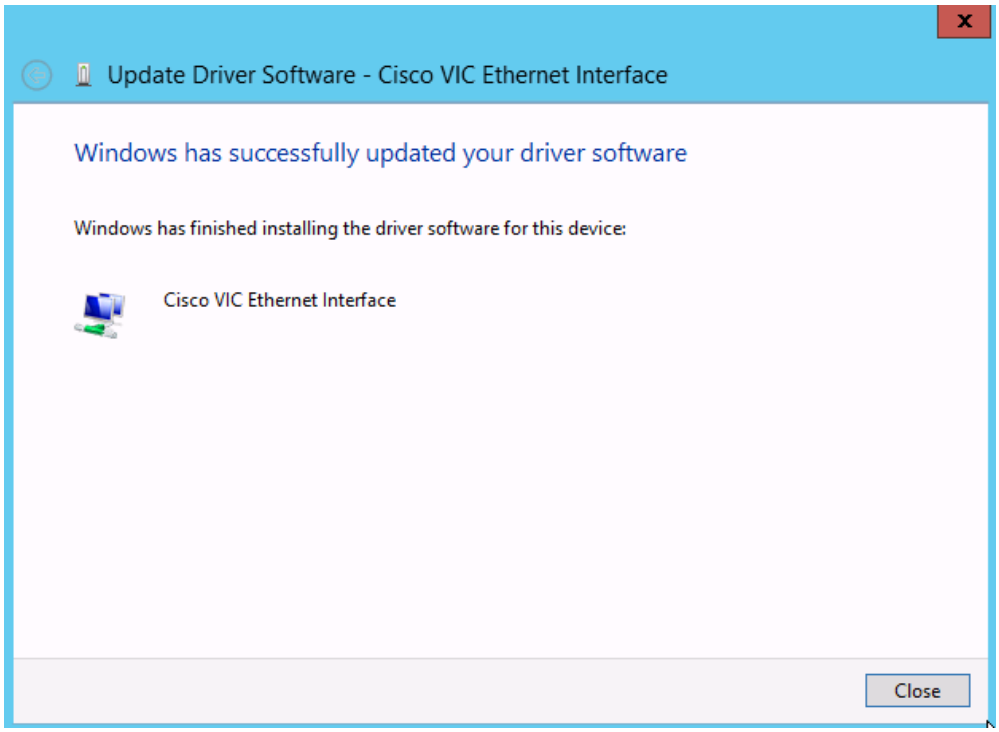
Install Windows eNIC Drivers

The following steps describe how to install all required network drivers.

1. In the Virtual Media Session manager, clear the **Mapped** checkbox for the Windows ISO.
2. Click **Add Image**.
3. Browse to the Cisco eNIC driver ISO, click **Open**.
4. Select the **Mapped** checkbox for the Cisco eNIC driver ISO.
5. Back in the KVM console open **Server Manager**, and select **Tools ->Computer Management**.
6. In Computer Manager select System Tools -> Device Manager -> Other devices



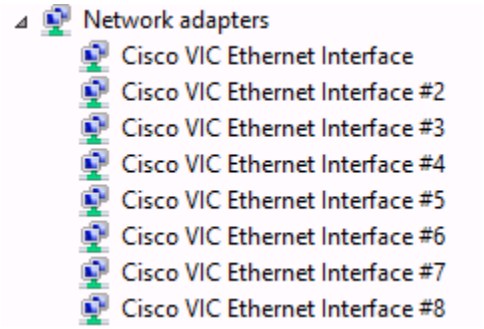
7. Right-click one of the Ethernet Controller, and select **Update Driver Software**.
8. Click **Browse** my computer for driver software.
9. Click Browse, and select the **CDROM drive**, click **OK**.
10. Click **Next >Close**.



11. Right click on the remaining Ethernet Controller and select **Update Driver Software**.
12. Click Search automatically for update driver software.
13. Click **Close**.
14. Repeat for the remaining Ethernet Controllers.

Note: Alternatively to steps 7 to 14, the Cisco eNIC driver can be loaded for all devices at once by issuing the command: *pnputil –i –a <directory>enic6x64.inf* where <directory> is the location of the eNIC driver.

15. All Cisco VIC Ethernet devices will appear under Network Adapters.



10.3 Install NetApp MPIO DSM

The following section describes how to install the NetApp DSM. For detailed information regarding the installation see the Administration and Installation Guide.

1. Download NetApp MPIO DSM http://support.netapp.com/NOW/download/software/mpio_win/4.0/ntap_win_mpio_4.0_setup_x64.msi
2. Launch the Installer, click **Next**
3. Click OK acknowledging the ALUA warning.
4. **Accept the EULA** and Click **Next**.
5. **Enter the license Key** and Click **Next**.
6. Leave **Use the default SYSTEM account checkbox** checked and Click **Next**.
7. Select **Yes, install the Hyper-V Guest Utilities**, and Click **Next**.
8. Click **Next** Through the driver information pane
9. Validate the installation path and click **Next**.
10. Click **Install**
11. When prompted reboot the host.

Sysprep Windows and Clean Up GoldMaster Service Profile

1. Create the Gold Master Boot LUN with sysprep. This command will shut down the server.

```
c:\windows\system32\sysprep\sysprep.exe /generalize /shutdown /oobe
```

2. When the server is off, open the Cisco UCS Manager. Select and expand the Service Profile Templates > root object.
3. Right-click Goldmaster and select Disassociate Service Profile.
4. Log in to the <<var_ntap_A_hostname>> controller with PowerShell.
5. Unmap the goldmaster igroup from the Gold Master Boot LUN.

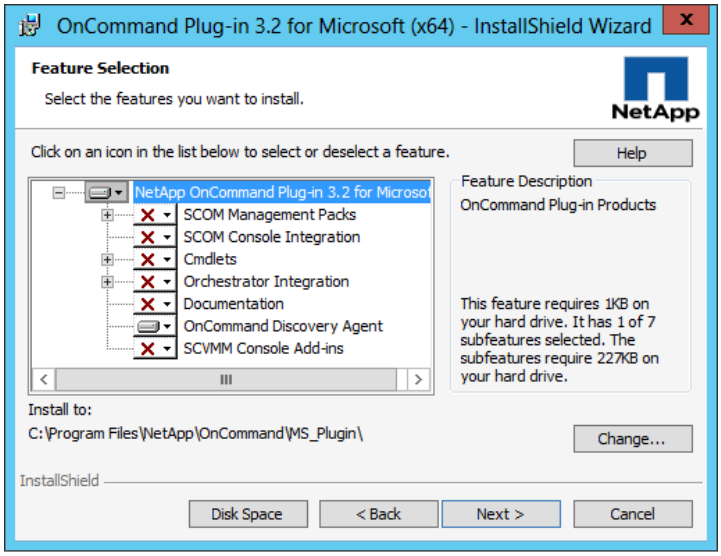
```
remove-nalunmap /vol/ucs/goldmaster/goldmaster.lun goldmaster
```

6. Remove the device aliases and the zones created for the Gold Master.

10.4 Install NetApp OnCommand Discovery Agent

All Hosts

1. Run the OnCommand Plug-in for Microsoft package.
2. Click **Next** on the welcome screen.
3. Click **Next** throught the installation path.
4. Uncheck everything except the **OnCommand Discovery Agent**, and click **Next**.



5. Click **Install**.
6. Click **Finish** to complete the installation.

11 Deploy Fabric Management Cluster from Gold Master

Instead of using Windows Deployment Services to automate the provisioning of Hyper-V hosts, the deployment process of the Hyper-V hosts takes advantage of the built-in LUN cloning capabilities of the NetApp storage.

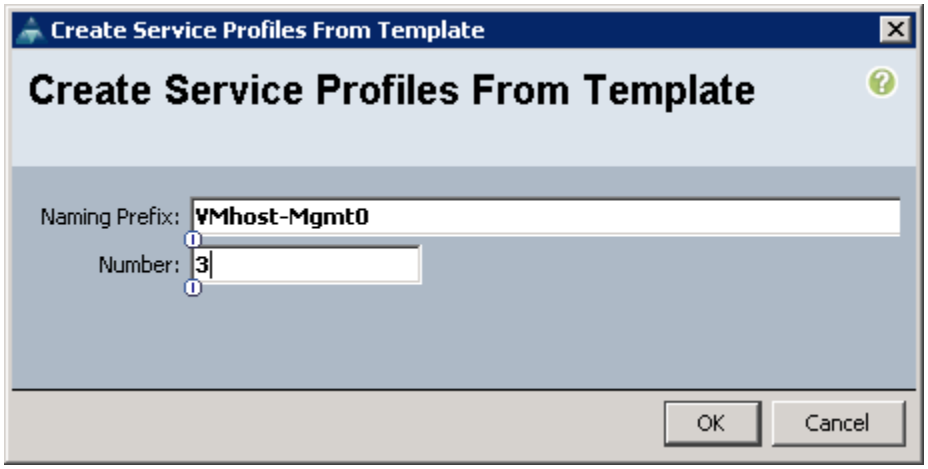
This section provides high-level walkthrough on how to deploy Hyper-V hosts for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- Fully configured Cisco UCS Service Profile Templates
- A Gold Master Boot LUN running Windows Server 2008 R2 (x64) has been created

11.1 Create Service Profiles

These steps provide details for creating a service profile from a template.

1. In the Cisco UCS Manager, select the `Servers` tab at the top left of the window.
2. Select `Service Profile Templates VMHost-Mgmt-Fabric-A`
3. Right-click `and select Create Service Profile From Template.`
4. Enter `VMHost-Mgmt0` for the service profile prefix.
5. Enter `3` for the number of service profiles to create.
6. Click `OK` to create the service profile.



7. Click `OK` in the message box.

11.2 Gather Necessary Information

After the Cisco UCS Service Profiles have been created (in the previous steps), the infrastructure blades in the environment each have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blades.

Table 10 vHBA WWPNs for Fabric A and Fabric B

Cisco UCS Service Profile Name	Fabric-A WWPN	Fabric-B WWPN
VMHost-Mgmt-01		
VMHost-Mgmt-02		
VMHost-Mgmt-03		

Note: To gather the information in the table above, launch the Cisco UCS Manager GUI, and in the left pane select the `Servers` tab. From there, expand `Servers > Service Profiles > root >`. Click each service profile and then click the `Storage` tab on the right. While doing so, record the WWPN information in the right display window for both vHBA_A and vHBA_B for each service profile in the table above.

11.3 Create Device Aliases

These steps provide details for configuring device aliases for the boot path.

Nexus 5548 A

1. Using the information in **Error! Reference source not found.**, Create device alias.

```
device-alias database.
  device-alias name VMHost-Mgmt-01_A pwwn <Fabric-A WWPN>.
  device-alias name VMHost-Mgmt-02_A pwwn <Fabric-A WWPN>.
  device-alias name VMHost-Mgmt-03_A pwwn <Fabric-A WWPN>.
exit.
device-alias commit.
copy running-config startup-config
```

Nexus 5548 B

- Using the information in **Error! Reference source not found.**, Create device alias.

```
device-alias database.
  device-alias name VMHost-Mgmt-01_B pwwn <Fabric-B WWPN>.
  device-alias name VMHost-Mgmt-02_B pwwn <Fabric-B WWPN>.
  device-alias name VMHost-Mgmt-03_B pwwn <Fabric-B WWPN>.
exit.
device-alias commit.
copy running-config startup-config
```

11.4 Create Zones for Each Service Profile

These steps provide details for configuring the zones for the boot path.

Nexus 5548 A

1. Create the Zones and Add Members

```
zone name VMHost-Mgmt-01_A vsan <Fabric A VSAN ID>.
  member device-alias VMHost-Mgmt-01_A.
  member device-alias controller_A_2a.
  member device-alias controller_B_2a
exit.
zone name VMHost-Mgmt-02_A vsan <Fabric A VSAN ID>.
  member device-alias VMHost-Mgmt-02_A.
  member device-alias controller_A_2a.
  member device-alias controller_B_2a
exit.
zone name VMHost-Mgmt-03_A vsan <Fabric A VSAN ID>.
  member device-alias VMHost-Mgmt-03_A.
  member device-alias controller_A_2a.
  member device-alias controller_B_2a
exit.
```

2. Create the Zoneset and Add the Necessary Members

```
zoneset name Flexpod vsan <Fabric A VSAN ID>.
  member VMHost-Mgmt-01_A.
  member VMHost-Mgmt-02_A.
  member VMHost-Mgmt-03_A.
exit.
```

3. Activate the Zoneset

```
zoneset activate name flexpod vsan < Fabric A VSAN ID>.
exit.
copy run start.
```

Nexus 5548 B

1. Create the Zones and Add Members

```
zone name VMHost-Mgmt-01_B vsan <Fabric B VSAN ID>.
  member device-alias VMHost-Mgmt-01_B.
  member device-alias controller_A_2b.
  member device-alias controller_B_2b
exit.
zone name VMHost-Mgmt-02_B vsan <Fabric B VSAN ID>.
  member device-alias VMHost-Mgmt-02_B.
  member device-alias controller_A_2b.
  member device-alias controller_B_2b
exit.
zone name VMHost-Mgmt-03_B vsan <Fabric B VSAN ID>.
  member device-alias VMHost-Mgmt-03_B.
  member device-alias controller_A_2b.
  member device-alias controller_B_2b
exit.
```

2. Create the Zoneset and Add the Necessary Members

```
zoneset name Flexpod vsan <Fabric B VSAN ID>.
  member VMHost-Mgmt-01_B.
  member VMHost-Mgmt-02_B.
  member VMHost-Mgmt-03_B.
exit.
```

3. Activate the Zoneset

```
zoneset activate name flexpod vsan < Fabric B VSAN ID>.
exit.
copy run start.
```

11.5 FlexClone Boot LUN

These steps provide details for cloning the boot lun from the goldmaster.

1. Start a Windows PowerShell session on the administrative host and import the Data ONTAP PowerShell Toolkit module.

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NaController <<var_ntap_A_hostname>> -credential root
```

3. Create a new Qtree to hold the boot LUN.

```
New-NaQtree /vol/ucs_boot/VMHost-Mgmt01
```

```
New-NaQtree /vol/ucs_boot/VMHost-Mgmt02
New-NaQtree /vol/ucs_boot/VMHost-Mgmt03
```

4. Create igroups.

```
New-NaIgroup -Name VMHost-Mgmt01 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>

New-NaIgroup -Name VMHost-Mgmt02 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>

New-NaIgroup -Name VMHost-Mgmt03 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>
```

5. Clone the boot LUN form the goldmaster boot LUN.

```
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-Mgmt01/boot.lun
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-Mgmt02/boot.lun
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-Mgmt03/boot.lun
```

4. Change the GUID of the LUN using the following command.

```
Set-NaLunSignature /vol/ucs_boot/VMHost-Mgmt01/boot.lun
Set-NaLunSignature /vol/ucs_boot/VMHost-Mgmt02/boot.lun
Set-NaLunSignature /vol/ucs_boot/VMHost-Mgmt03/boot.lun
```

5. Map the boot LUN to the new iGroup.

```
Add-NaLunMap -Path /vol/ucs_boot/VMHost-Mgmt01/boot.lun -InitiatorGroup VMHost-Mgmt01
Add-NaLunMap -Path /vol/ucs_boot/VMHost-Mgmt02/boot.lun -InitiatorGroup VMHost-Mgmt02
Add-NaLunMap -Path /vol/ucs_boot/VMHost-Mgmt03/boot.lun -InitiatorGroup VMHost-Mgmt03
```

11.6 Boot Service Profiles

Complete the following steps to boot each new service profile.

All Hosts

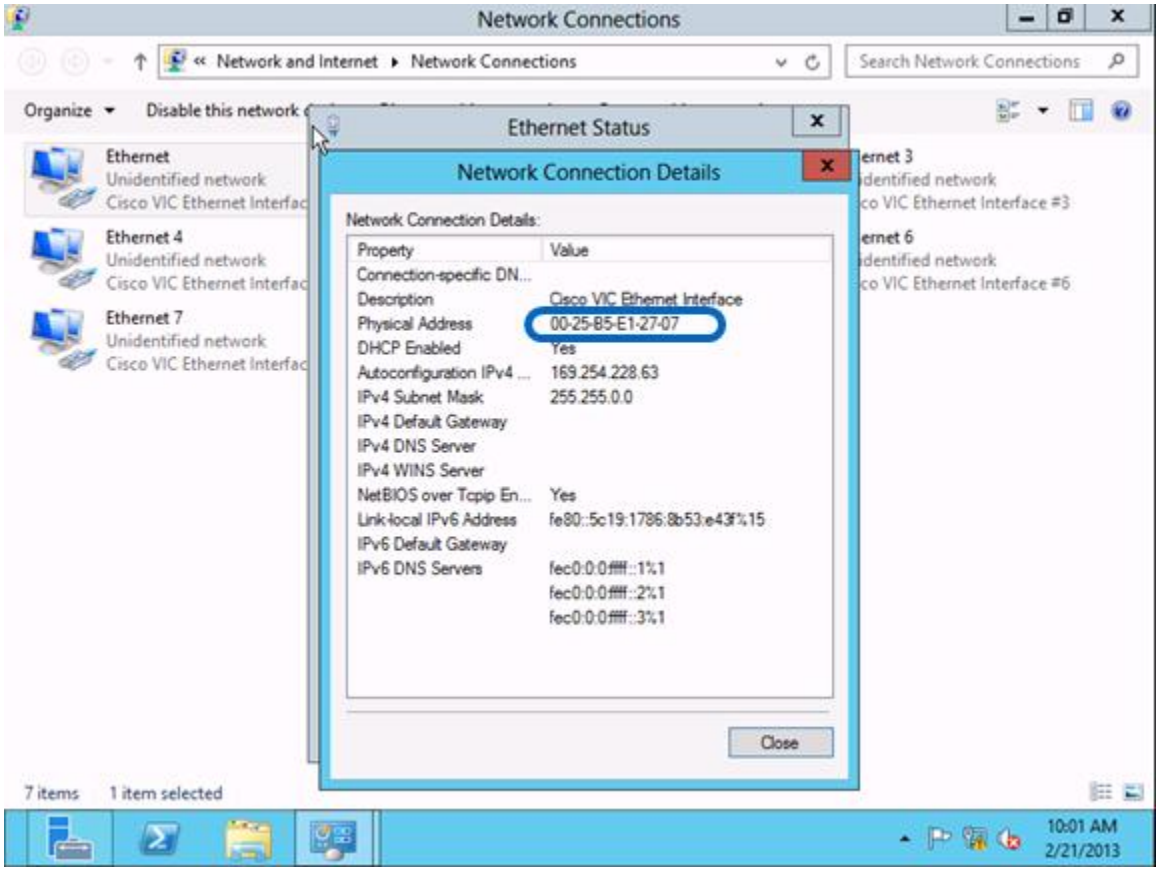
1. Back in the Cisco UCS Manager, right-click on Service profile and select Associate with Server Pool.
2. From the Pool Assignment box, select the Infra_Pool and click OK and OK again to acknowledge.
3. Right-click the <Hyper-V hostname> and select KVM Console.
4. Click Boot Server, the service profile will then pull a server from the VM-Host-Infra, and configure the hardware per the service profile.
5. Back in Cisco UCS Manager right-click <Hyper-V Hostname>, and select KVM Console.
6. Click Boot Server, the service profile will then pull a server from the Infra_Pool, and configure the hardware per the service profile.
7. When the server has fully booted Windows will enter the out of box experience. Accept the EULA, and click Accept.
8. Enter the region and language settings and Click Next.
9. Enter a new Administrator Password, and click Finish.
10. Repeate for each service profile.

11.7 Configure Windows Networking for FlexPod

The following steps describe how to rename the network for each Hyper-V host.

All Hosts

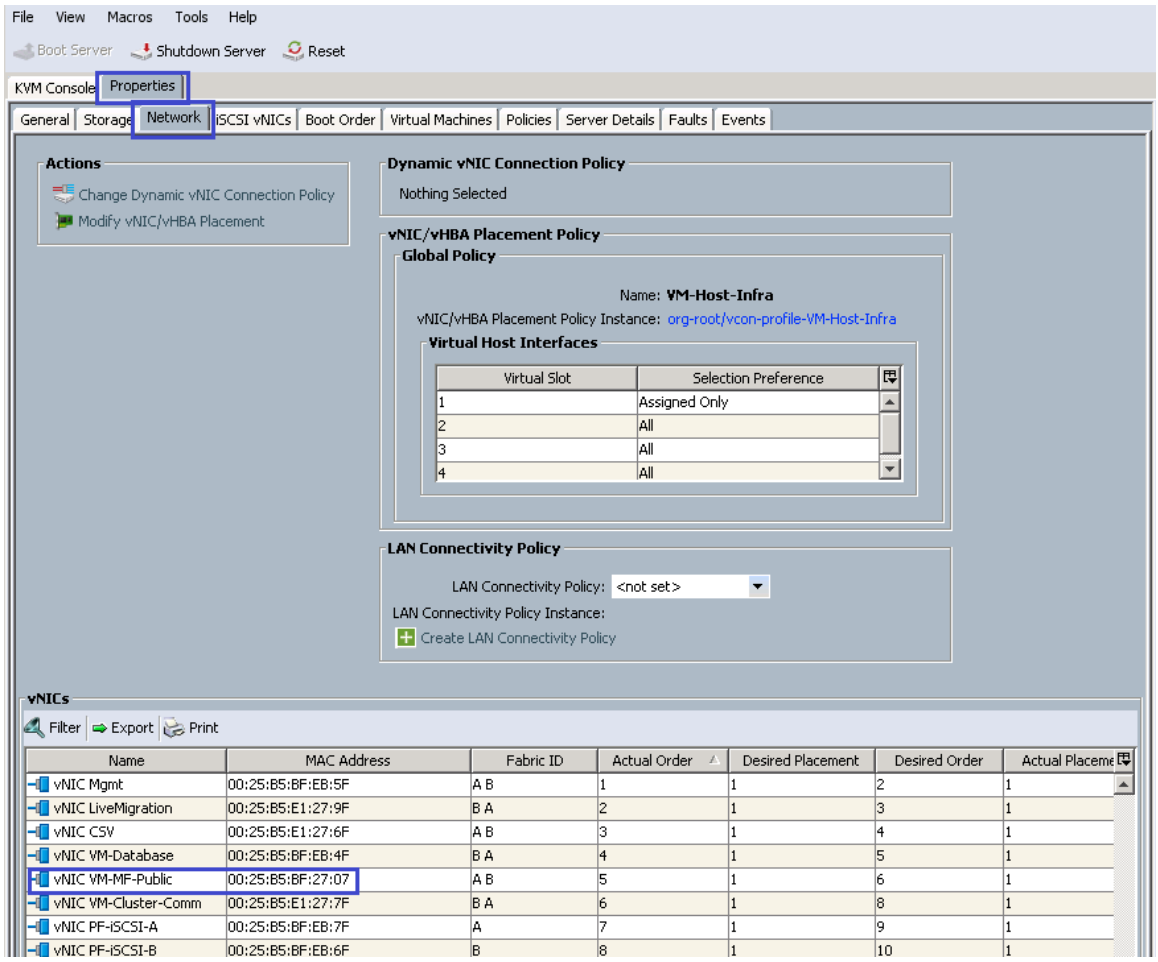
1. In server Manger select Local Server on the left.
2. Click on the `IPv4 address assigned by DHCP, IPv6 enabled` link to launch the network connections control panel.
3. One at a time right click on each eNIC, and select Status.
4. Click Details, and note the Physical Address.



Note: The following PowerShell command provides a list of the adapters with their associated MAC addresses it can be used instead of performing steps 3 through 5 for each NIC.

```
Gwmi Win32_NetworkAdapter | Where{$_.MACaddress -ne $Null} | FT NetConnectionID,
MACaddress
```

5. In the KVM console select Properties -> Network. Locate the vNIC.

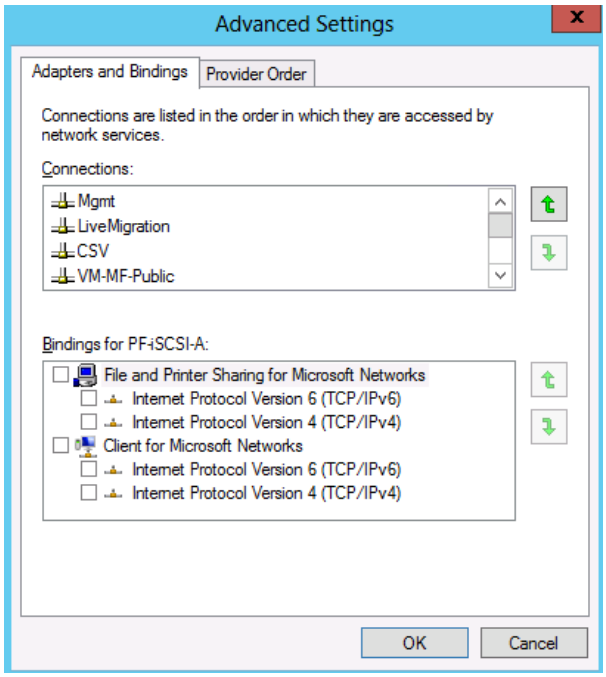


6. Identify the vNIC with the MAC Address noted in step 3.
7. Back in windows rename the LAN adapter to reflect the network it is associated with.
8. Set the appropriate IP settings for that adapter.

Note: Assign IP Addresses to the LiveMigration, CSV, and Mgmt adapters.

9. Repeat for each eNIC in windows.
10. In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings
11. Select the adapter and use the arrows to move it up or down in binding order.
12. The recommended binding order is:
    - Mgmt
    - LiveMigration
    - CSV
    - VM-MF-Public
    - VM-Database
    - VM-Cluster-Comm
    - PF-iSCSI-A
    - PF-iSCSI-B

13. Select the PF-iSCSI-A connection.
14. In the Bindings for PF-iSCSI-A list box, clear the check box next to File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
15. Repeat steps 13 and 14 for the PF-iSCSI-B connection.



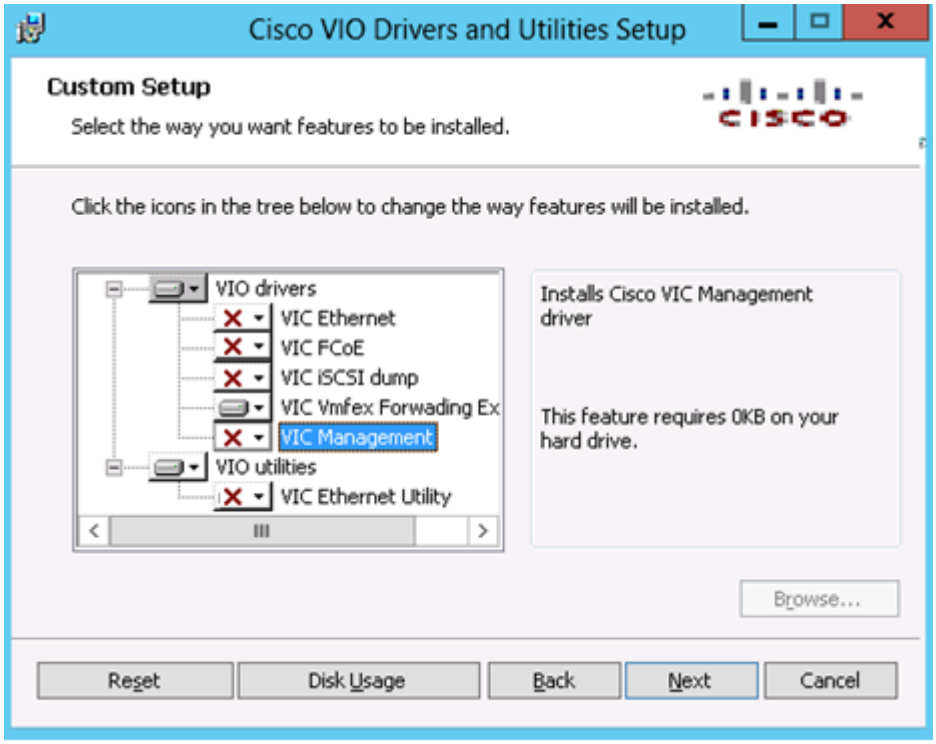
11.8 Install Cisco Virtual Switch Forwarding Extensions for Hyper-V

Cisco Virtual Switch Forwarding Extensions for Hyper-V enable SR-IOV capability when using VM-FEX for Hyper-V. The installation package is located on the UCS drivers ISO image starting with version 2.1. The installation package file name is CSCO_VIO_INSTALLER_64_2.x.x.msi. It is located in the Windows\installers\Cisco\MLOM\W2K12\x64 directory.

All Hosts

1. Run CSCO_VIO_INSTALLER_64_2.x.x.msi with administrator rights.
2. Click `Next` in the welcome screen.
3. `Accept the EULA` and click `Next`.
4. Select `Custom setup`.
5. Deselect the following options:
   - VIC Ethernet
   - VIC FCoE
   - VIC iSCSI Dump
   - VIC Management
   - VIC Ethernet Utility

Note: Only the option VIC VMfex Forwarding Extension should be installed.



6. Click `Next`.
7. Click `Install`.
8. Click `Finish` to complete the installation.

11.9 Create Hyper-V Virtual Network Switches

All Hosts

1. Open a powershell command window.
2. Create the Hyper-V virtual switches with the following parameters:

Virtual Network Name	Connection Type	Enable SR-IOV	Interface Name	Share Network with Management Host
Mgmt	External	No	Mgmt	Yes
Database	External	No	VM-Databas	No
VM-Cluster-Comm	External	No	VM-Cluster-Comm	No
VF-iSCSI-A	External	Yes	PF-iSCSI-Fabric-A	No
VF-iSCSI-B	External	Yes	PF-iSCSI-Fabric-B	No

3. Create virtual switch Mgmt

```
New-vmswitch –name Mgmt –NetAdapterName Mgmt –AllowManagementOS $true
```

4. Create virtual switch VM-Database

```
New-vmswitch –name VM-Database –NetAdapterName VM-Datbase –AllowManagementOS $false
```

5. Create virtual switch VM-Cluster-Comm.

```
New-vmswitch –name VM-Cluster-Comm –NetAdapterName VM-Cluster-Comm -AllowManagementOS
$false
```

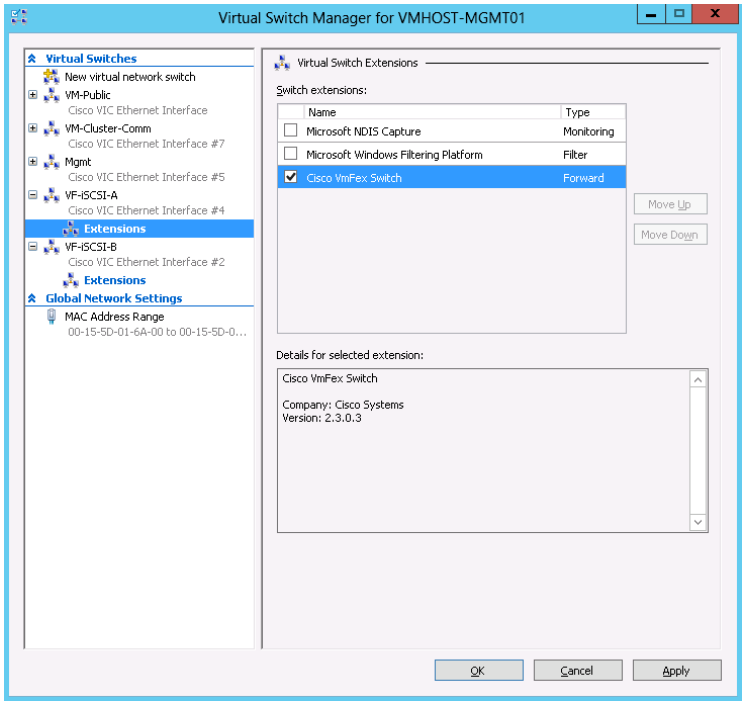
6. Create virtual switch VF-iSCSI-A.

```
New-vmswitch –name VF-iSCSI-A –NetAdapterName PF-iSCSI-A -AllowManagementOS $false –
EnableIov $true
```

7. Create virtual switch VF-iSCSI-B.

```
New-vmswitch –name VF-iSCSI-B –NetAdapterName PF-iSCSI-B -AllowManagementOS $false –
EnableIov $true
```

8. Open Hyper-V Manager
    a. Select Hyper-V Virtual Switch Manger in the action pane.
    b. Expand the VF-iSCSI-A virtual switch.
    c. Select Extensions under the VF-iSCSI-A virtual switch.
9. Check the box next to Cisco VMFex Switch.



10. Click Apply.
11. Repeat for virtual switch VF-iSCSI-B.

11.10 Domain Controller Virtual Machines

Most environments will already have an active directory infrastructure and will not require additional domain controllers to be deployed for the Hyper-V FlexPod. Refer to Microsoft documentation for installing Active Directory domain controllers in case additional Active Directroy domain controllers are required.

11.11 Prepare Nodes for Clustering

The following section describes how to prepare each node to be added to the Hyper-V cluster.

All Hosts

1. Rename the Host.

```
Rename-Computer -NewName <hostname> -restart
```

2. Add the host to Active Directory.

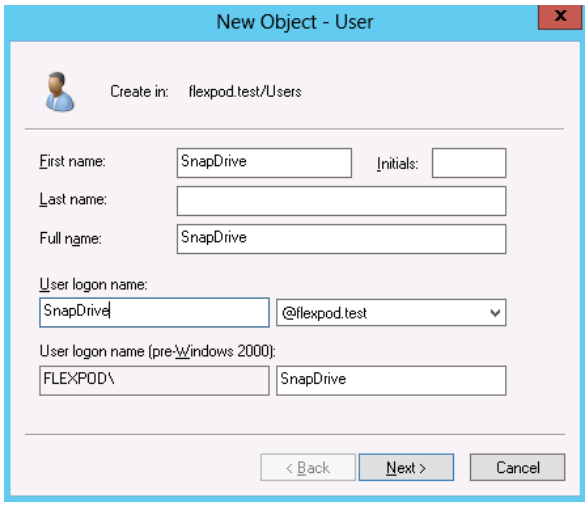
```
Add-Computer -DomainName <domain_name> -Restart
```

11.12 Install NetApp SnapDrive

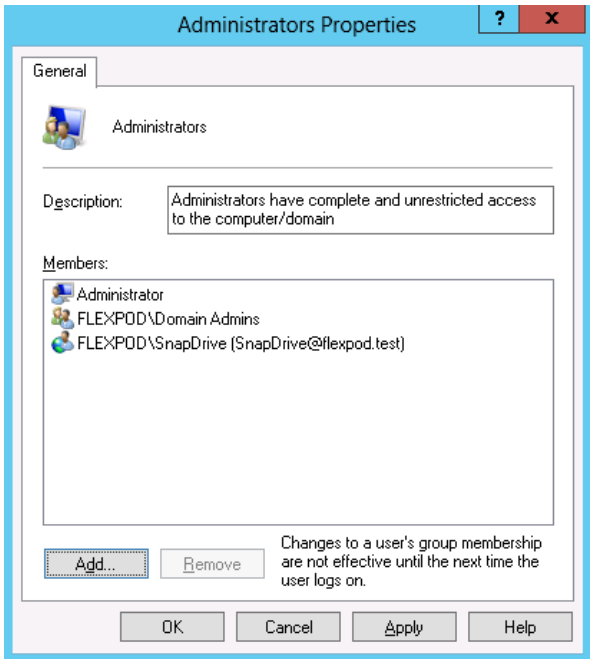
The following section describes how to installation of the NetApp SnapDrive Windows. For detailed information regarding the installation see the Administration and Installation Guide.

Service Account Preparation

1. In active directory create a SnapDrive service account note this account requires no special delegation.

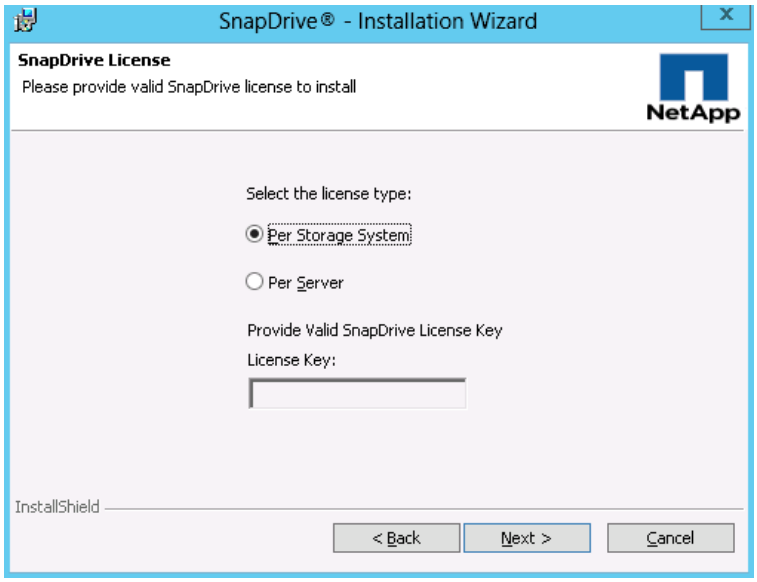


2. Add the SnapDrive service account to the local Administrators group in Windows.

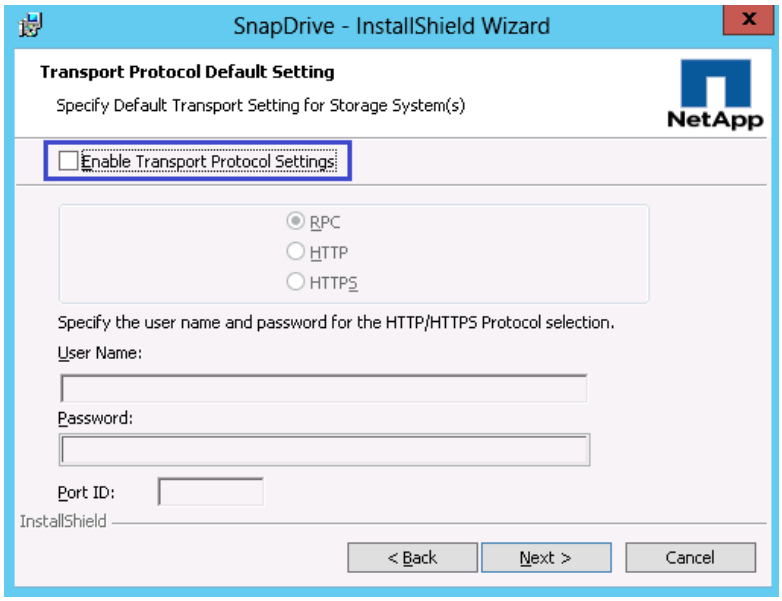


All Hosts

1. Download SnapDrive installer http://support.netapp.com/NOW/download/software/snapdrive_win/6.5/SnapDrive6.5_x64.exe
2. Launch the Installer, click `Next`.
3. `Accept the EULA` and click `Next`.
4. Select the Storage based Licensing method and click Next.



5. Enter your User Name, and Organization information, and click `Next`.
6. Validate the installation path and click `Next`.
7. Check the `Enable SnapDrive to communicate through the Windows Firewall` checkbox and click `Next`.
8. Enter the Account information for the Snapdrive service account, Click `Next`.
9. Click `Next`, through the SnapDrive Web Service Configuration.
10. Uncheck the `Enable Transport Protocol Settings`, and click `Next` .



11. Leave `Enable Protection Manger Integration` Unchecked, and click `Next`.
12. Click `Install`.
13. After the installation is finished. Launch a NEW PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.

Note: A new prompt is required to register the sdcli executable.

14. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_controller1>> -IP <<var_controller1_e0m_ip>>
sdcli preferredIP set -f <<var_controller2>> -IP <<var_controller2_e0m_ip>>
```

15. Configure SnapDrive transport protocol authentication configuration for each controller.

```
sdcli transport_protocol set -f <<var_controller1>> -type https -user root -pwd
<<var_admin_passwd>>
sdcli transport_protocol set -f <<var_controller2>> -type https -user root -pwd
<<var_admin_passwd>>
```

11.13 Install NetApp SnapManager for Hyper-V

The following section describes how to installation of the NetApp SnapManger for Hyper-V. For detailed information regarding the installation see the Administration and Installation Guide.

Service Account Preparation

1. In active directory create a SMHV service account note this account requires no special delegation.
2. Add the SMHV service account to the local Administrators group in Windows.

All Hosts

1. Download the SnapManger for Hyper-V installer from http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/1.2/SMHV1.2_NetApp_x64.exe
2. Launch the Installer, click Next.
3. Accept the EULA and click Next.
4. Select the Storage based Licensing method and click Next.

5. Enter your User Name, and Organization information, and click Next.
6. Validate the installation path and click Next.
7. Enter the Account information for the SMHV service account, Click Next.
8. Click Next, through the SMHV Web Service Configuration.
9. Click Install.

11.14 Install VM-FEX Port Profile Management Utilities in Hyper-V

All Hosts

1. Run the VM-FEX Port Profile Management Utilities installation package VMFEX_ToolS_64_2.3.2.msi.
2. Click **Next** on the welcome screen.
3. Accept the license agreement and click **Next**.
4. Click the **Custom** installation button.
5. Click **Next**.
6. Click **Install**.
7. Click **Finish** to complete the installation.

11.15 Create a Cluster

One Server Only

1. Launch a PowerShell prompt with administrative permissions, by right clicking on the PowerShell icon and selecting Run as Administrator.
2. Create a new cluster.

```
New-Cluster -Name <cluster_name> -Node <Node1>, <Node2>, <node3>, -NoStorage -
StaticAddress <cluster_ip_address>
```

3. Rename Cluster Networks

```
Get-ClusterNetworkInterface | ? Name -like *CSV* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'CSV'}
Get-ClusterNetworkInterface | ? Name -like *LiveMigration* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'LM'}
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Mgmt'}
```

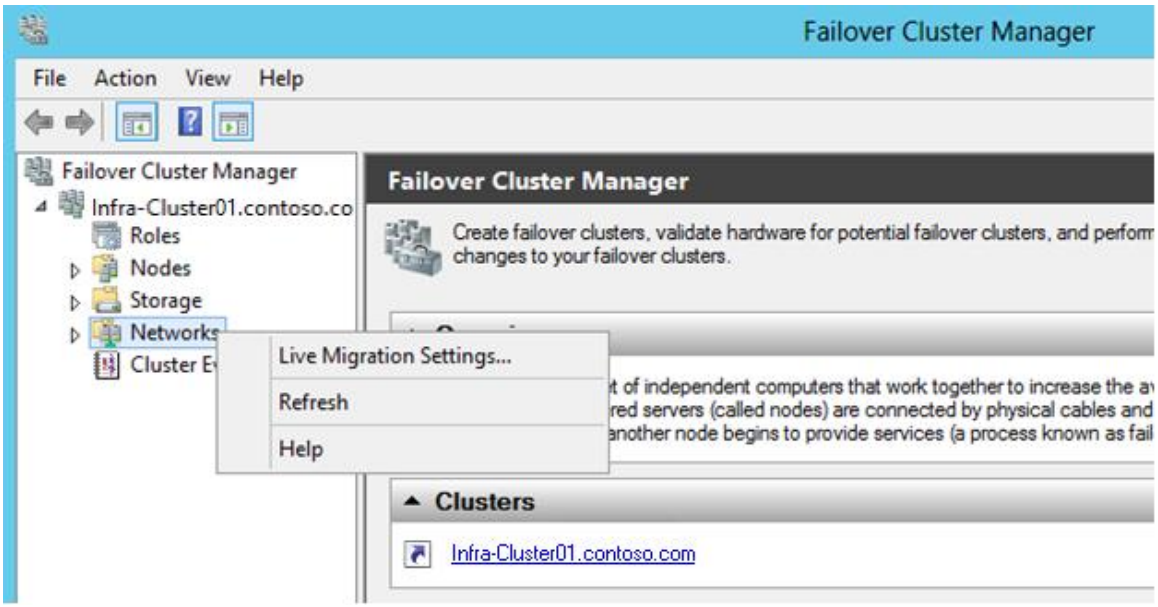
4. Designate the CSV network.

```
(Get-ClusterNetwork -Name CSV).Metric = 900
```

11.16 Configure Live Migration Network

One Server Only

1. Open Failover Cluster Manger from Server Manager select Tools -> Failover Cluster Manger.
2. Expand the Cluster tree on the left, and right click on Networks, select Live Migration Settings…



3. Deselect all but the LiveMigration network and click OK.

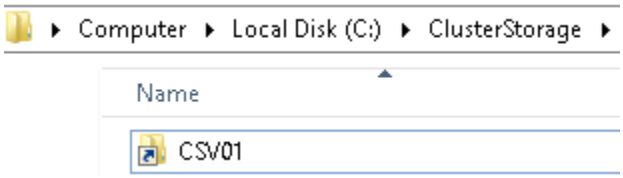
11.17 Create CSV LUN for VM Storage

One Server Only

1. Open a PowerShell prompt and move the Available Storage cluster group by running.

```
Move-ClusterGroup "Available Storage" -Node $env:COMPUTERNAME | Start-ClusterGroup
```

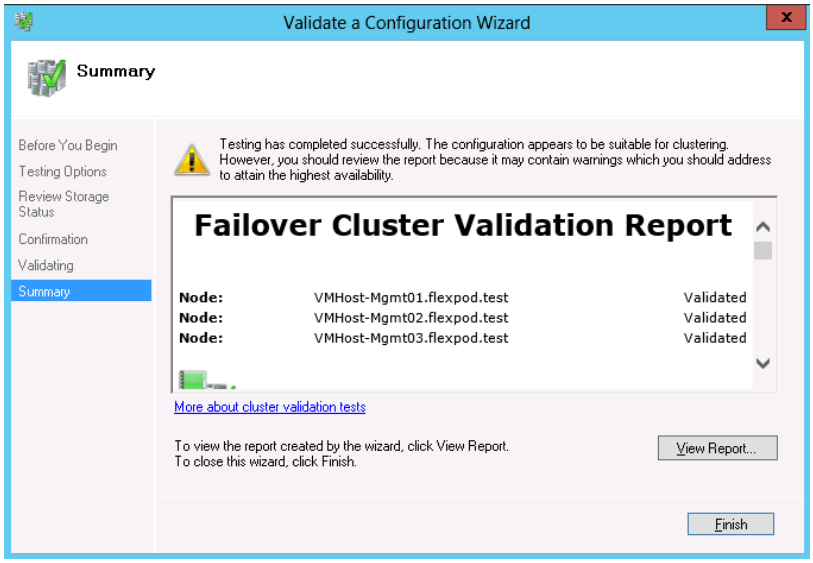
2. Open SnapDrive from the start screen to configure cluster storage.
3. From SnapDrive, Open the Server name, then Open the Disks Icon.
4. Right-click the Disks Icon and choose to **Create Disk**.
5. Type in the IP Address of the controller that contains the infra CSV Volume.
6. When connected, open the controller tree and select the infra CSV Volume.
7. Type in the name of the LUN in the LUN NAME box, click **Next**.
8. Select **Shared (Microsoft Cluster Services only)** and click **Next**.
9. Validate that all nodes of the cluster are shown and click **Next**.
10. Select **Do not assign a Drive letter or Volume Mount Point**, set the LUN size to be **1tb** and click **Next**.
11. Click **Next** through the Volume properties confirmation.
12. **Select the FCP WWPN** to Map the LUN to click **Next**.
13. Select **Automatic** igroup management and Click **Next**.
14. Select **Add to cluster shared volumes**, and click **Next**.
15. Click Finish.
16. In Cluster Manager, Click the Storage node in the tree view and select the disk object.
17. Right click the newly created CSV disk and select properties.
18. Change the name of the CSV disk to one you prefer.
19. Click okay to accept the new name.
20. Use Explore to rename the new CSV disk.



11.18 Validated the Cluster

Run the cluster validation wizard to verify that the cluster is operating correctly.

1. Open Failover Cluster Manager.
2. Click Validate Cluster… In the action pane.
3. Proceed through the wizard and select the option to run all tests.



4. Review and correct any failures that are listed in the validation report.

Note: The following warnings are expected to be reported by the validation wizard. These warnings can safely be disregarded.

Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node VMHost-Mgmt01.flexpod.test.

Test Disk 0 does not support SCSI-3 Persistent Reservations commands needed to support clustered Storage Pools. Some storage devices require specific firmware versions or settings to function properly with failover clusters. Please contact your storage administrator or storage vendor to check the configuration of the storage to allow it to function properly with failover clusters.

12 Create Gold Master Template VM

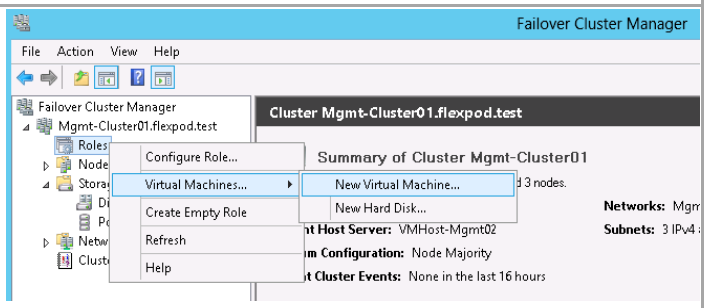
Instead of using Windows Deployment Services to automate the provisioning Hyper-V virtual machines, the deployment process of Virtual Machines takes advantage of the built-in cloning capabilities of the NetApp storage.

This section provides high-level walkthrough on how to create the Gold Master CSV LUN and Gold Master Virtual Machine for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

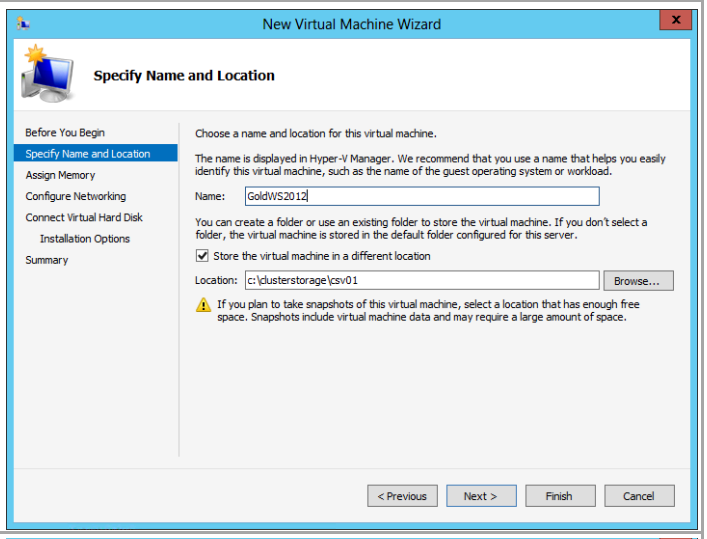
- NetApp PowerShell Toolkit 1.7 or higher installed on Hyper-V cluster nodes
- Access to Windows 2012 installation ISO image
- Cisco UCS B-Series Blade Server Software Bundle ISO

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

1. 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.

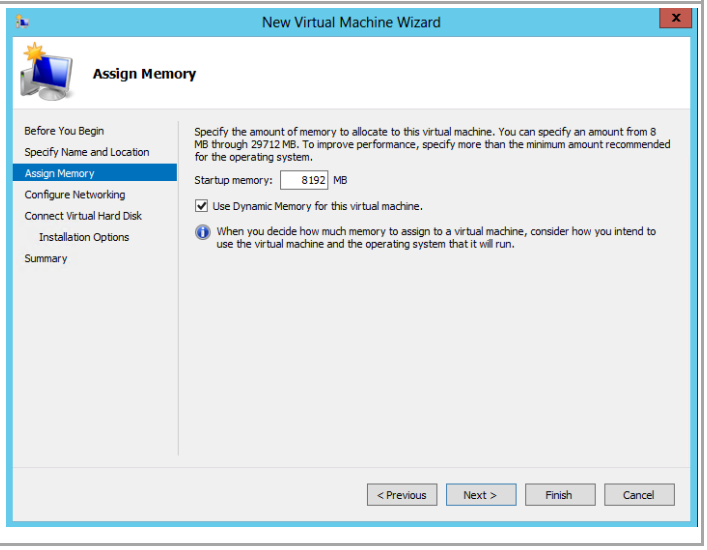


2. The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:
   a. **Name** – *specify the name of the virtual machine based on the naming conventions of your organization.*
3. Select the **Store the virtual machine in a different location** checkbox. In the **Location** text box, specify the location of the cluster shared volumes (CSV) on your fabric management host cluster.
4. Click **Next** to continue.

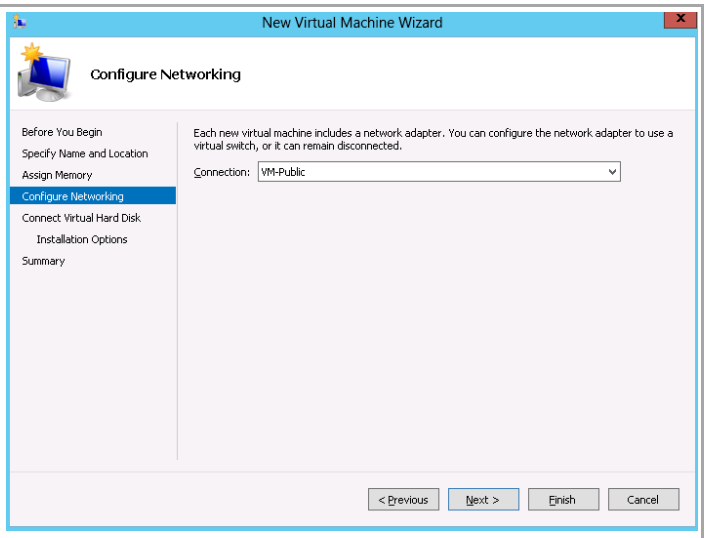


5. In the **Assign Memory** dialog, provide the following value:
   a. **Memory** – *specify the amount of memory in megabytes (MB) required for each virtual machine. Identify this value in the configuration table above.*
6. Click **Next** to continue.

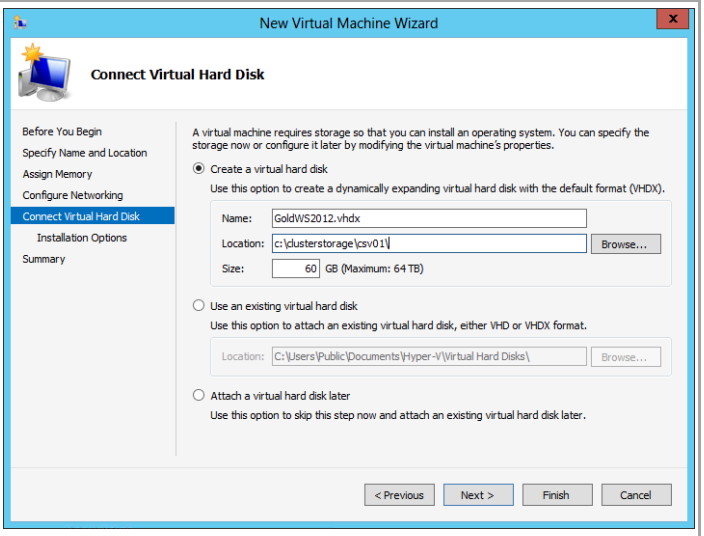
Note: for virtual memory, the products will post a warning if memory is below 8 GB and each virtual machine must have at least 2 GB of startup random access memory (RAM) if dynamic memory is enabled.



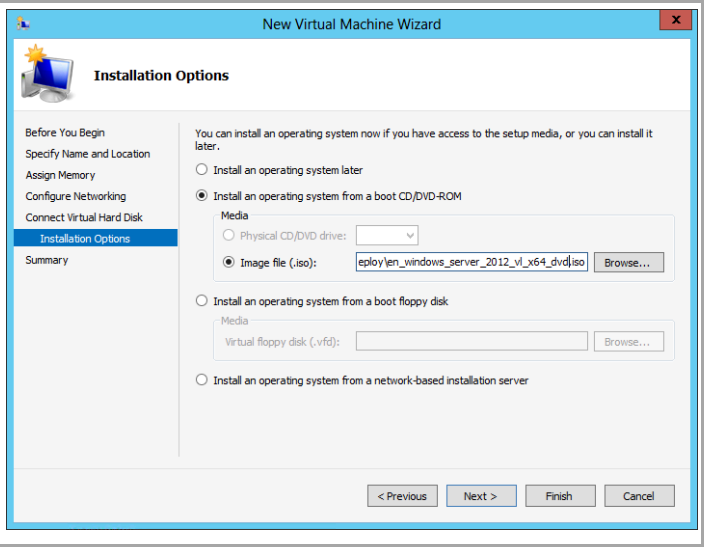
7. In the **Configure Networking** dialog, provide the following value:
    a. **Connection** – specify the VM-Public Virtual Switch network connection n the drop-down menu.
8. Click **Next** to continue.



9. In the **Connect Virtual Hard Disk** dialog, select the **Create a virtual hard disk** option and provide the following values:
    a. **Name** – *specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.*
    b. **Location** – *accept the default location of the CSV on your fabric management host cluster combined with the virtual machine name.*
    c. **Size** – *specify the size of the VHD (for operating system partitions this should be 60 GB).*
10. Click **Next** to continue.

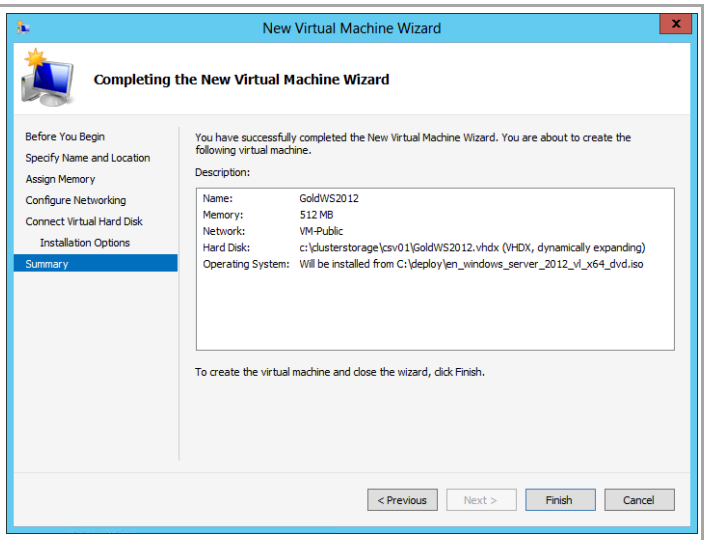


11. In the **Installation Options** dialog, select the **Install an operating system from a boot CD/DVD-ROM** option and **Image file (.iso):** Specify the path the to Windows Server 2012 iso.
12. Click **Next** to continue.

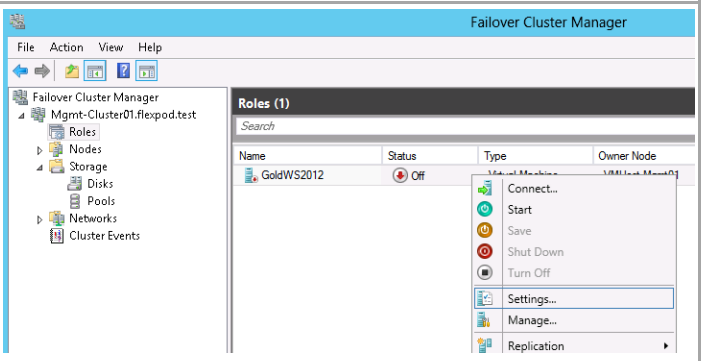


13. The **Completing the New Virtual Machine Wizard** dialog will display the selections made during the wizard. Click **Finish** to create the virtual machine based on the options selected.

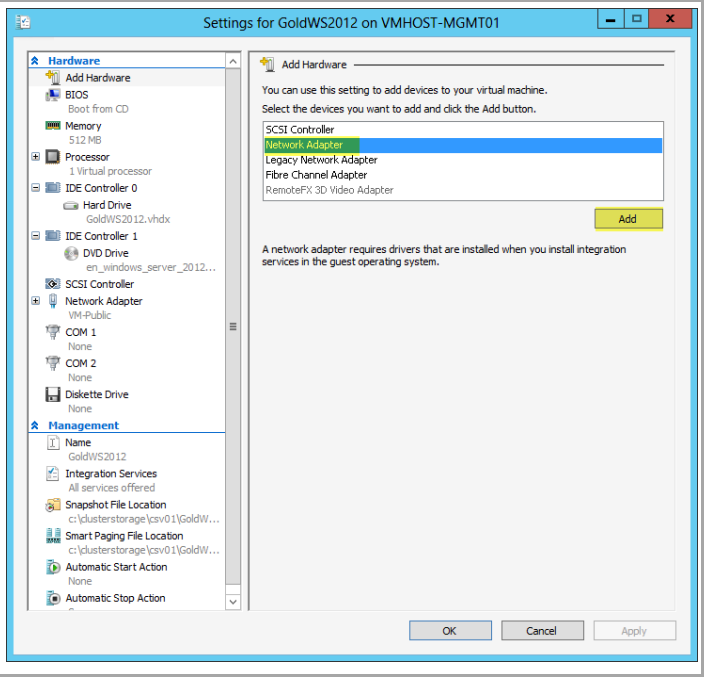
Note: this operation must be completed for each fabric management virtual machine.



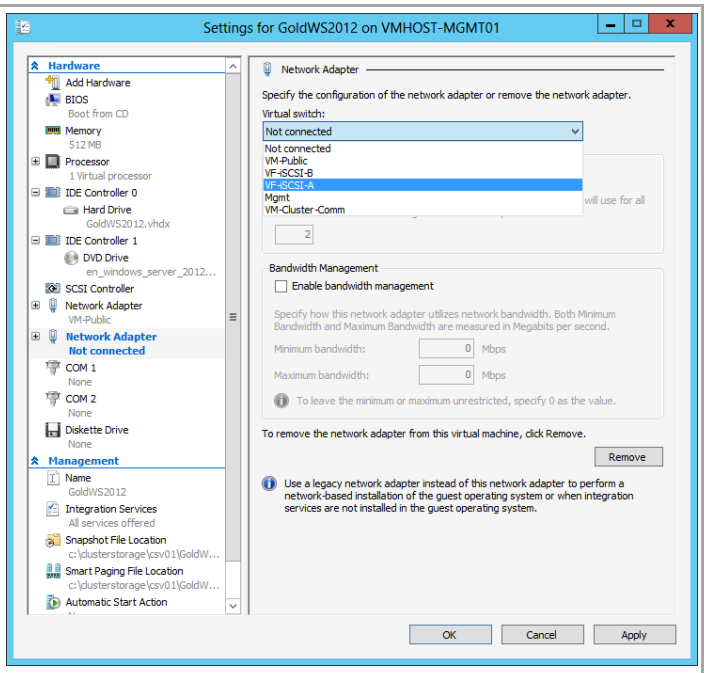
14. Using Failover Cluster Manager, right click the GoldWS2012 virtual machine and select Settings. The virtual machine needs to be in an off state.



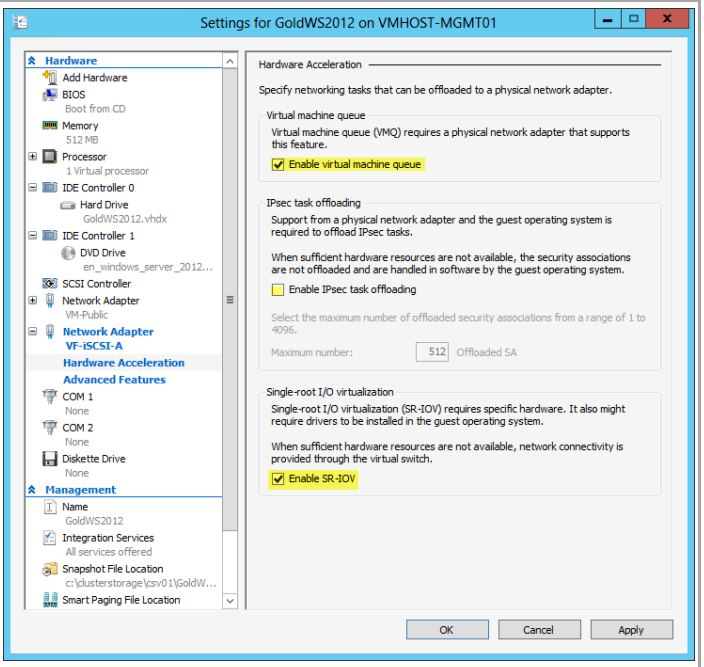
15. Select **Add Hardware** in the hardware list. Select **Network Adapter** in the Add Hardware list and click **Add**.



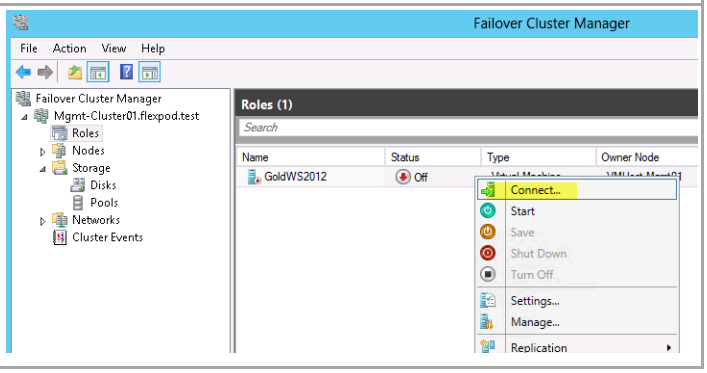
16. Select **VF-iSCSI-A** in the virtual switch dropdown box. Leave the **Enable Virtual LAN identification** checkbox **unchecked**.



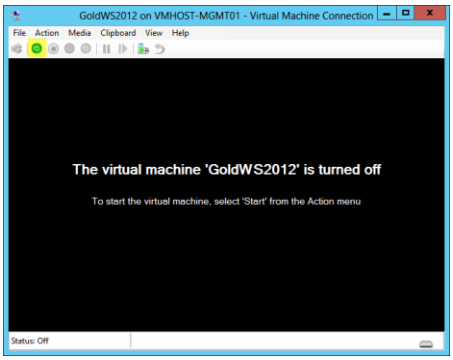
17. **Expand** the network adapter **VF-iSCSI-A** in the left pane and select **Hardware Acceleration**.
18. Uncheck the checkbox Enable IPSec Task offloading
19. Check the checkbox Enable SR-IOV
20. Click **OK** button.

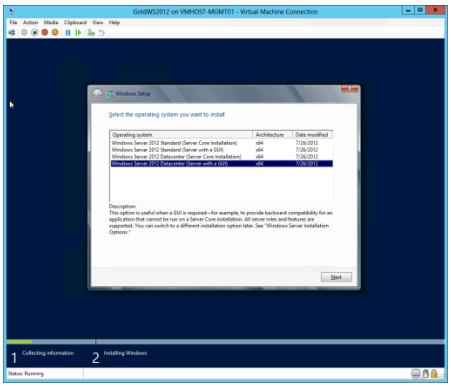


21. Back in Failover Cluster Manager right click on GoldWS2012 and select **Connect**.



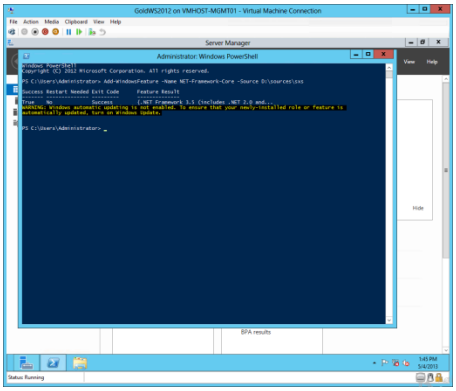
22. Click the **PowerON** Button to power on the VM and boot into the Windows Server 2012 Installer.
23. After the installer is finished loading, Enter the relevant region information and click **Next**.
24. Click Install now.
25. Enter the Product Key and click **Next**.
26. Select Windows Server 2012 Datacenter (Server with a GUI) and click Next.
27. You may optionally remove the GUI after the Hyper-V cluster is operational.
28. After reviewing the EULA, Check the I accept the license terms, and click Next.
29. Select Custom: Install Windows only (advanced).
30. Select the Drive 0 as the installation location for Windows. Click **Next** to continue with the install.
31. When Windows is finished installing enter an Administrator password on the settings page and click Finish.



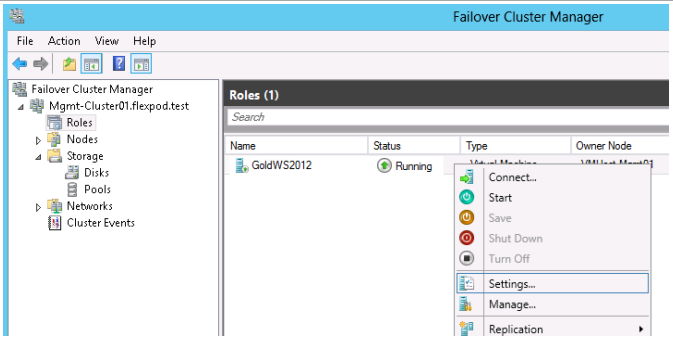


32. Log in to the Server console and launch a PowerShell Prompt. Install .Net 3.5 by running the following command:

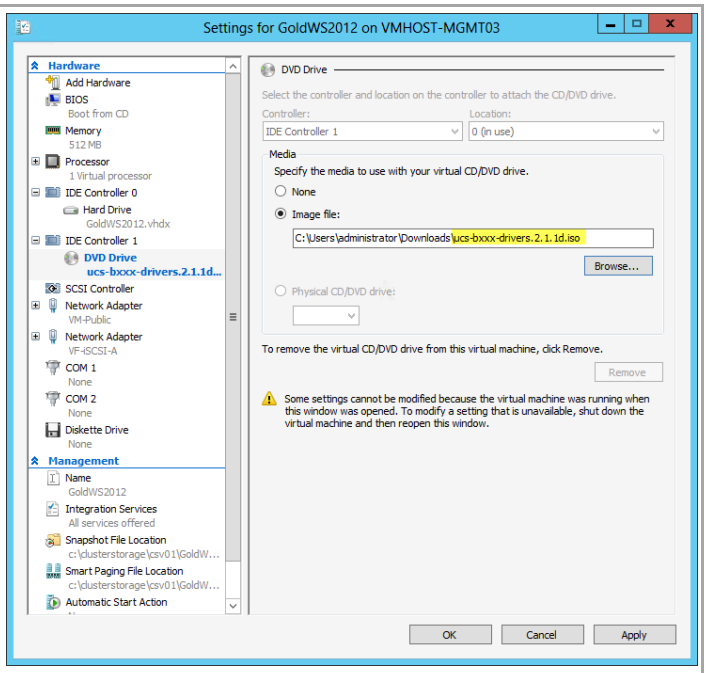
```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```



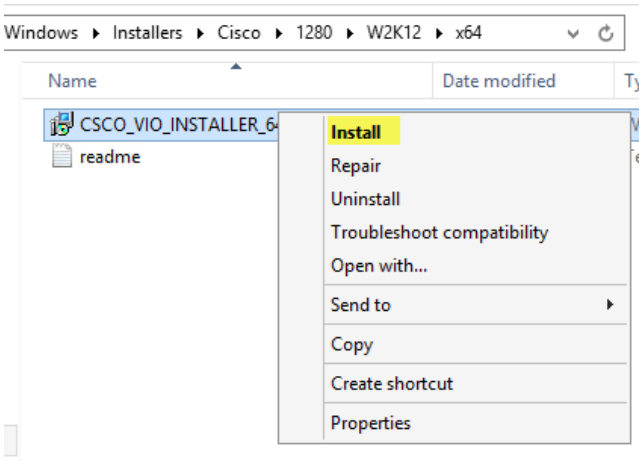
33. Using Failover Cluster Manager, right-click the GoldWS2012 virtual machine and select Settings.



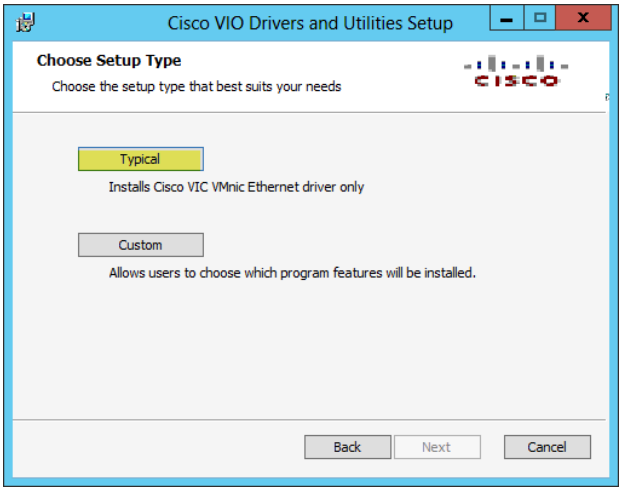
34. Attach the Cisco UCS B-Series Blade Server Software Bundle ISO to the VM.



35. In the GoldMaster VM run the Cisco VIO installer D:\Windows\Installers\Cisco\1280\W2K12\x64\CSCO_VIO_INSTALLER_64_*version*.msi

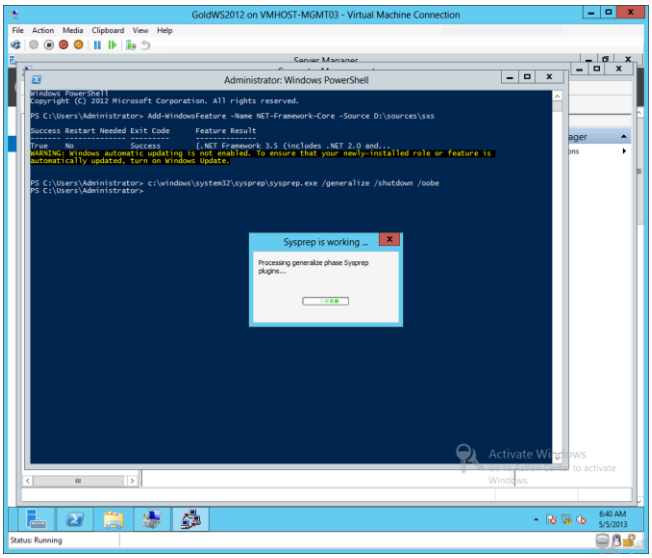


36. Install the Cisco VM FEX VIO Driver:
37. From the Welcome screen click **Next**.
38. Accept the EULA, and Click Next.
39. Select a **Typical** Install.
40. Click **Install**.
41. When the installer finished click **Close**.



42. Back in the powershell prompt run the following command to sysprep the OS.

c:\windows\system32\sysprep\sysprep.exe /generalize /shutdown /oobe



13 Deploy Fabric Management Virtual Machines

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 three-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.

Component Roles	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
SQL Server Cluster Node 1	8	16	60
SQL Server Cluster Node 2	8	16	60
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 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 portal	8	16	60
Service Manager Data Warehouse	8	16	60
Infrastructure (SMI-S Age)	2	4	60
Cisco Nexus 1000V VMS 1	1	4	4
Cisco Nexus 1000V VMS 2	1	4	4
Totals	**76**	**164 GB**	**788 GB**

The Fabric Managmetn virtual machines can be deployed either by hand through Failover cluster manager or using the supplied PowerShell script. The automated manner is recommended, however may require modification if the deployment does not match the configuration cover in this deployment guide.

13.1 Automated Creation and Configuration

The following PowerShell script will create all the VM's for the Fabric Management cluster using the assumptions of this Deployment Guide. To run, paste into an elevated PowerShell prompt with an account that is administrator on the storage controller.

```
(@{"Name"="SCSQL01";"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCSQL02" ;"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCVMM01" ;"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCVMM02" ;"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCAC01"  ;"CPU"="4";"memory"="8" ;"Cluster"=$false},
@{"Name"="SCOM01"  ;"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCOM02"  ;"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCOR01"  ;"CPU"="4";"memory"="8" ;"Cluster"=$false},
@{"Name"="SCOR02"  ;"CPU"="4";"memory"="8" ;"Cluster"=$false},
@{"Name"="SCSM01"  ;"CPU"="4";"memory"="16";"Cluster"=$false},
@{"Name"="SCSM02"  ;"CPU"="4";"memory"="16";"Cluster"=$false},
@{"Name"="SCSM03"  ;"CPU"="8";"memory"="16";"Cluster"=$false},
```

```
@{"Name"="SCInfra" ;"CPU"="2";"memory"="4";"Cluster"=$false}) | ForEach-Object {
    $Name,$mem,$cpu = $_.Name, $(([int]$_.memory) * 1GB),$_.cpu
    # Change this to the name of your CSV.
    $CSV = 'CSV01'
    # Use FlexClone to rapidy provition the New VHDX.
    Try
    {
      Copy-NaHostFile -SourceFile "C:\ClusterStorage\${CSV}\GoldWS2012.vhdx" `
            -DestinationFile "C:\ClusterStorage\${CSV}\${name}.vhdx"
    }
    catch
    {
        Write-Warning "Sis-Clone Error:$($_.exception.Message);reverting to file copy"
        Copy-Item -Path "C:\ClusterStorage\${CSV}\GoldWS2012.vhdx"
             -DestinationFile "C:\ClusterStorage\${CSV}\${name}.vhdx"
    }
    # Create the new VM
    $VM = New-VM -BootDevice ide -SwitchName VM-Database MF-Public `
     -Path "C:\ClusterStorage\${CSV}\" -Name $name `
     -VHDPath "C:\ClusterStorage\${CSV}\${name}.vhdx"
    # Set the VMs processors
    $VM | Set-VMProcessor -Count $CPU
    # Set the VMs Memory
    $VM | Set-VMMemory -DynamicMemoryEnabled $true -StartupBytes $mem -MinimumBytes
($mem/2)
    # Set the VLAN for the vNIC, comment out or change VLAN ID to match your deployment.
    $VM | Get-VMNetworkAdapter | Set-VMNetworkAdapterVlan -VlanId 1001 -Access
    # IF a cluster VM add CLuster-COmm and VM-Fex Nics
    If ($_.Cluster)
    {
        $VM | Add-VMNetworkAdapter -SwitchName VM-Cluster-Comm
        $VM | Add-VMNetworkAdapter -SwitchName VF-iSCSI-A |
            Set-VMNetworkAdapter -IovQueuePairsRequested 1 -IovWeight 100 -IPsecOffload 0
        $VM | Add-VMNetworkAdapter -SwitchName VF-iSCSI-B |
            Set-VMNetworkAdapter -IovQueuePairsRequested 1 -IovWeight 100 -IPsecOffload 0
    }
    # Add VM to the cluster
    Add-ClusterVirtualMachineRole -Name $Name -VMName $Name
}

# Create the Cisco Nexus 1000v VSM
"N1KV-VSM01", "N1KV-VSM01" | ForEach-Object {
    $vm = New-VM -name $_ -BootDevice ide -SwitchName Mgmt -MemoryStartupBytes 2gb `
        -Path "C:\ClusterStorage\${CSV}\" -NewVHDSizeBytes 4gb `
        -NewVHDPath "C:\ClusterStorage\${CSV}\$_.vhdx"
    $vm | Add-VMNetworkAdapter -SwitchName Mgmt
    $vm | Add-VMNetworkAdapter -SwitchName Mgmt
    Add-ClusterVirtualMachineRole -Name $_ -VMName $_
}
```

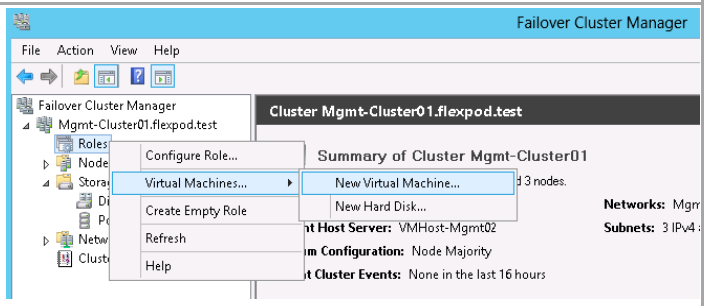
13.2 Manual Creation and Configuration

Create Fabric Management Virtual Guests

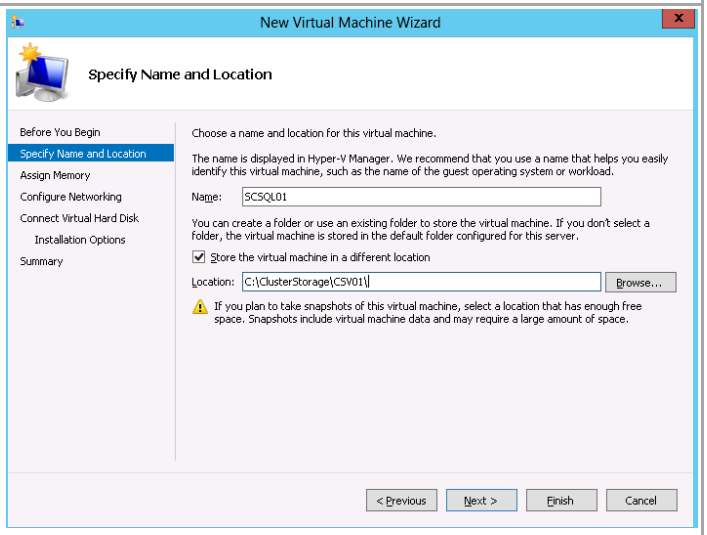
Windows Failover Cluster Manager is used to create the fabric management virtual machines. The installation of the required Windows operating systems can utilize existing customer automated deployment Solutions or a manual build of each virtual machine.

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

1. 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.

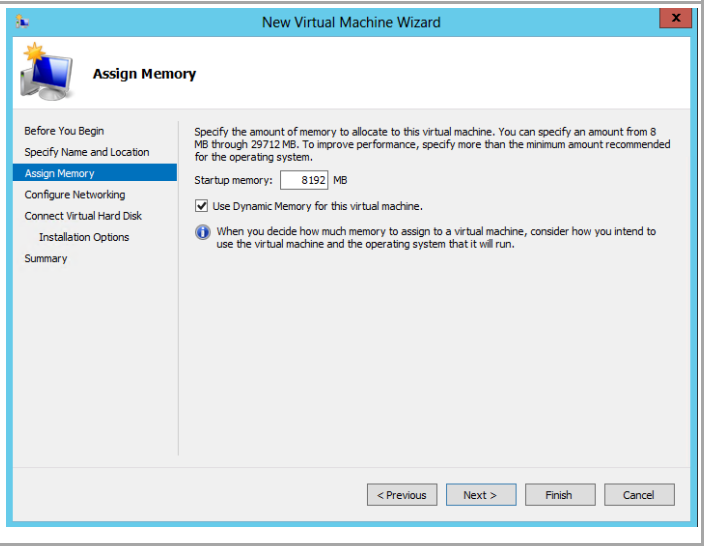


2. The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following value:
   a. **Name** – *specify the name of the virtual machine based on the naming conventions of your organization.*
3. Select the **Store the virtual machine in a different location** checkbox. In the **Location** text box, specify the location of the cluster shared volumes (CSV) on your fabric management host cluster.
4. Click **Next** to continue.

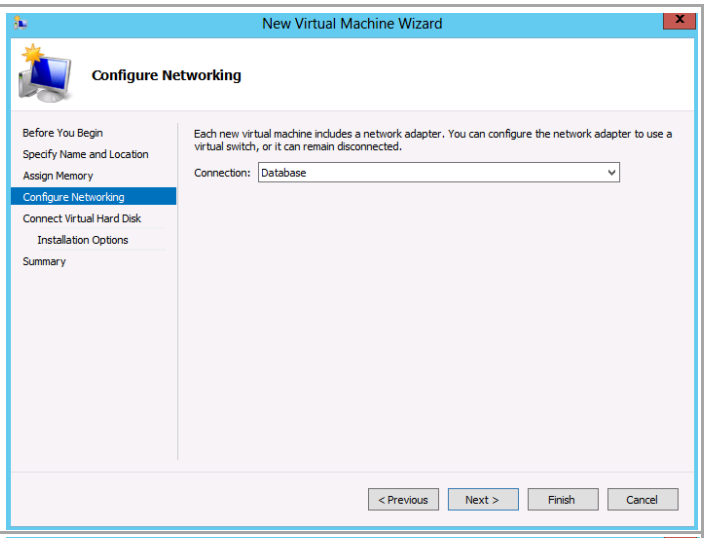


5. In the **Assign Memory** dialog, provide the following value:
   a. **Memory** – *specify the amount of memory in megabytes (MB) required for each virtual machine. Identify this value in the configuration table above.*
6. Click **Next** to continue.

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.

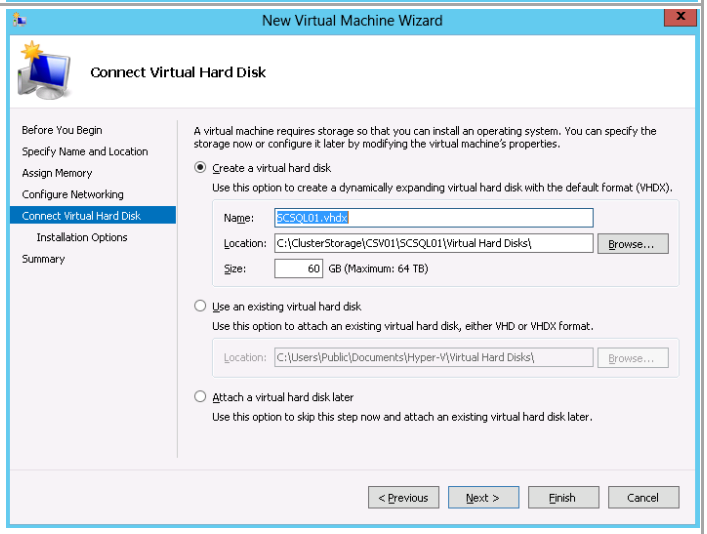


7. In the **Configure Networking** dialog, provide the following value:
    a. **Connection** – specify the Database Virtual Switch network connection n the drop-down menu.
8. Click **Next** to continue.

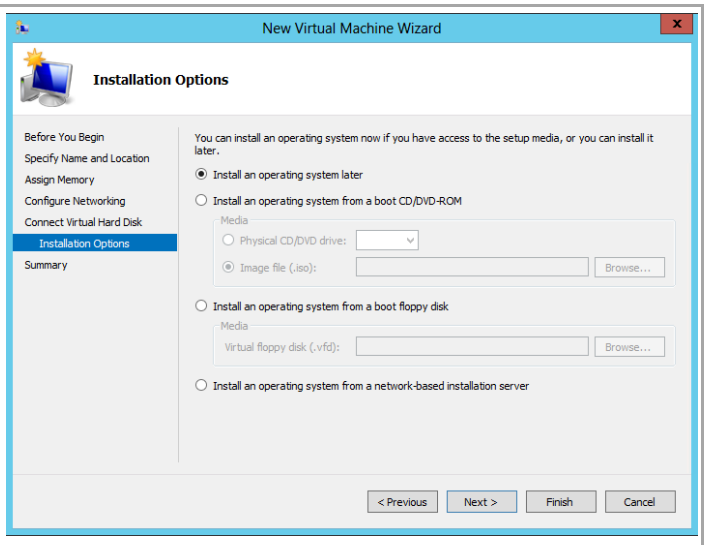


9. In the **Connect Virtual Hard Disk** dialog, select the **Create a virtual hard disk** option and provide the following values:
    a. **Name** – *specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.*
    b. **Location** – *accept the default location of the CSV on your fabric management host cluster combined with the virtual machine name.*
    c. **Size** – *specify the size of the VHD (for operating system partitions this should be 60 GB).*
10. Click **Next** to continue.

Note: Absent any automated imaging process for the new VMs, a VHD (with Windows Server 2008 R2 or 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.

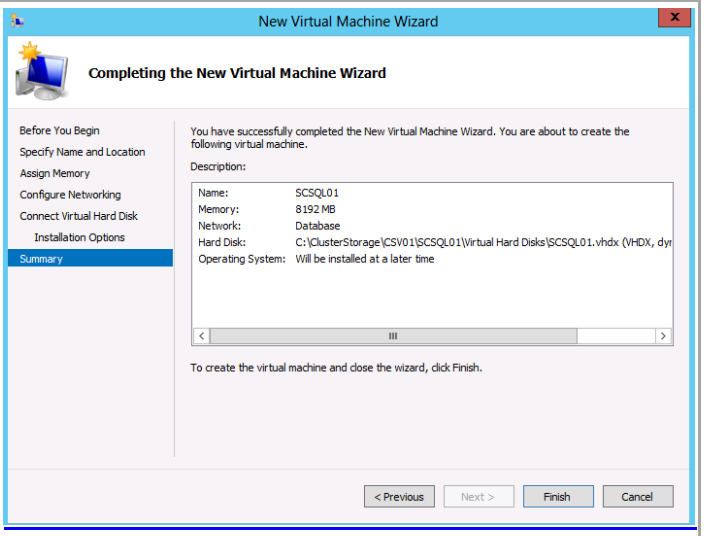


11. In the **Installation Options** dialog, select the **Install an operating system later** option and click **Next** to continue.

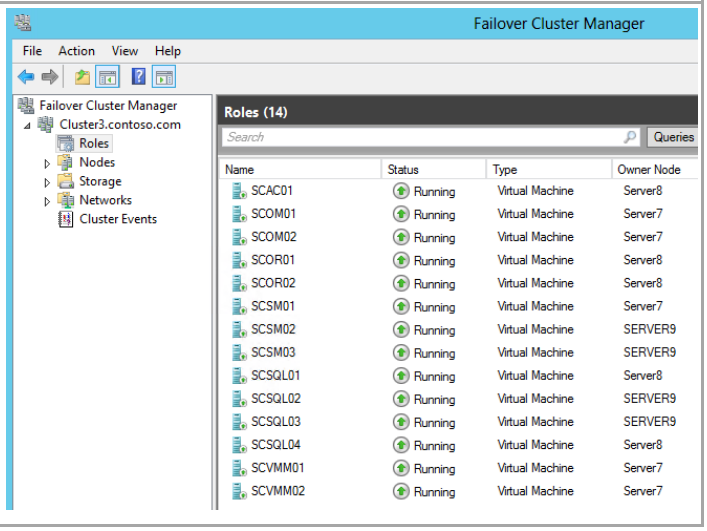


12. The **Completing the New Virtual Machine Wizard** dialog will display the selections made during the wizard. Click **Finish** to create the virtual machine based on the options selected.

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



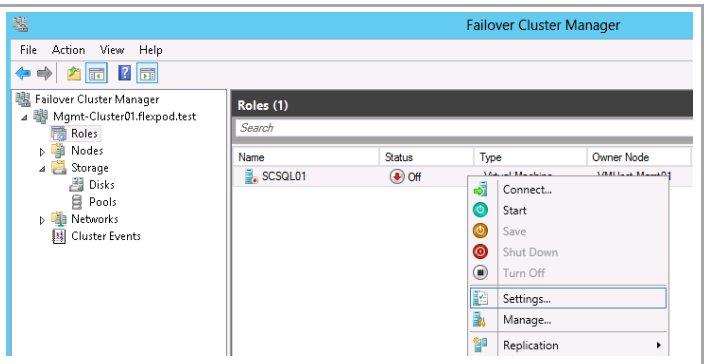
13. After completion, the virtual machines will be available for management in the **Services and applications** node of the **Failover Cluster Manager**.



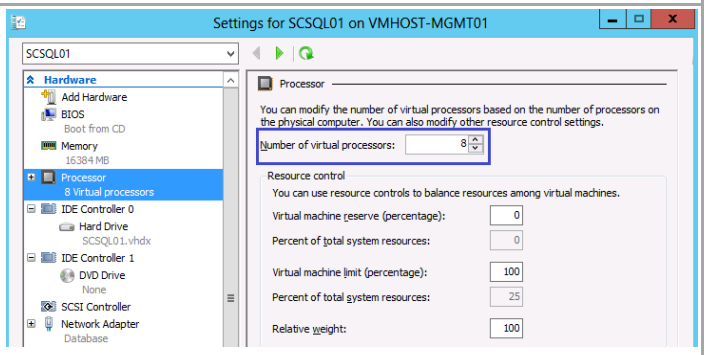
Modify Virtual Machine Settings

Each virtual machine is configured with one virtual processor and one network adapter. The virtual machine configuration must be updated to configure the appropriate number of virtual processors.

1. Using Failover Cluster Manager, right click the SQL Server virtual machine and select Settings. The virtual machine needs to be in an off state.

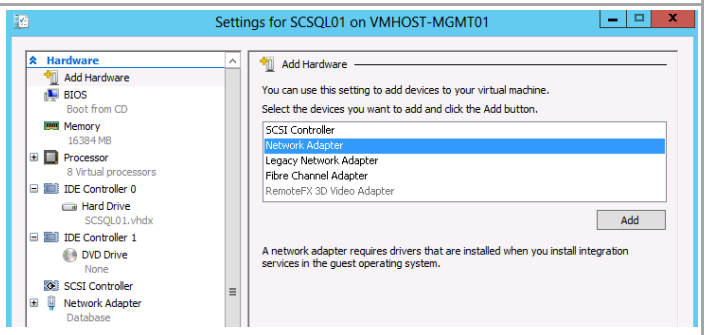


2. Select **Processor** in the hardware list and set the appropriate number of processors for the specific virtual machine role.

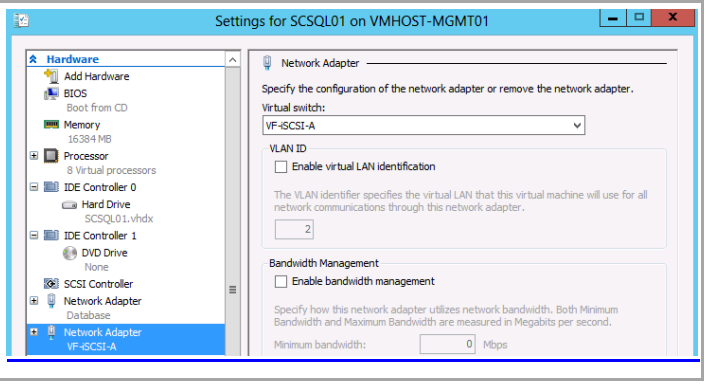


3. For virtual machines the SQL Server virtual machines, select **Add Hardware** in the hardware list. Select **Network Adapter** in the Add Hardware list and click **Add**.

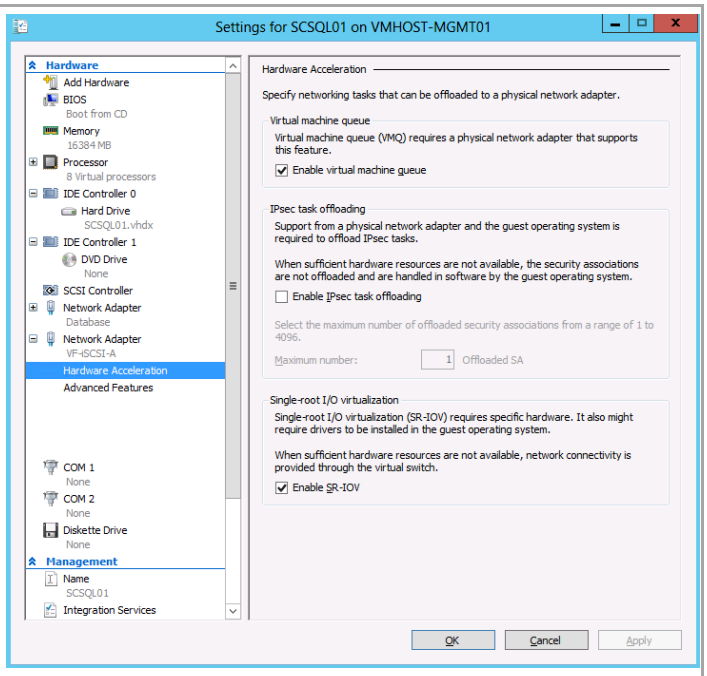
Note: These additional adapters must be added to the SQL Server virtual machines for use as iSCSI initiators.



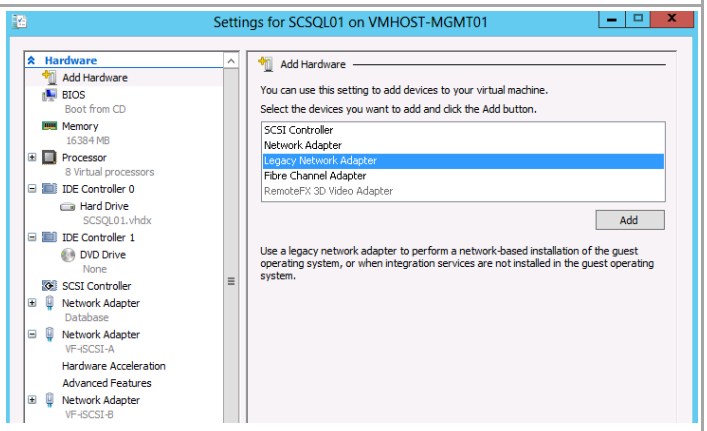
4. Select **VF-iSCSI-A** in the virtual switch dropdown box. Leave the **Enable Virtual LAN identification** checkbox **unchecked**.



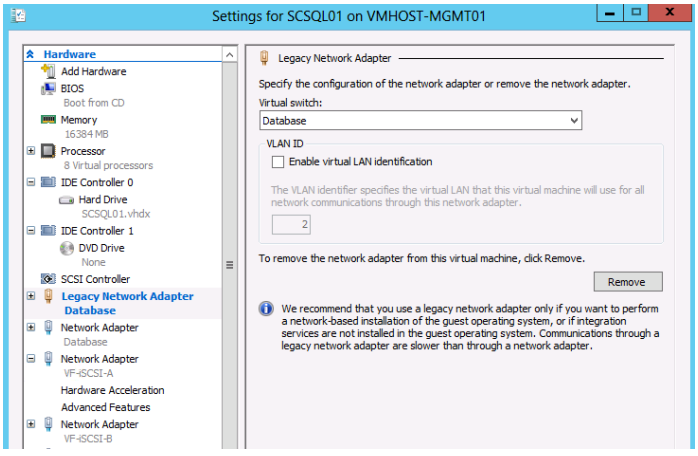
5. Expand the network adapter VF-iSCSI-A in the left pane and select Hardware Acceleration. Check the checkbox Enable SR-IOV and uncheck the checkbox Enable IPSec Task offloading. Click Apply button.
6. Repeat the procedure to add and configure the second network adapter for the **VF-iSCSI-B** network.



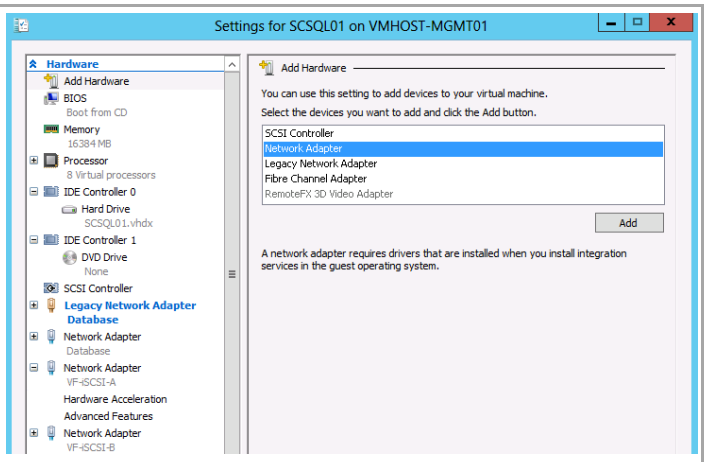
7. Virtual machines that use PXE boot to install Windows need to have a Legacy Network Adapter added. Select **Add Hardware** in the hardware list. Select **Legacy Network Adapter** in the Add Hardware list and click **Add**.



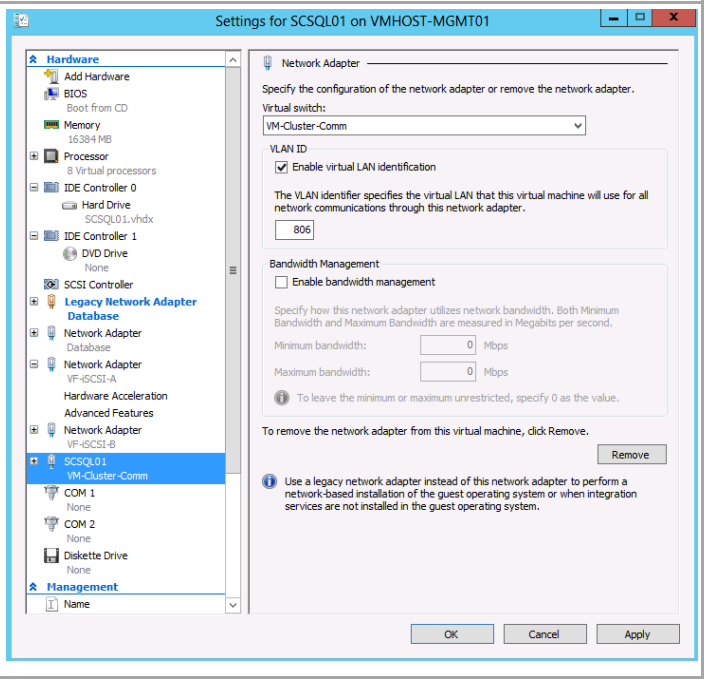
8. Select **VM-Public** in the virtual switch dropdown box. Leave the **Enable Virtual LAN identification** checkbox **unchecked.**
9. The legacy network adapter can be removed from the virtual machine settings after the PXE boot Windows installation completes.



10. For virtual machines the SQL Server virtual machines, select **Add Hardware** in the hardware list. Select **Network Adapter** in the Add Hardware list and click **Add**.
11. These additional adapters must be added to the SQL Server virtual machines for use as and additional cluster communication network path.



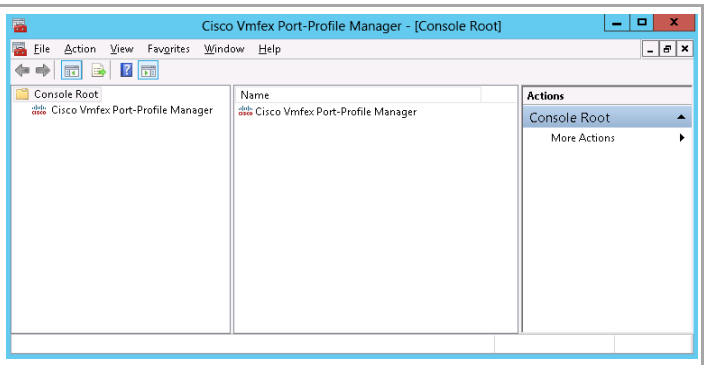
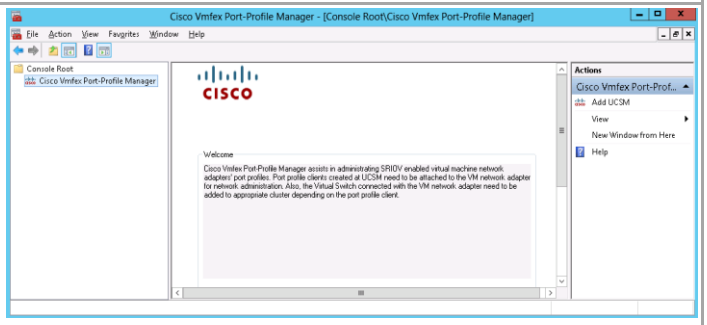
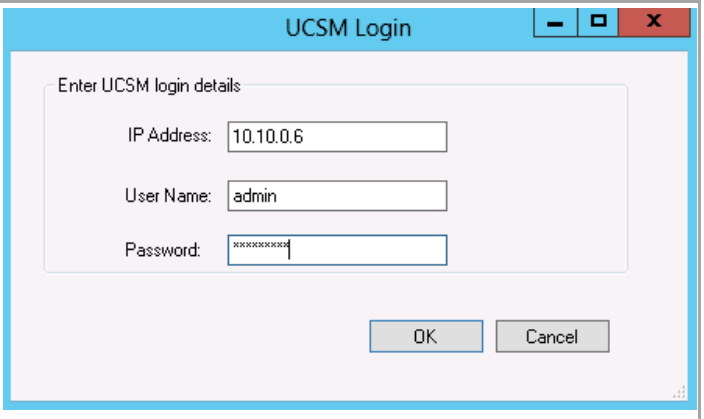
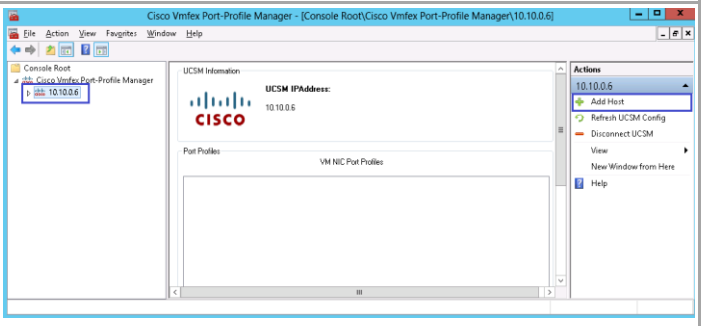
12. Select **VM-Cluster-Comm** in the virtual switch dropdown box. **Check** the **Enable Virtual LAN identification** checkbox. Set the VLAN ID for this network. Click OK to complete close the window.

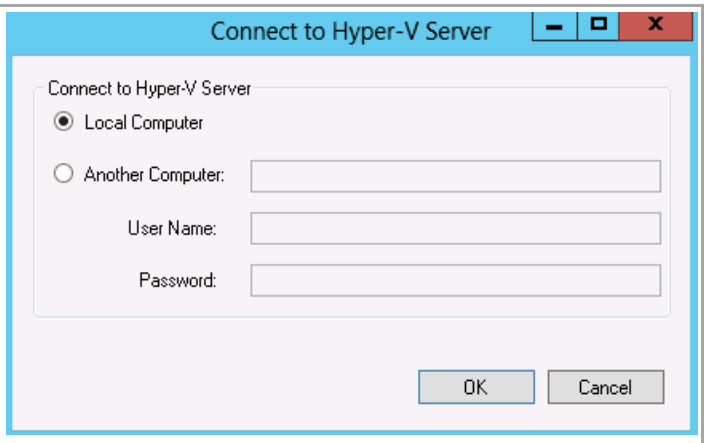
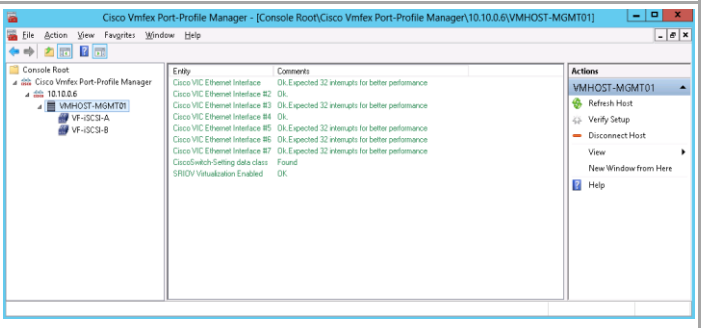
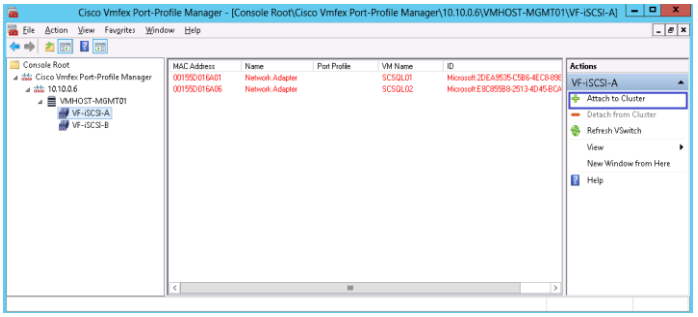


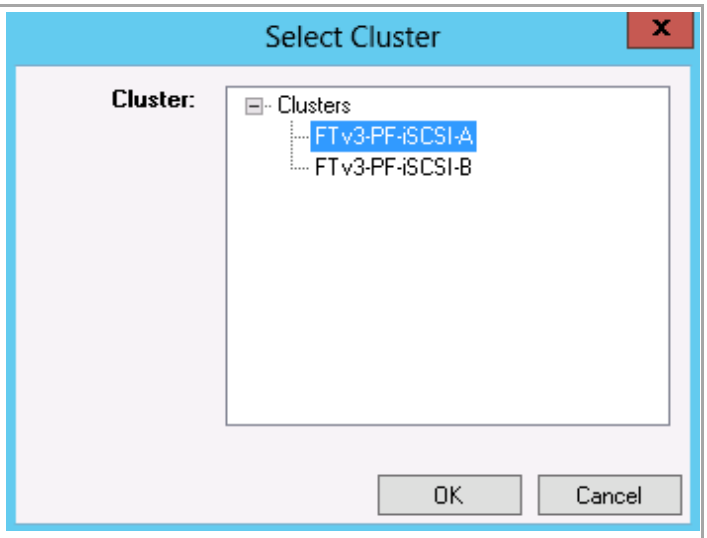
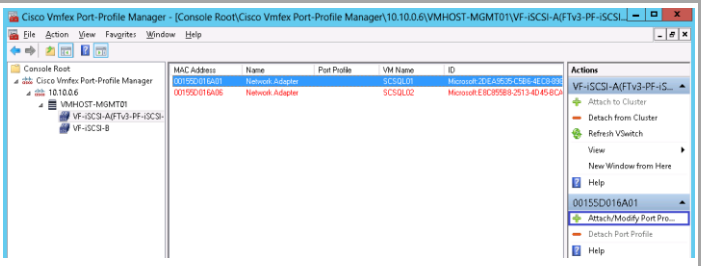
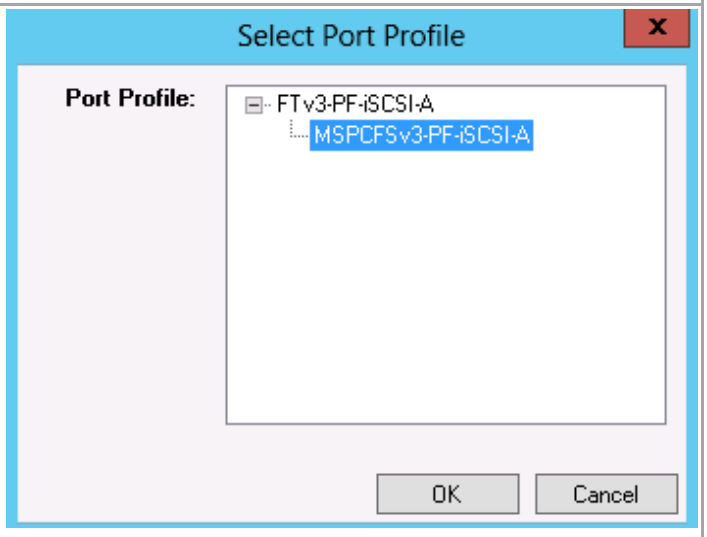
Install Windows Server on the Virtual Machines

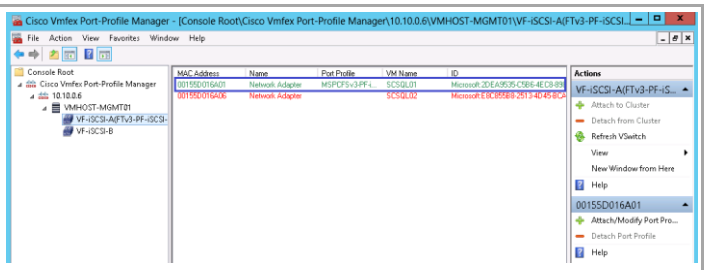
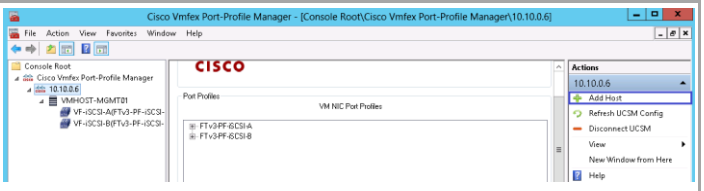
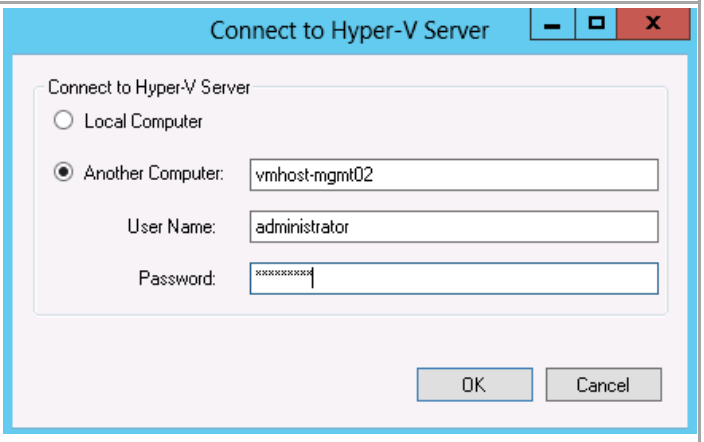
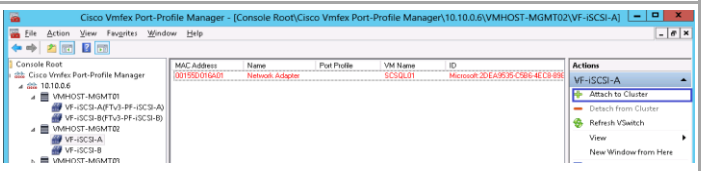
Windows Server can now be installed into the virtual machines. Windows can be installed using an .ISO file with the installation image or from a WDS server using PXE boot.

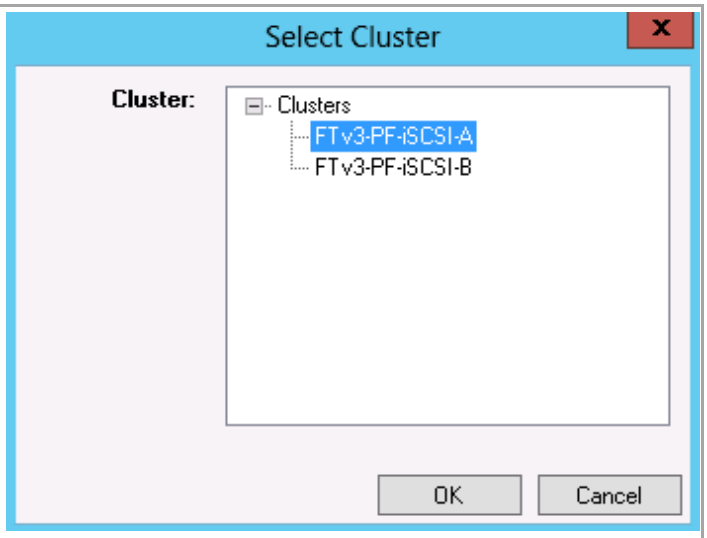
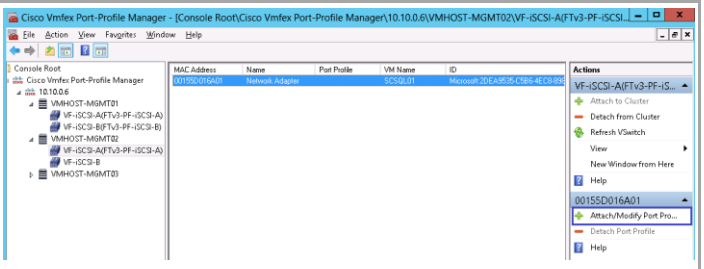
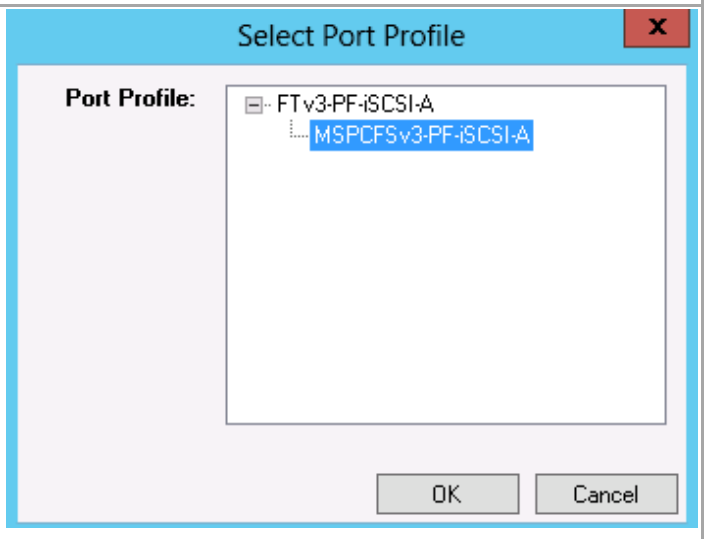
13.3 Attach VM FEX Port Profile to the Clustered Virtual Machines

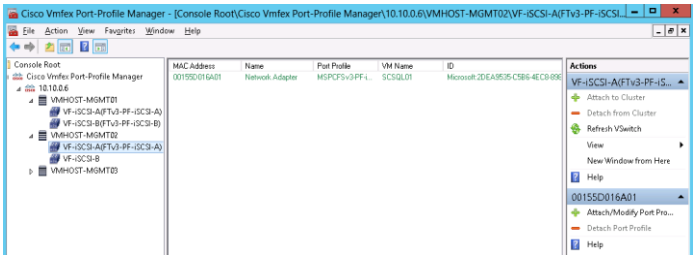
1. On the host that owns the SQL, and VMM virtual machines, run the Cisco VM-FEX Port – Profile Manager Utility located at: C:\Program Files\Cisco Systems\VIO Software\Utilities\Ethernet Utilities\Vmfex Utilities\Snapin.	
2. Select CiscoVMFEX Port-Profile Manger in the left tree view and click Add UCSM in the action pane.	
3. Enter the Cisco UCS Manager IP address, User Name and Password. Click OK.	
4. Expand Vmfex Port Profile Manager in the left tree pain and click the Cisco UCS Manager instance added in the previous step. Click Add Host in right action pane.	

5. Select Local Computer and Click OK.	
6. The local host is added in the tree view pane on the left. Select the host in the right tree view pane to view the status in the middle pane.	
7. Select the network adapter in the left tree view pane. The adapter entry in the middle pane indicates in red text indicates that this adapter is not been attached to a port profile. Click **Attach to Cluster** in the right action pane.	

8. Select the logical switch for the corresponding adapter VF-iSCSI-A and click OK.	
9. Click the device in the middle pane and select Attach/Modify Port Profile in the action pane.	
10. Select the logical switch for the corresponding adapter VF-iSCSI-A and click OK.	

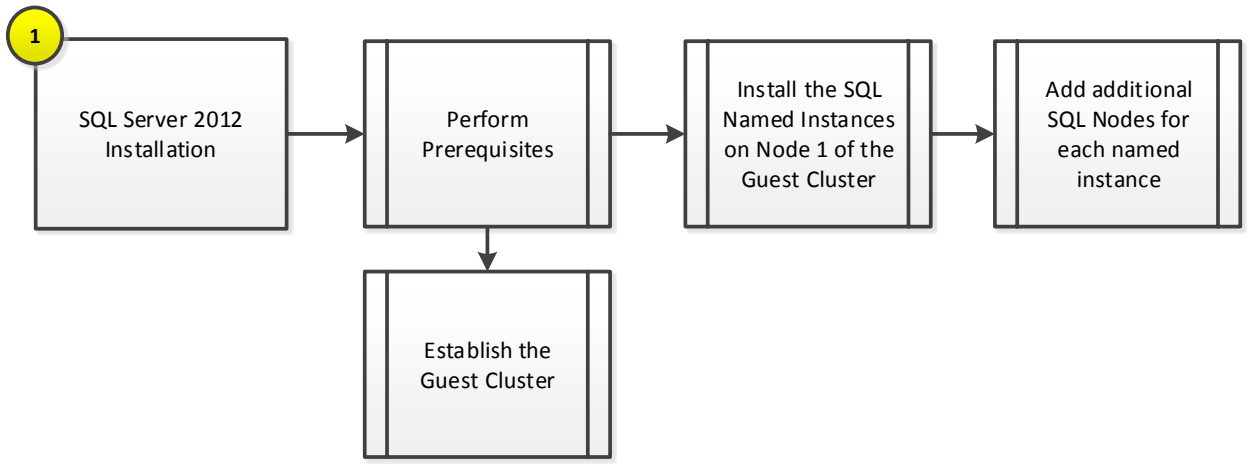
11. Check the middle pane to verify the adapter with the attached port profile in green text. 12. Repeat these steps for the second port profile VF-iSCSI-B. Make sure you connect the second port profile to the same virtual machine as the first port profile.	
13. Using Failover Cluster Manager, move the SQL Server virtual machine to vmhost-mgmt02.	
14. In the Vmfex Port Profile Manager click the Cisco UCS Manager instance added in the previous step. Click Add Host in right action pane.	
15. Select Another Computer. Enter the host name, user name, and password for the second host. Click OK. 16. Repeat this procedure to add the third host vmhost-mgmt03.	
17. Select the network adapter in the left tree view pane. The adapter entry in the middle pane indicates in red text indicates that this adapter is not been attached to a port profile. Click **Attach to Cluster** in the right action pane.	

18. Select the logical switch for the corresponding adapter VF-iSCSI-A and click OK.	
19. Click the device in the middle pane and select Attach/Modify Port Profile in the action pane.	
20. Select the logical switch for the corresponding adapter VF-iSCSI-A and click OK.	

21. Check the middle pane to verify the adapter with the attached port profile in green text. 22. Repeat these steps for the second port profile VF-iSCSI-B. Make sure you connect the second port profile to the same virtual machine as the first port profile.	
23. Using Failover Cluster Manager, move the SQL Server virtual machine to vmhost-mgmt03 and repeat the port profile connection proceedure.	

14 SQL Server 2012 Failover Cluster Installation

The SQL Server 2012 failover cluster installation process includes the following high-level steps:



14.1 Overview

There is a decision point in the SQL Server architecture that must occur prior to deployment. There are multiple valid SQL Server deployment scenarios, as follows:

- Architecture
  - Physical servers
  - Virtual machines
- Storage
  - Fibre Channel (not feasible for virtual machines in guest failover cluster)
  - iSCSI
  - SAS (not feasible for virtual machines in guest failover cluster)

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.[1] The following assumptions are made prior to installation:

1. Two to four base virtual machines running Windows Server 2012 have been provisioned for SQL Server.
   a. 15 iSCSI LUNs have been assigned to the virtual machine guests.
   b. One LUN – quorum (1 GB)
2. 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

[1] The SQL Server 2012 builds that were released after SQL Server 2012 was released - http://support.microsoft.com/kb/2692828.

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 11 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

14.2 Pre-Requisites

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

[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

Accounts

Verify that the following accounts have been created:

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

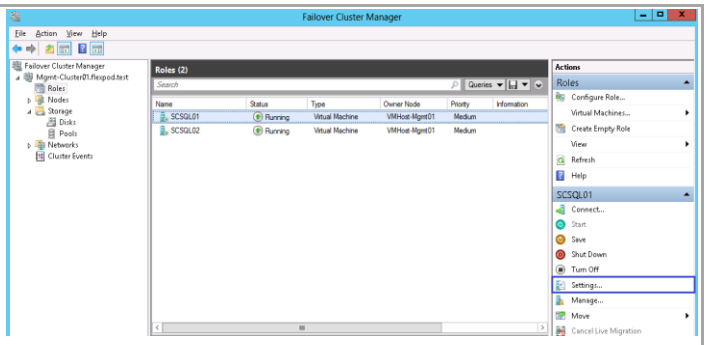
Groups

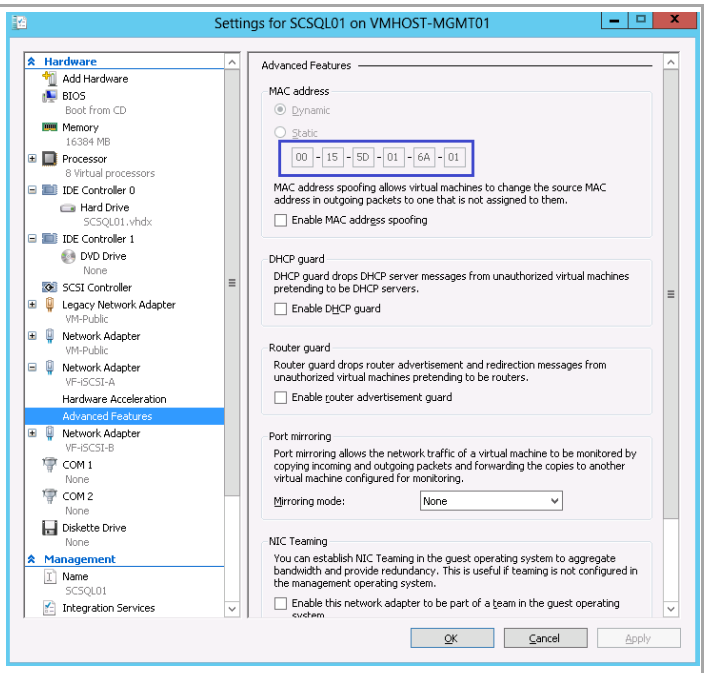
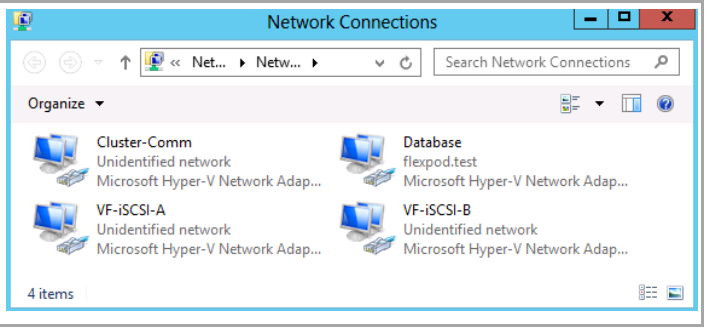
Verify that the following security groups have been created:

Security group name	Group scope	Members
<DOMAIN>\FT-SQL-Admins	Universal	All SQL Server Administrators for the fabric management Solution.

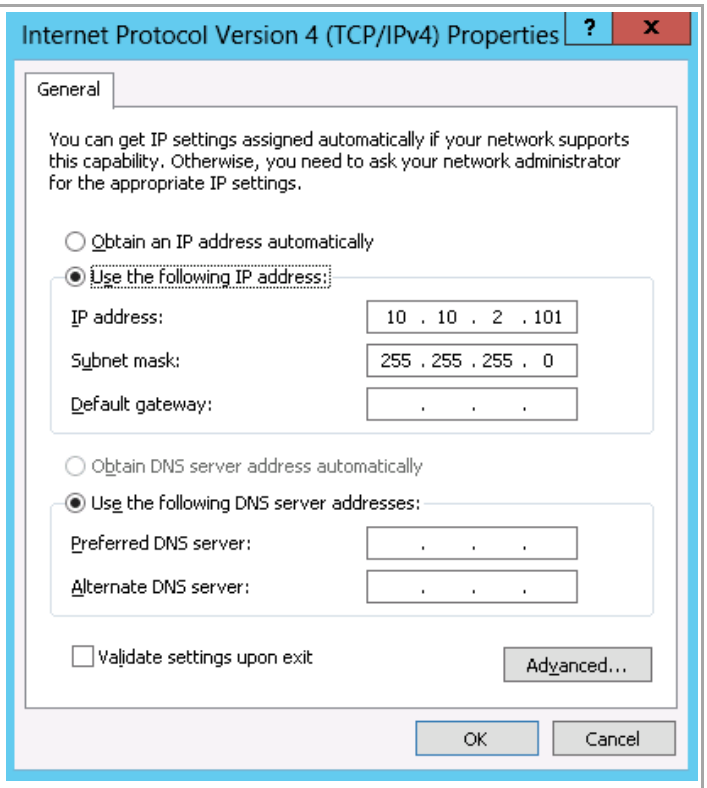
14.3 Configure the Network Interfaces for the SQL Server Virtual Machine

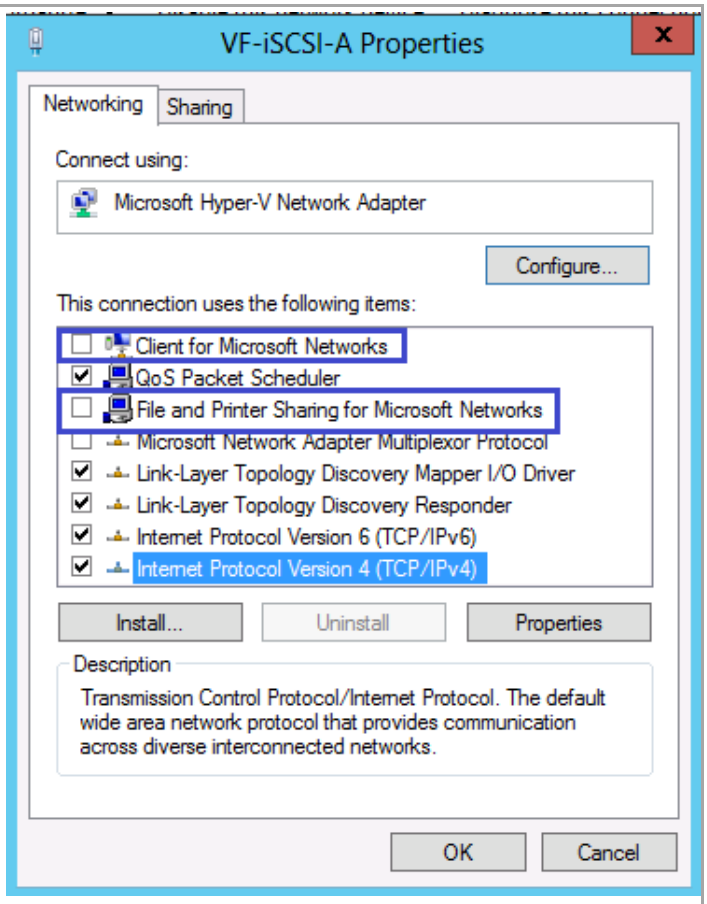
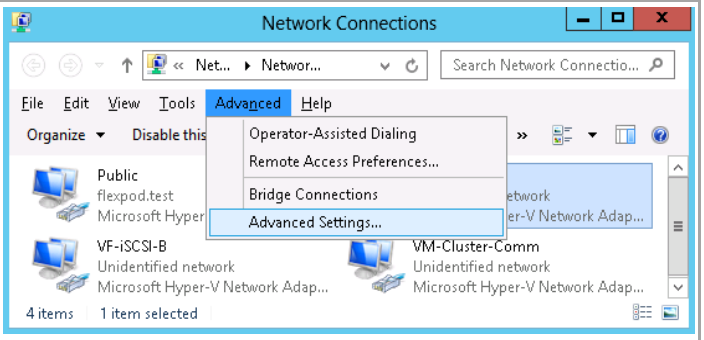
1. Open Failover Cluster Manger and select Roles in the tree view. Select the previously created SQL Server virtual machine. Select Settings… in the action pane.



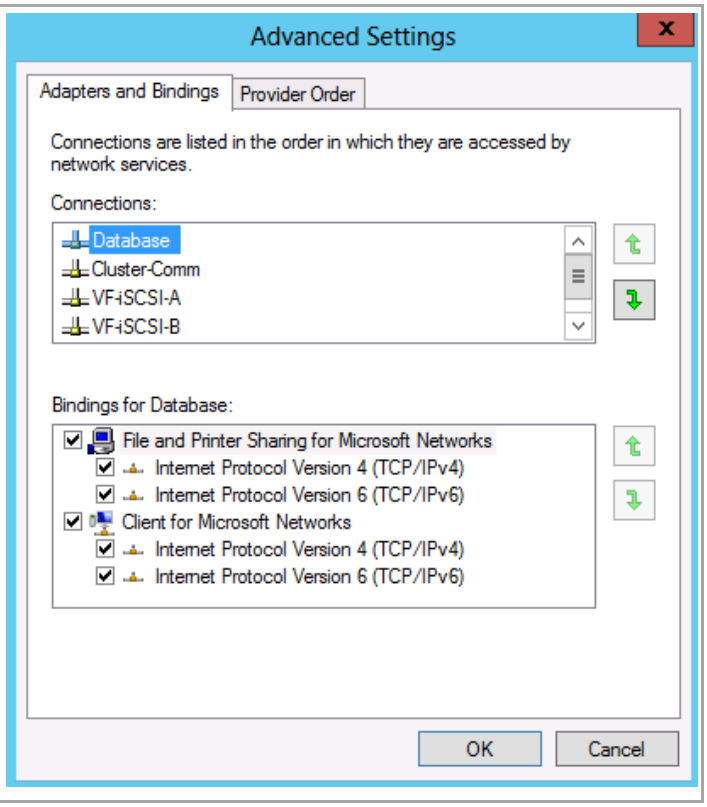
2. Expand the each Network Adapter in the left had device list and select click Advanced Features. Record the MAC address for each network adapter. 3. Click Cancel to close the Settings Window for the virtual machine.	
4. Open the Network Connections windows and rename the LAN adapter to reflect the network it is associated with.	

5. Set the appropriate IP settings for each adapter. Use static IP address for the iSCSI networks and the cluster communication network.



6. In the iSCSI-A and iSCSI-B Properties window uncheck the following: a. Client for Microsoft Networks. b. File and Printer Sharing for Microsoft Networks.	
7. In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings.	

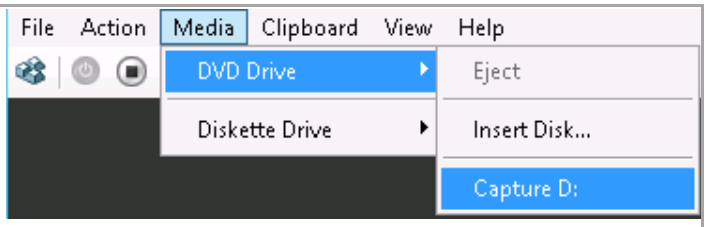
8. Select the adapter and use the arrows to move it up or down in binding order.
9. The recommended binding order is:
   - Database
   - VM-Cluster-Comm
   - VF-iSCSI-A
   - VF-iSCSI-B



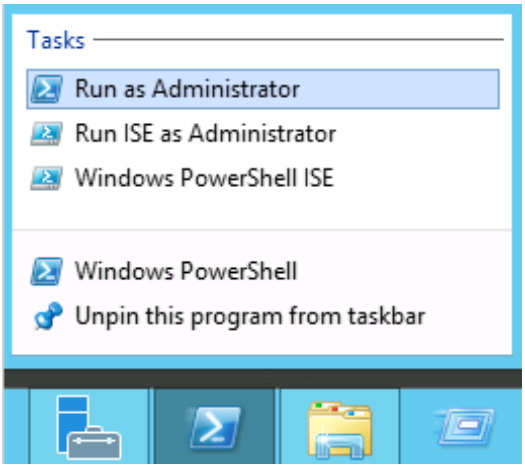
Install Windows Features in the SQL Server Virtual Machine

Perform this procedure on both SQL Server Virtual Machines.

1. Verify that the Windows installation disk is mapped to D: drive.



2. Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.



3. Add the .Net 3.5 feature by entering the following command:

```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```

```
PS C:\Users\administrator.FLEXPOD> Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {.NET Framework 3.5 (includes .NET 2.0 and...

PS C:\Users\administrator.FLEXPOD>
```

4. Add Failover Cluster, MPIO and Management Tools by entering the following command:

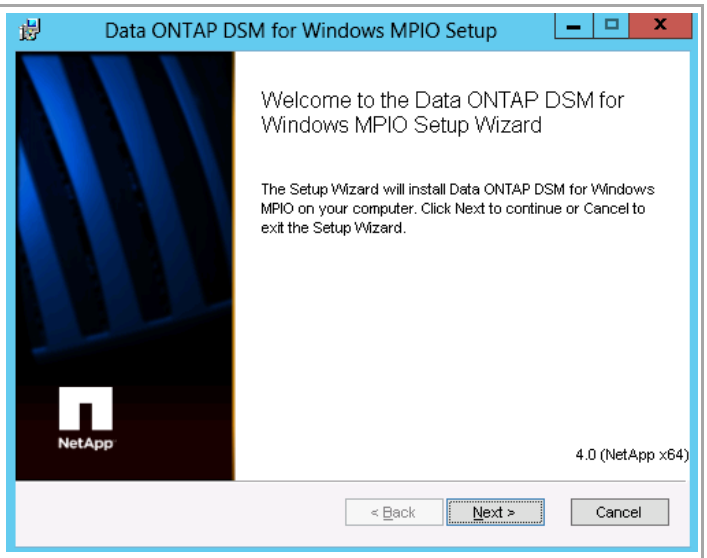
```
Add-WindowsFeature Failover-Clustering, Multipath-IO -IncludeManagementTools
```

```
PS C:\Users\administrator.FLEXPOD> Add-WindowsFeature failover-clustering, Multipath-IO -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Failover Clustering, Remote Server Admini...

PS C:\Users\administrator.FLEXPOD>
```

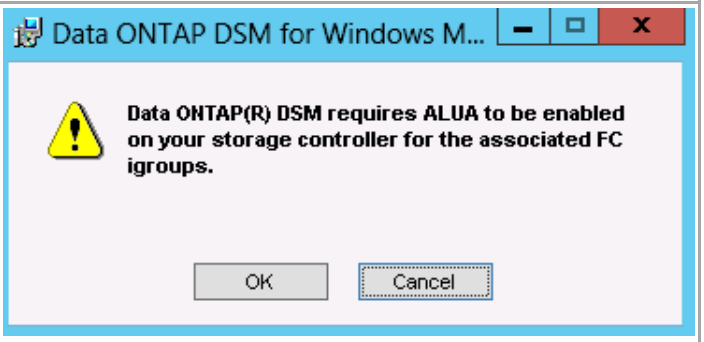
Install NetApp MPIO DSM

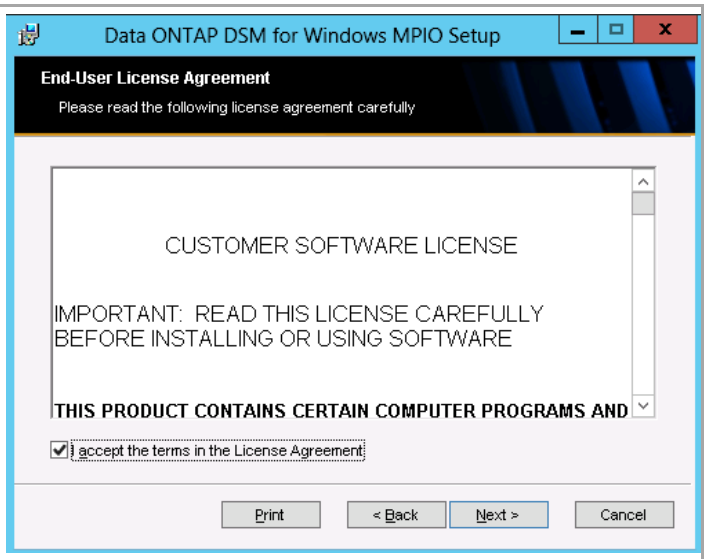
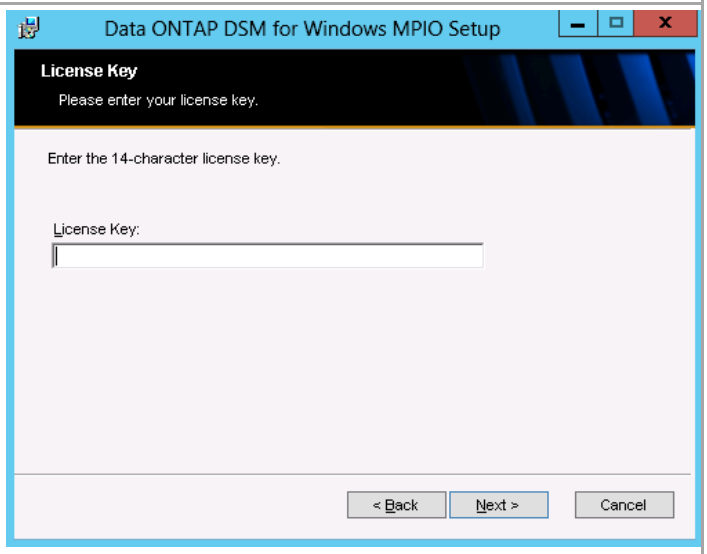
Perform this procedure on both SQL Server Virtual Machines.

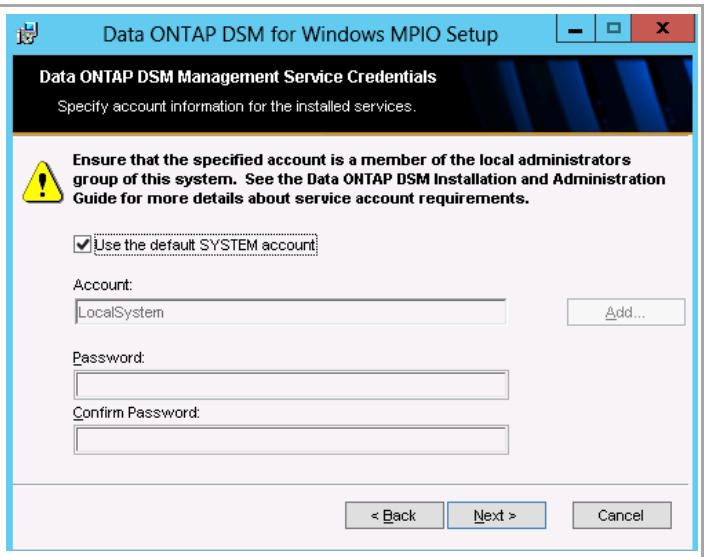
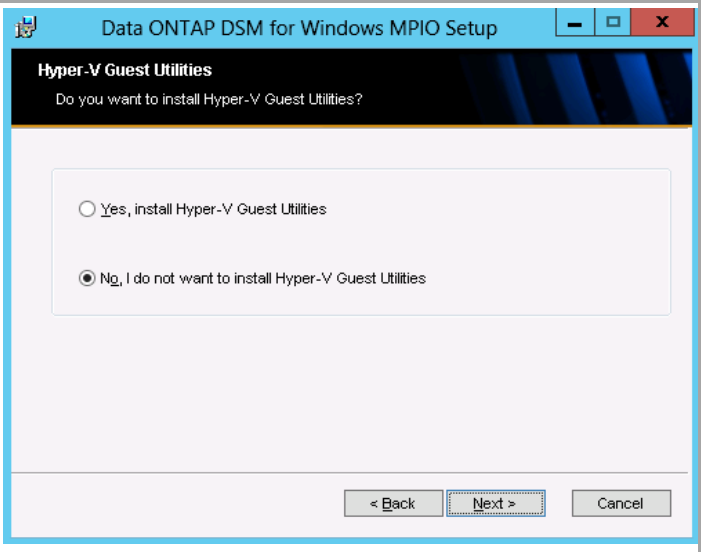
1. Launch the NetApp DSM Installer, click `Next`.

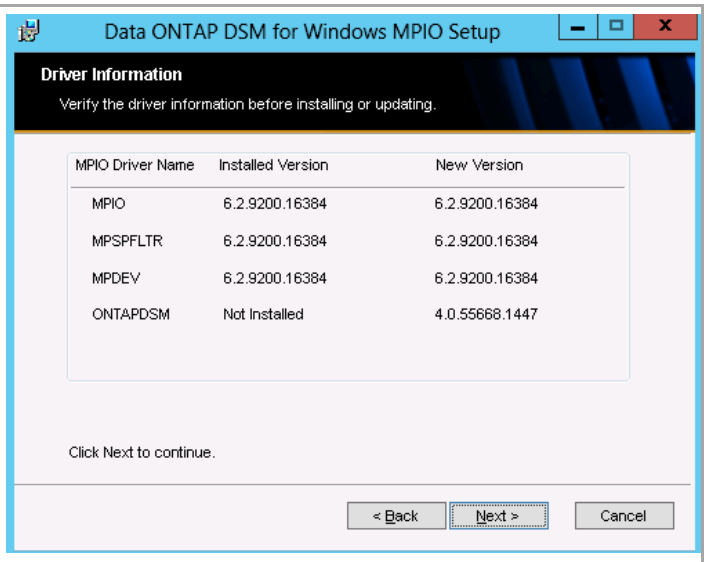
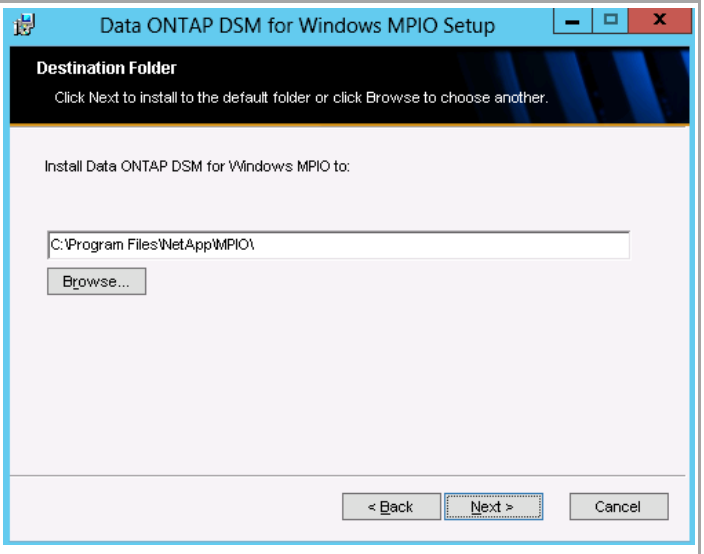


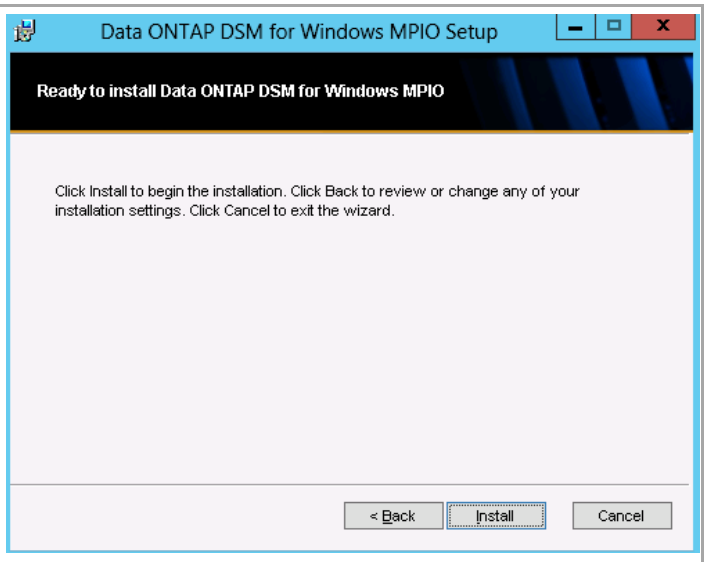
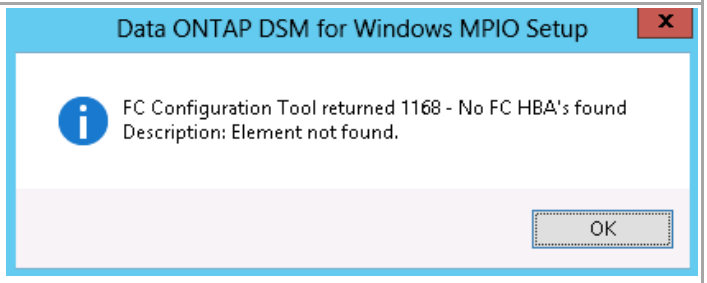
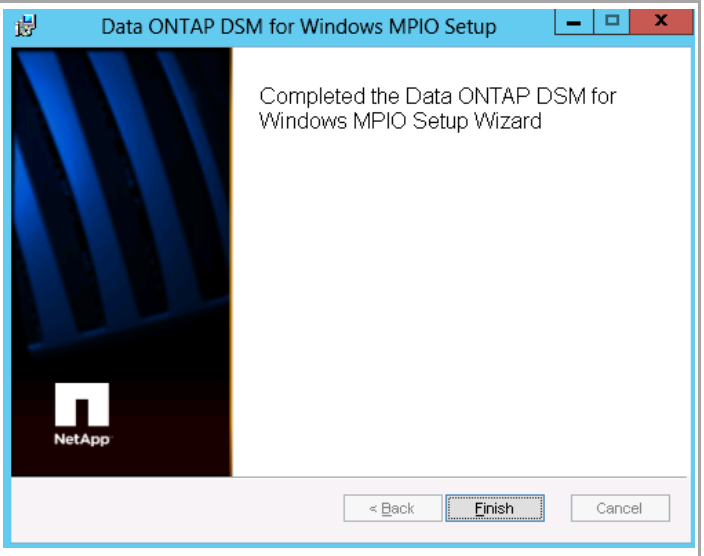
2. Click `OK` acknowledging the ALUA warning.

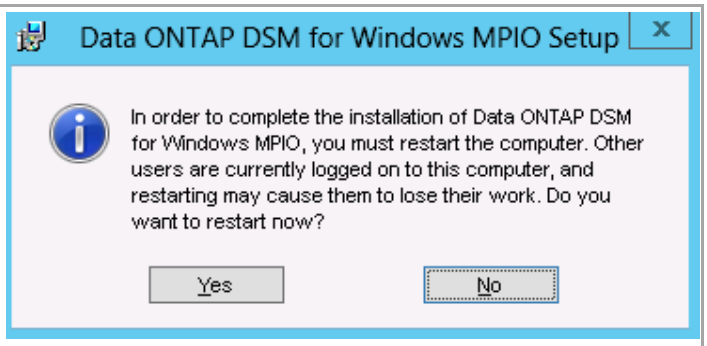


3. Accept the EULA and Click Next.	
4. Enter the license Key and Click Next.	

5. Leave `Use the default SYSTEM account checkbox` checked and Click `Next`.	
6. Select `No, I do not want to install the Hyper-V Guest Utilities`, and Click `Next`.	

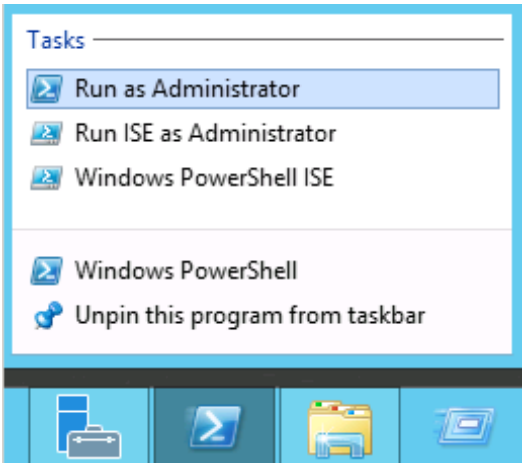
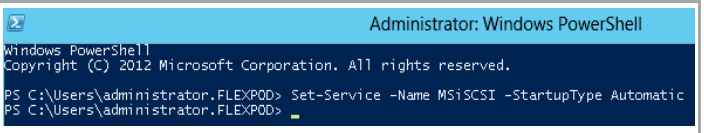
7. Click `Next` Through the driver information pane.	
8. Validate the installation path and click `Next`.	

9. Click `Install`.	
10. Acknowledge the warning that No Fibre Channel HBA's were found.	
11. Click Finish to close the wizard.	

12. When prompted reboot the host.	

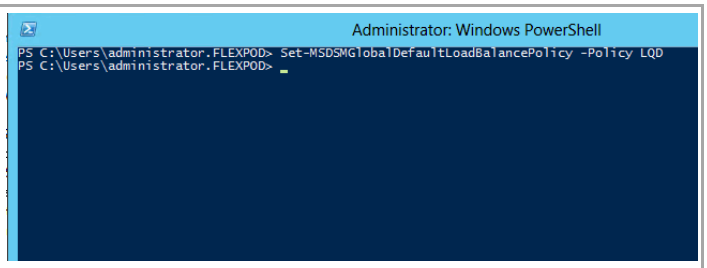
Configure Windows Host iSCSI Initiator

Perform this procedure on both SQL Server Virtual Machines. The following steps describe how to configure the built in Microsoft iSCSI initiator.

1. Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.	
2. Execute the following commands to configure the iSCSI service to start automatically `Set-Service -Name MSiSCSI -StartupType Automatic`	
3. Execute the following commands to start the iSCSI Service. `Start-Service -Name MSiSCSI`	
4. Execute the following commands to configure MPIO to claim any iSCSI device `Enable-MSDSMAutomaticClaim -BusType iSCSI`	

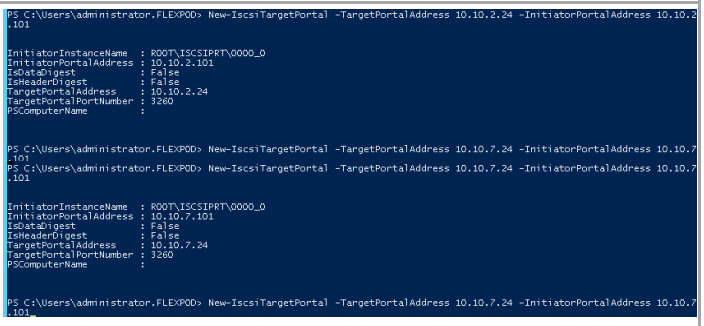
5. Execute the following commands to set the default load balance policy of all newly claimed devices to round robin.

```
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy LQD
```



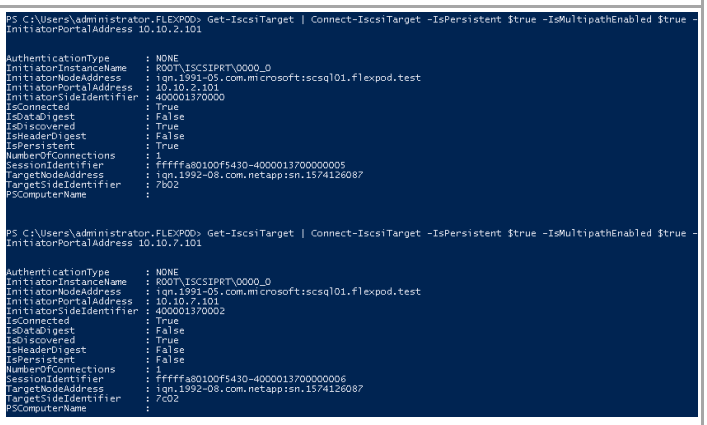
6. Execute the following commands to configure an iSCSI target for each controller.

```
New-IscsiTargetPortal -TargetPortalAddress <controller1_iscsia_ip> -InitiatorPortalAddress <iscsia_ipaddress>

New-IscsiTargetPortal -TargetPortalAddress <controller2_iscsia_ip> -InitiatorPortalAddress <iscsia_ipaddress>
```



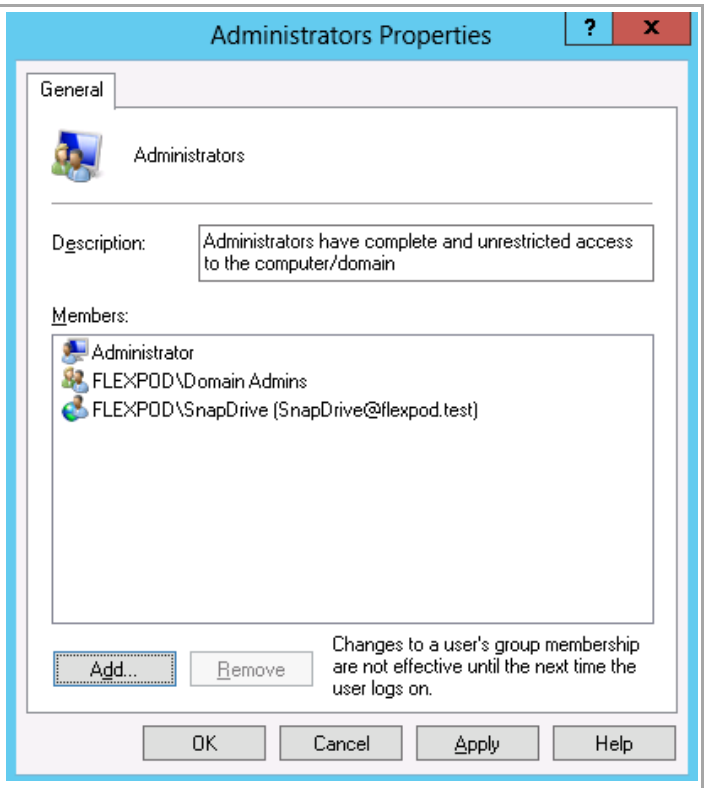
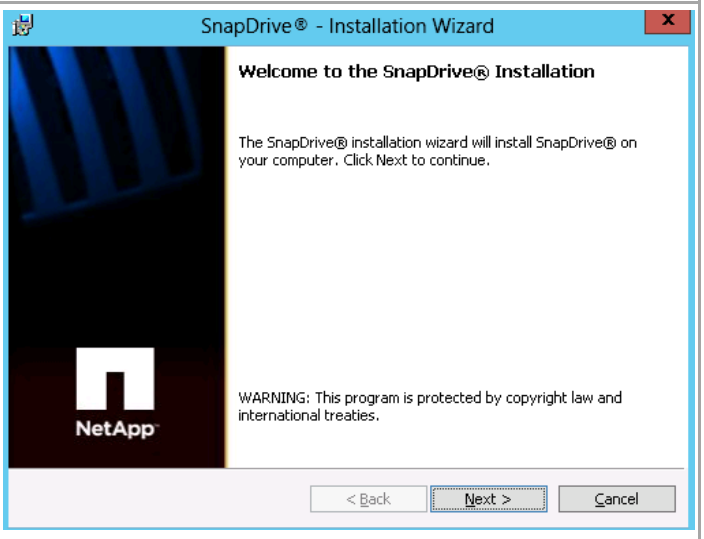
7. Execute the following commands to connect a session for each iscsi Network to each target.

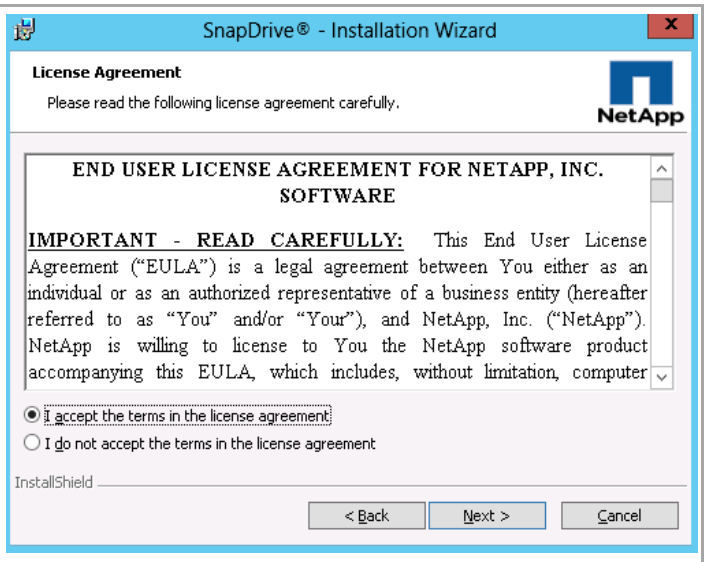
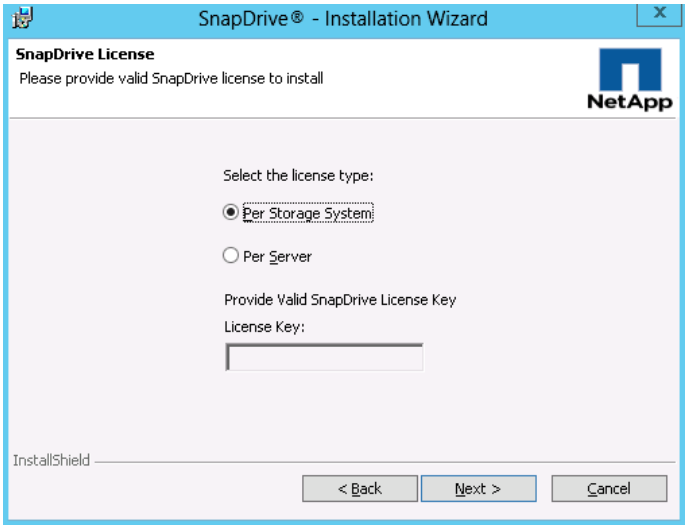
```
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsia_ipaddress>

Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsib_ipaddress>
```

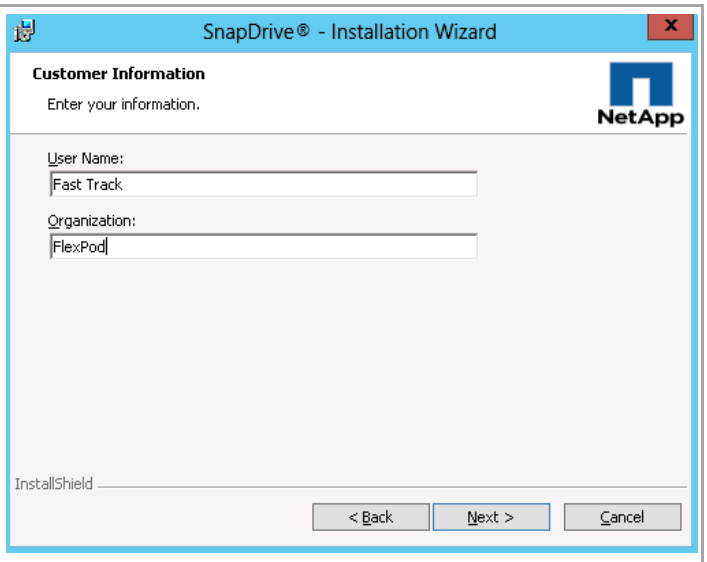
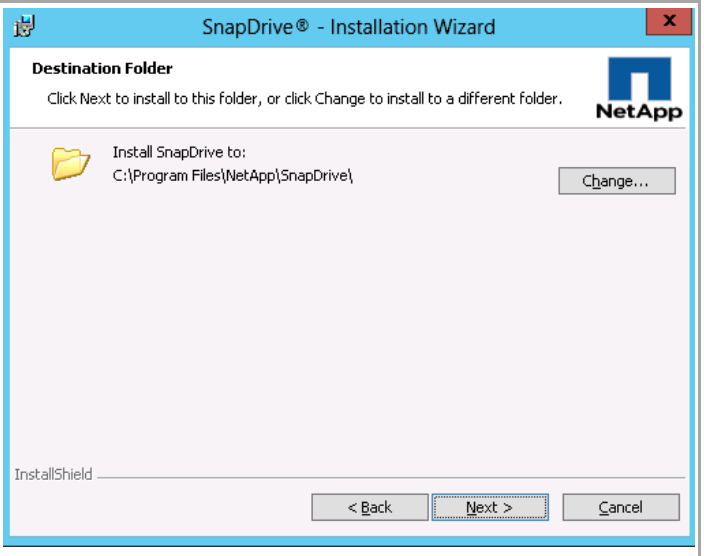


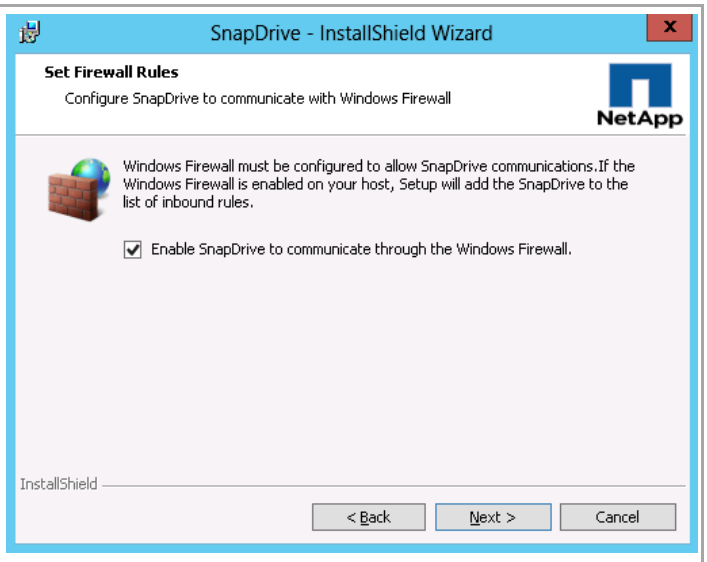
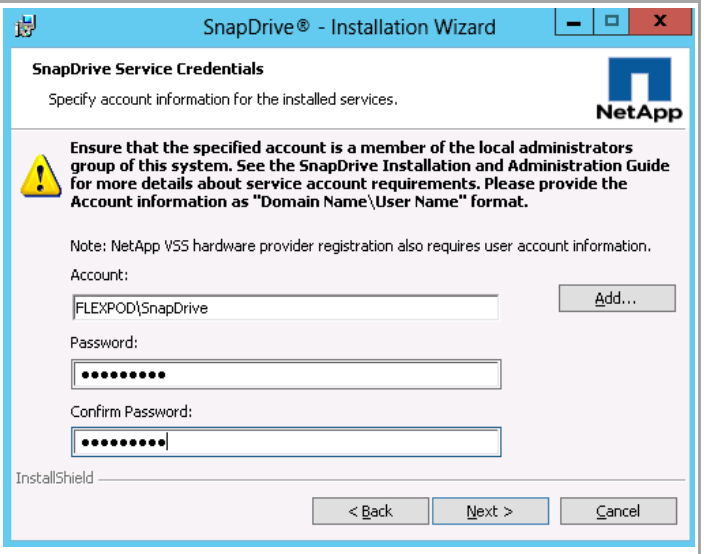
Install NetApp SnapDrive in the SQL Server Virtual Machines

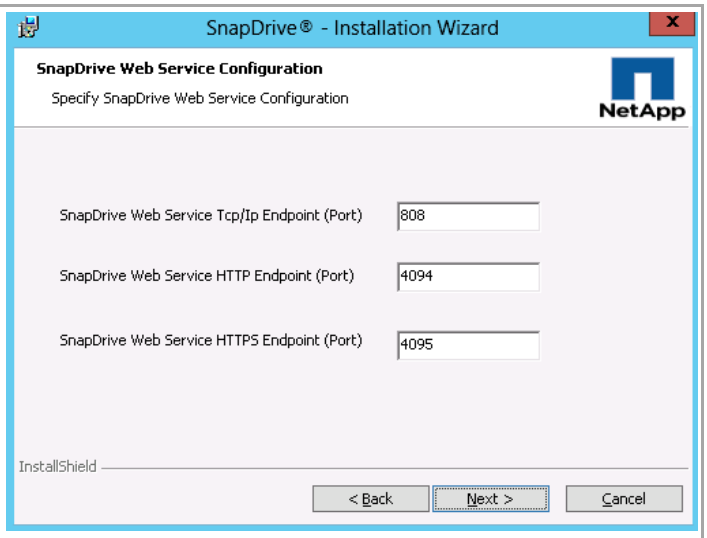
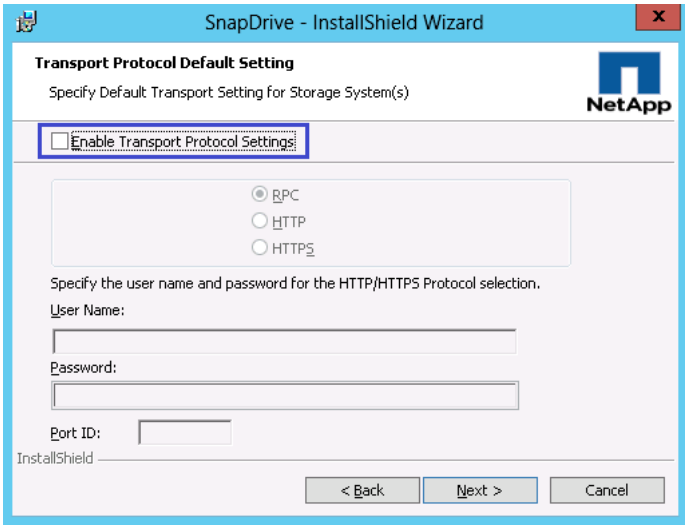
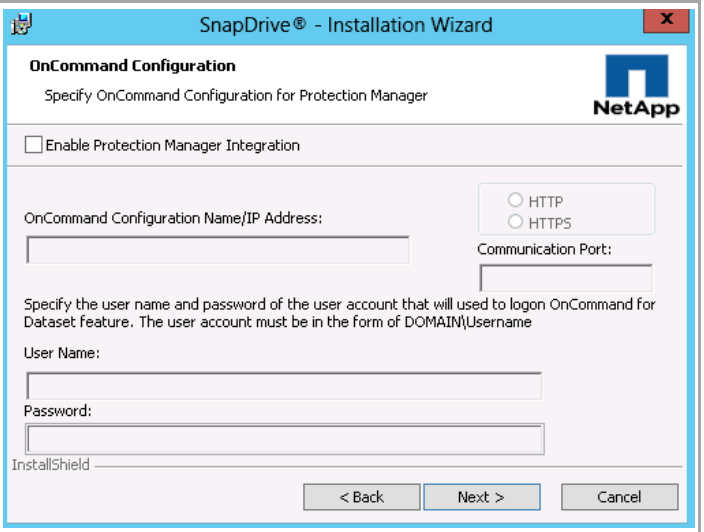
Perform this procedure on both SQL Server Virtual Machines.

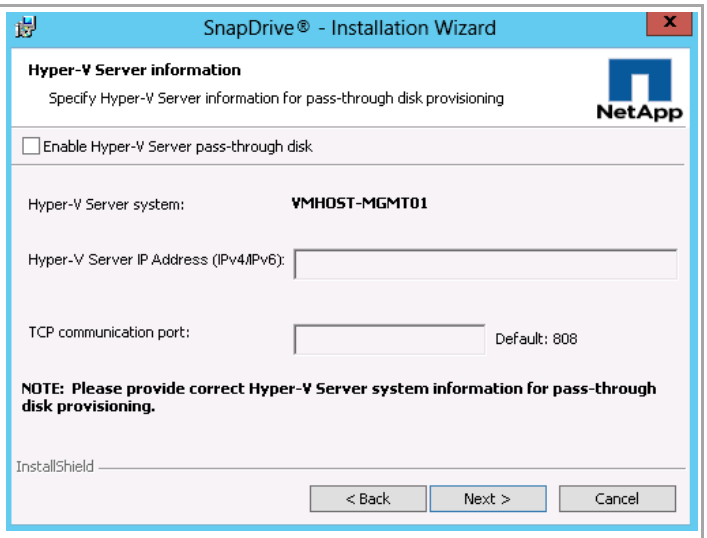
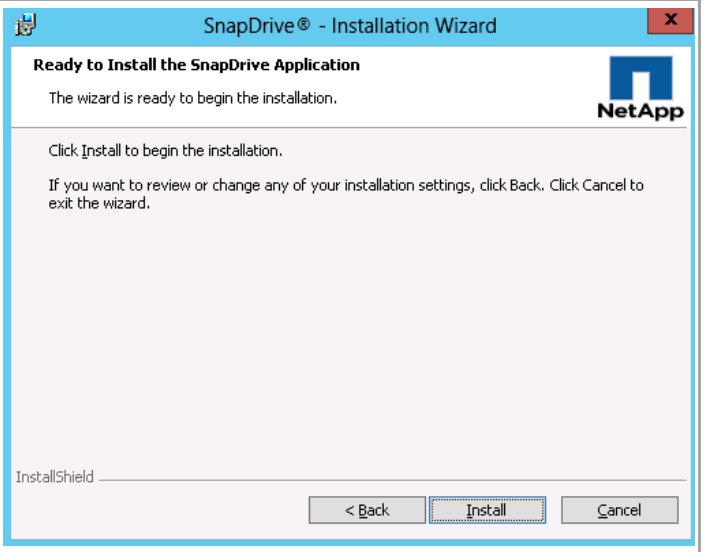
1. Add the SnapDrive domain account to the local administrators group in the SQL Server virtual machine.	
2. Launch the SnapDrive Installer, click `Next`.	

3. Accept the EULA and click Next.	
4. Select the Storage based Licensing method and click Next.	

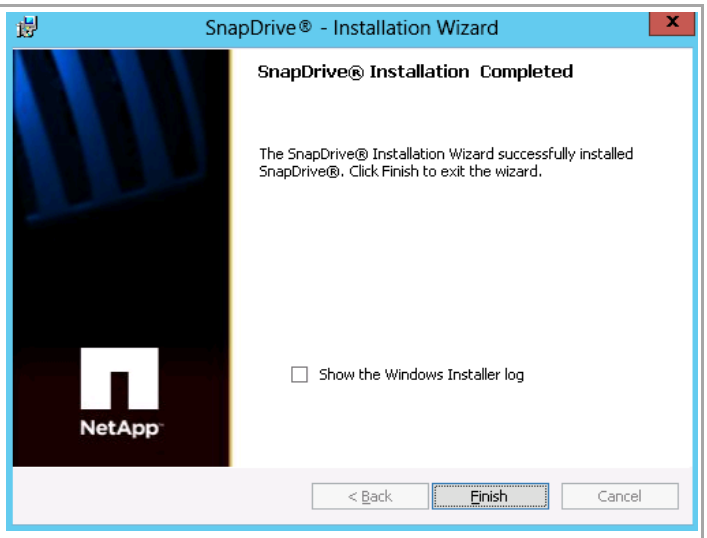
5. Enter your User Name, and Organization information, and click `Next`.	
6. Validate the installation path and click `Next`.	

7. Check the `Enable SnapDrive to communicate through the Windows Firewall` checkbox and click `Next`.	
8. Enter the Account information for the Snapdrive service account, Click `Next`.	

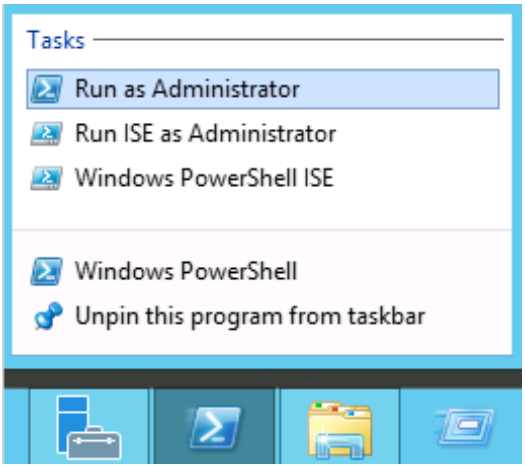
9. Click `Next`, through the SnapDrive Web Service Configuration.	
10. Uncheck the `Enable Transport Protocol Settings`, and click `Next`.	
11. Leave `Enable Protection Manger Integration` Unchecked, and click `Next`.	

12. Leave `Enable Hyper-V Server pass-through disk` Unchecked, and click `Next`.	
13. Click `Install`.	

14. Click Finish to close the installation wizard window.

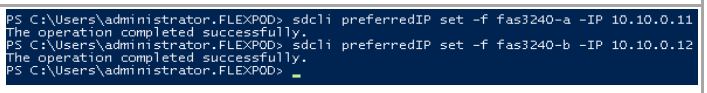


15. After the installation is finished. Launch a NEW PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.
16. A new prompt is required to register the sdcli executable.



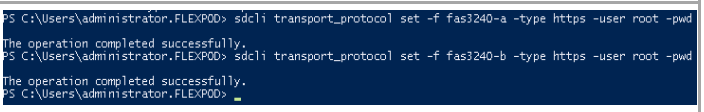
17. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_controller1>>
-IP <<var_controller1_e0m_ip>>
sdcli preferredIP set -f <<var_controller2>>
-IP <<var_controller2_e0m_ip>>
```



18. Configure SnapDrive transport protocol authentication configuration for each controller.

```
sdcli transport_protocol set -f
<<var_controller1>> -type https -user root -
pwd <<var_admin_passwd>>
sdcli transport_protocol set -f
<<var_controller2>> -type https -user root -
pwd <<var_admin_passwd>>
```



Establish the SQL Server Guest Cluster

This section assumes storage with iSCSI interface is available and the customer is implementing a SQL Server guest cluster, the following steps can be followed to create the SQL Server guest cluster. Note that the SQL Server guest cluster can also use fibre channel storage for clustering the virtual

fibre channel adapter in Windows Server 2012 Hyper-V. While SMB shares can be used for SQL Server failover clusters, SQL Server Analysis Services is a requirement for the Fast Track design and is not compatible with SMB shares.

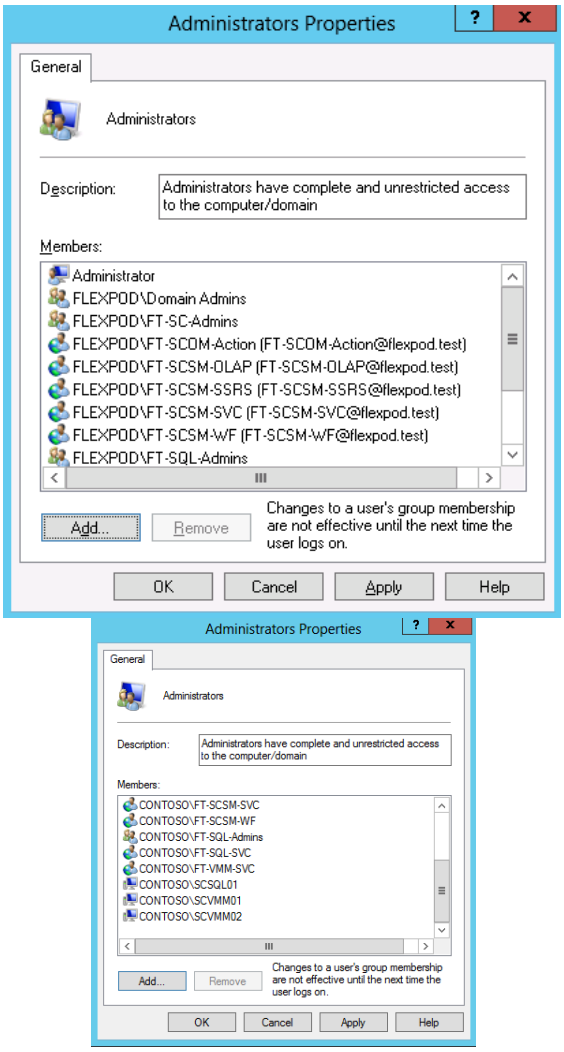
The first step in installing SQL Server is to create the guest cluster using iSCSI. To do this, access to iSCSI LUNs is required to allow each guest virtual machine in the cluster to access shared storage. Prior to completing the following steps, the storage should be provisioned and presented to the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

1. One LUN – quorum (1 GB).
2. Two LUNs for each fabric management component instance (14 LUNs for all products).

During the provisioning process, four virtual machines were built to the specifications outlined in the Fast Track Reference Architecture Guide to support SQL Server operations for fabric management. When created, the iSCSI targets must be configured within each virtual machine to make them accessible by each candidate cluster node.

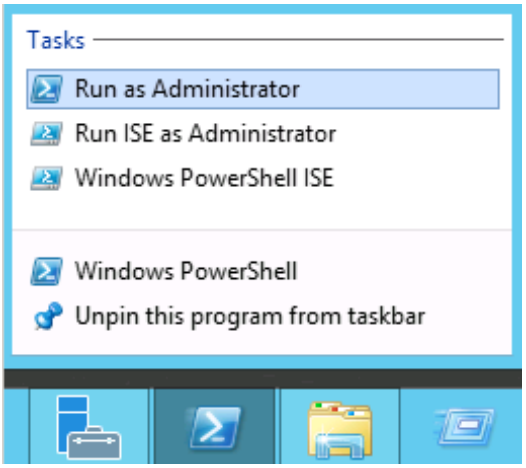
Perform the following steps on **all fabric management SQL Server** virtual machines.

1. Log on to the first node in the SQL Server cluster as a user with local admin rights.
2. Verify that the following accounts and/or groups are members of the Local Administrators group on the first and second SQL Server nodes:
    a. Fast Track SQL Server service account.
    b. Fast Track SQL Server Admins group.
    c. Virtual Machine Manager computer accounts.
    d. Fast Track Service Manager OLAP account.
    e. Fast Track Service Manager SSRS account.
    f. Fast Track Service Manager workflow account.
    g. Fast Track Service Manager service account.
    h. Fast Track Operations Manager action account.
    i. Fast Track Virtual Machine Manager service account.



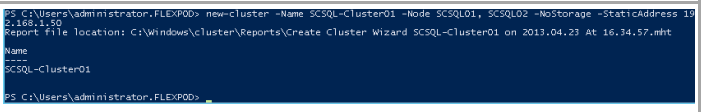
Note: Create a the Windows Failover Cluster in the two SQL Server virtual machines previsioned in the earlier step. Perform the following procedure on one of the SQL Server virtual machines.

1. Launch a PowerShell prompt with administrative permissions, by right clicking on the PowerShell icon and selecting **Run as Administrator**.



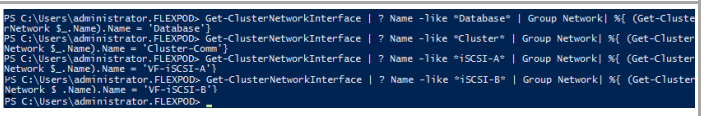
2. Create a new cluster by executing the following command

```
New-Cluster -Name <cluster_name> -Node
<Node1>, <Node2>, <node3>, -NoStorage -
StaticAddress <cluster_ip_address>
```

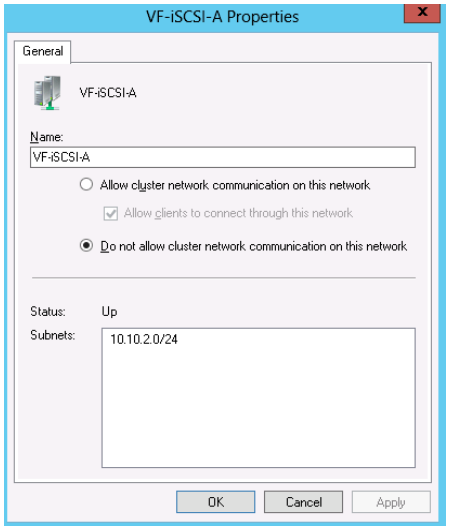


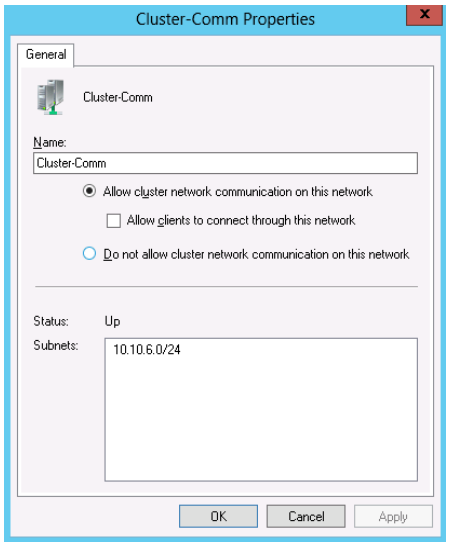
3. Rename the cluster networks to match there function.

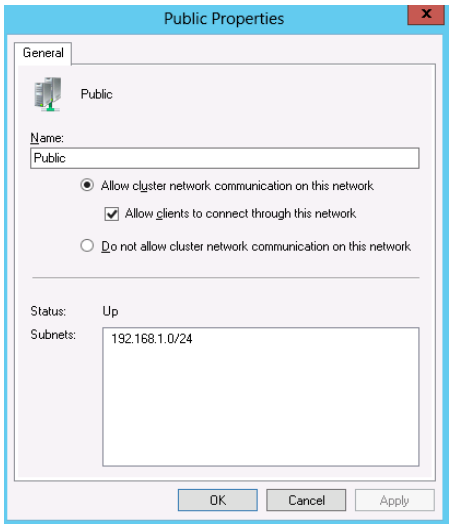
```
Get-ClusterNetworkInterface | ? Name -like
*Database* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'Database'}

Get-ClusterNetworkInterface | ? Name -like
*Cluster* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'Cluster-
Comm'}

Get-ClusterNetworkInterface | ? Name -like
*iSCSI-A* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'VF-iSCSI-A'}

Get-ClusterNetworkInterface | ? Name -like
*iSCSI-B* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'VF-iSCSI-B'}
```



4. Using Failover Cluster Manager, expand the Networks object in the left tree view. Right-click each network and select properties.
5. **Disable** cluster communication for the VF-iSCSI-A and VF-iSCSI-B networks.
6. **Uncheck** Allow clients to comment through this network for the Cluster-Comm network.
7. **Check** Allow clients to comment through this network for the Public network.







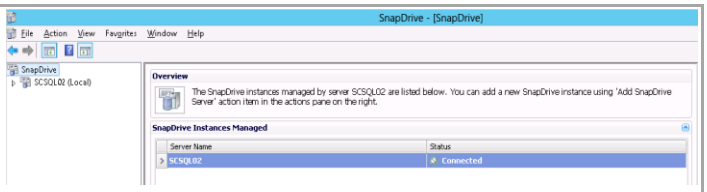
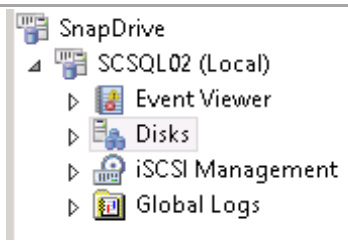
Create and Map iSCSI LUNs using SnapDrive for SQL Server

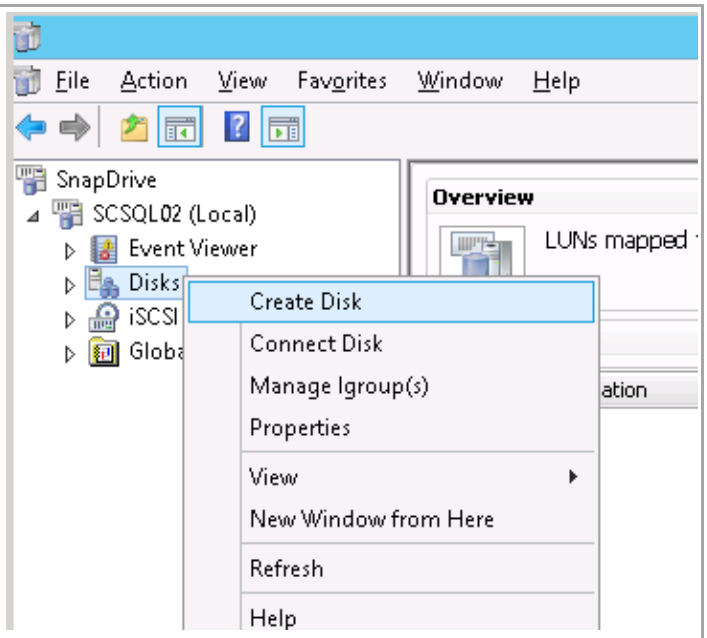
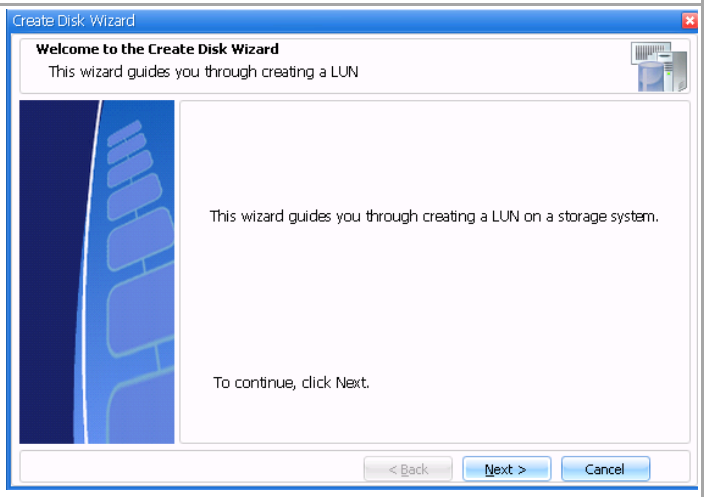
Create SQL Server database LUNs using SnapDrive. The LUN sizes and perpose are listed below. Perform this action from the one node in the SQL Server Cluster.

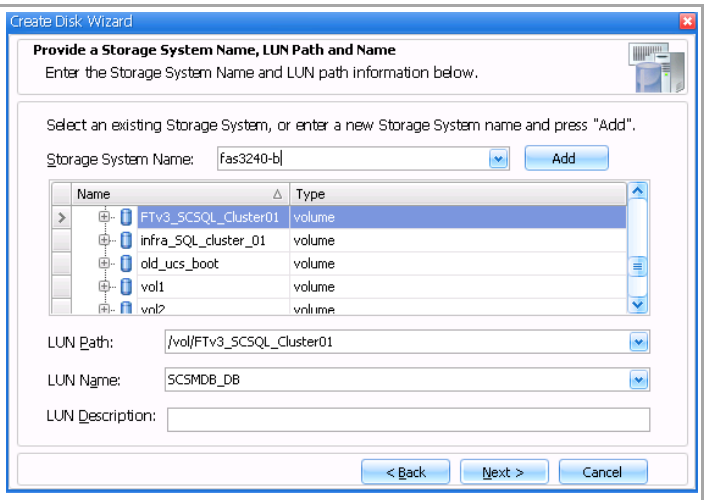
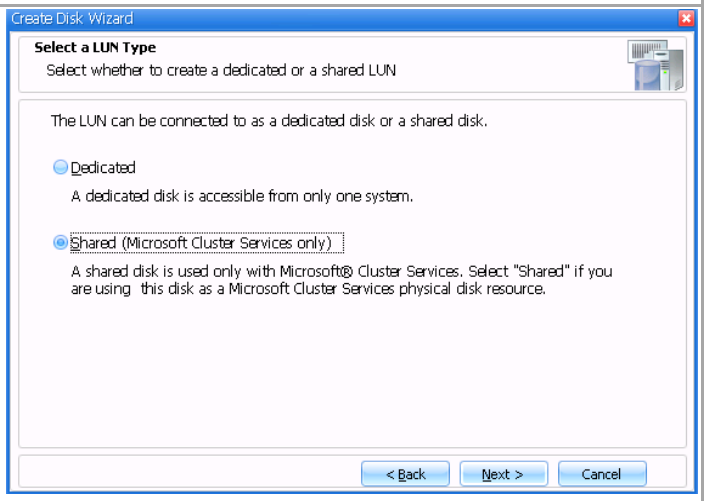
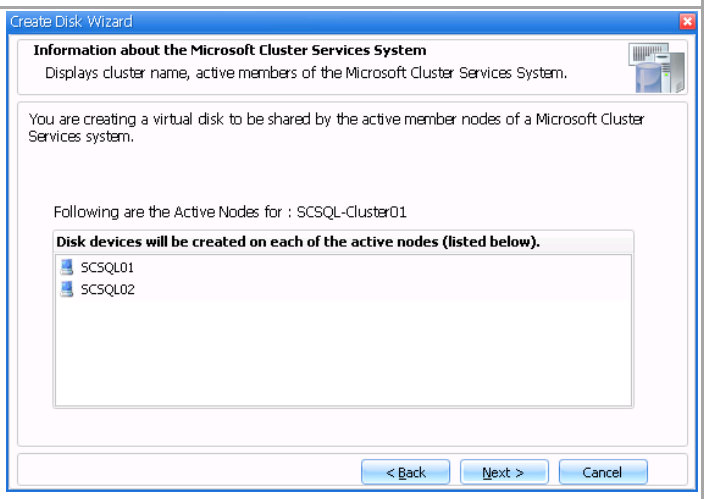
Table 12 SQL Server Database and Quorum LUNs

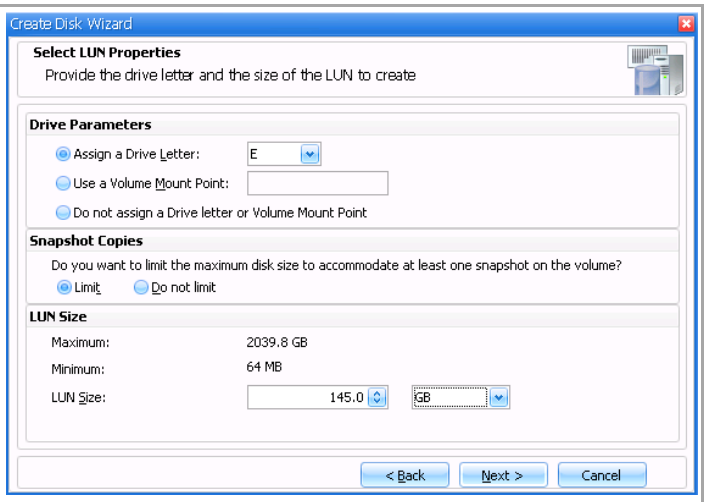
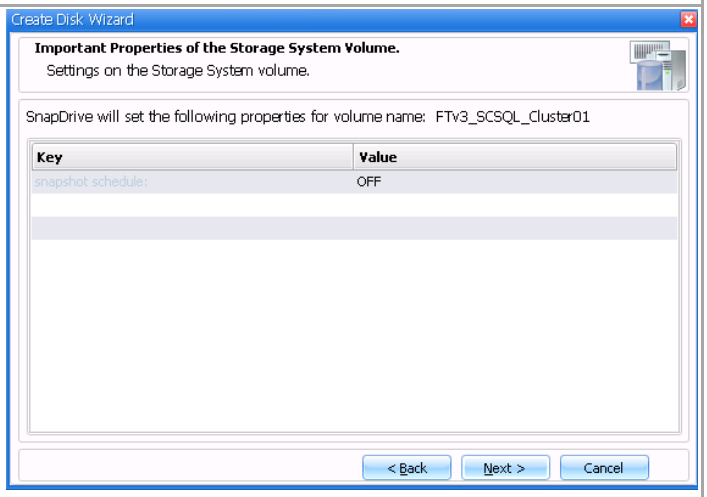
LUN	Component(s)	Instance Name	Purpose	Size	Drive Letter
LUN 1/2	Service Manager Management	SCSMDB	Instance Database and Logs	145 GB/70 GB	Database E: Logs F:
LUN 3/4	Service Manager Data Warehouse	SCSMDW	Instance Database and Logs	1 TB/ 500 GB	Database G: Logs H:
LUN 5/6	Service Manager Analysis Service	SCSMAS	Instance Database and Logs	8 GB/4 GB	Database I: Logs J:
LUN 7/8	Service Manager SharePoint Farm Orchestrator App Controller	SCDB	Instance Database and Logs	10 GB/5 GB	Database K: Logs L:
LUN 9/10	Virtual Machine Manager Windows Server Update Services	SCVMMDB	Instance Database and Logs	6 GB/3 GB	Database M: Logs N:
LUN 11/12	Operations Manager	SCOMDB	Instance Database and Logs	130 GB/65 GB	Database O: Logs P:
LUN 13/14	Operations Manager Data Warehouse	SCOMDW	Instance Database and Logs	1 TB/ 500 GB	Database Q: Logs R:
LUN 15	N/A	N/A	SQL Server Failover Cluster Quorum	1 GB	none

Note: The Operations Manager and Service Manager database sizing assumes a managed infrastructure of 8,000 virtual machines.

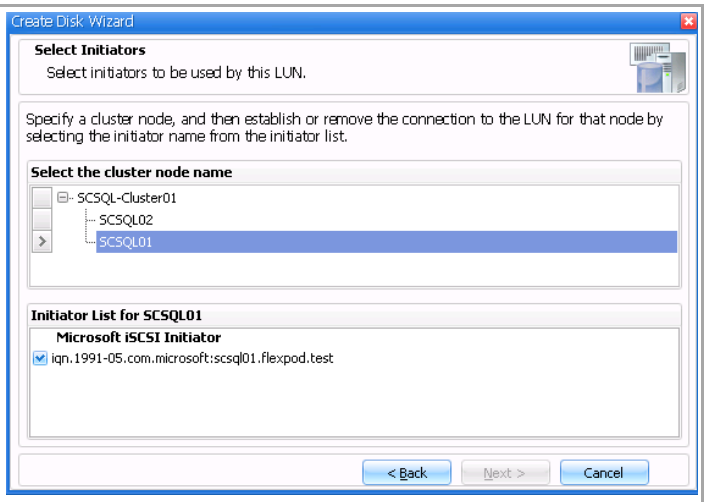
1. Open SnapDrive from the start screen to configure cluster storage.	
2. Expand server name object in the left tree view, and select the disk object.	

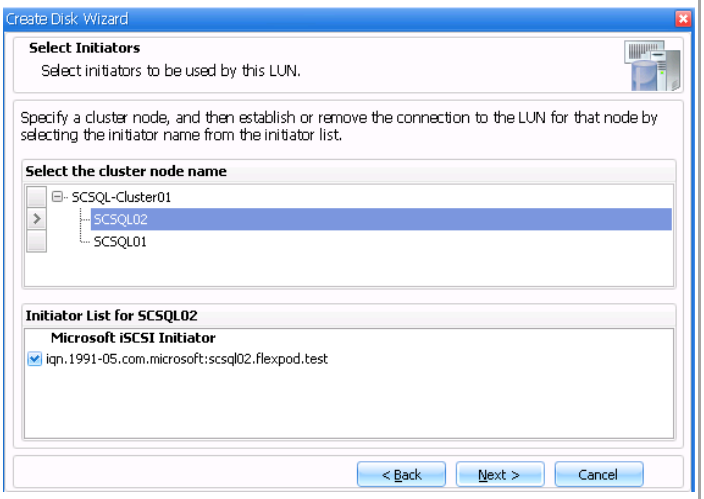
3. Right-click the Disks Icon and choose to Create Disk.	
4. Click Next on the welcome screen.	

5. Enter in the IP Address or host name of the controller in the Storage System Name field and click Add. 6. Select the volume from the volume list. 7. Enter the LUN name and click Next.	
8. Select Shared (Microsoft Cluster Service) click Next.	
9. Review the list of cluster nodes and click Next.	

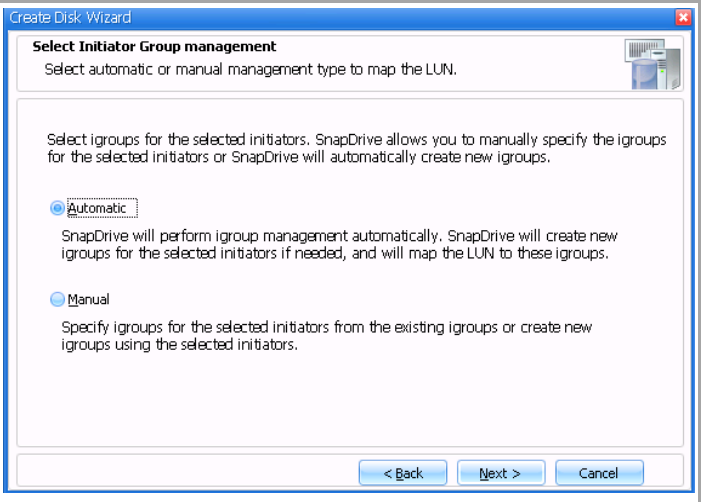
10. Assigned the drive letter and set the LUN size based on the table above and click Next.	
11. Review the automatic snapshot setting for the target volume and click Next.	

12. In the Select Initiators screen, Select each cluster node and check the Microsoft iSCSI initiator IQN to use for the LUN mapping. Click Next.

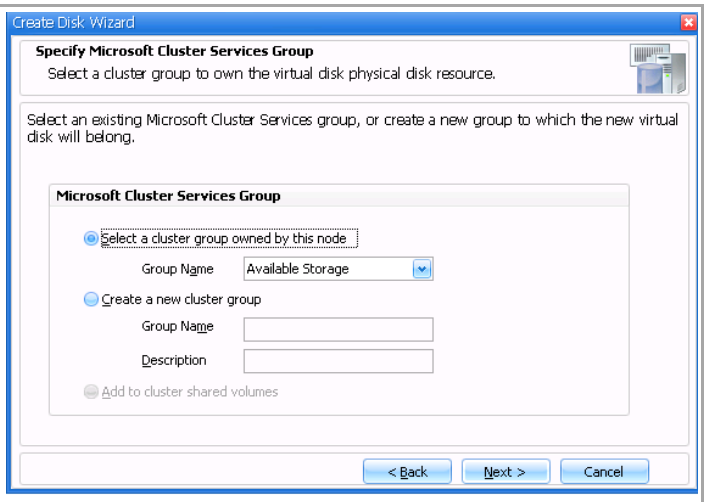




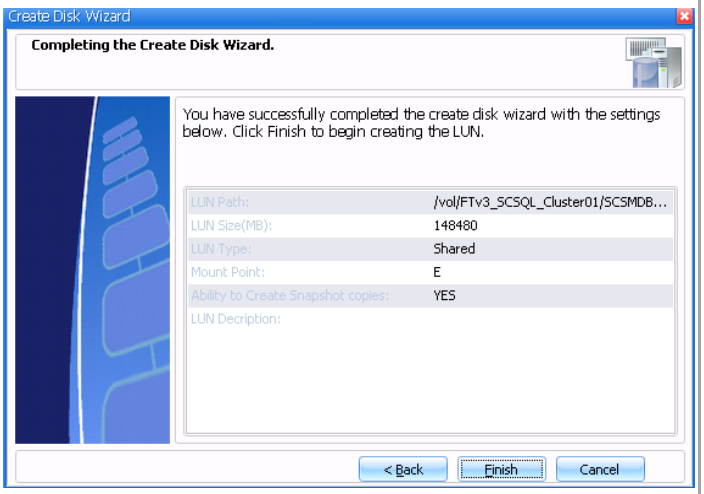
13. Select Automatic igroup management and Click Next.



14. Select the cluster group owned by this node and select the Available Storage group.

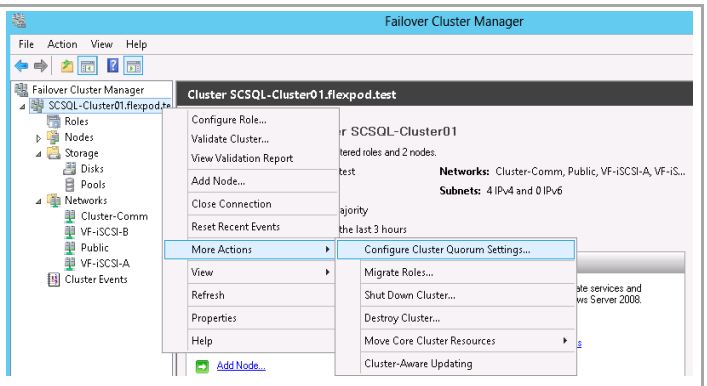


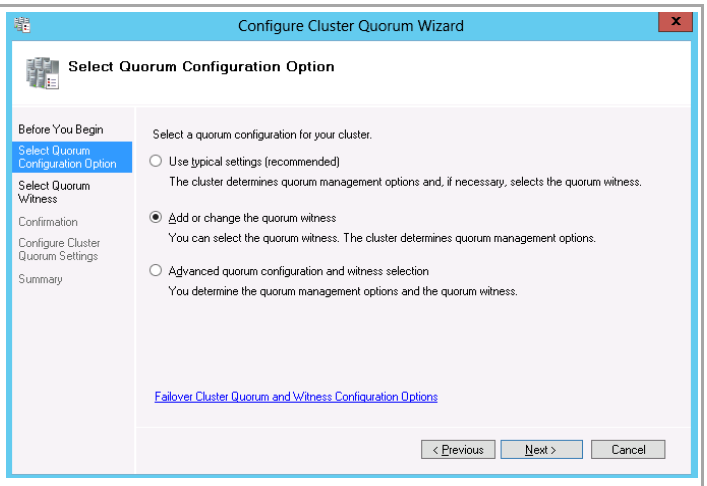
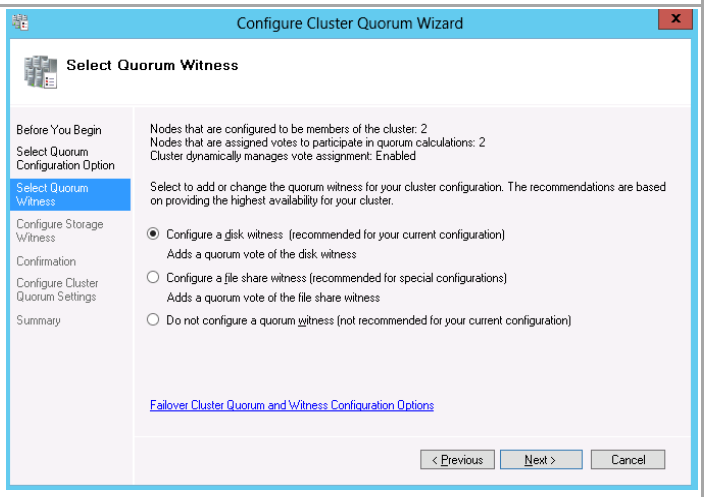
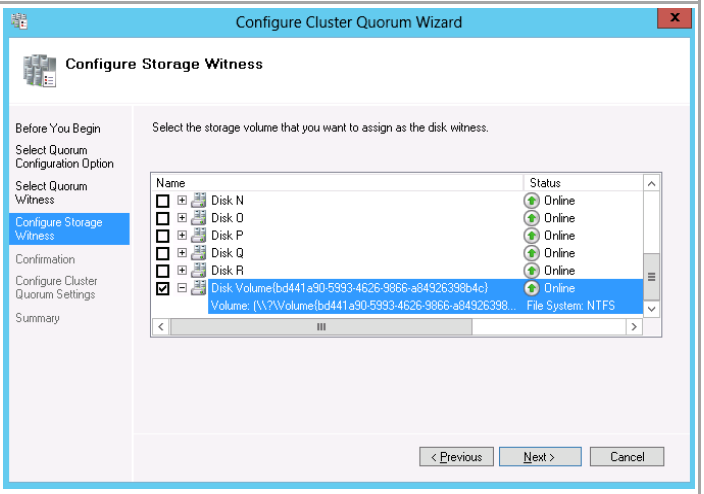
15. Review the parameters and click Finish.
16. Repeat this operation for each LUN in the table above.
17. Database and transaction log LUNs may be distributed among both storage controllers.

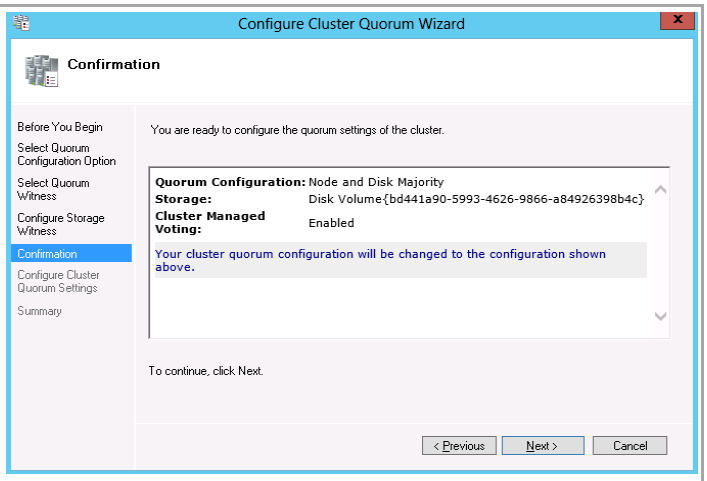
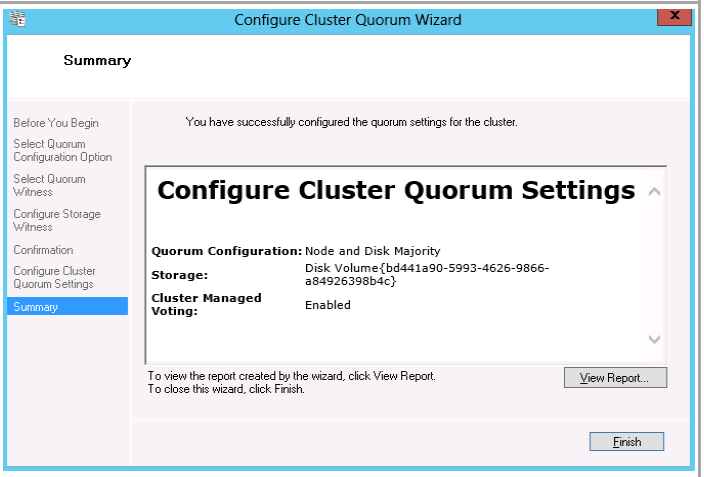


Change the SQL Server Cluster to Use a Quorum Disk

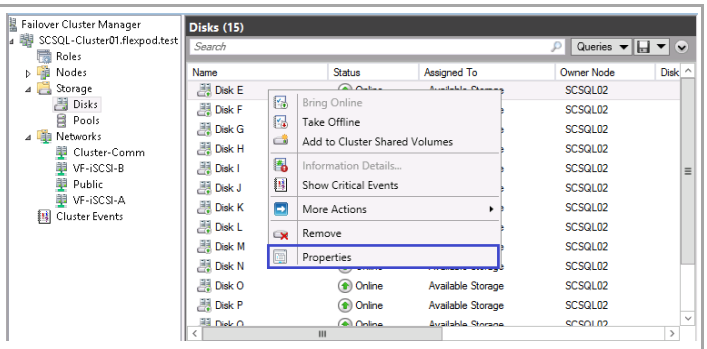
1. In failover cluster manager, select **More Actions** in the action pane and click **Configure Cluster Quorum Settings...**
2. The following comdlet can be used to assign the quorum disk as an alternative to using Failovor Cluster Manager.
3. Set-ClusterQuorum -NodeAndDiskMajority <ClusterQuorumDisk>



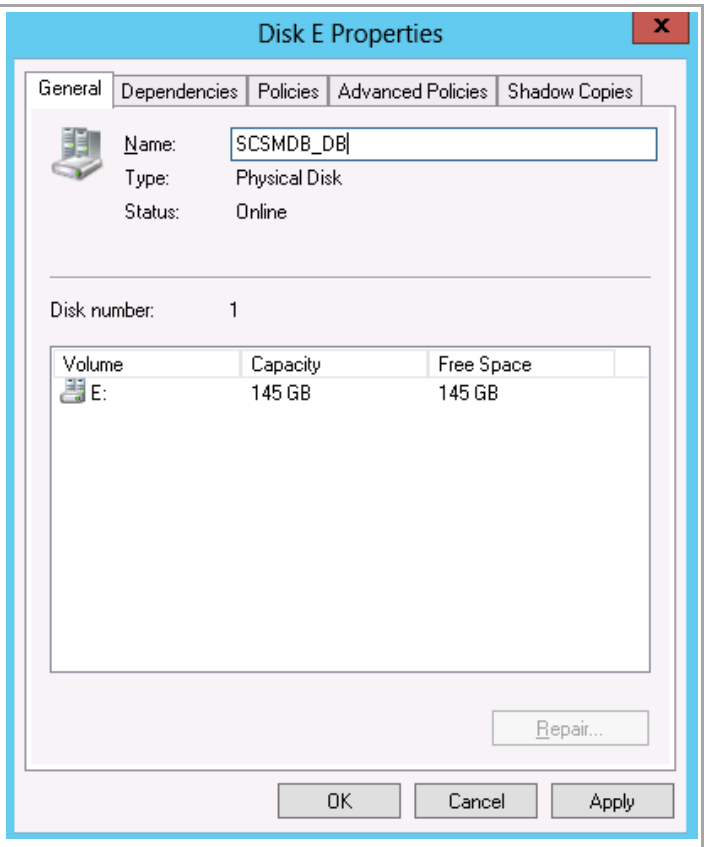
4. Select **Add or Change the quorum witness**, and click **Next**.	
5. Select **Configure a disk witness** and click **Next**.	
6. **Select the LUN** without a drive letter that was previously created to be the quorum LUN. Click **Next**.	

7. Confirm the settings and click **Next.**	
8. **Review the results** and click **Finish to close the wizard screen.**	

Assign SQL Cluster Disk Names

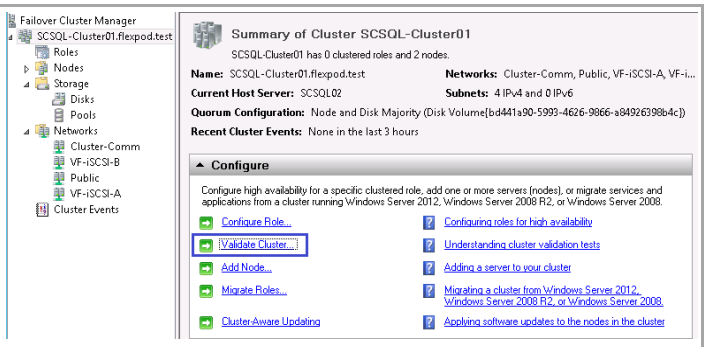
1. Select the SQL Server cluster in the left tree view. Expand the Storage object and select Disks. Right click each disk in the middle pane and select properties.	

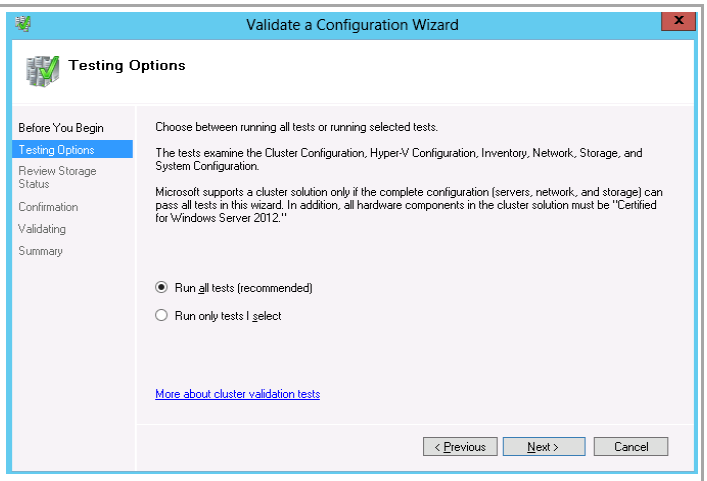
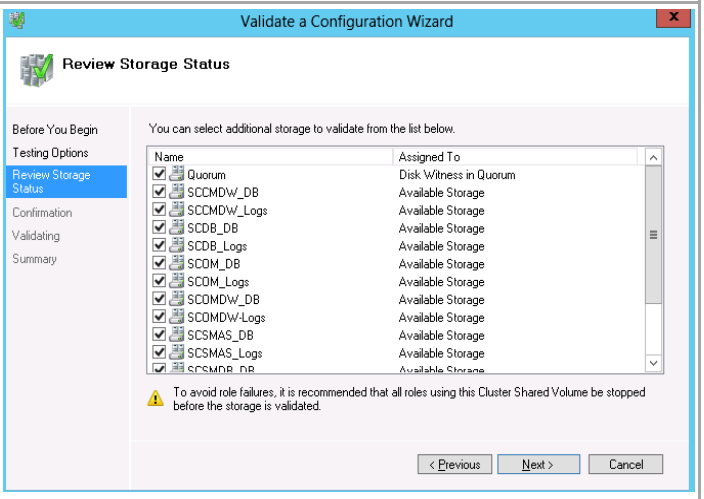
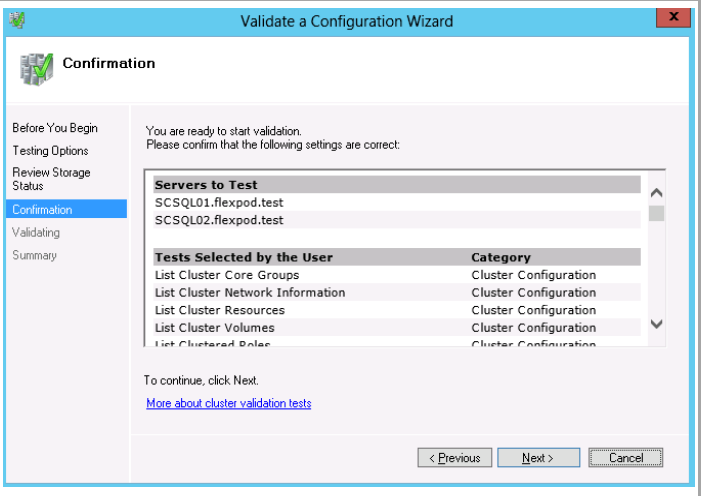
2. In the Name field, enter a name that reflects the LUN names used in section 13.3.
3. Repeat this procedure for all cluster disks.



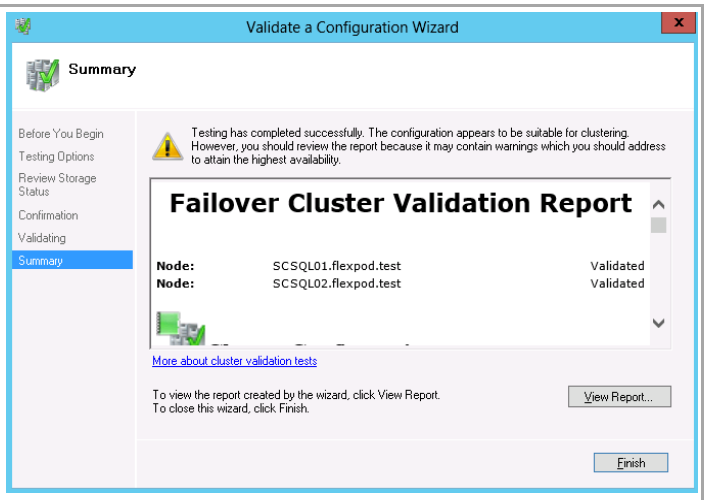
Validated the SQL Server Cluster

1. Select the SQL Server cluster in the left tree view and click Validate Cluster.



2. Select **Run all tests** and click Next.	
3. Select all the disks on the cluster and Click Next.	
4. Confirm the selected options and click **Next**.	

5. Review and correct any failures that are listed in the validation report.
6. The following warnings are expected to be reported by the validation wizard. These warning can safely be disregarded.



Note: The following warnings are expected to be reported by the validation wizard. These warning can safely be disregarded.

Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xn0000000c, SERVICE ACTION RESERVATION KEY 0xc0000000d, for Test Disk y from node SCSQL01.flexpod.test.

Note: n and y are variable numbers.

Create Required User Accounts and Security Groups

While each System Center 2012 SP1 component installation section in this document outlines the individual accounts and groups required for each installation and operation, a short summary appears in the tables below. The following Microsoft Active Directory® Domain Services (AD DS) user accounts are required for the Fast Track System Center 2012 SP1 installation:

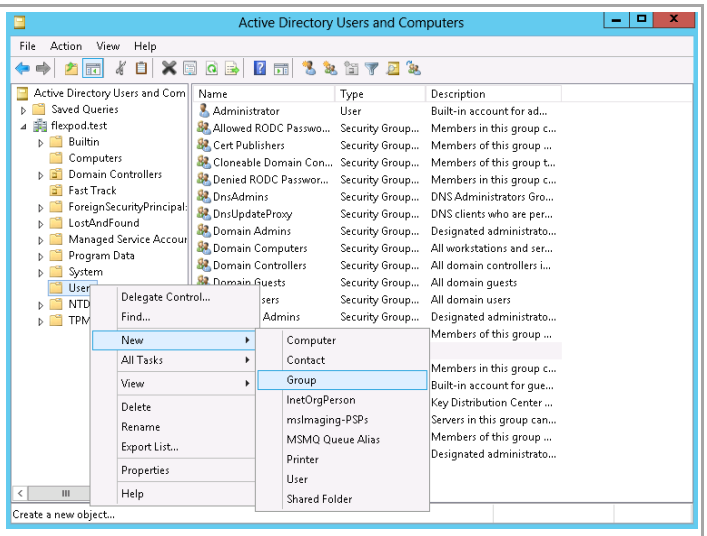
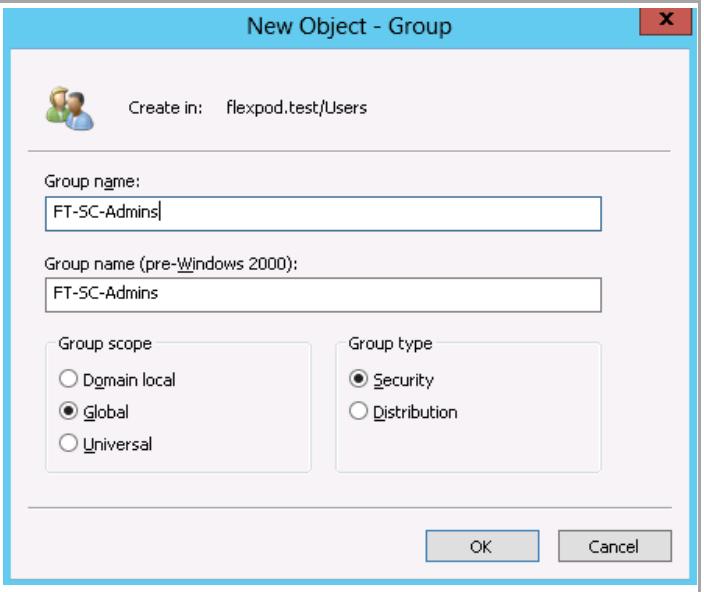
Component	User account	Suggested name	Description
System Center	Component installation account	FT-SCInstall	This optional account is used to install all System Center 2012 components.
SQL Server	SQL Server instance service account	FT-SQL-Service	This account is used as the service account for all instances 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.

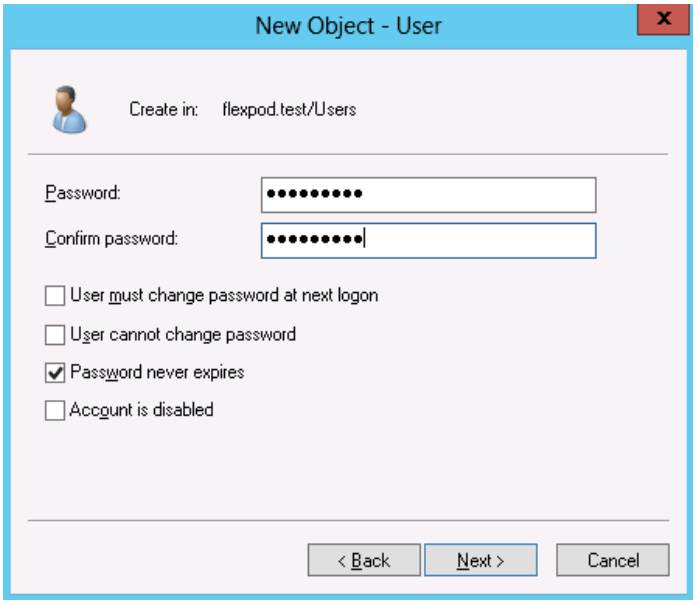
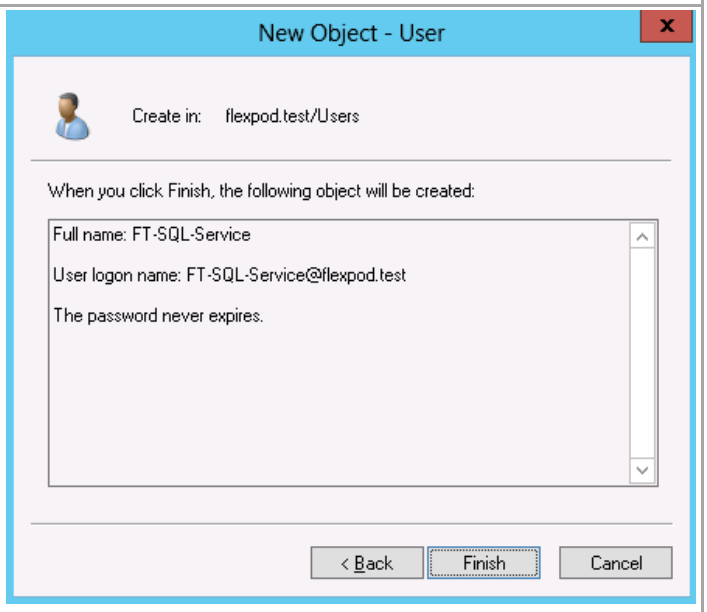
Component	User account	Suggested name	Description
Operations Manager	Data reader account	FT-SCOM-DR	The data reader account is used to define which account credentials Microsoft SQL Server® 2008 Reporting Services uses to run queries against the Operations Manager reporting Data Warehouse.
Virtual Machine 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, make sure that the new account has a SQL Server login in the ServiceManager database and 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® 2008 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.

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

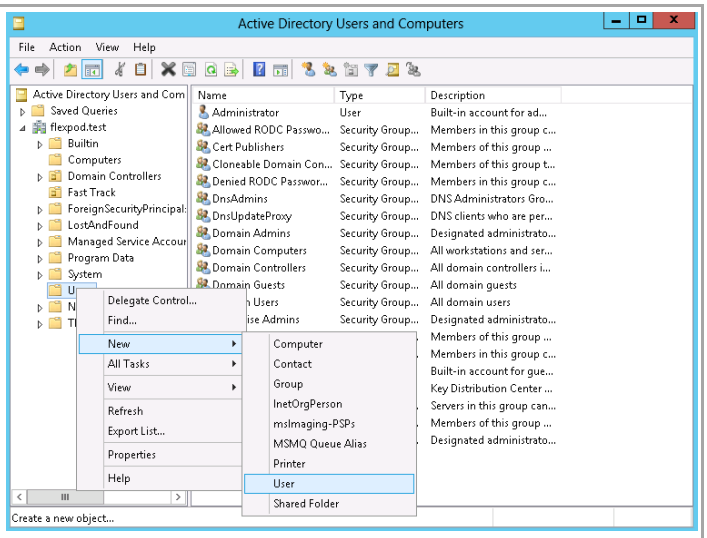
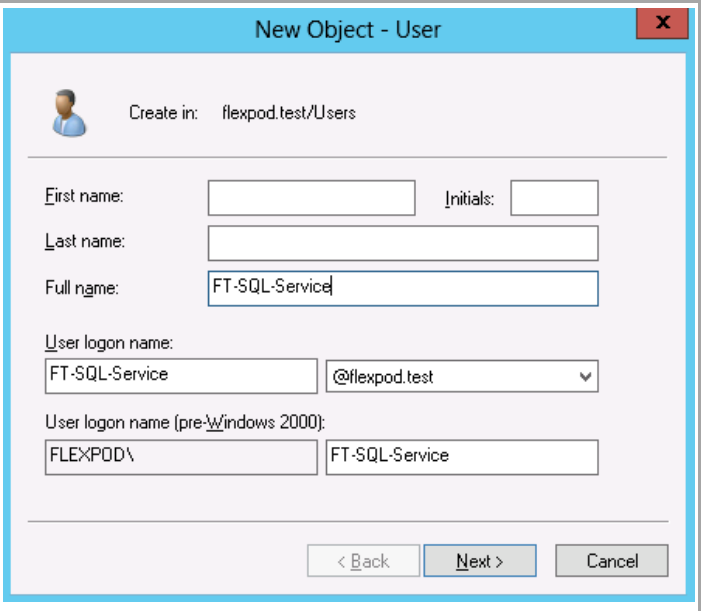
Component	Group	Name	Group notes
System Center 2012	System Center Administrators	FT-SC-Admins	This group's members are full Admins on all System Center components.
SQL Server	SQL Server Administrators	FT-SQL-Admins	This group's members are sysadmins on all SQL Server instances and local administrators 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-SCVMM-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.

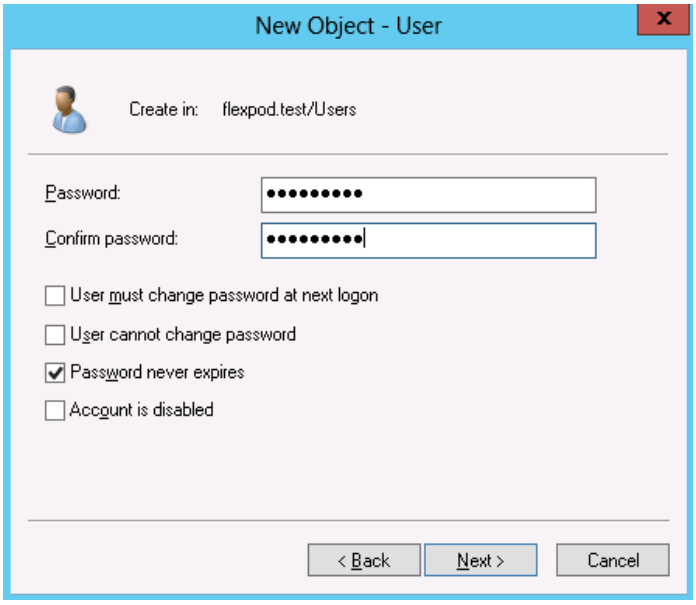
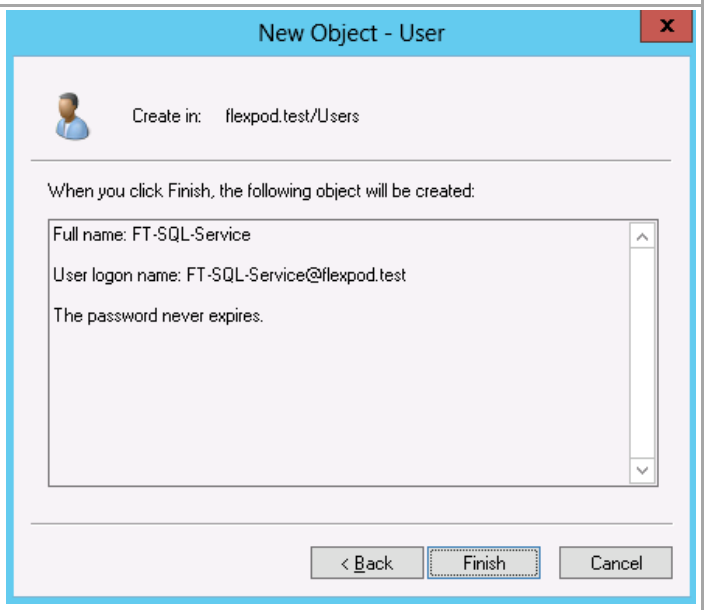
Note: Repeat the following procedure for all user accounts listed in the table above.

1. In Active Directory Users and Computers, select the users object in the left tree view. Right click the Users object, select New and Group.	
2. Enter the user group name in the Group name fields. Accept the default group scope options. Click Okay to create the group. 3. Repeat this procedure for all groups in the table above.	

4. Enter the password and password policy. Click next.	
5. Click Finish to create the user account.	

Note: Repeat the following procedure for all user groups listed in the table above.

1. Open Active Directory Users and Computers. Select the users object in the left tree view. Right click the Users object, select New and User.	
2. Enter the user account name in the Full Name and User logon name fields. Click Next.	

3. Enter the password and password policy. Click next.	
4. Click Finish to create the user account.	

14.4 Install SQL Server 2012 SP1

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

Prior to performing installation of the SQL Server 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.

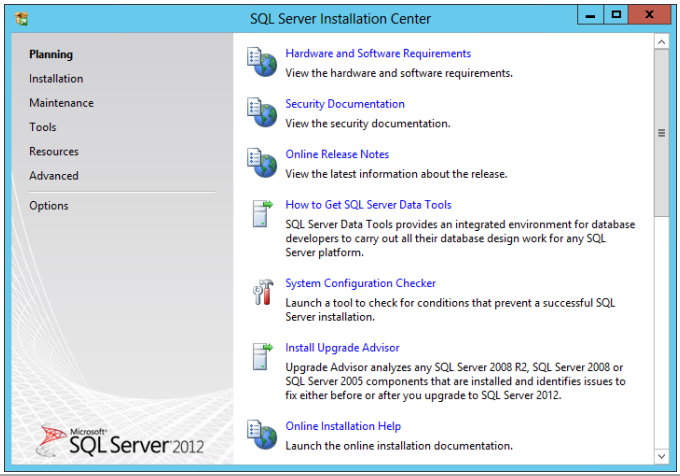
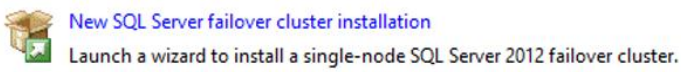
Component	Service Manager management server	Service Manager Data Warehouse server	Service Manager analysis server	App Controller, Orchestrator, Microsoft SharePoint® services Farm and WSUS	Virtual Machine Manager	Operations Manager	Operations Manager Data Warehouse
SQL Server Instance Name	SCSMDB	SCSMDW	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[4]	10434	10435	10436
SQL Server Instance Preferred Owners	Node2, Node4	Node2, Node4	Node2, Node4	Node1, Node4	Node1, Node4	Node3, Node4	Node3, Node4

The template provided in an appendix of this document should assist with capturing this information for the installation process. When gathered, the following steps are provided to perform installation.

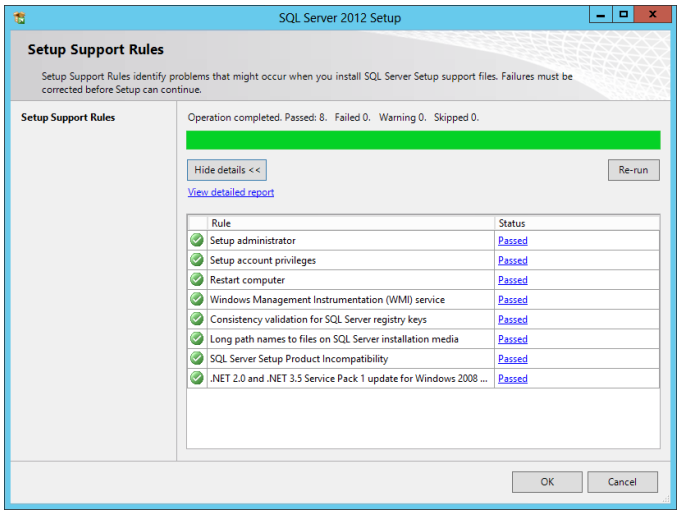
Note: At this point during the installation, the first node of the SQL Server cluster must have ownership of the LUNs.

▶ 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.

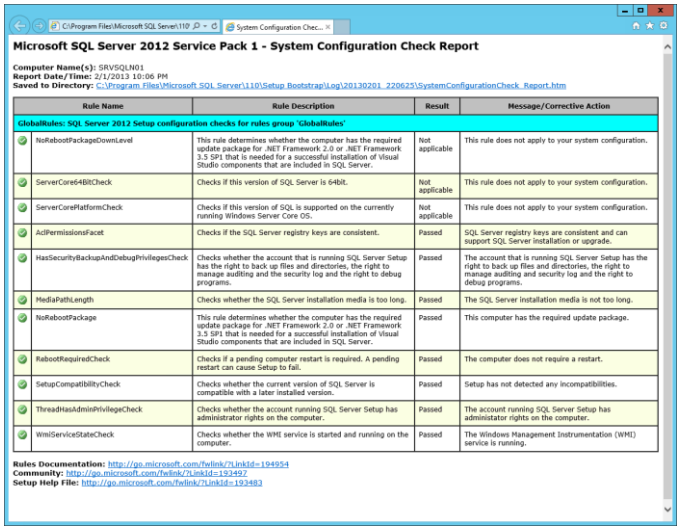
[4] Note that the SCDB instance must be configured to port 1433 if the Cloud Services Process Pack will be used.

1. As outlined before, Fast Track requires separate instances for each System Center product. The instances associated with these products are: a. SCSMDB (Service Manager database instance). b. SCSMDW (Service Manager Data Warehouse instance). c. SCSMAS (Service Manager SQL Analysis Services instance). d. SCDB (Shared App Controller, Orchestrator, Service Manager self-service portal Microsoft SharePoint® Foundation 2010 services and WSUS database instance). e. SCVMMDB (Virtual Machine Manager database instance and optional WSUS database instance). f. SCOMDB (Operations Manager database instance). g. SCOMDW (Operations Manager Data Warehouse instance). 2. 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.	
3. 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.	
4. From the **SQL Server Installation Center**, click the **New SQL Server failover cluster installation** link.	

5. 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.

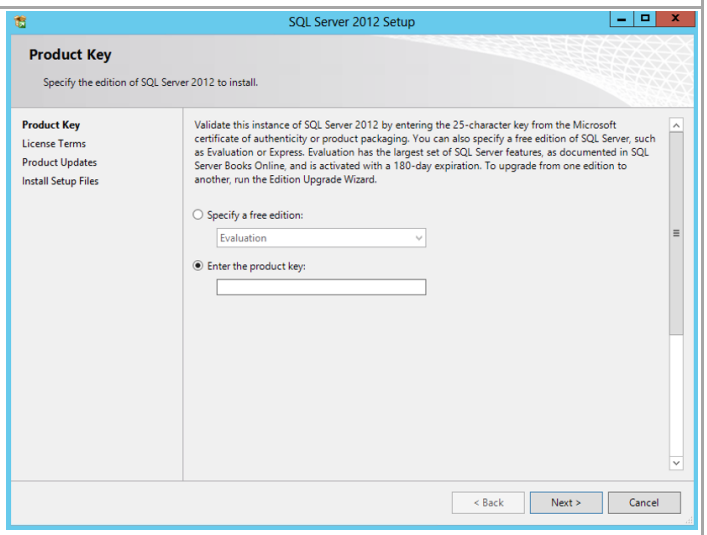


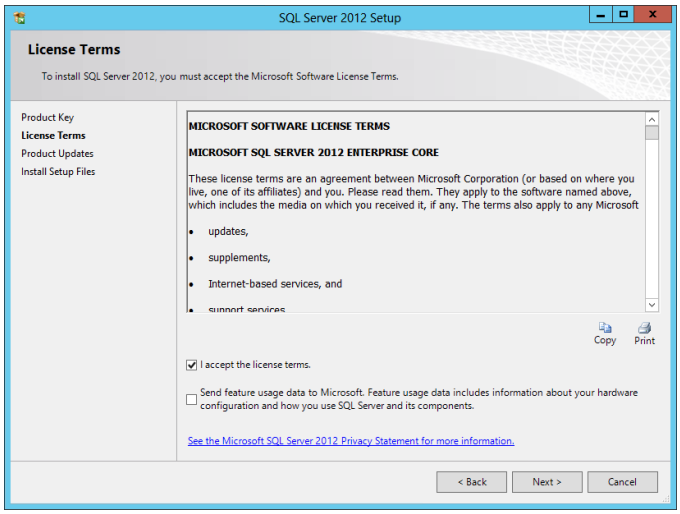
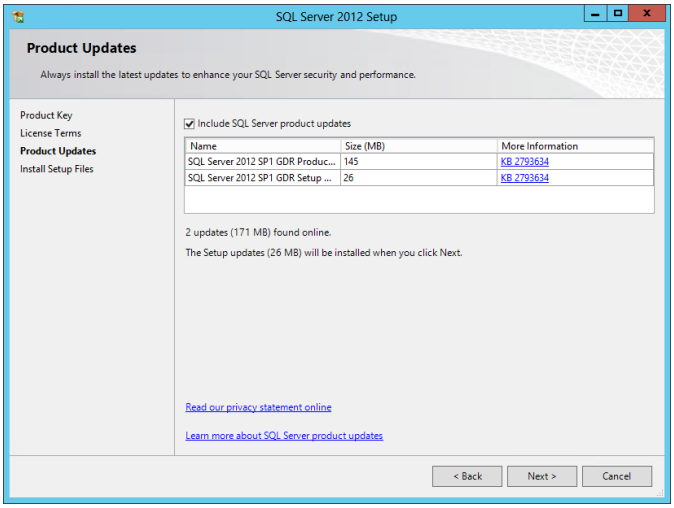
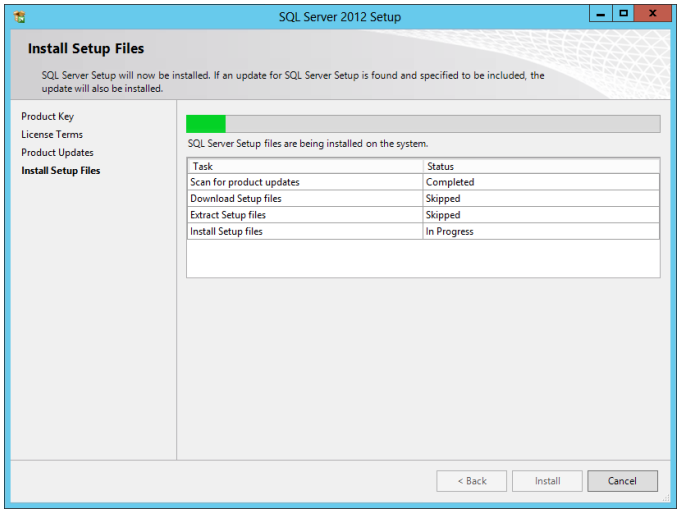
6. If the **View detailed report** link is selected, the following report is available.



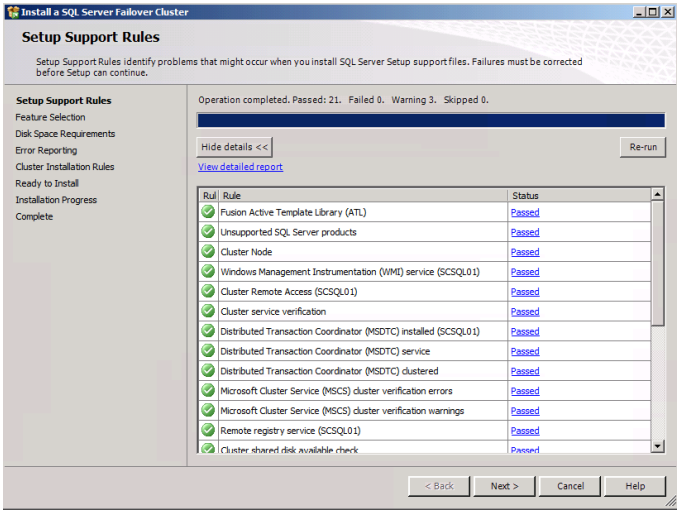
7. In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

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.

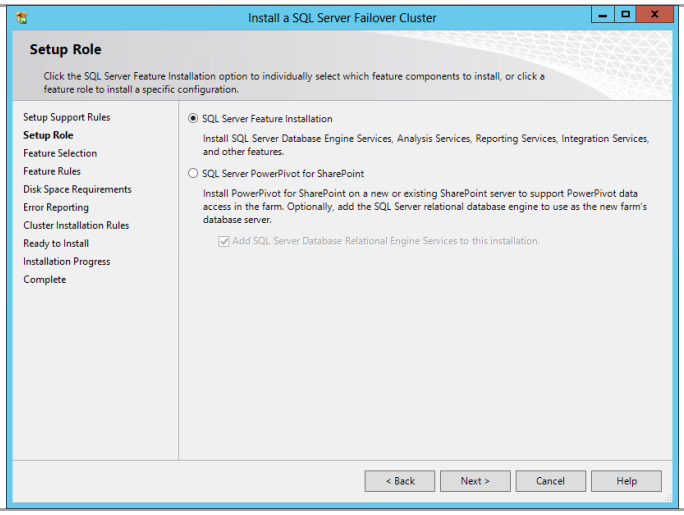


8. In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.	
9. In the **Product Updates** dialog, select the **Include SQL Server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

11. 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.

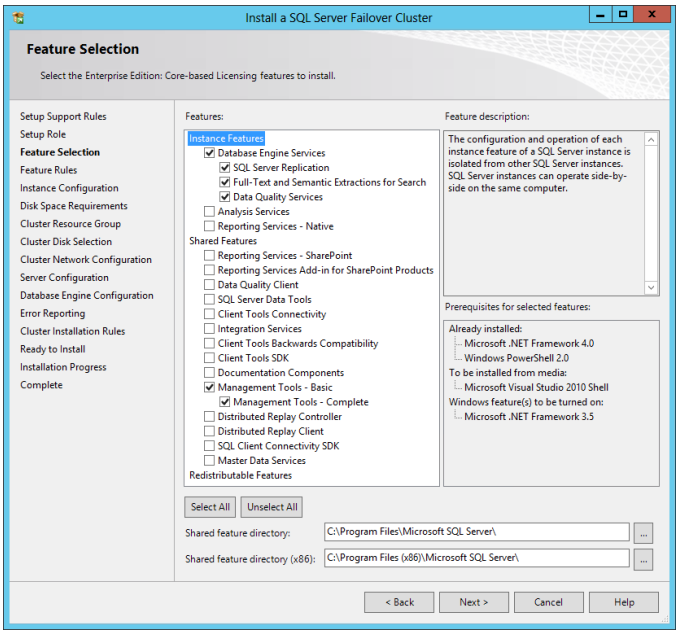


12. In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.

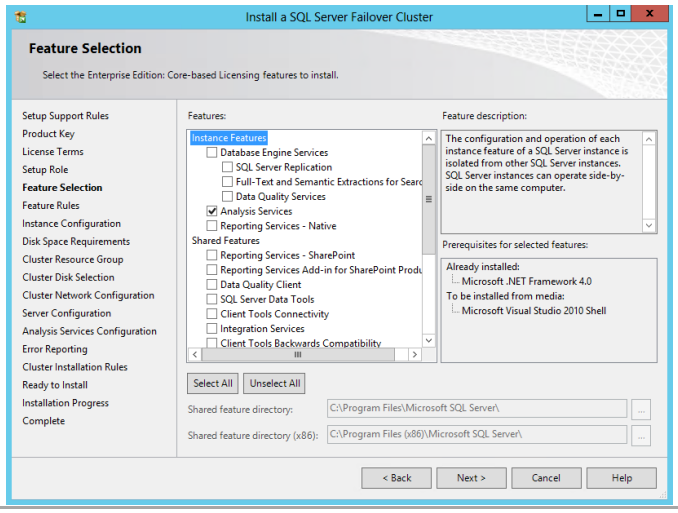


13. In the **Feature Selection** dialog, features for the various instances will be selected. Note that not all features are supported for failover cluster installations, so the features for Fast Track are limited to the features as listed below. SQL Server with failover clusters requires the selection 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:
    a. SCDB
    b. Database Engine Services
    c. SCOMDB
    d. Database Engine Services
    e. SCOMDW
    f. Database Engine Services
    g. SCSMAS
    h. Analysis Services
    i. SCSMDB
    j. Database Engine Services
    k. SCSMDW
    l. Database Engine Services
    m. SCVMMDB
    n. Database Engine Services
14. 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.

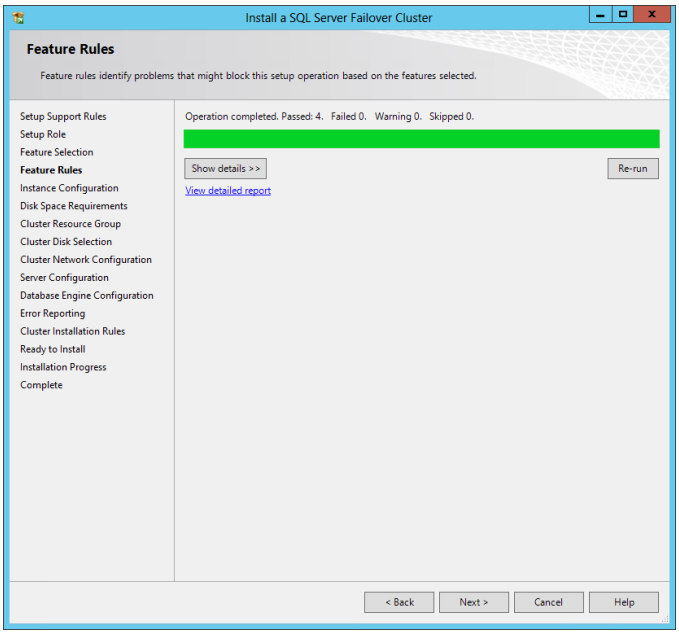
Database Engine Services (all instances except SCSMAS):



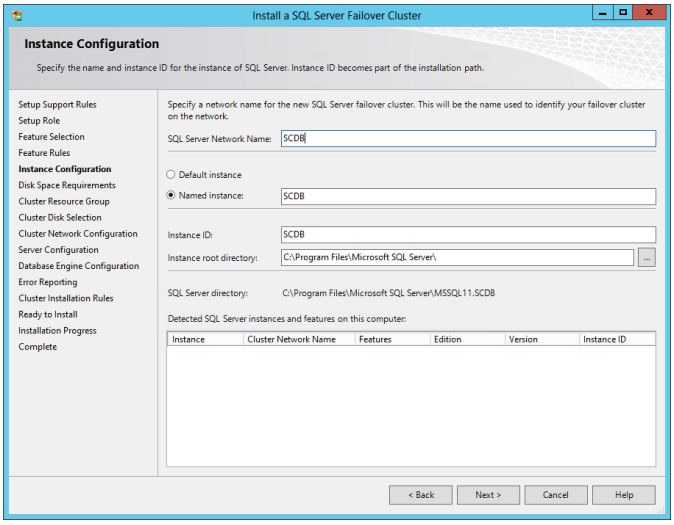
Analysis Services (SCSMAS instance only):



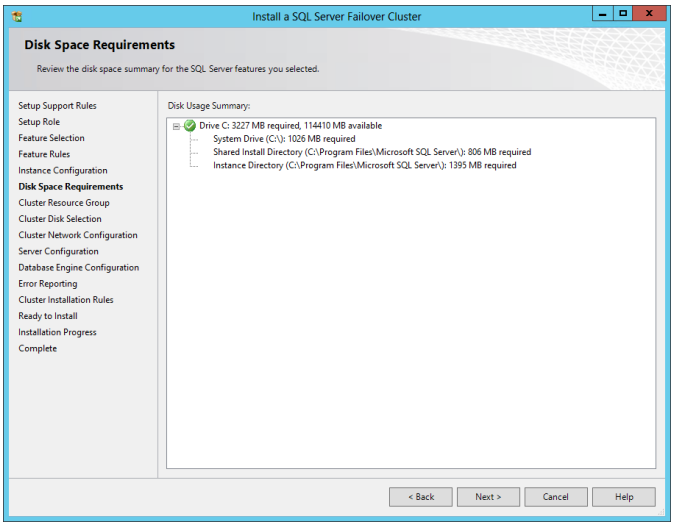
15. In the **Feature Rules** dialog click **Next** to continue. The **Show details** and **View detailed report** can be viewed if required.



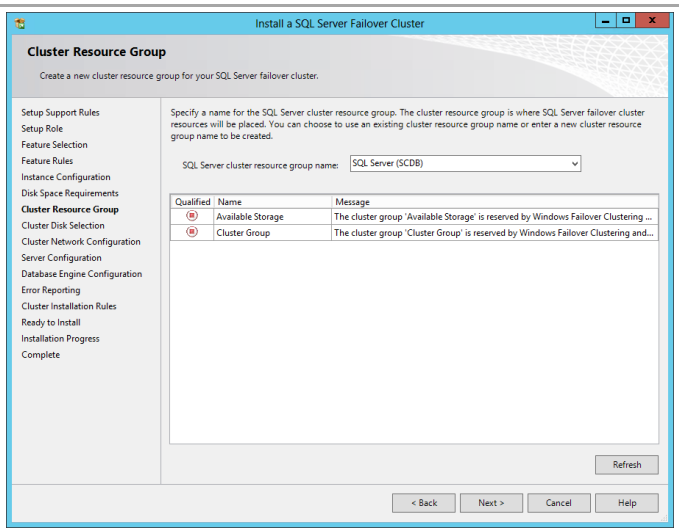
16. In the **Instance Configuration** dialog, make the following selections (refer to the worksheet created earlier):
17. **SQL Server Network Name** – *specify the cluster network name of the failover cluster instance being installed.*
18. Select the **Named instance** option. In the provided text box, specify the instance name being installed.
19. **Instance ID** – *specify the instance name being installed. Verify that it matches the **Named instance** value.*
20. **Instance root directory** – *accept the default location of %ProgramFiles%\Microsoft SQL Server.*
21. Click **Next** to continue.



22. In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.

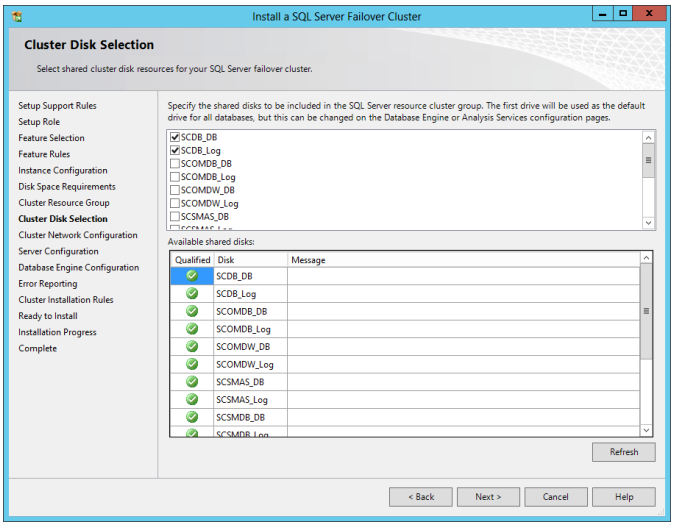


23. In the **Cluster Resource Group** dialog, in the **SQL Server cluster resource group name** drop-down menu, accept the default value of **SQL Server (*<InstanceName>*).** Click **Next** to continue.

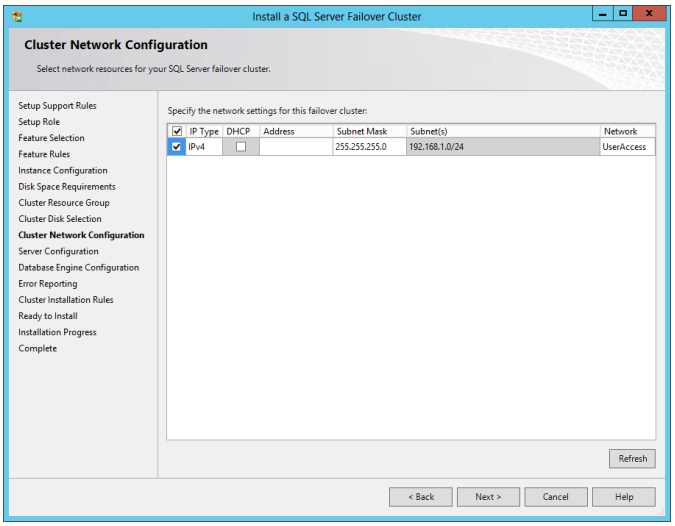


24. In the **Cluster Disk Selection** dialog, refer to the worksheet created earlier to make the proper disk selections. Two cluster disks will be selected to support separation of databases and logs for each database instance. Make the selections by selecting the appropriate **Cluster Disk** check boxes and click **Next** to continue.

Note: Cluster disks can be renamed in Failover Cluster Manager to friendly names as illustrated in this dialog.

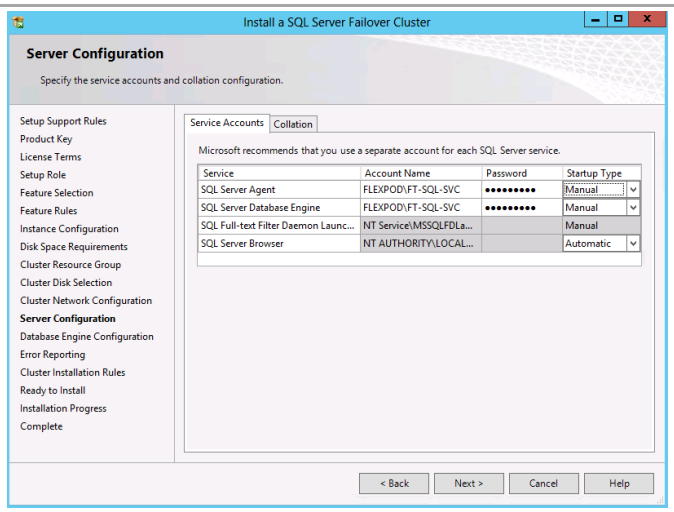


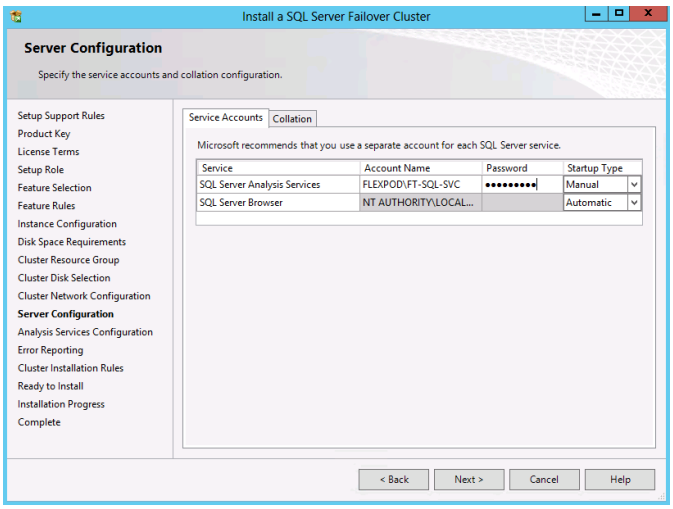
25. In the **Cluster Network Configuration** dialog, refer to the worksheet created earlier to assign the correct IP for each instance. Clear the **DHCP** check box if you are using static addressing and enter the IP address in the **Address** field text box. When complete, click **Next** to continue.



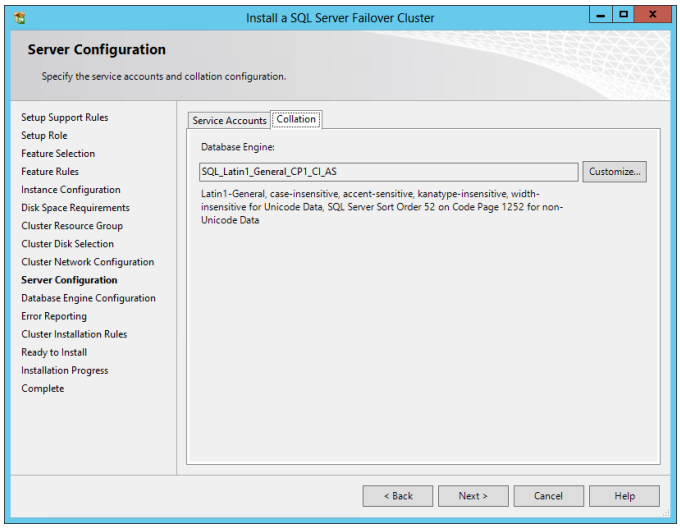
26. In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services.

Note: 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.

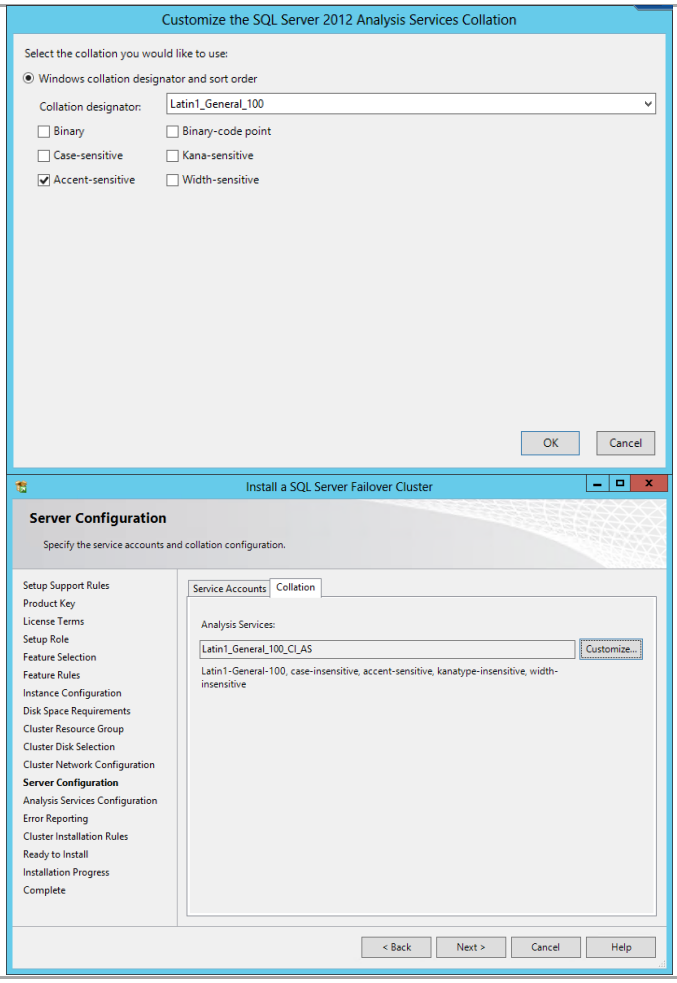




27. In the same **Server Configuration** dialog, select the **Collation** tab. Accept the default collation in the **Database Engine** field (unless multiple language support is required in Service Manager[5]) and click **Next** to continue.

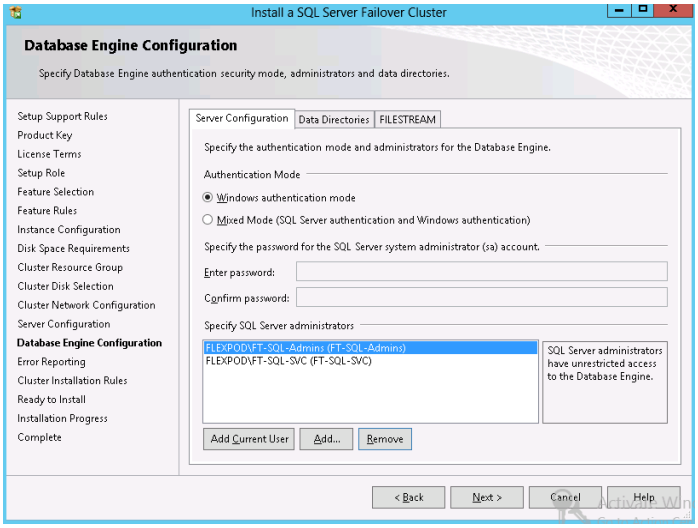


Note: In the case of **Service Manager instances**, the collation must be specified differently. This is done through the **Customize...** button. In these cases you can select accent and case sensitivity along with other collation designators. The following example is provided.



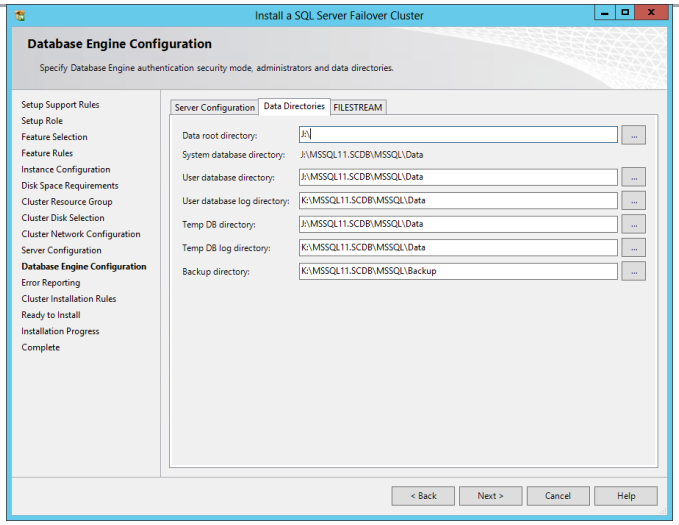
5 http://social.technet.microsoft.com/wiki/contents/articles/7784.collation-in-system-center-2012-service-manager.aspx.

28. In the **Database Engine Configuration** dialog select the **Account Provisioning** 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.



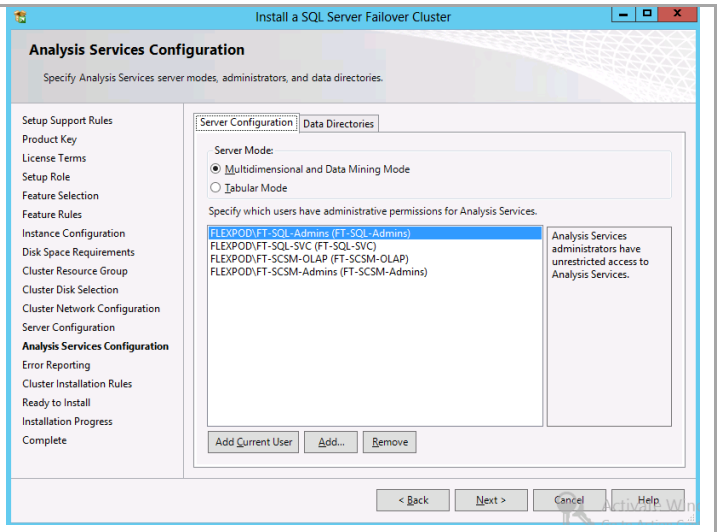
29. In the same **Database Engine Configuration** dialog, select the **Data Directories** tab. The proper drive letter or mount point associated with the Cluster Disk resource for SQL Server data should be specified. If not, verify that the proper Cluster Disk resource check boxes were selected earlier 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 database log 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. When 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.

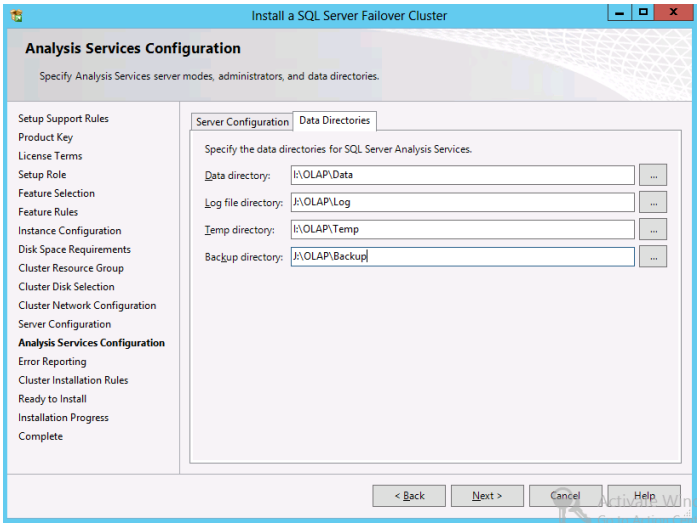


Note: In instances that contain Analysis Services within the **Analysis Services Configuration** dialog, click the **Server Configuration** tab. In the Specify which users have administrative permissions for Analysis Services section, click Add Current User to add the current installation user. Click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

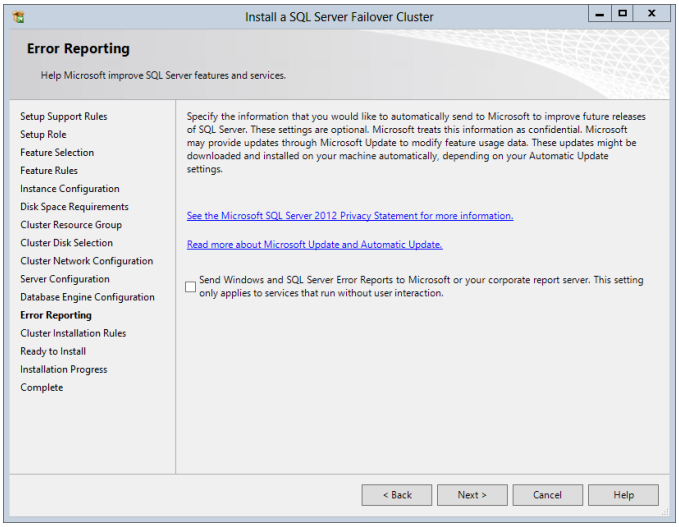
- Service Manager instance:
- Fast Track SQL Server Admins group
- Fast Track SQL Server Service account
- Fast Track SM Admins group
- Fast Track SM OLAP account



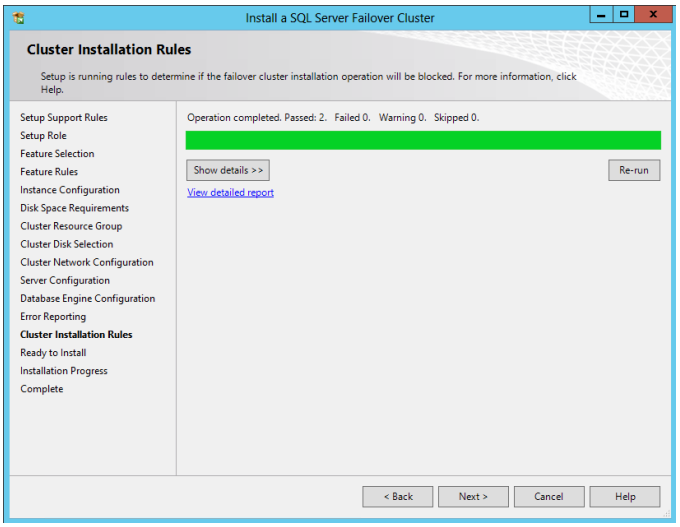
30. For instances with Analysis Services, use the following configuration:
    a. On the **Data Directories** tab, set the Data directory, and Temp directory to the cluster disk configured for the database files. Set the Log file directory and the Backup directory to the cluster disk configured for the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



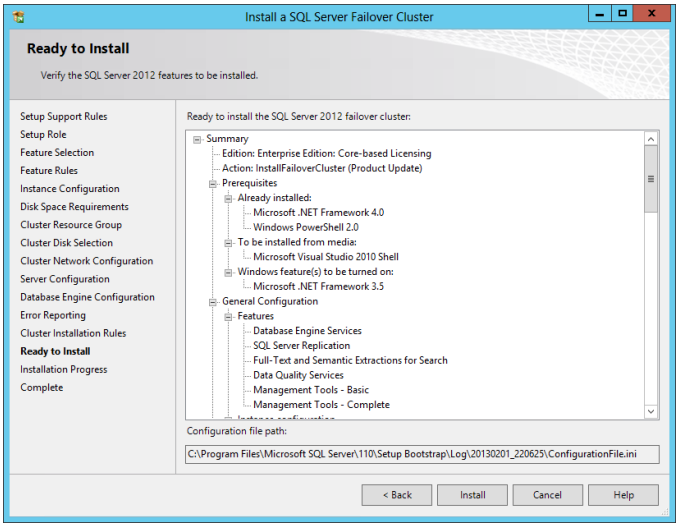
32. In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



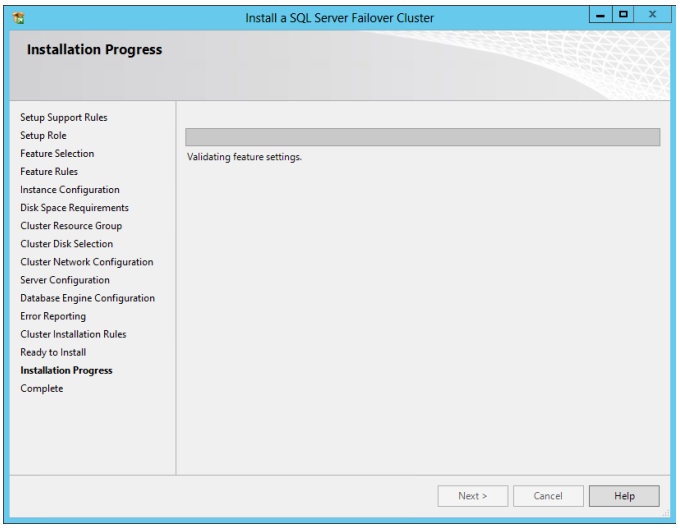
33. In the **Cluster Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

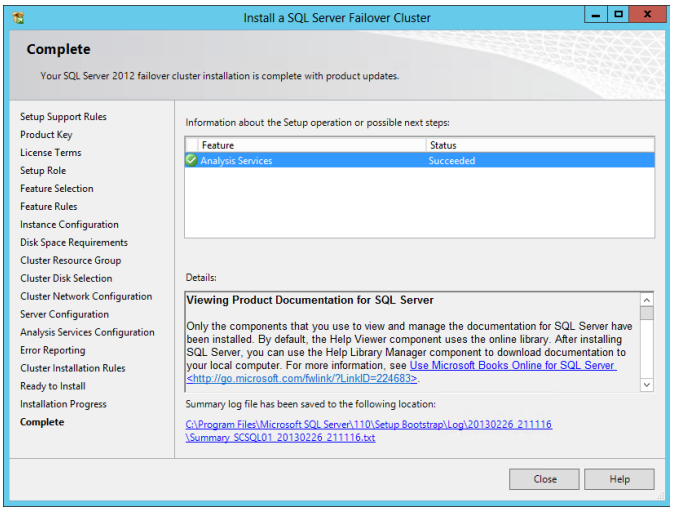
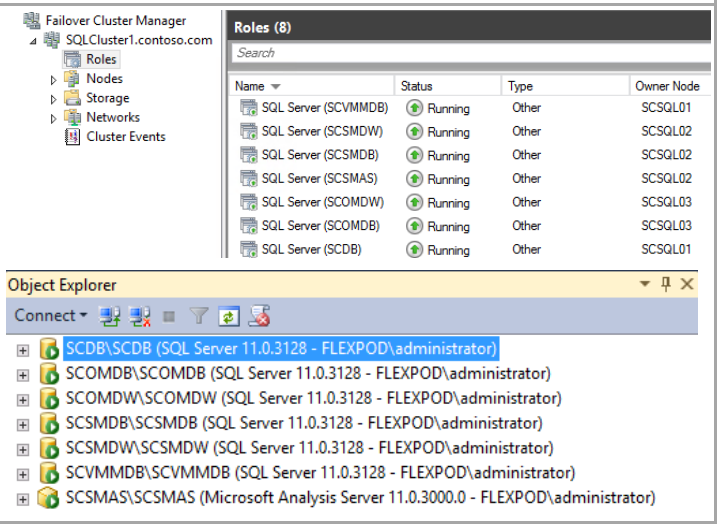


34. In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



35. In the **Installation Progress** dialog, the installation progress will be displayed.



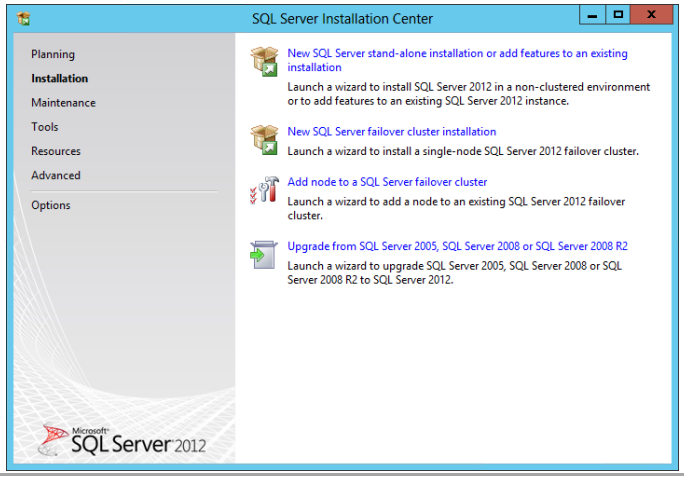
36. When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.	
37. Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).	
38. Verify the installation by inspecting 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 Server Named Instances on the Guest Cluster (Node 2)

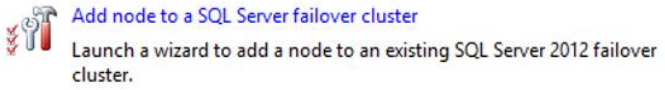
When the creation of all required SQL Server instances on Node 1 is complete, the second node can be added to each instance of the cluster. Follow the steps below to begin the installation of additional nodes of the cluster.

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

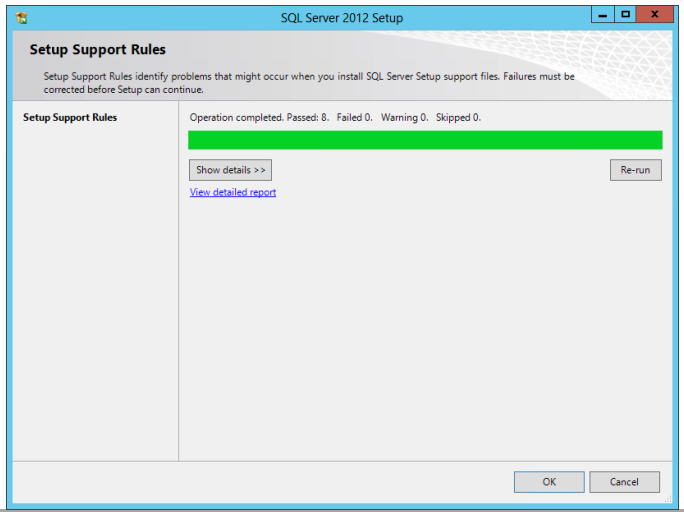
1. From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear.



2. From the **SQL Server Installation Center** click the **Add node to a SQL Server failover cluster** link.

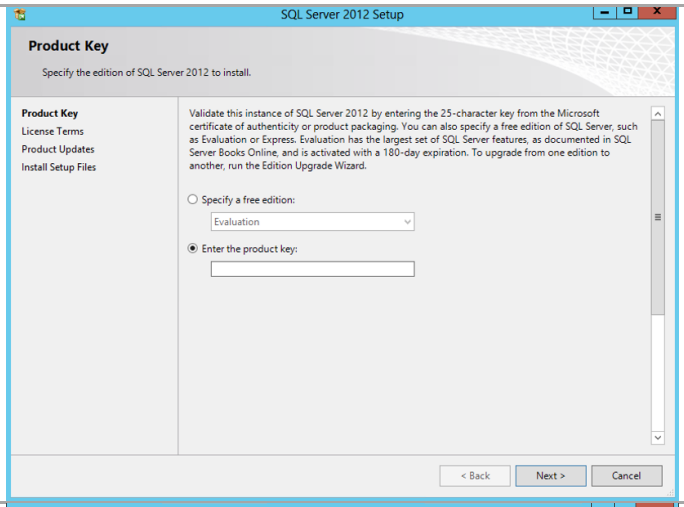


3. The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

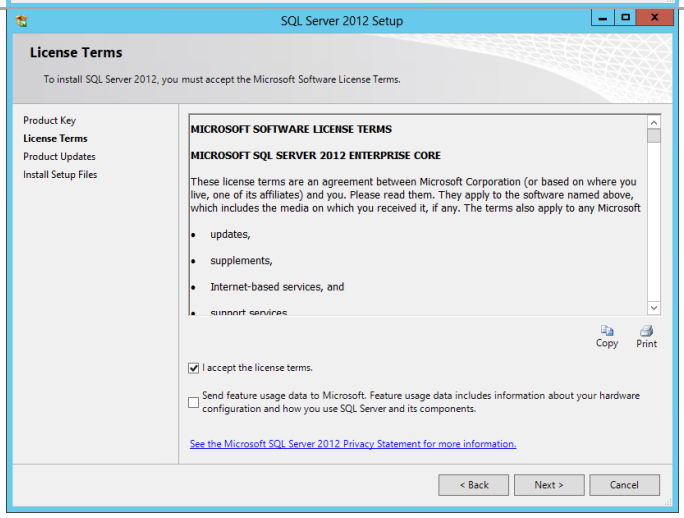


4. In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

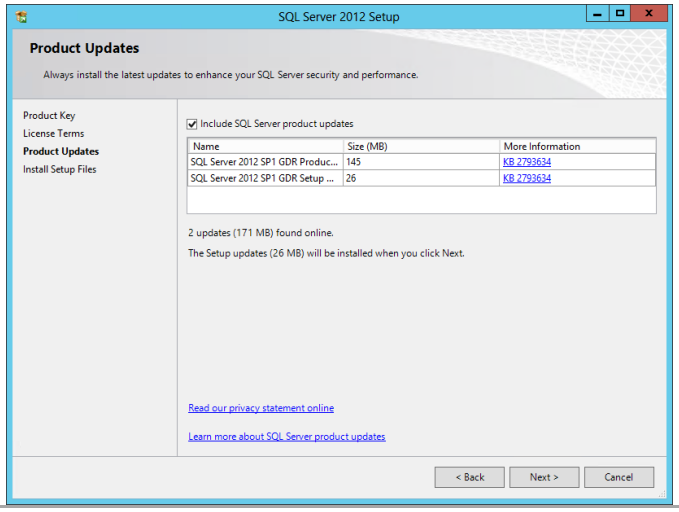
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



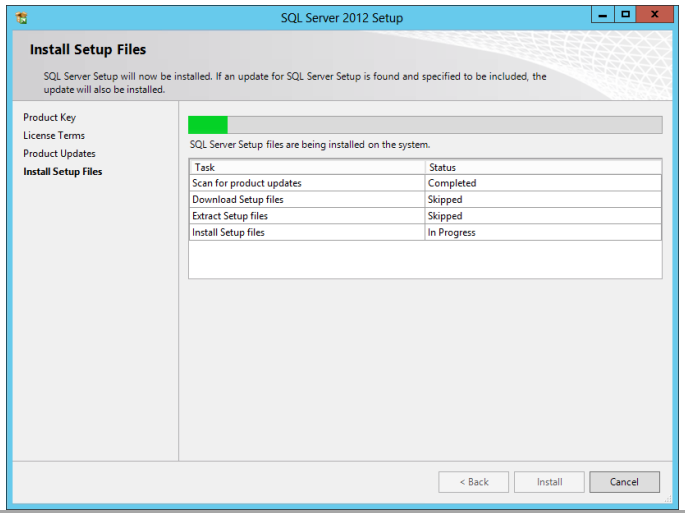
5. In the **License Terms** dialog, select the **I accept the license terms** checkbox. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.



6. In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.

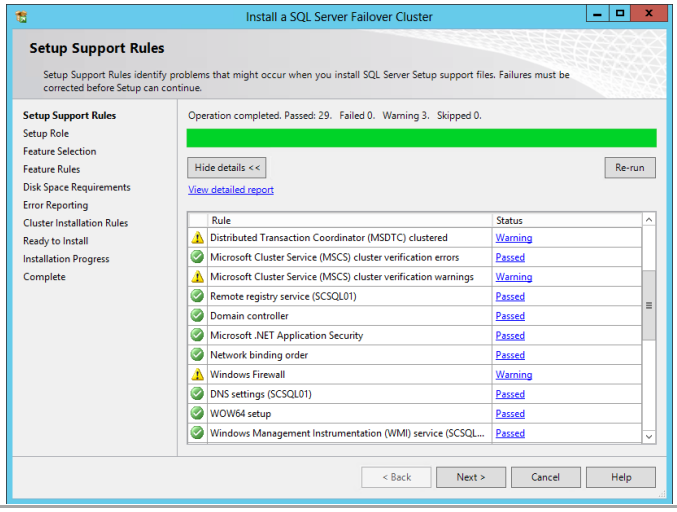


7. In the **Install Setup Files** dialog, click **Install** and allow the support files to install.

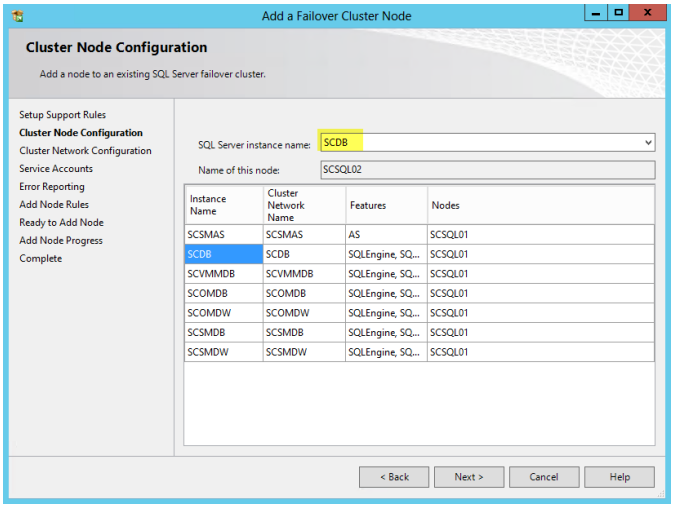


8. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Click **Next** to continue.

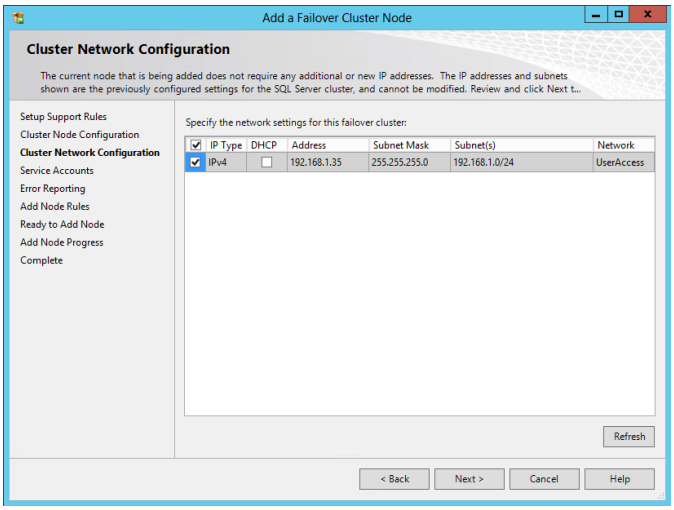
Note: The use of MSDTC is not required for the System Center 2012 SP1 environment.



9. 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.

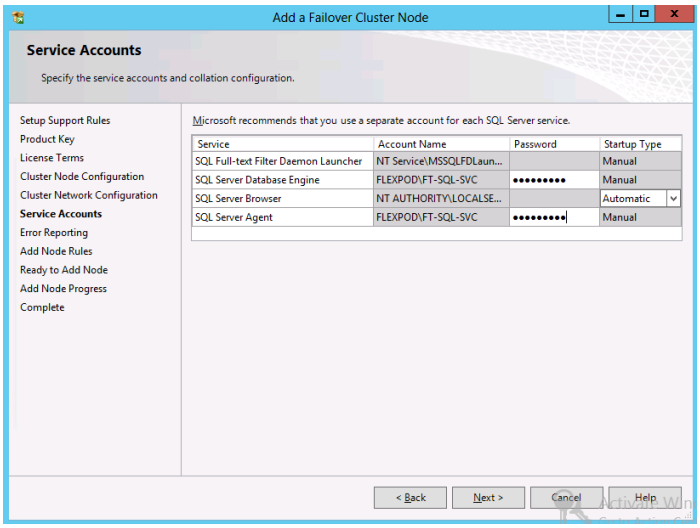


10. In the **Cluster Network Configuration** dialog, the network configuration values are displayed and set based on the existing failover cluster instance values from the first node and cannot be modified. Click **Next** to continue.

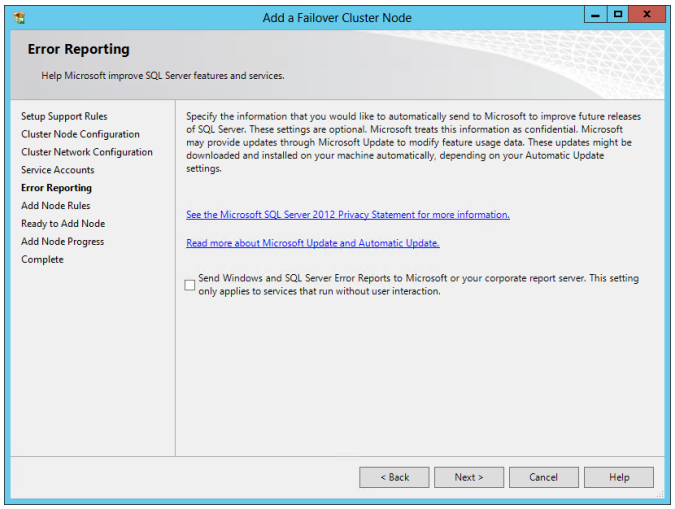


11. In the **Service Accounts** dialog, specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services. When complete, click **Next** to continue.

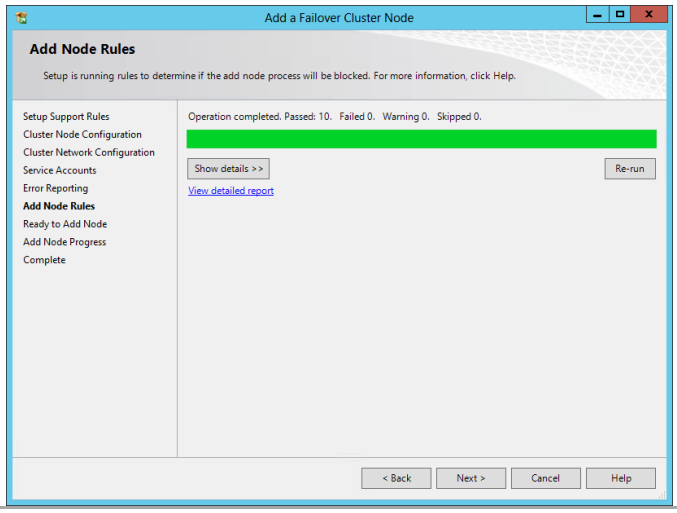
Note: for the SCSMAS instance only, an additional password must be supplied for the **SQL Server Analysis Services** service account.



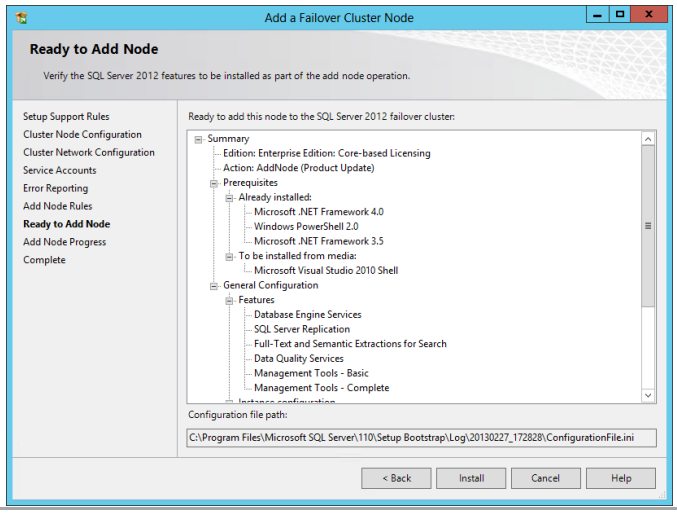
12. In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



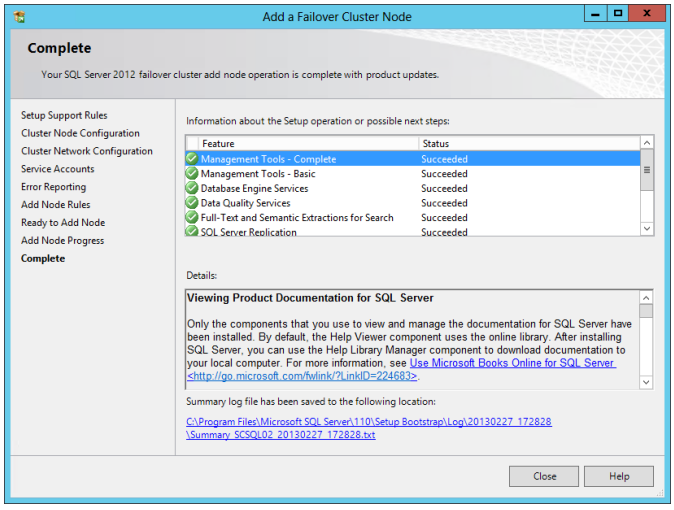
13. In the **Add Node Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



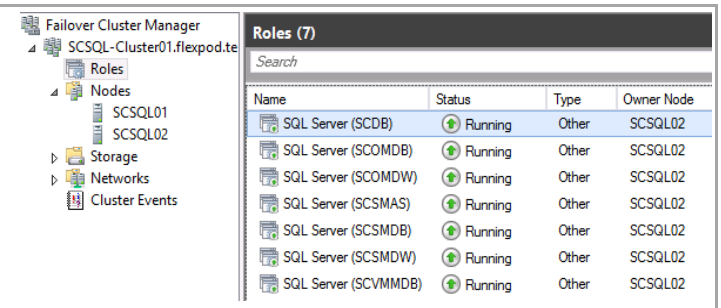
14. In the **Ready to Add Node** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the second SQL Server node for the selected instance.

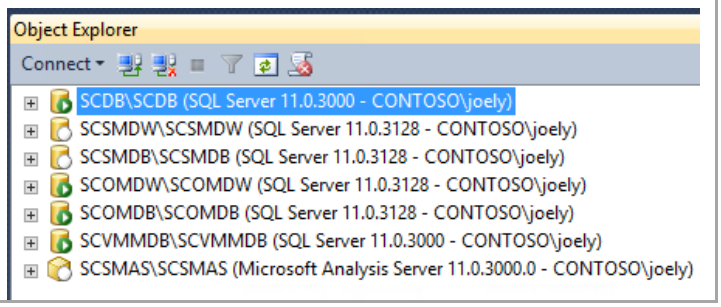


15. When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.
16. Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).



17. 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.





14.5 Post-Installation Tasks

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

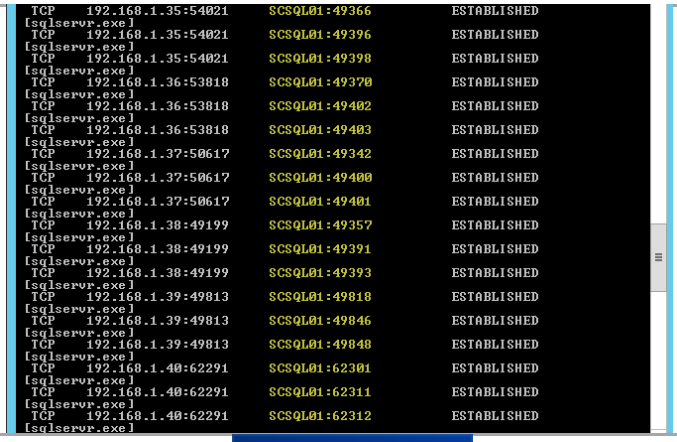
Configure Windows Firewall Settings for SQL Named Instances

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.

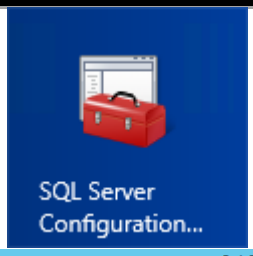
This process is described in TechNet[6] and instructions are provided in this document.

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

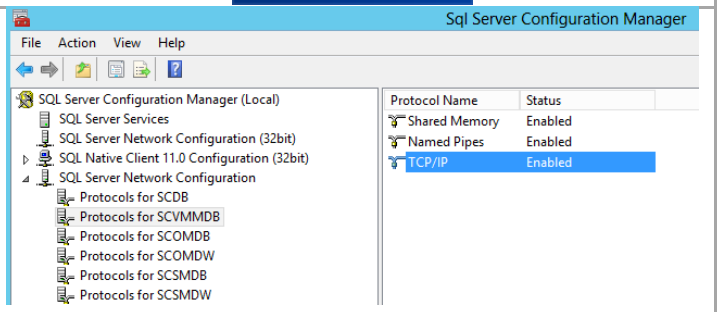
1. Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt execute the following command: **netstat –b**
2. Notice the existing dynamic ports used by the SQLSERVER.EXE sessions.



3. On the first SQL Server node open **SQL Configuration Manager**.

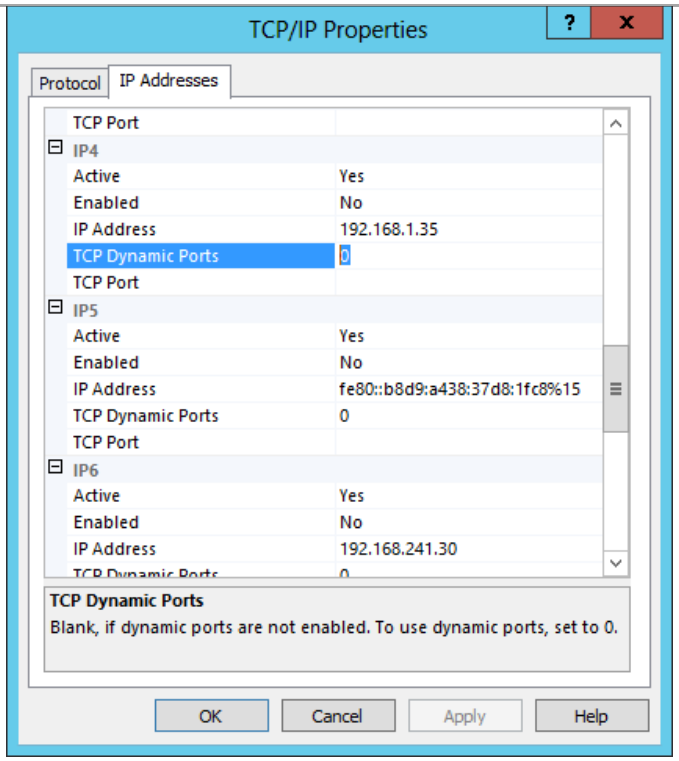


4. In the **SQL Server Configuration Manager** console pane, expand the **SQL Server Network Configuration** node and then expand the **Protocols for the <instance name>** node. When selected, double-click **TCP/IP** from the available protocol names to observe its properties.

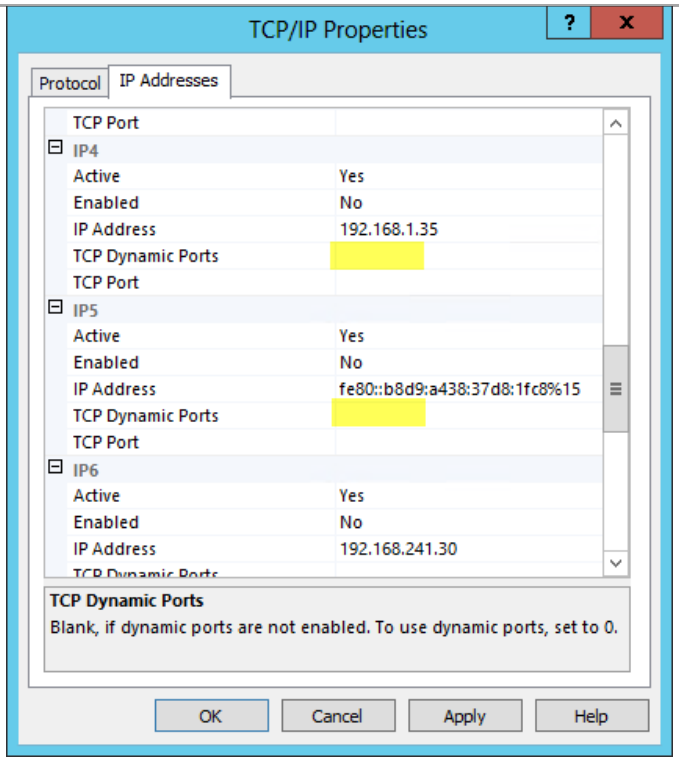


[6] Configure a Server to Listen on a Specific TCP Port - http://technet.microsoft.com/en-us/library/ms177440(v=sql.110).aspx

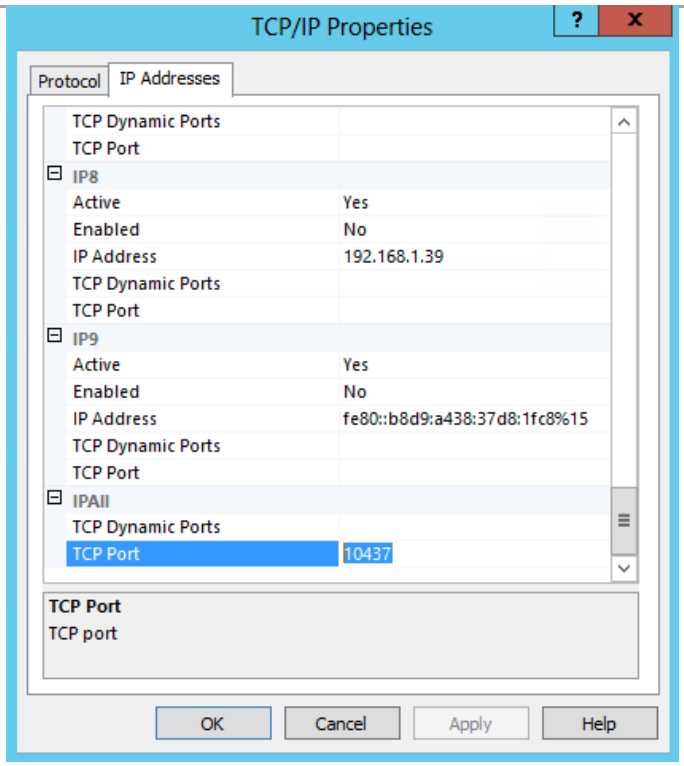
5. In the **TCP/IP Properties** dialog, select the **IP Addresses** tab, several IP addresses appear in the format IP1, IP2, up to IPAll. Each address will include several values:
6. **Active** - *Indicates that the IP address is active on the computer. Not available for IPAll.*
7. **Enabled** - *If 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.*
8. **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.*
9. **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.*
10. **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.*
11. 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.



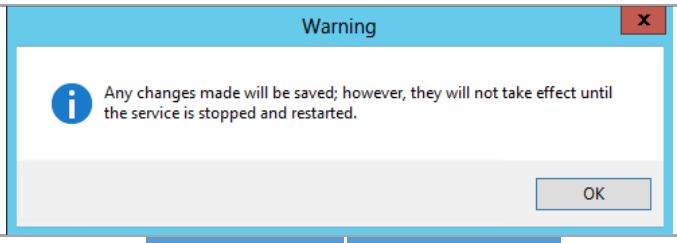
12. Within the dialog, browse to each IP address section for the instance and delete the numerical value (0) from the **TCP Dynamic Ports** field.



13. 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.



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



14. Repeat these steps to set a static port for each database service instance.
15. Reference the SQL settings table at the beginning of this section for the default values used in this guide.
16. When 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.

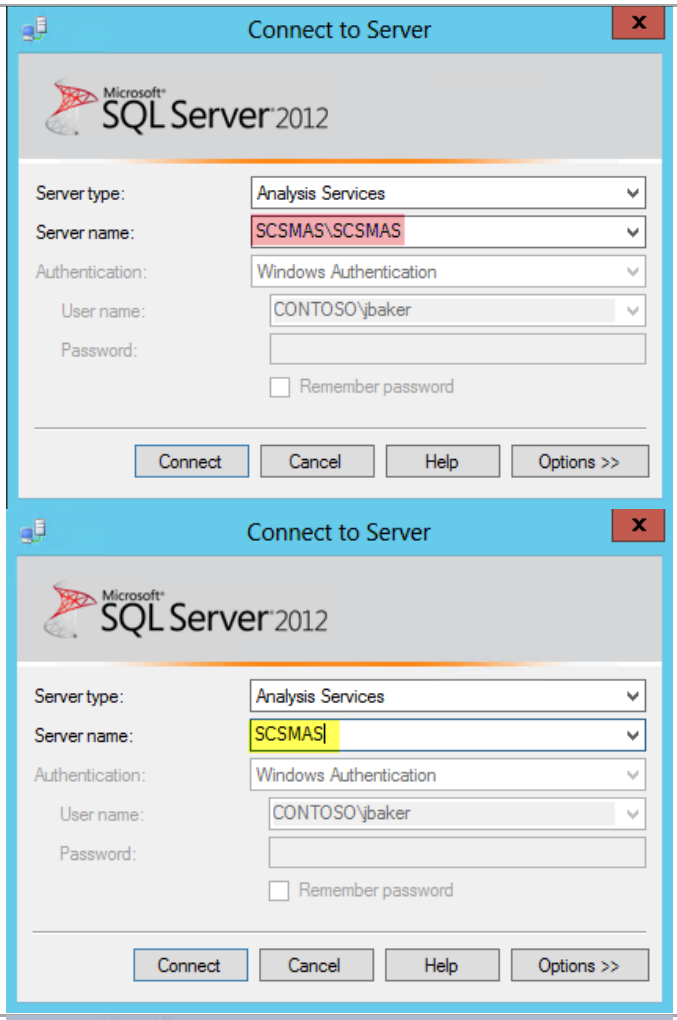
SQL Instance	Listening Port
SCDB	1433
SCVMMDB	10434
SCOMDB	10435
SCOMDW	10436
SCSMDB	10437
SCSMDW	10438
SCSMAS	10439

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

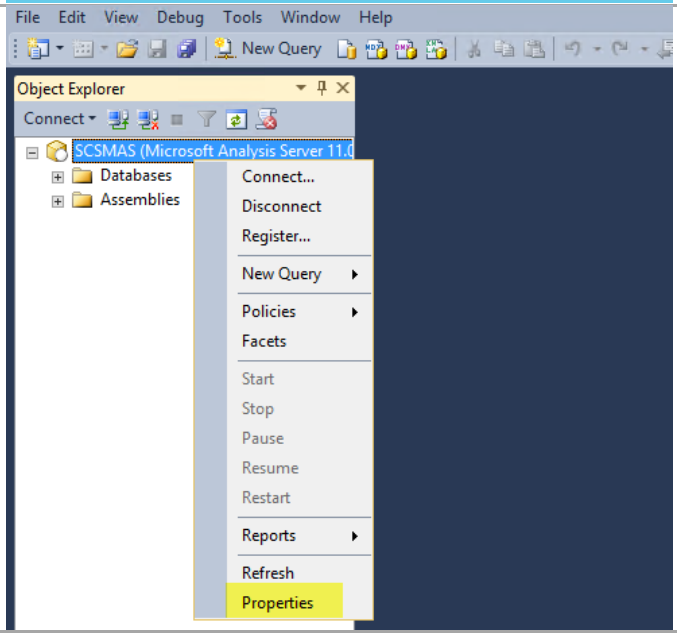
17. Open **SQL Server Management Studio**.

18. 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.

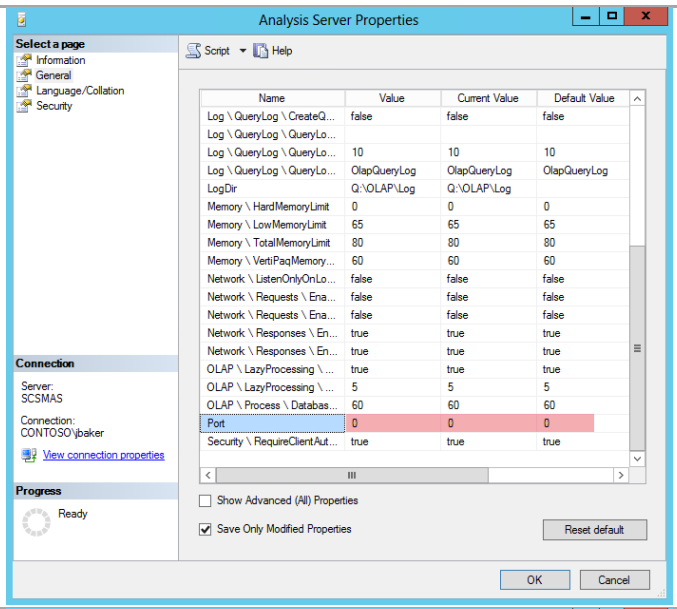
Note: Be sure the account you are logged on with is a member of the FT-SQL-Admins domain group or has otherwise been defined as a SQL sysadmin for the instance.



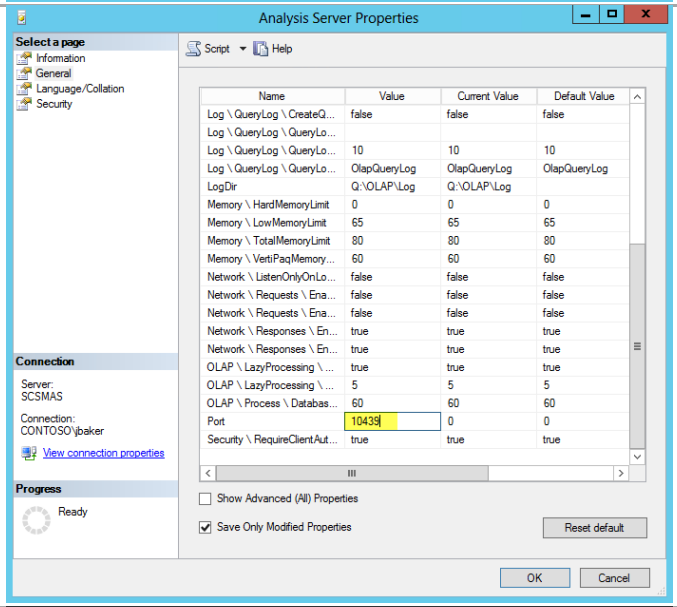
19. When connected to the instance in **SQL Management Studio**, right-click the SSAS instance and select **Properties**.



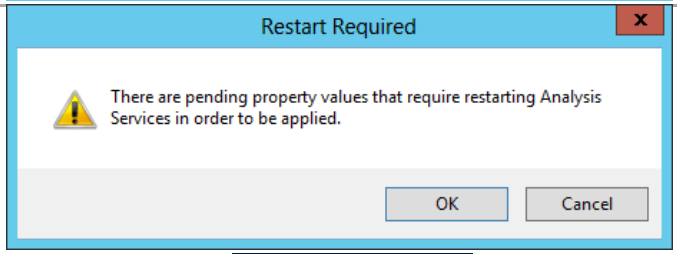
20. In the Analysis Server Properties dialog, select the **General** tab and then select **Port** (SQL listening port) from the **Name** column. By default the value will be set to "0" (zero) to specify a dynamic port.



21. In the same dialog, specify an appropriate static port value then click **OK** to save the changes.

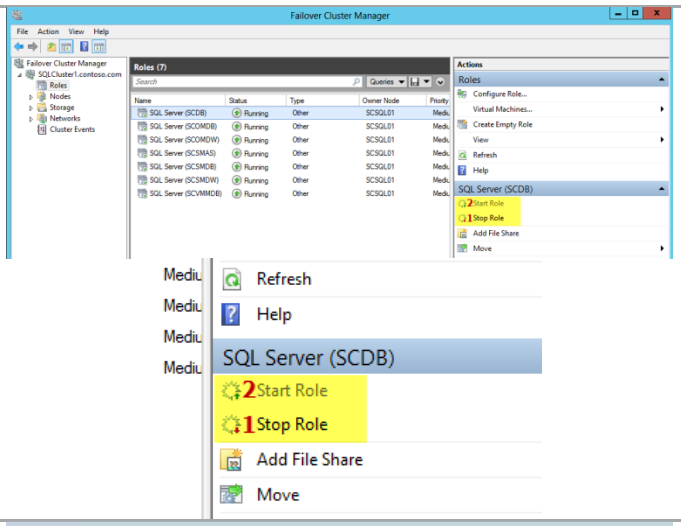


22. A dialog will appear outlining that a restart is required. Click **OK** and close SQL Management Studio.

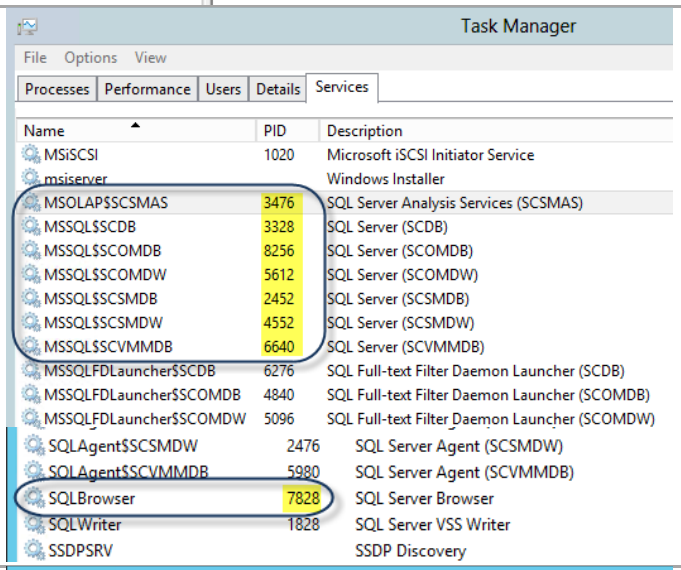


23. Open **Failover Cluster Manager** and expand the **Roles** node.

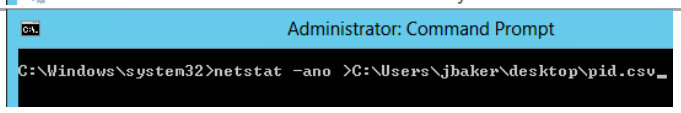
24. To apply the new port settings, in **Failover Cluster Manager** select each SQL Server instance. In the action pane, select **Stop Role** to stop the service for each instance. Restart each instance by selecting **Start Role** from the action Pane. Close the **Failover Cluster Manager** console.



25. 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.



26. 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 -an`** to export the output to a CSV file.

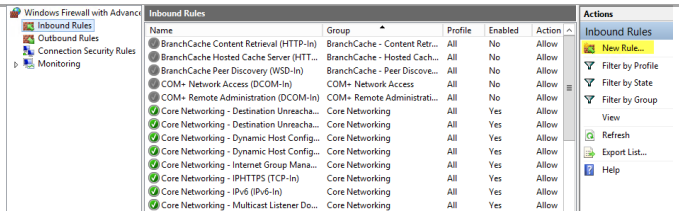


27. Import the CSV file into Excel and then format the data into a table.
28. Filter on the PID column, selecting only the PIDs you documented from the task manager step previously and then filter on the state column selecting only the listening and blank values.
29. The resulting table should confirm that all of the SQL instances are listening on only the static port assigned previously.
30. 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.

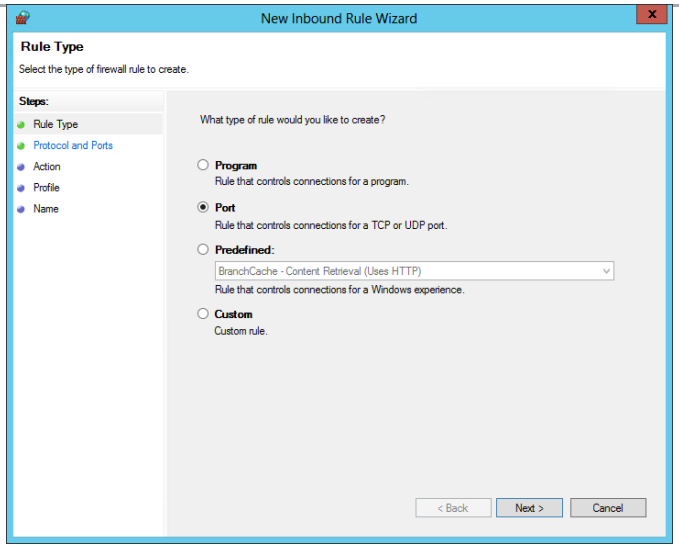
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING	7828
TCP	192.168.1.35:1433	0.0.0.0:0	LISTENING	3328
TCP	192.168.1.36:10434	0.0.0.0:0	LISTENING	6640
TCP	192.168.1.37:10435	0.0.0.0:0	LISTENING	8256
TCP	192.168.1.38:10436	0.0.0.0:0	LISTENING	5612
TCP	192.168.1.39:10437	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

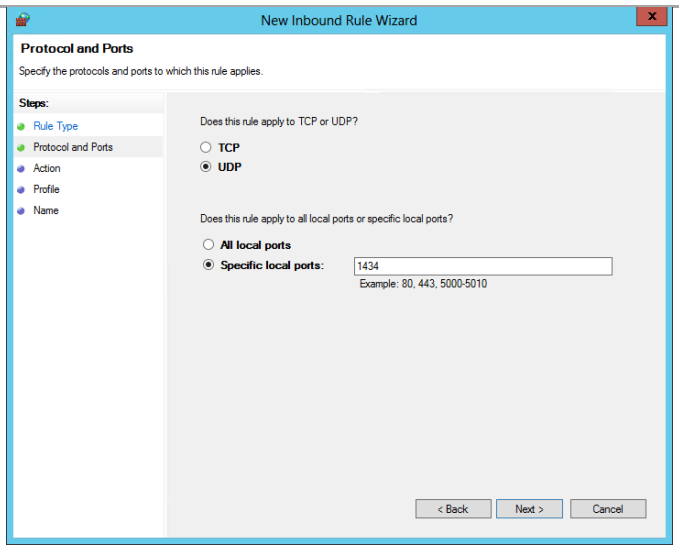
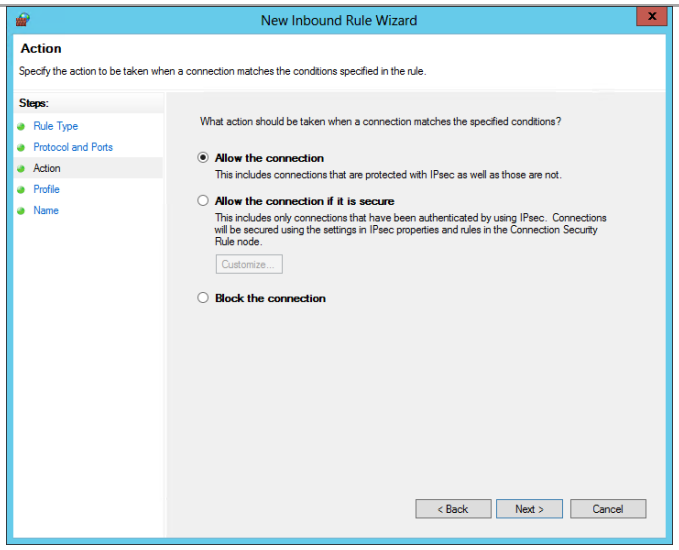
31. When completed, configure the Windows Firewall Rule for the SQL Browser Service. To perform this action, on each node in the Windows Failover Cluster that will host SQL instances, open the **Windows Firewall with Advanced Security** MMC console.

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

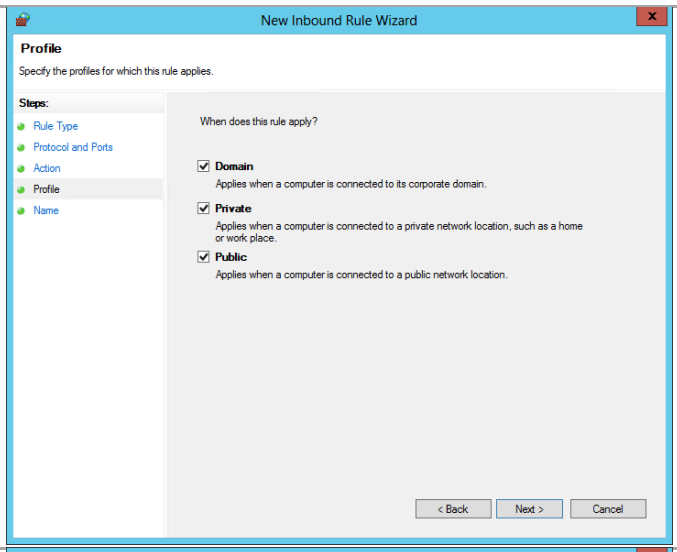


33. In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.

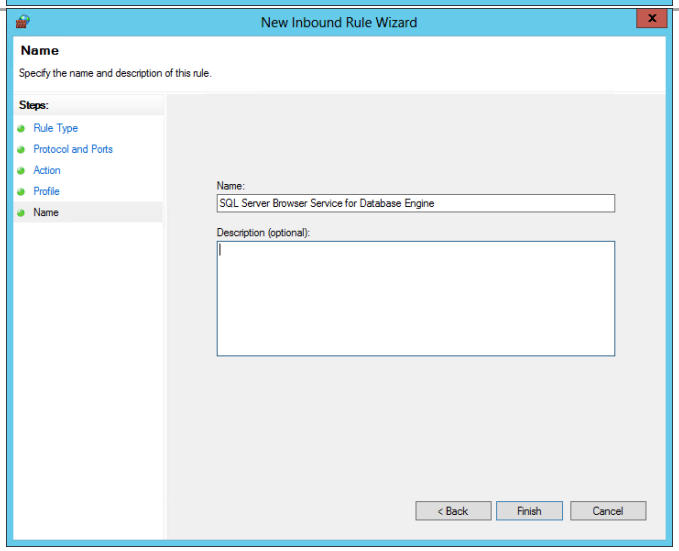


34. On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input 1434 to enable access to the SQL Browser service for Database Engine instances. Click **Next** to continue.	
35. On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.	

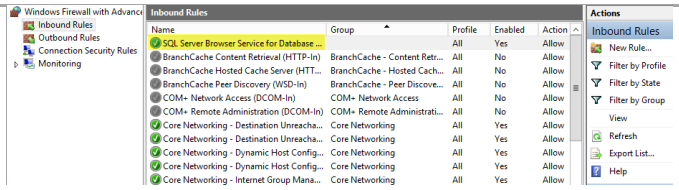
36. On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.
37. Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.



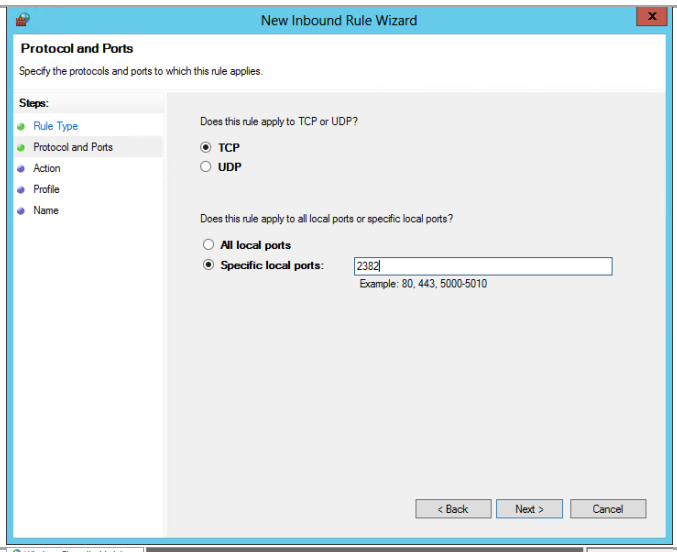
38. Specify a name for the new rule such as "*SQL Server Browser Service for Database Engine*" and click **Finish**.



39. Note 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.

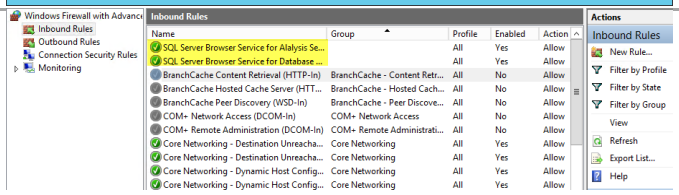


40. Repeat the previously outlined steps to create the new rule, however on the **Protocol and Ports** page, select both the **TCP** and **Specific local ports** radio buttons. Specify the value of **2382** to enable access to the **SQL Browser service for the Analysis Server** instance.

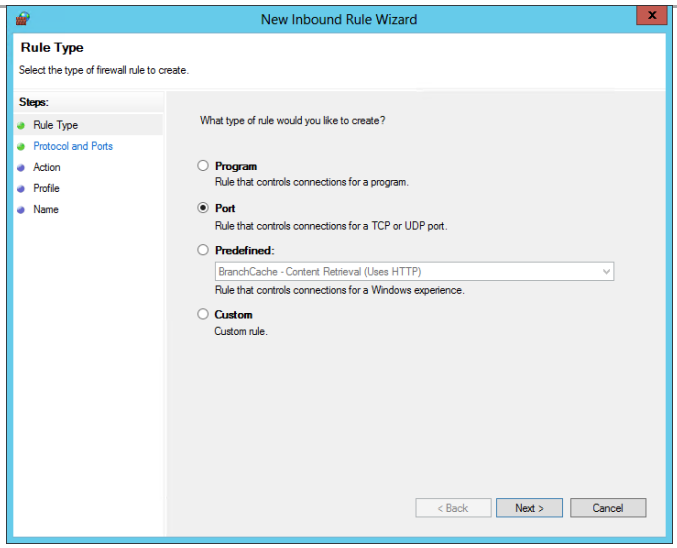


Note: Additional new rule listed in the Inbound Rules pane.

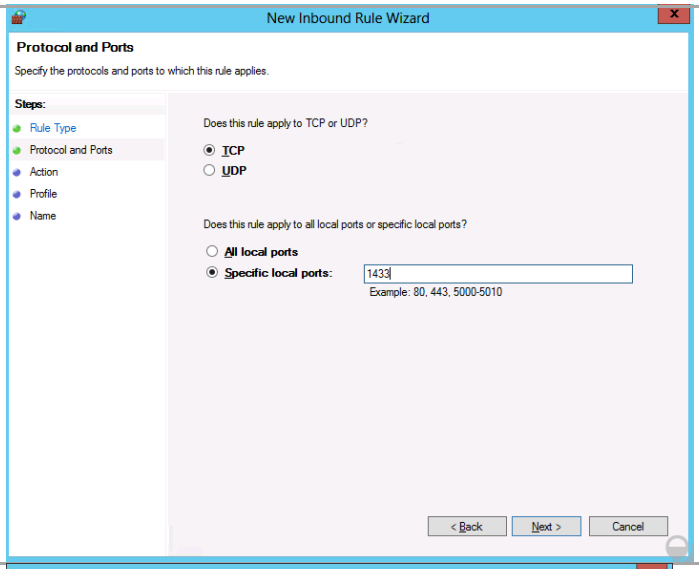
41. Next the inbound Windows Firewall rule for each of the SQL instances must be created and configured. From the same dialog, select **New Rule** from the action pane to create the firewall rule for the first named instance.



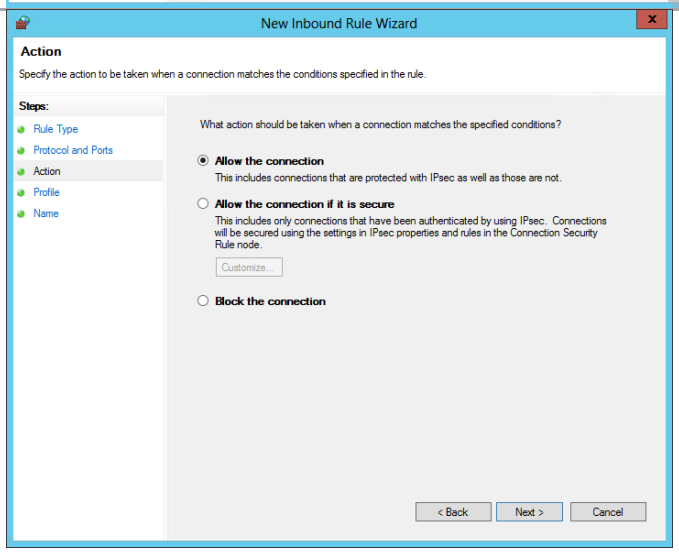
42. In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.



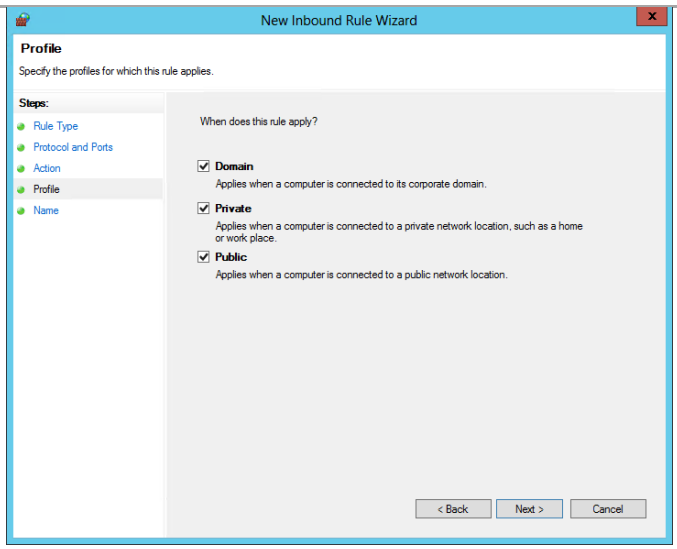
43. On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input the specific local TCP/IP port to enable access to the first named SQL instance. In this example to enable access to the SQL instance SCDB the port specified is 1433.
44. Click **Next** to continue.



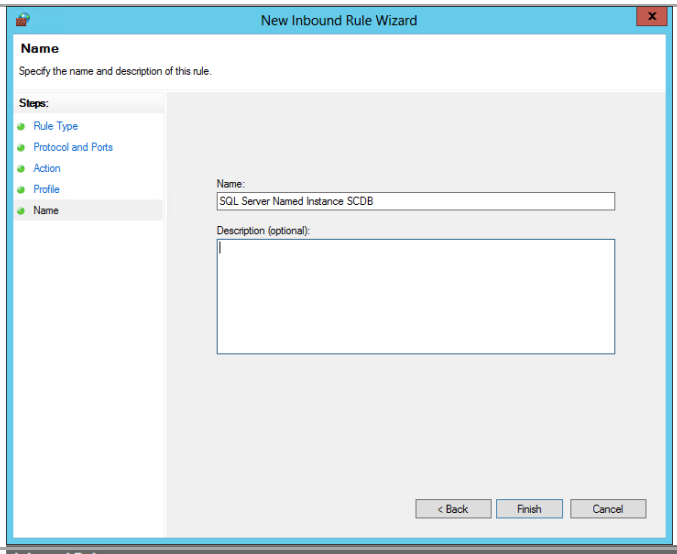
45. On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.



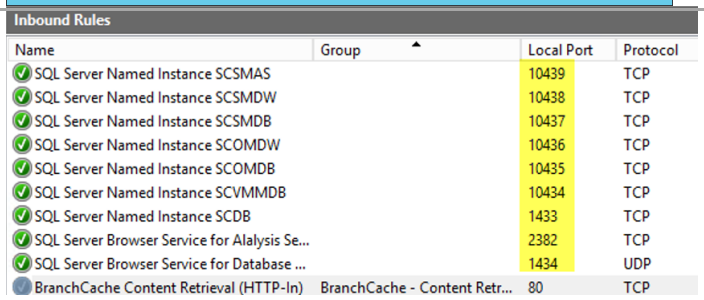
46. On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.
47. Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.



48. Specify a name for the new rule such as "*SQL Server Named Instance SCDB*" and click **Finish**.



49. 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.



50. 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
```

51. To create the rules on the remote nodes through PowerShell, the following commands are provided as an example.

Note: 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 Alaysis 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
```

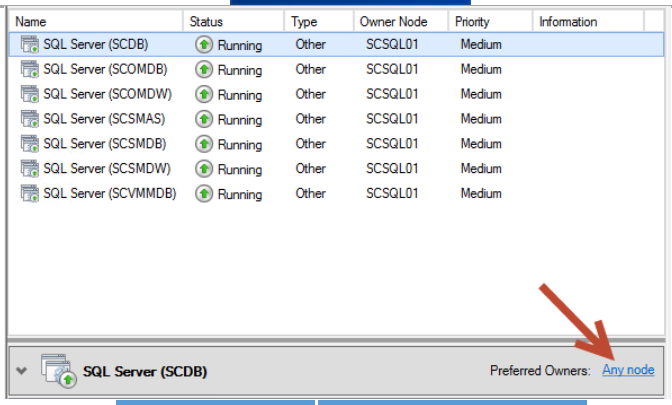
Assign Preferred Owners for SQL Instances in Failover Cluster Manager

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 **one fabric management SQL Server node** virtual machine.

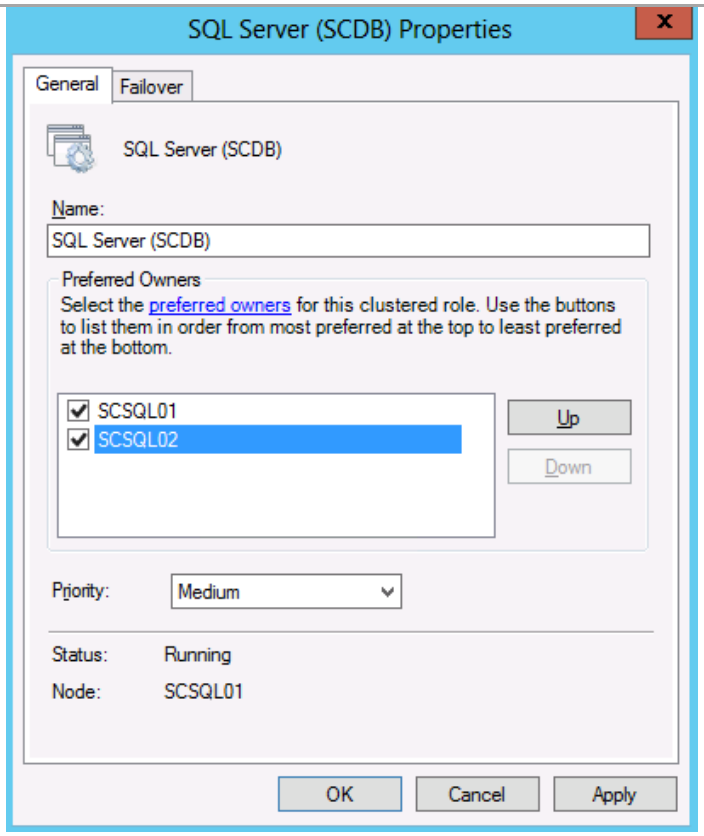
1. On any SQL Server cluster node, open **Failover Cluster Manager** and expand the **Roles** node.

2. 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.
3. 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.
4. 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**.

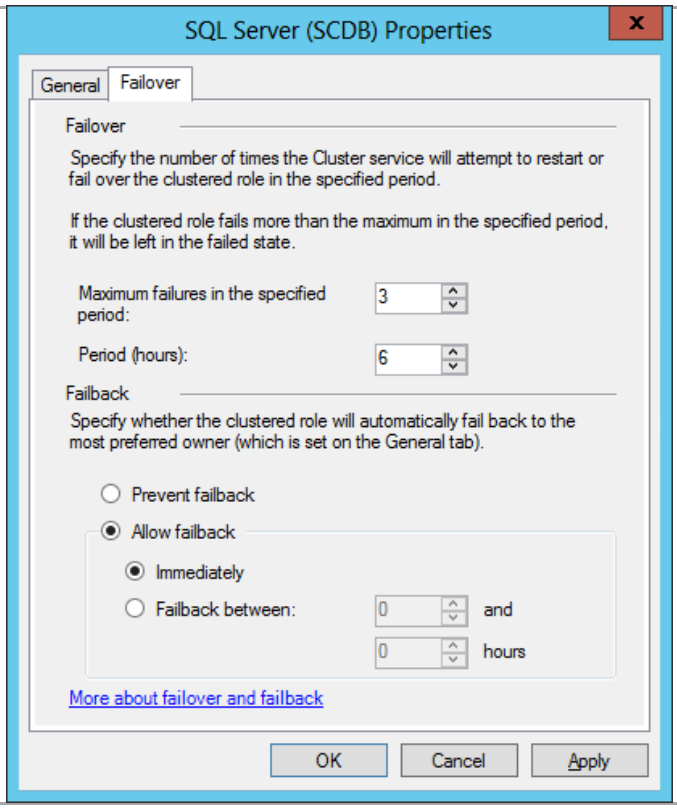


SQL Instance	Preferred Owners
SCDB	Node1, Node2
SCVMMDB	Node1, Node2
SCOMDB	Node1, Node2
SCOMDW	Node2, Node1
SCSMDB	Node2, Node1
SCSMDW	Node2, Node1
SCSMAS	Node2, Node1

5. 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.

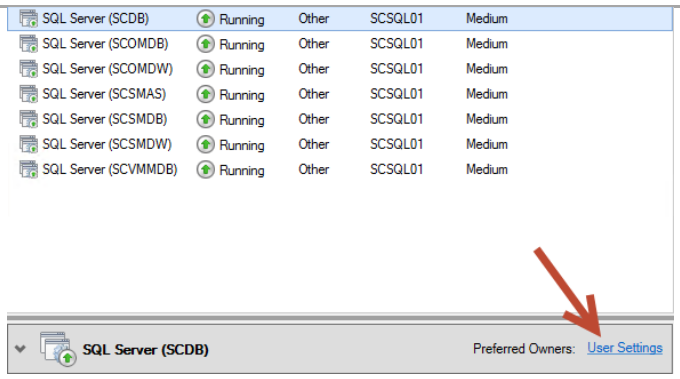


6. In the **SQL Server Properties** dialog, select the **Failover** tab. In the **Failback** section, select the **Allow failback** and **Immediately** radio buttons. Click **OK** to save the changes.

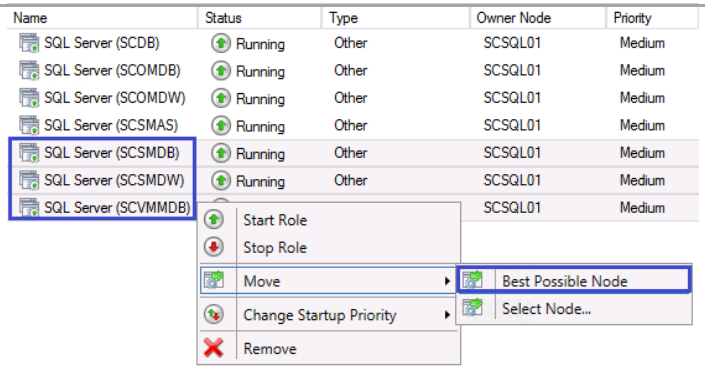


Note: The value for the **Preferred Owners** link now displays a value of *User Settings*.

7. Repeat this process for each SQL Server instance.

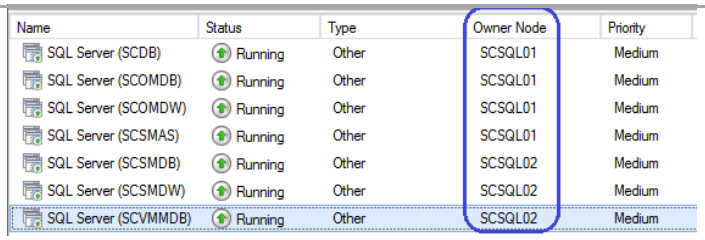


8. When all instances have been configured correctly for Preferred Owners you must initiate a planned failover to balance the SQL Server instances across nodes.
9. In **Failover Cluster Manager**, select the roles for each of the five SQL Instances that should not run on Node1 (SCSMDB, SCSMDW, SCVMMDB).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



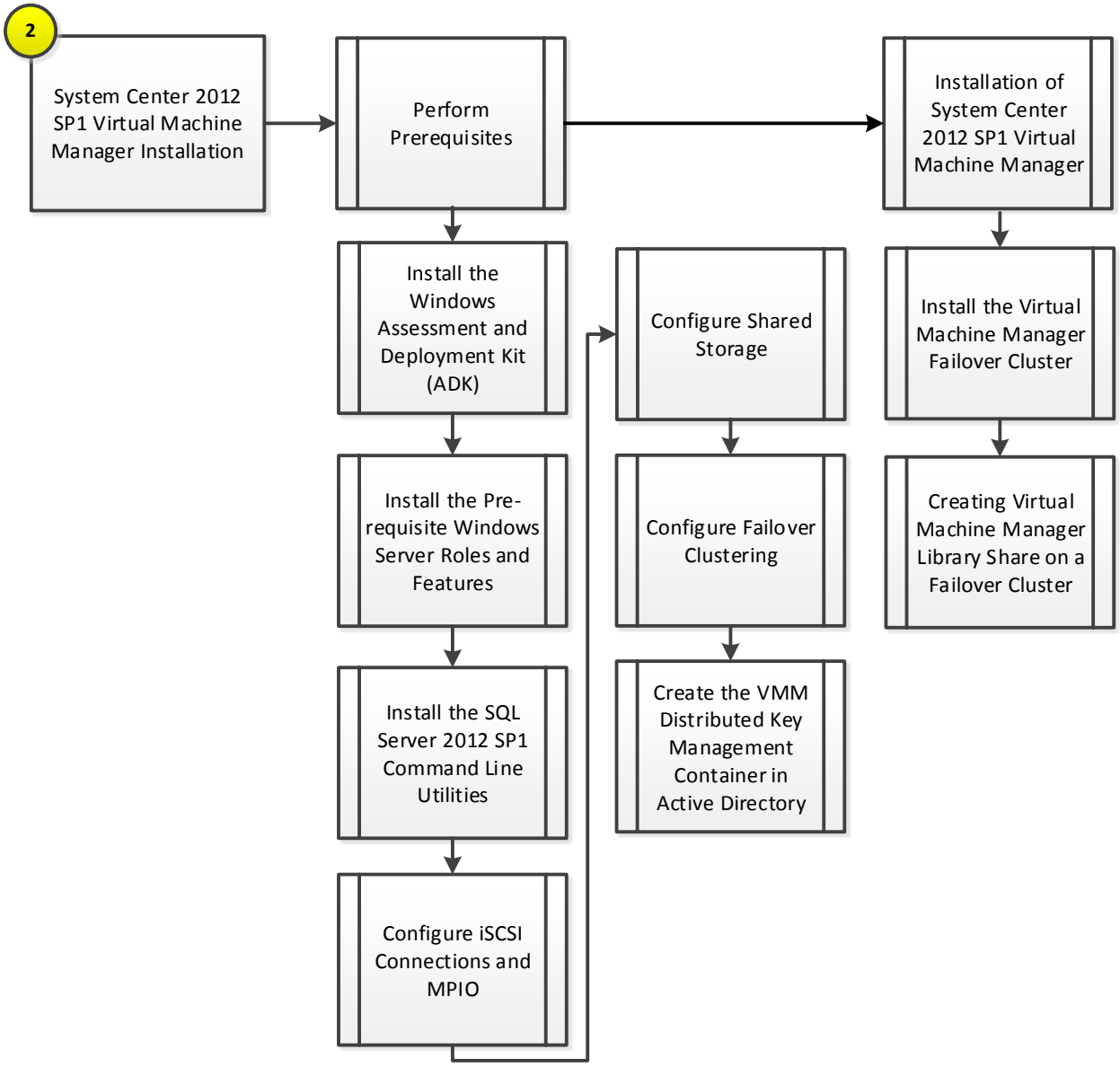
10. When the moves are completed, all Instances should be distributed across Node1 and Node2.

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.



15 Virtual Machine Manager

The System Center 2012 Virtual Machine Manager installation process includes the following high-level steps:



15.1 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
    - If using iSCSI, requires at least one dedicated virtual network adapter for iSCSI 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.

15.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

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:

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

Security group name	Group scope	Members
		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[7].

Install the Windows Assessment and Deployment Kit

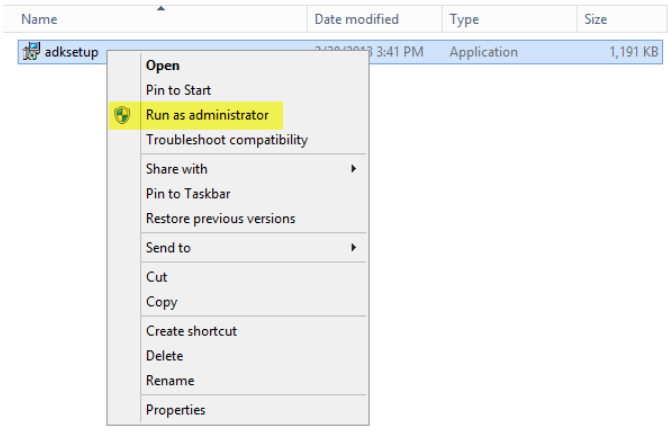
The Virtual Machine Manager installation requires that the Windows Assessment and Deployment Kit (ADK) be installed on the Virtual Machine Manager management server. The Windows ADK can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=30652.

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

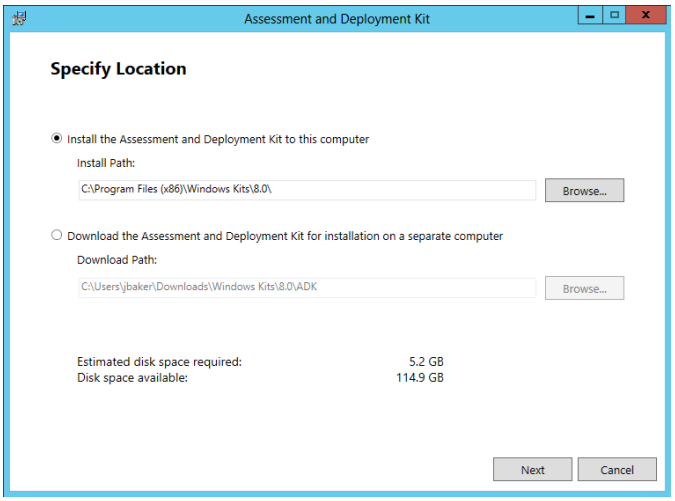
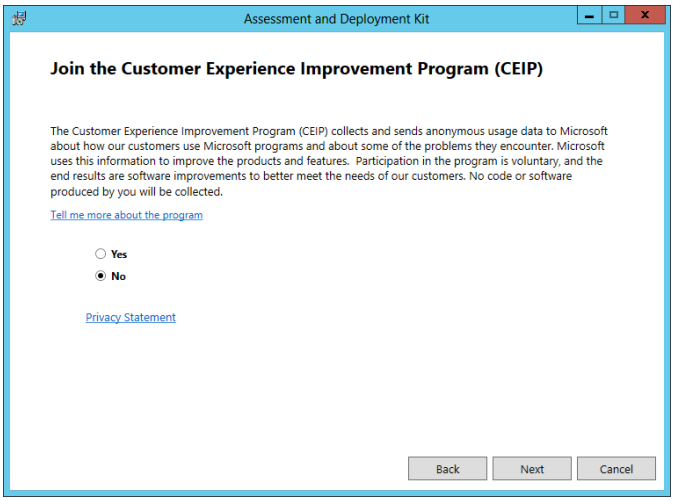
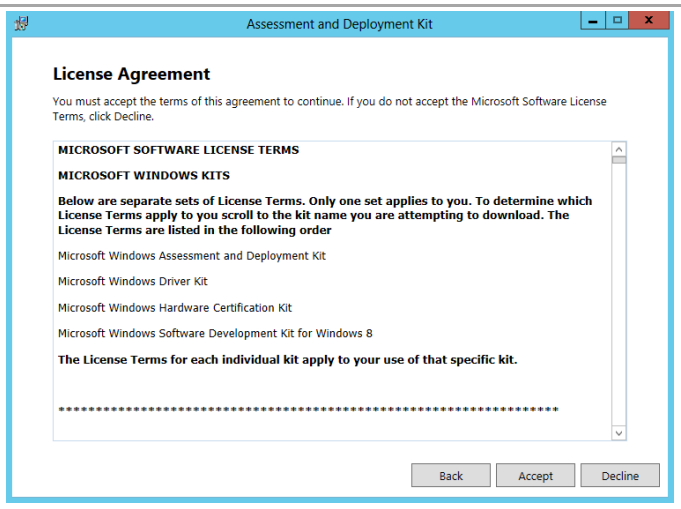
The following steps outline how to install the Windows ADK on the Virtual Machine Manager management server.

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

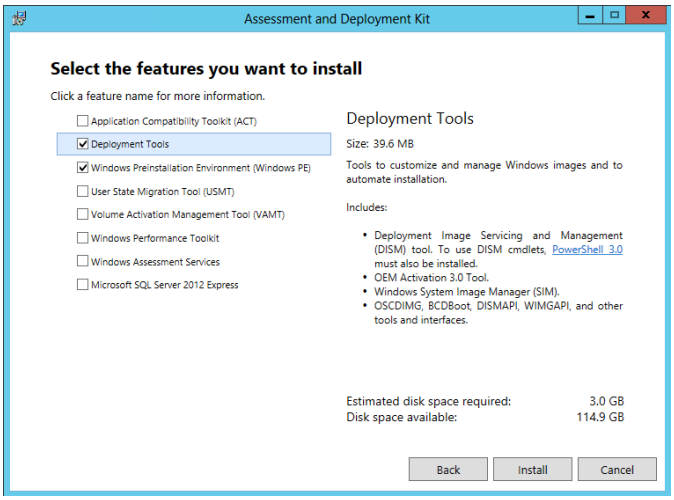
1. From the Windows ADK installation media source, right-click **adksetup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



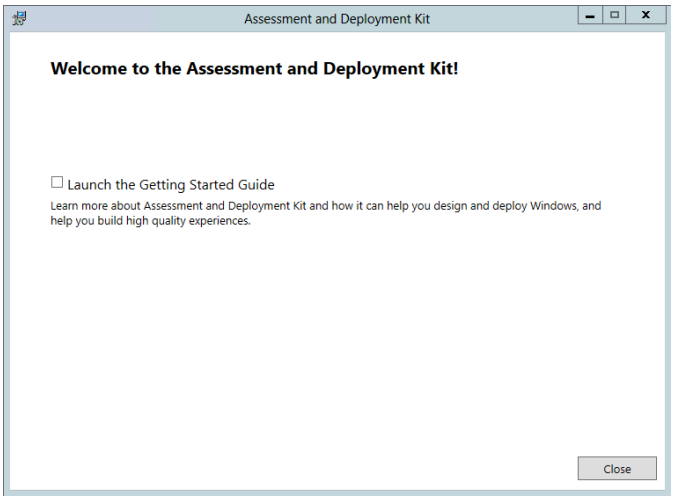
[7] Creating User Roles in VMM - http://technet.microsoft.com/en-us/library/gg696971.aspx.

2. 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.	
3. 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.	
4. In the **License Agreement** dialog, click **Accept** to continue.	

5. In the **Select the features you want to install** dialog, select the following option checkboxes:
6. **Deployment Tools**
7. **Windows Preinstallation Environment (Windows PE)**
8. Ensure all other option checkboxes are deselected. Click **Next** to begin the installation.



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

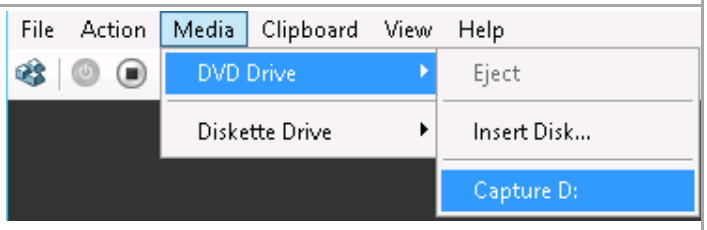


15.3 Install the Pre-Requisite Windows Server Roles and Features

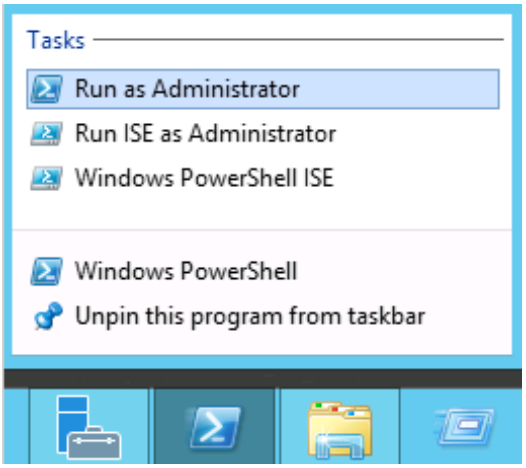
The Virtual Machine Manager installation requires the WSUS Administration Tools to be installed on the Virtual Machine Manager management servers. In addition, the MPIO and Failover Clustering Features must be installed. Follow the steps below to install the pre-requisite roles and features on the Virtual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

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

1. Verify that the Windows installation disk is mapped to D: drive.

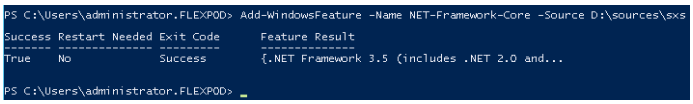


2. Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.

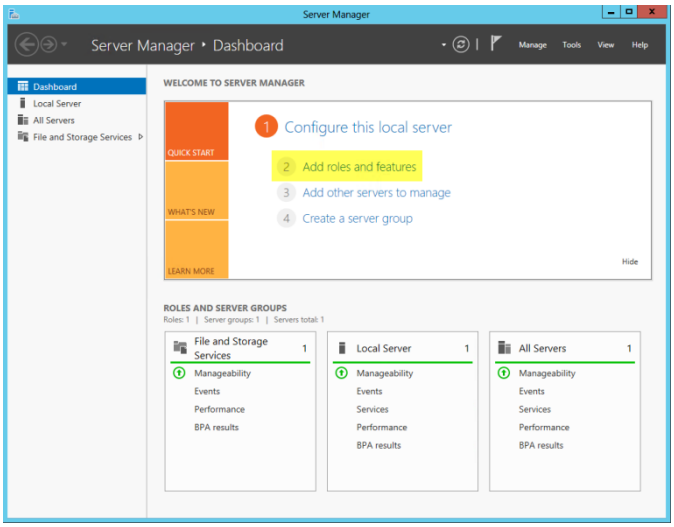


3. Add the .Net 3.5 feature by entering the following command:

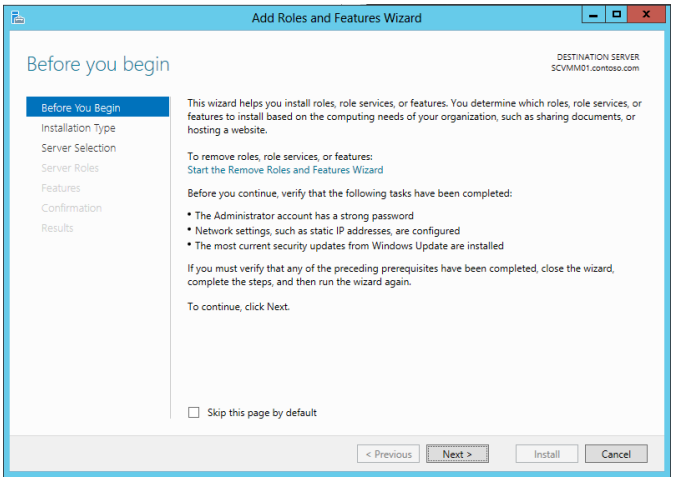
```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```



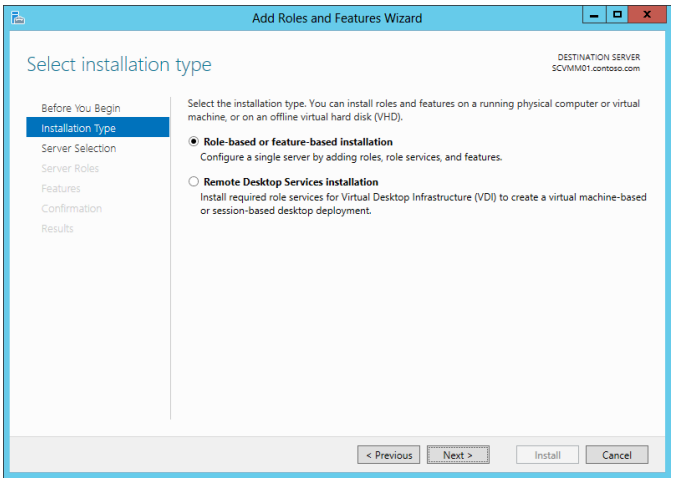
4. Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



5. The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, click **Next** to continue.

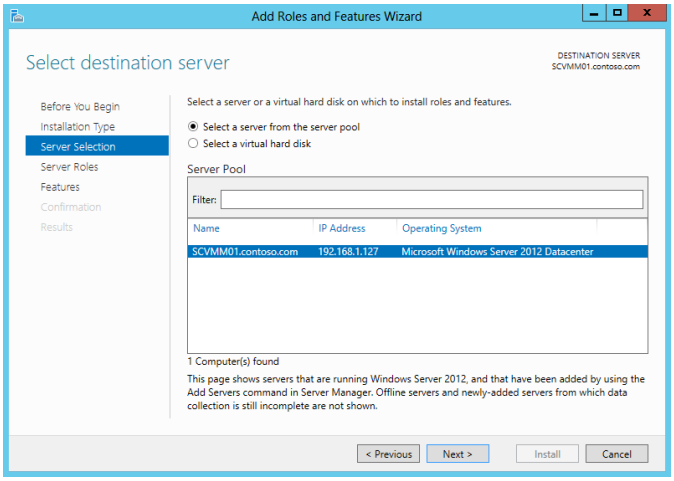


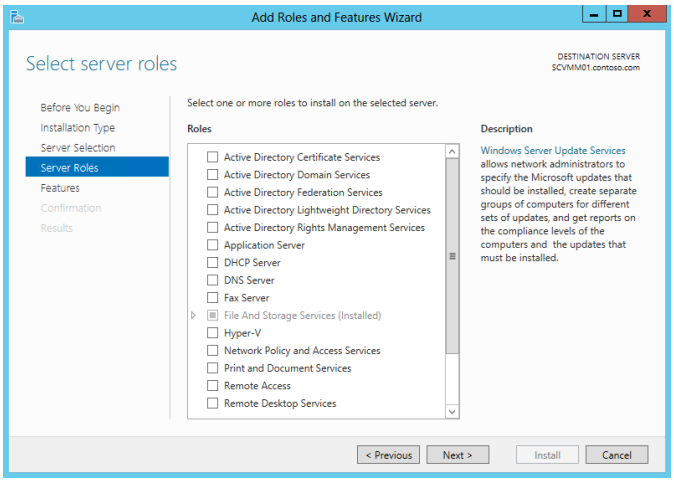
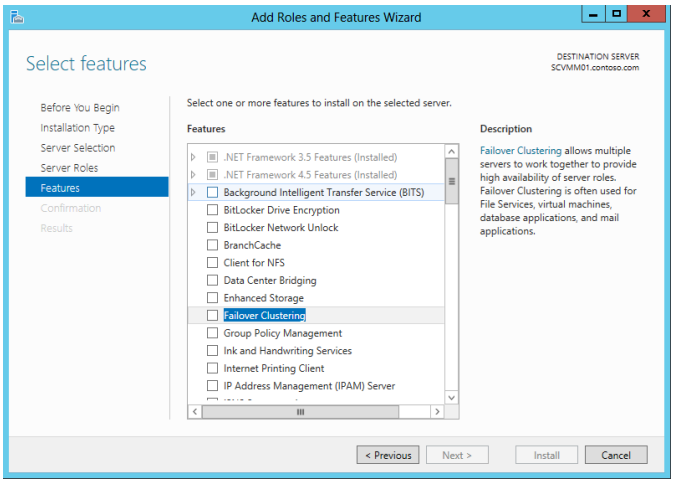
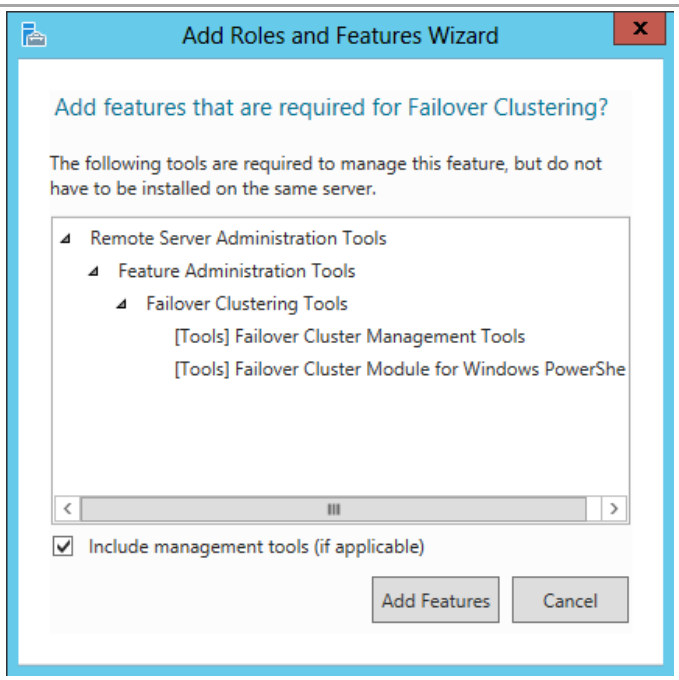
6. In the **Select Installation Type** dialog, you are presented with two options:
    a. *Role-based or Feature-based installation* – Traditional installation of roles and features to enable discrete functionality on the operating system.
    b. *Remote Desktop Services scenario-based installation* – Installation of a pre-determined combination of roles, features and configurations to support a Remote Desktop (Session Virtualization) or VDI scenario
7. Select the **Role-based or Feature-based installation** radio button and click **Next** to continue.



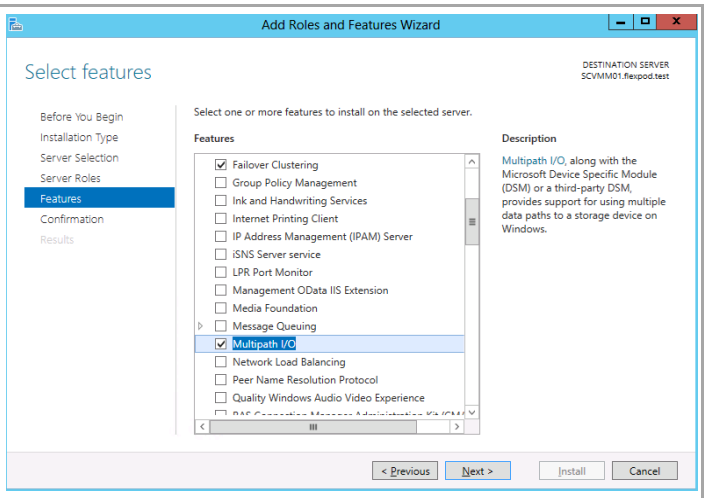
8. In the **Select destination server** dialog, you are presented with two options:
    a. *Select a server from the server pool* – This option allows you to select a server from the managed pool of systems defined within Server Manager.
    b. *Select a virtual hard disk* – This option allows for roles to be installed to staged VHD files for offline servicing purposes.
9. For this installation, select the **Select a server from the server pool** radio button, select the local server and click **Next** to continue.

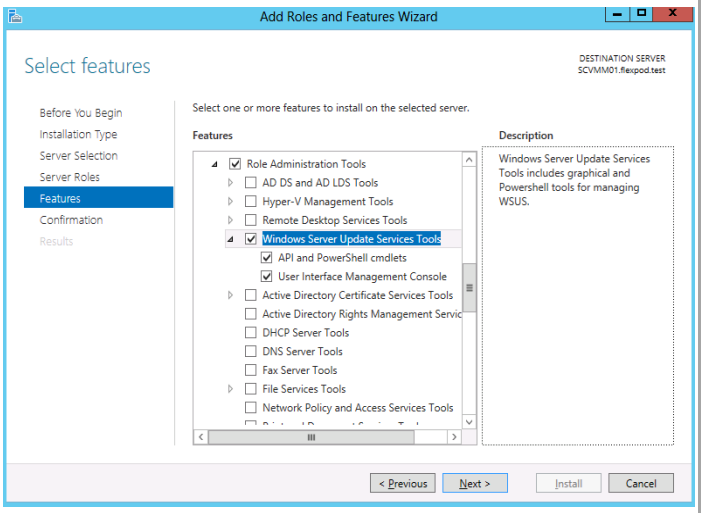
Note: While many servers may be presented in the Select a server from the server pool option, only one can be selected at a time for role and feature installation operations. To enable installs across multiple hosts, the configuration can be saved at the end of the wizard and applied to multiple systems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



10. In the **Select Server Roles** dialog, do not make any additional selections and click **Next** to continue.	
11. In the Features dialog, select Failover Clustering.	
12. 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.	

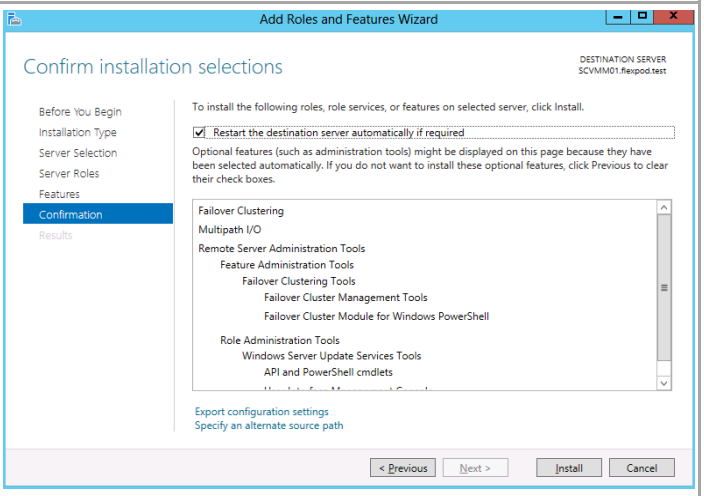
13. Next select the **Multipath I/O** and the **Windows Server Update Services Tools** top level features. Click Next to continue.



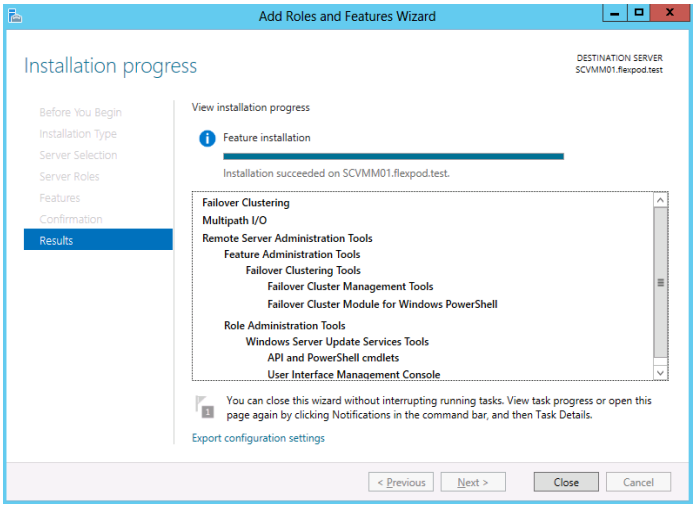


14. In the **Confirm installation selections** dialog, verify that the Multipath I/O and Failover Clustering features are selected. Ensure that the **Restart each destination server automatically if required** is selected. This is especially important for remote role/feature installation. Click **Install** to begin installation.

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

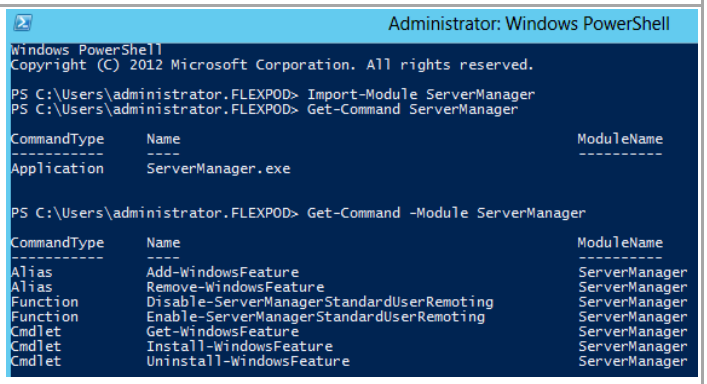


15. The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



Note: While the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.

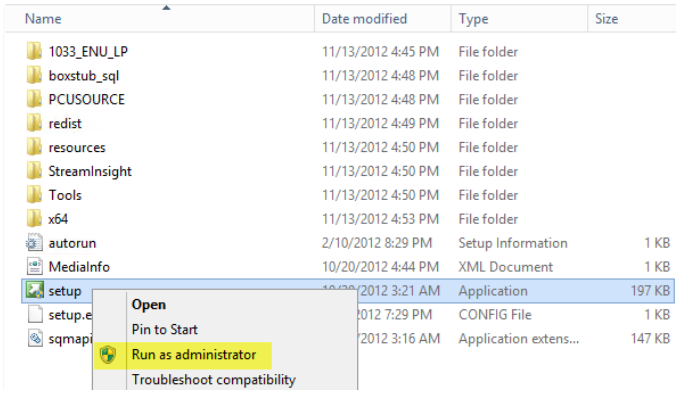
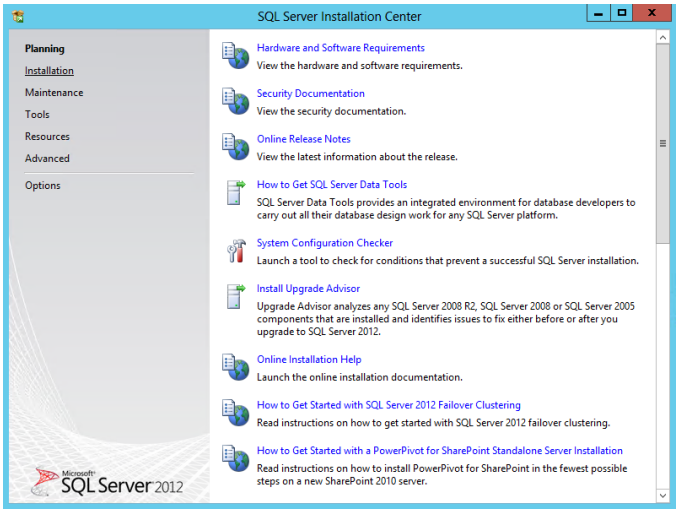
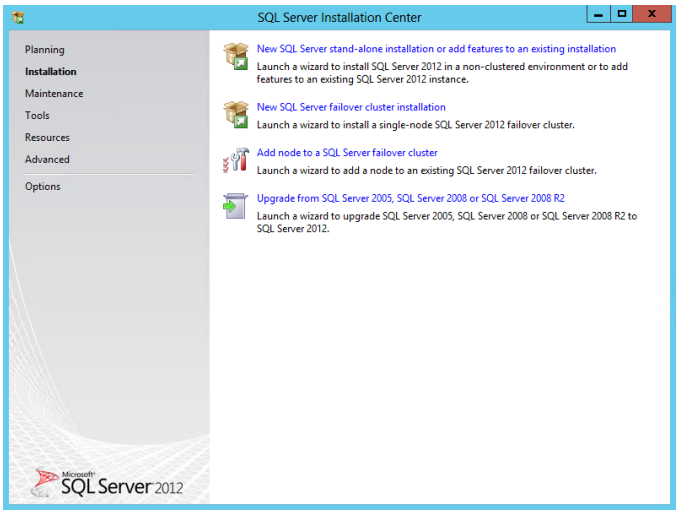
```
Add-WindowsFeature –Name getFailover-
Clustering, Multipath-IO, UpdateServices-RSAT
-IncludeManagementTools –Restart
```



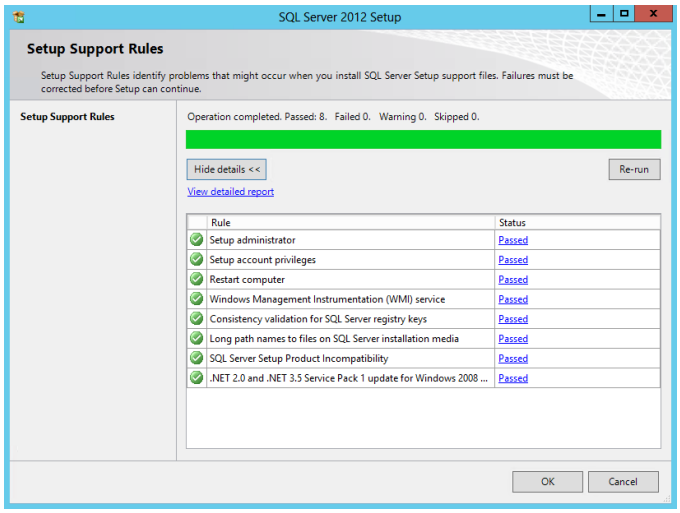
Install the SQL Server 2012 SP1 Command Line Utilities

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.

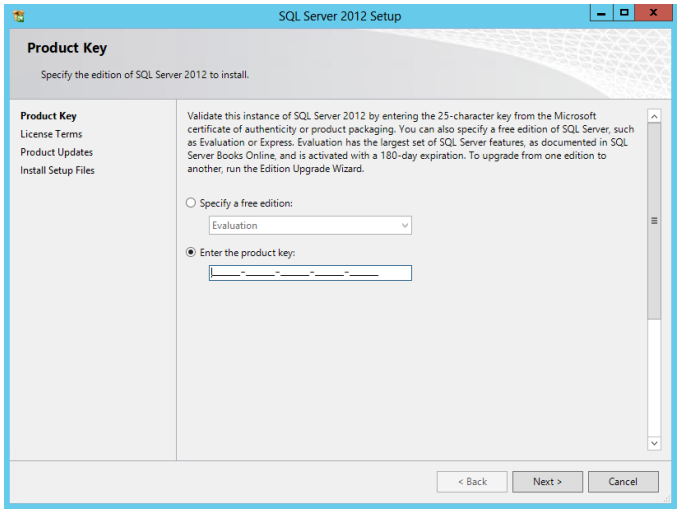
1. From the SQL Server 2012 with SP1 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.	
2. The **SQL Server Installation Center** will appear. Select **Installation**.	
3. From the **SQL Server Installation Center,** click the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

4. 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.

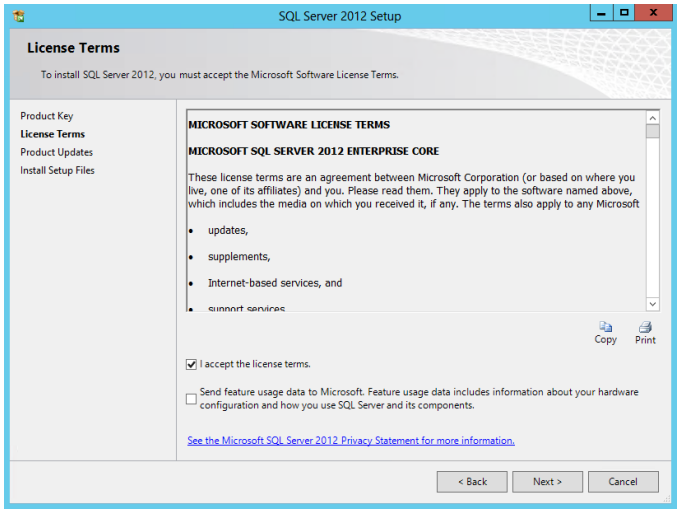


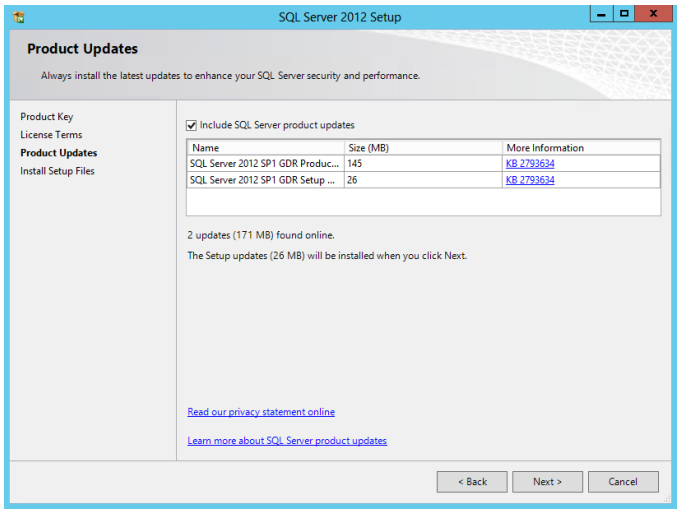
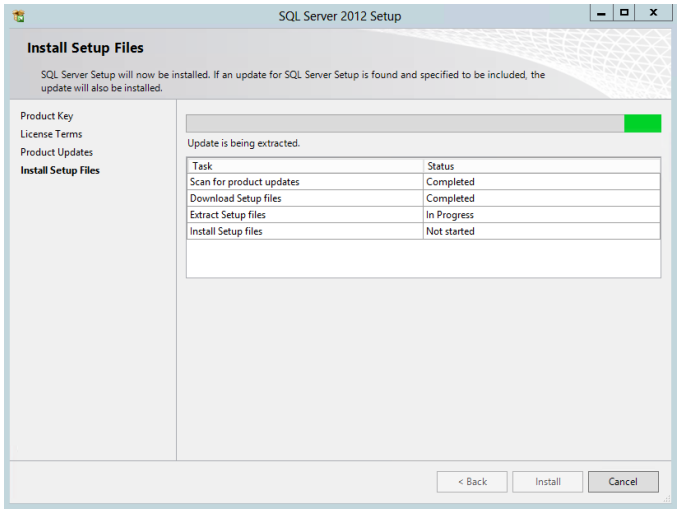
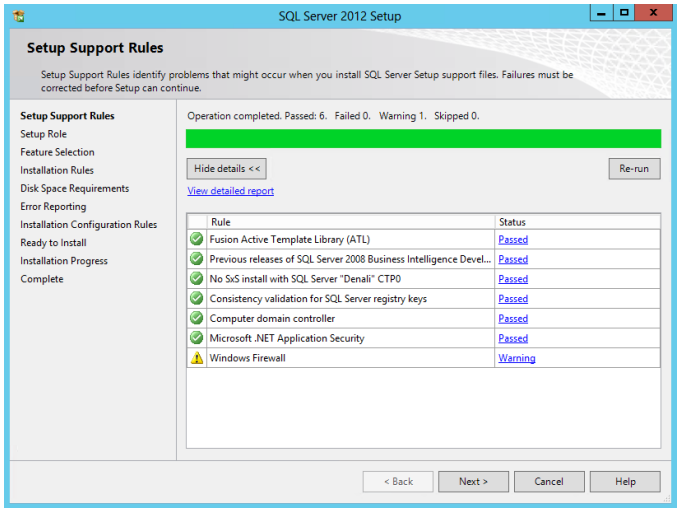
5. In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

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.

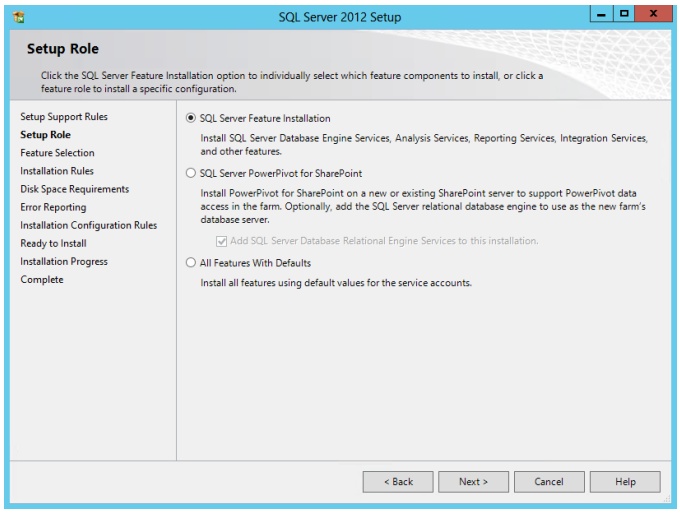


6. In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.

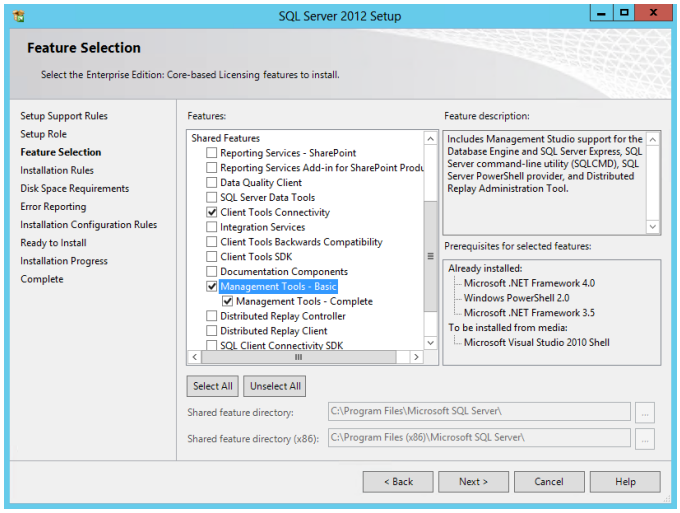


7. In the Product Updates dialog, leave the **Include SQL Server product updates**, selection checked and click **Next**.	
8. On the **Install Setup Files** dialog the update and install process will be displayed.	
9. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status.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

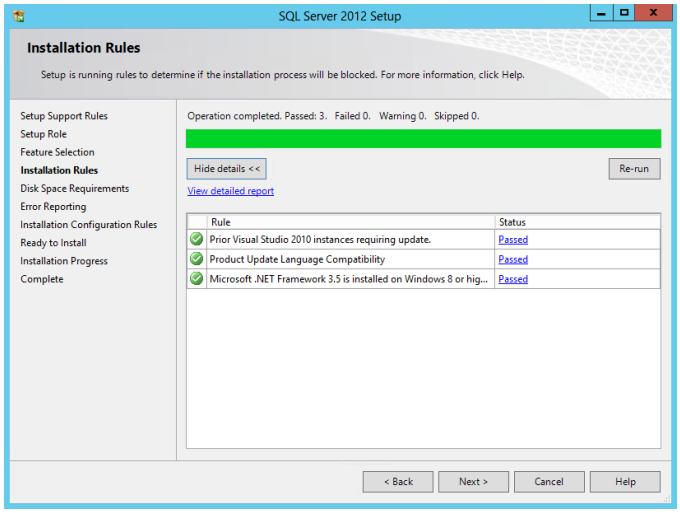
10. In the **Setup Role** dialog, select the **SQL Server Feature Installation** option and click **Next** to continue.



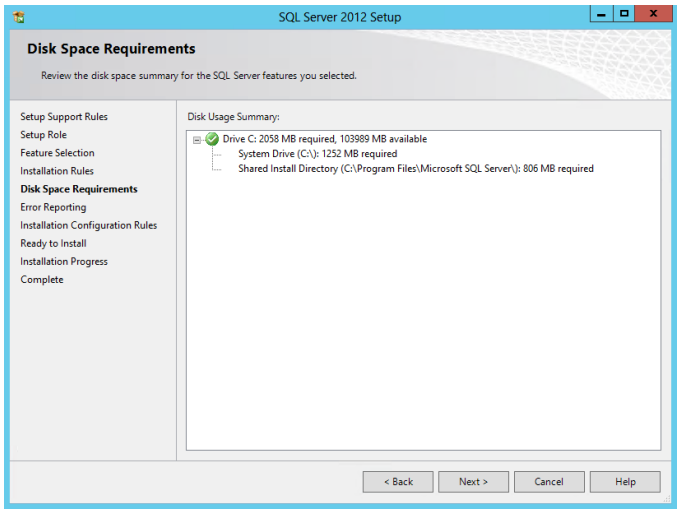
11. In the **Feature Selection** dialog, select the **Client Tools Connectivity**, **Management Tools – Basic** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.



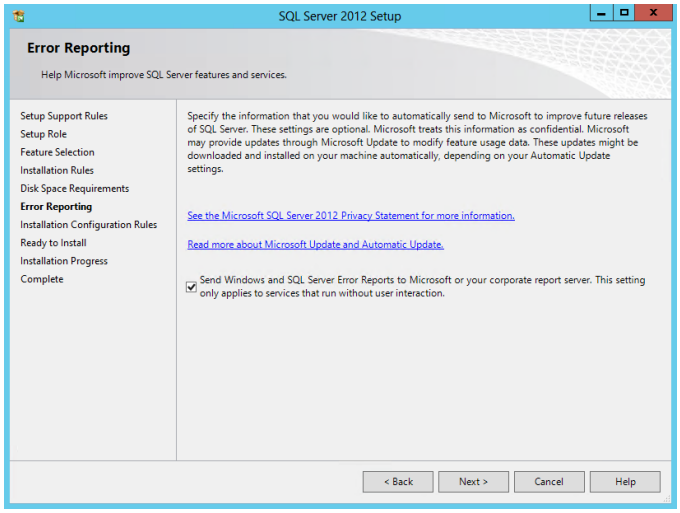
12. In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



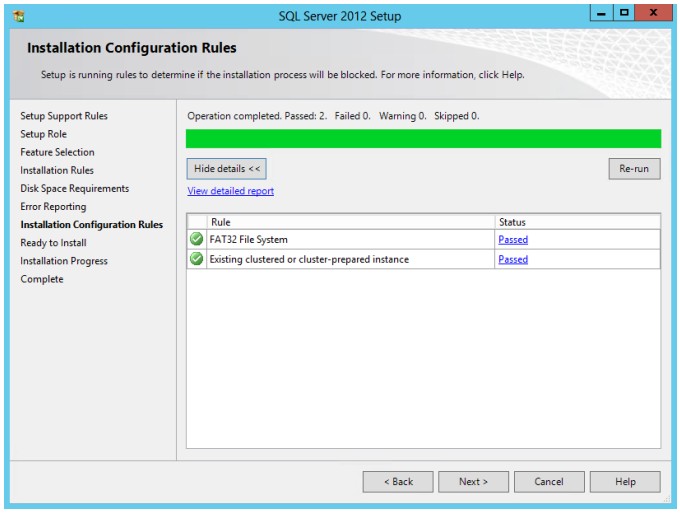
13. In the **Disk Space Requirements** dialog, verify that the installation has enough space on the target drive and click **Next** to continue.



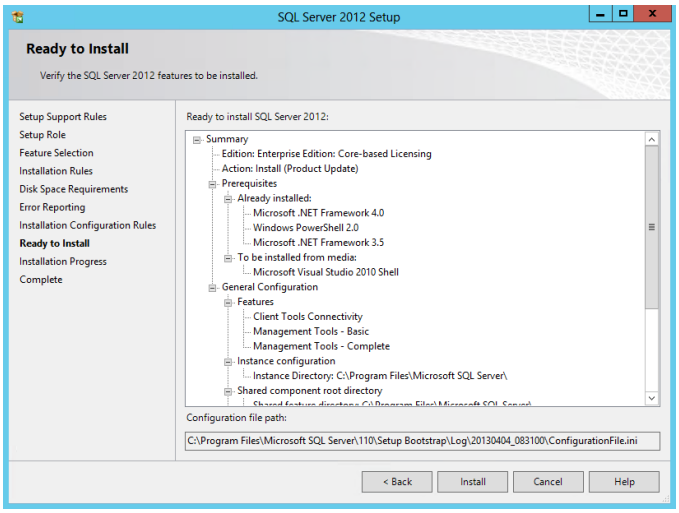
14. In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



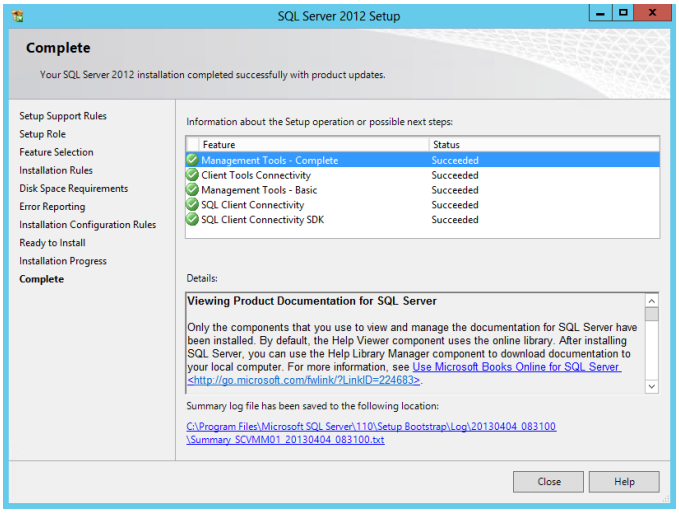
15. In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



16. 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.

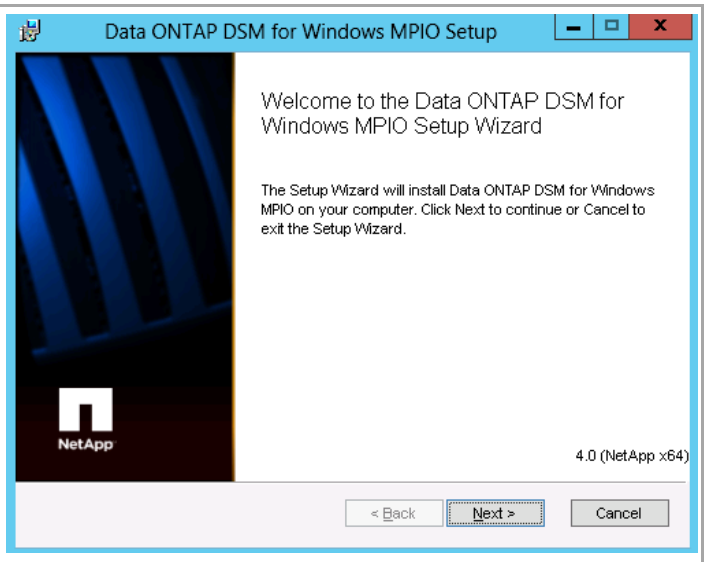
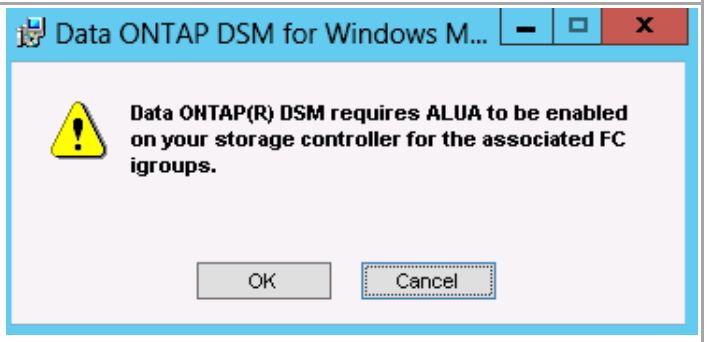
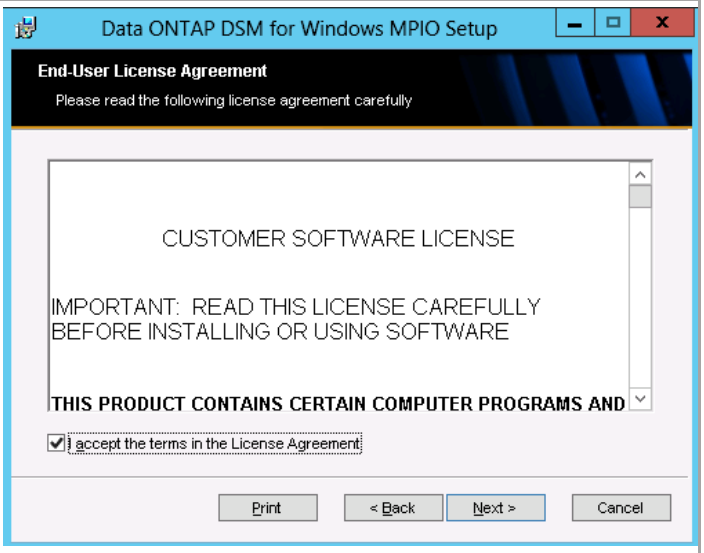


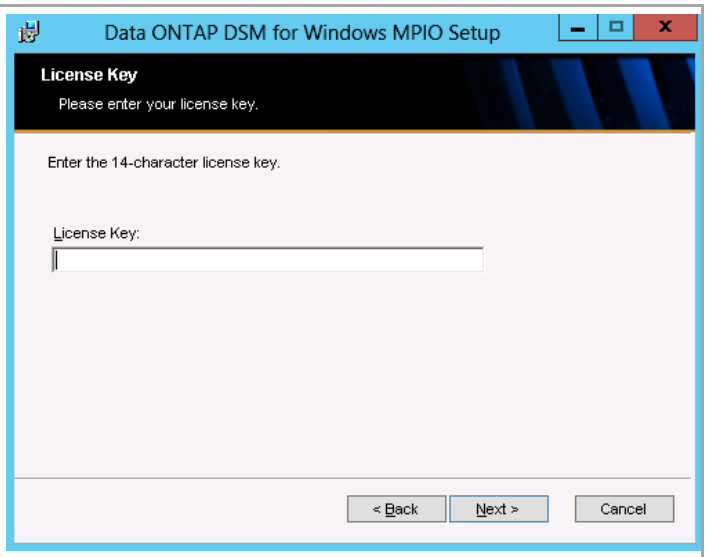
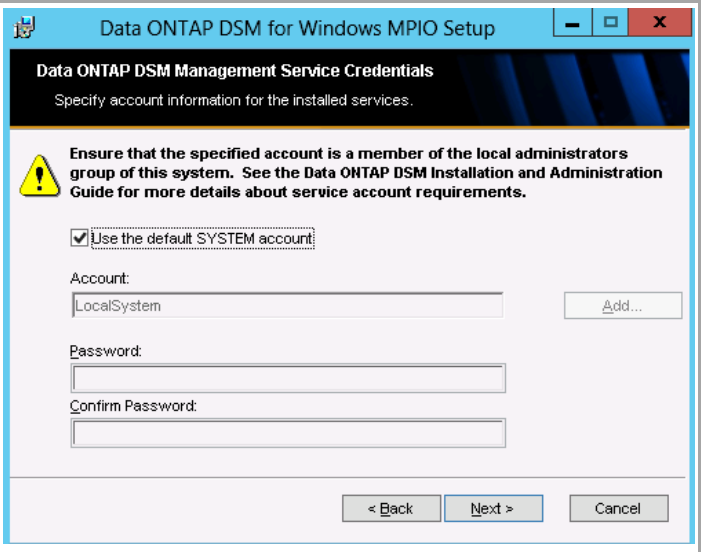
17. When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of SQL Server tools.

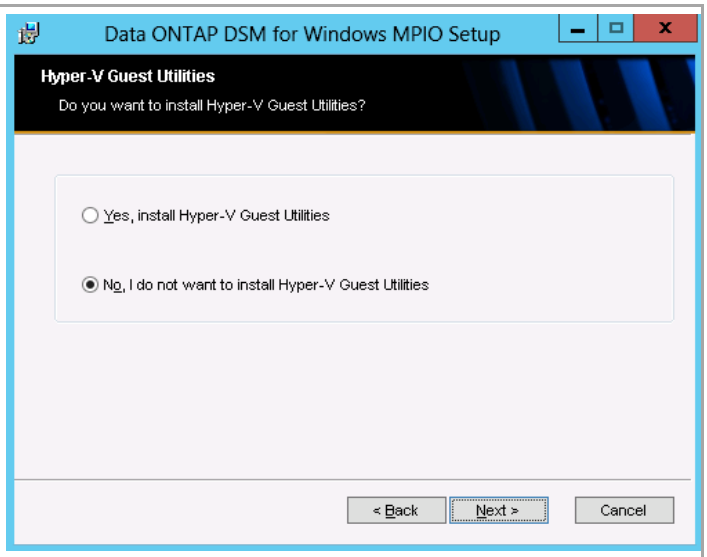
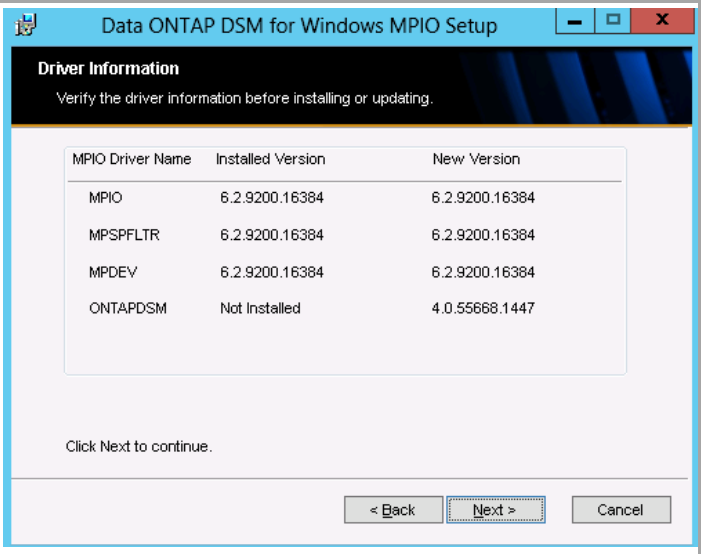


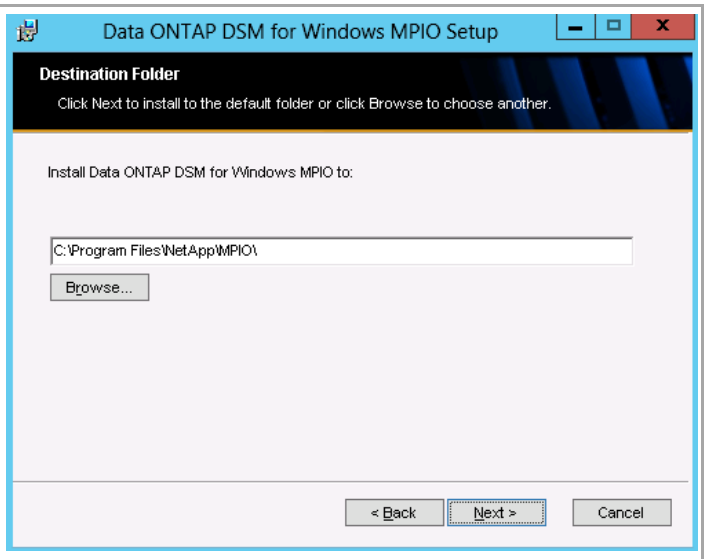
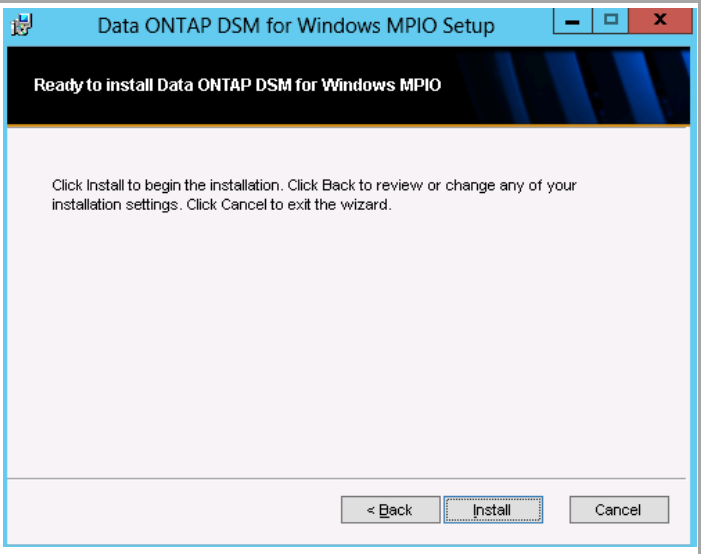
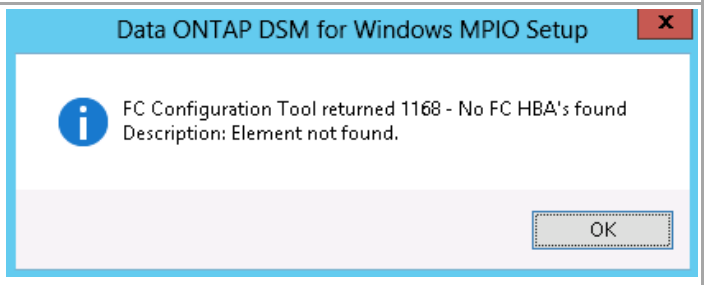
Install NetApp MPIO DSM

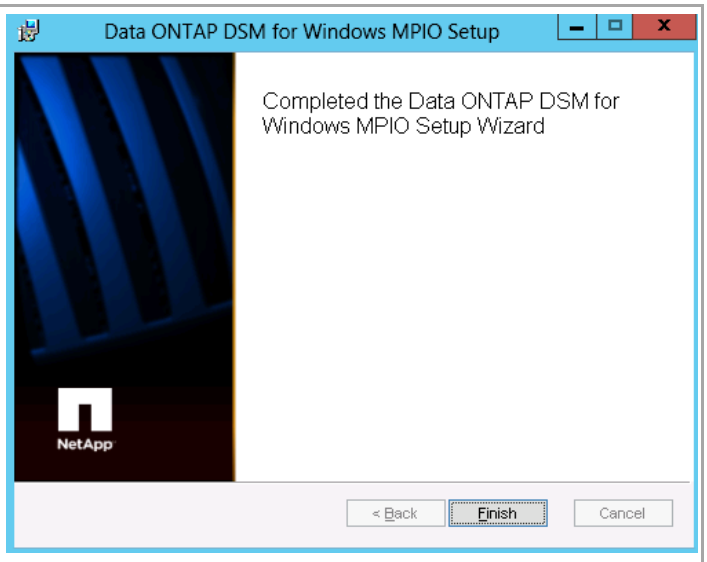
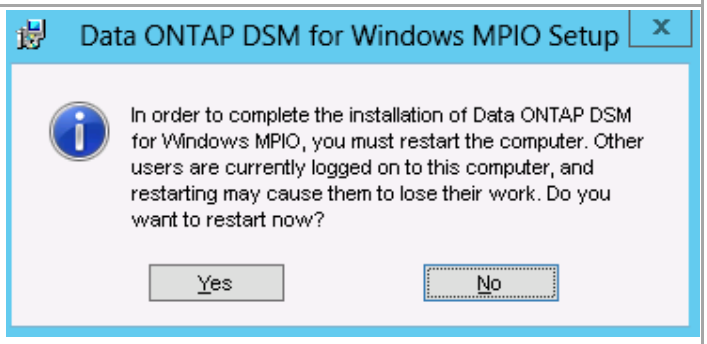
Perform this procedure on both VMM Server Virtual Machines.

1. Launch the NetApp DSM Installer, click `Next`.	
2. Click `OK` acknowledging the ALUA warning.	
3. Accept the `EULA` and Click `Next`.	

4. Enter the license Key and click `Next`.	
5. Leave `Use the default SYSTEM account checkbox` checked and Click `Next`.	

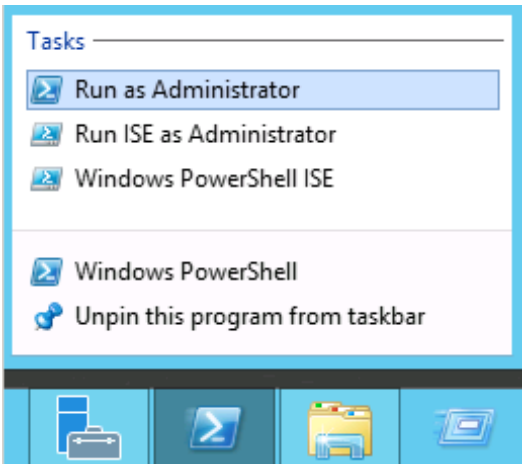
6. Select `No, I do not want to install the Hyper-V Guest Utilities`, and Click `Next`.	
7. Click `Next` through the driver information pane.	

8. Validate the installation path and click `Next`.	
9. Click `Install`.	
10. Acknowledge the warning that No Fibre Channel HBA's were found.	

11. Click Finish to close the wizard.	
12. When prompted reboot the host.	

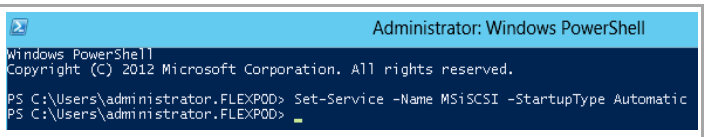
Configure Windows Host iSCSI initiator

Perform this procedure on both VMM Server Virtual Machines. The following steps describe how to configure the built in Microsoft iSCSI initiator.

1. Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.	

2. Execute the following commands to configure the iSCSI service to start automatically

```
Set-Service -Name MSiSCSI -StartupType Automatic
```

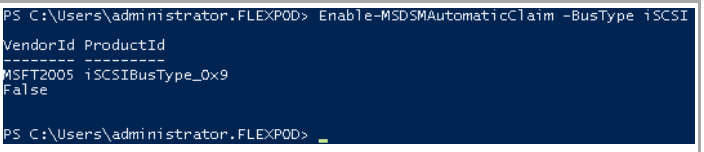


3. Execute the following commands to start the iSCSI Service.

```
Start-Service -Name MSiSCSI
```

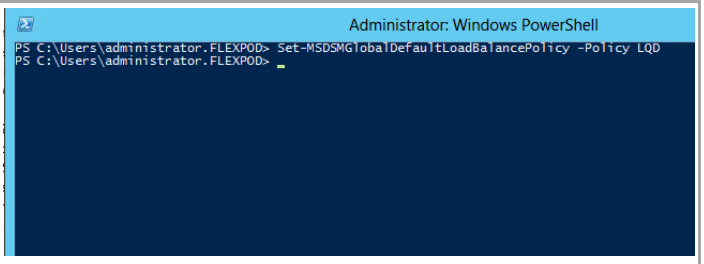
4. Execute the following commands to configure MPIO to claim any iSCSI device

```
Enable-MSDSMAutomaticClaim -BusType iSCSI
```



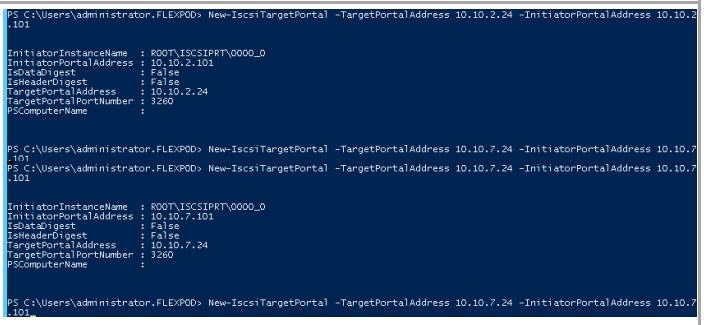
5. Execute the following commands to set the default load balance policy of all newly claimed devices to round robin.

```
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy LQD
```



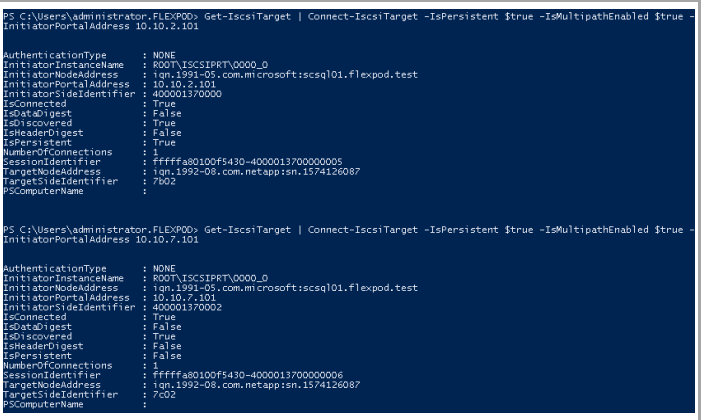
6. Execute the following commands to configure an iSCSI target for each controller.

```
New-IscsiTargetPortal -TargetPortalAddress <controller1_iscsia_ip> -InitiatorPortalAddress <iscsia_ipaddress>

New-IscsiTargetPortal -TargetPortalAddress <controller2_iscsia_ip> -InitiatorPortalAddress <iscsia_ipaddress>
```



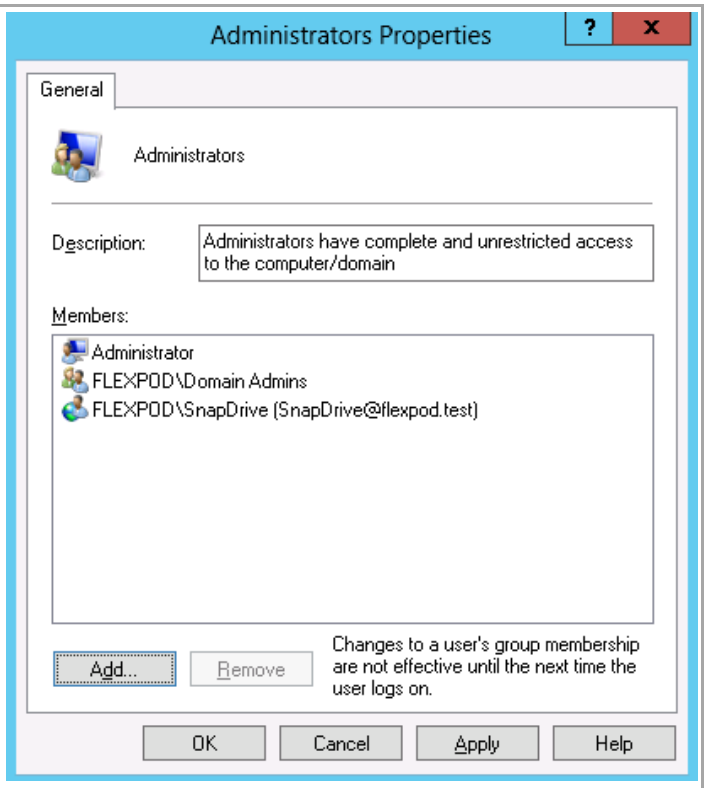
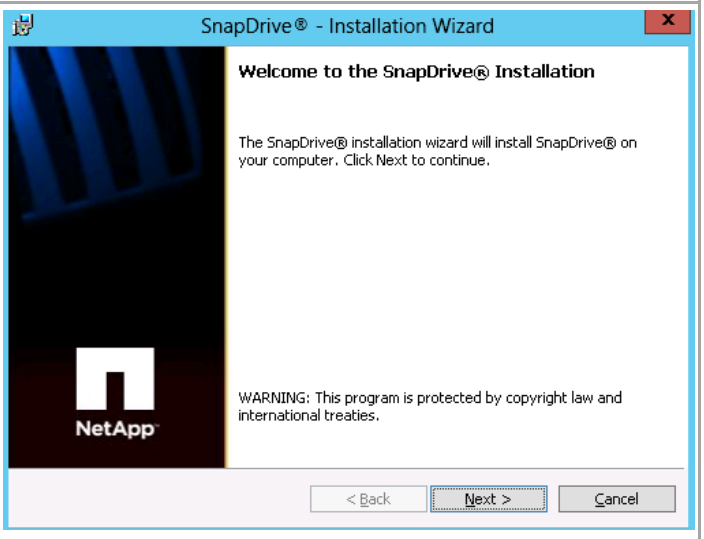
7. Execute the following commands to connect a session for each iscsi Network to each target.

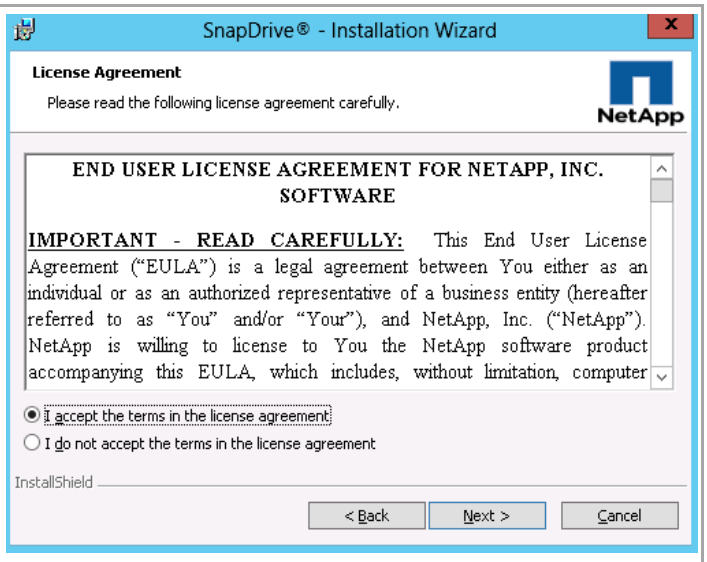
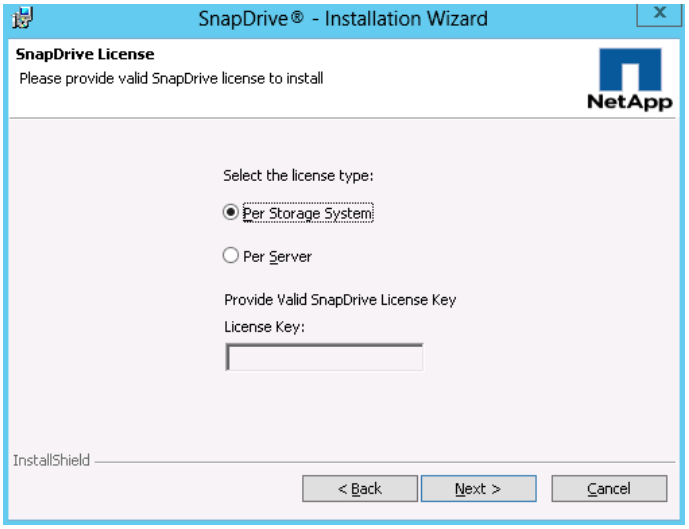
```
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsia_ipaddress>

Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsib_ipaddress>
```

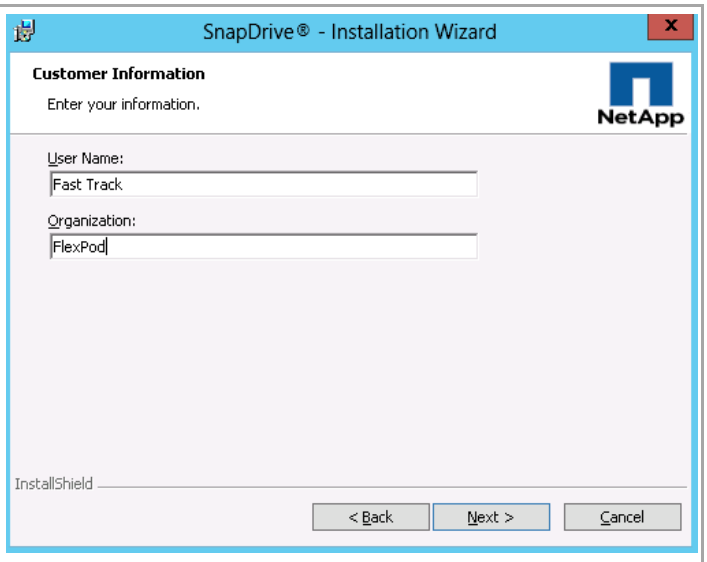
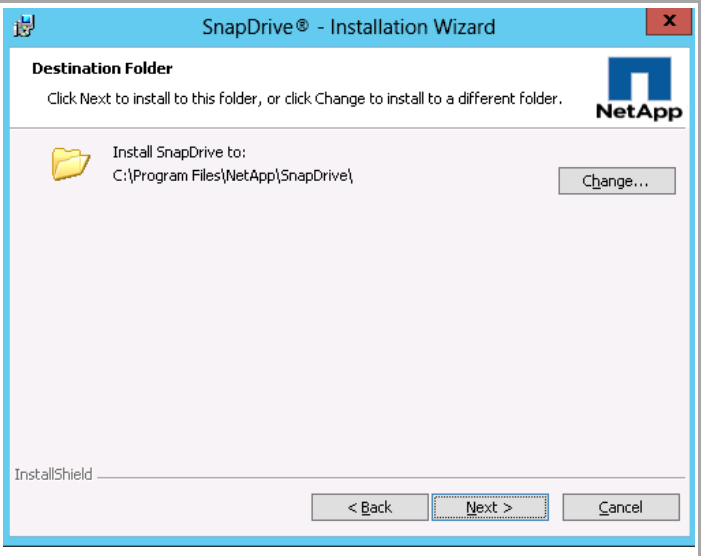


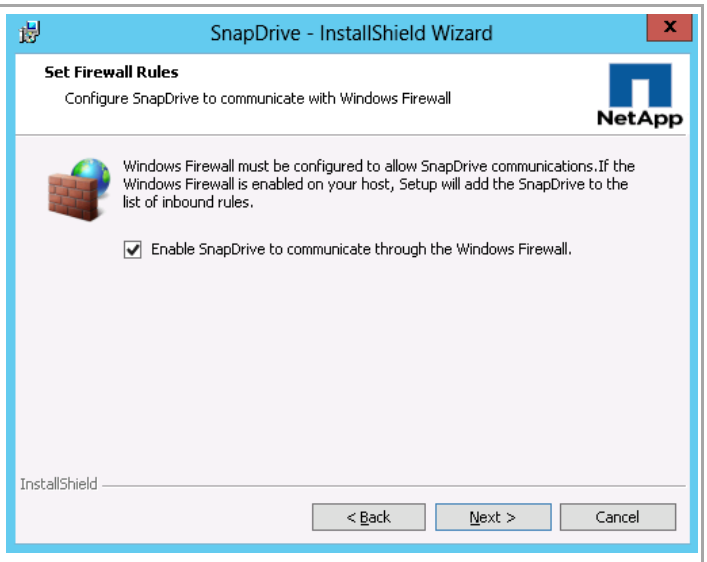
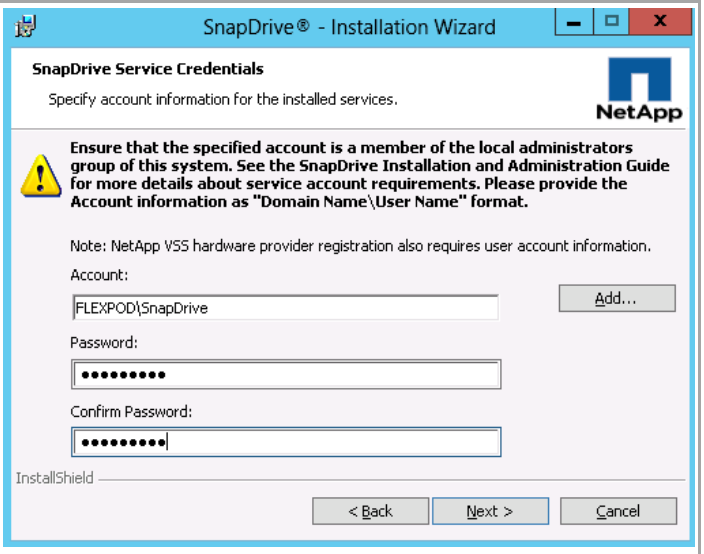
Install NetApp SnapDrive

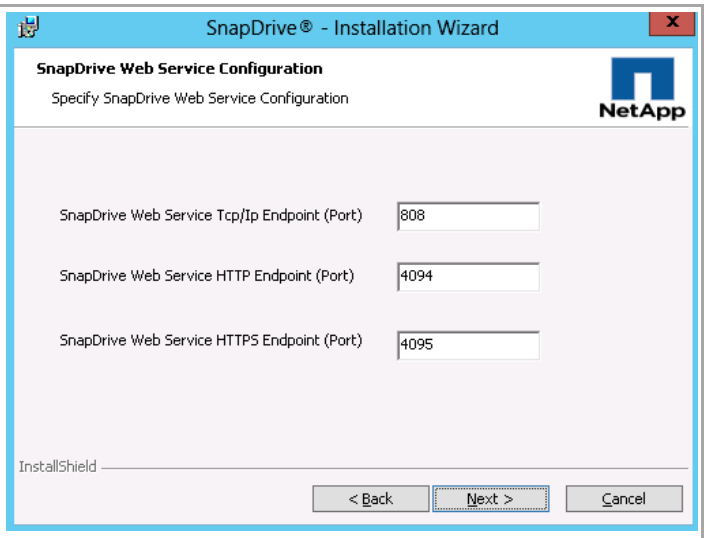
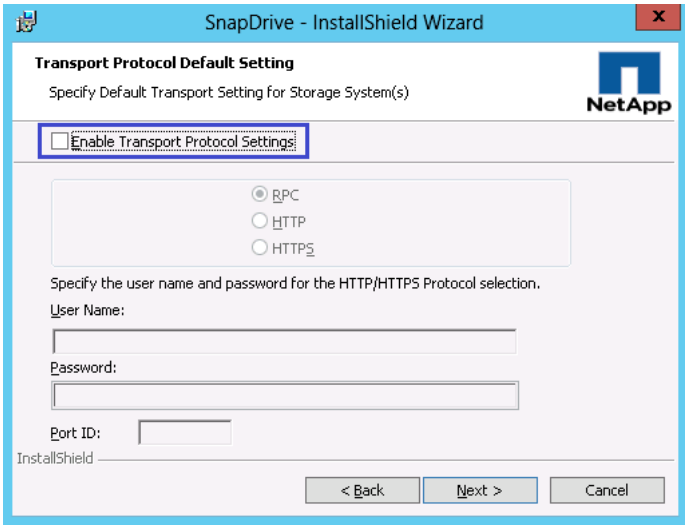
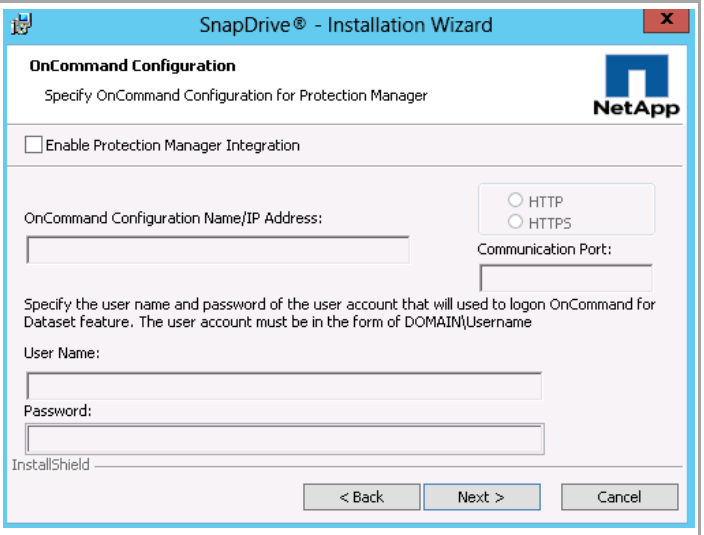
Note: Perform this procedure on both VMM Server Virtual Machines.

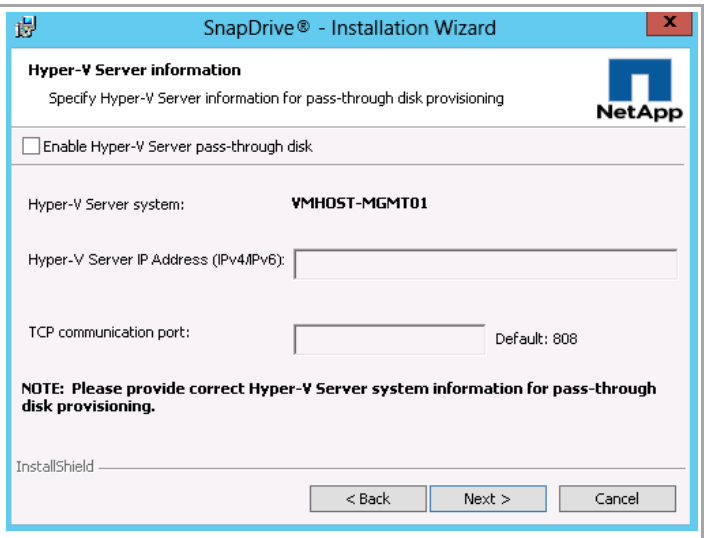
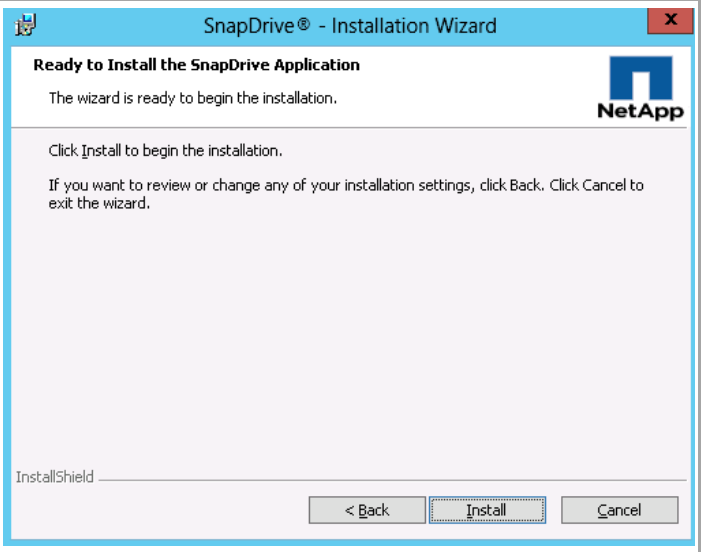
1. Add the SnapDrive domain account to the local administrators group in both VMM virtual machines.	
2. Launch the SnapDrive Installer, click `Next`.	

3. Accept the EULA and click Next.	
4. Select the Storage based Licensing method and click Next.	

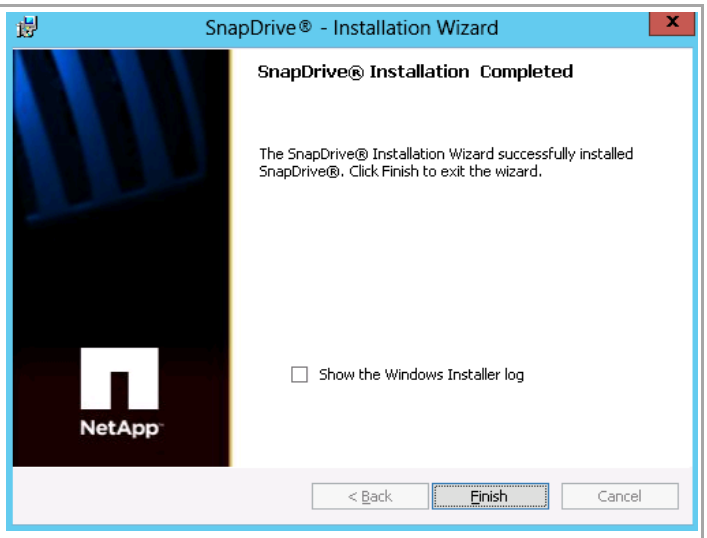
5. Enter your User Name, and Organization information, and click `Next`	
6. Validate the installation path and click `Next`.	

7. Check the `Enable SnapDrive to communicate through the Windows Firewall` checkbox and click `Next`.	
8. Enter the Account information for the Snapdrive service account, Click `Next`.	

9. Click `Next`, through the SnapDrive Web Service Configuration.	
10. Uncheck the `Enable Transport Protocol Settings`, and click `Next`.	
11. Leave `Enable Protection Manger Integration` Unchecked, and click `Next`.	

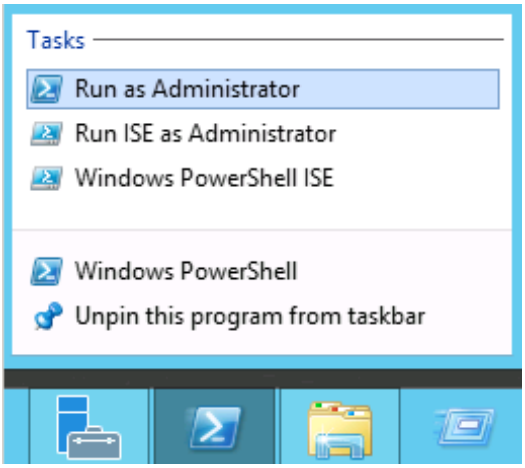
12. Leave `Enable Hyper-V Server pass-through disk` Unchecked, and click `Next`.	
13. Click `Install`.	

14. Click Finish to close the installation wizard window.



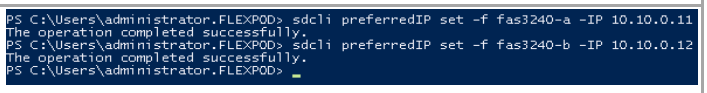
15. After the installation is finished. Launch a NEW PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.

Note: A new prompt is required to register the sdcli executable.



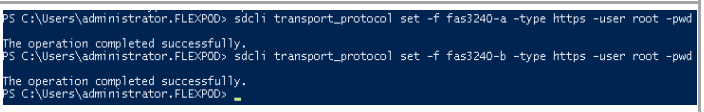
16. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_controller1>>
-IP <<var_controller1_e0m_ip>>
sdcli preferredIP set -f <<var_controller2>>
-IP <<var_controller2_e0m_ip>>
```



17. Configure SnapDrive transport protocol authentication configuration for each controller.

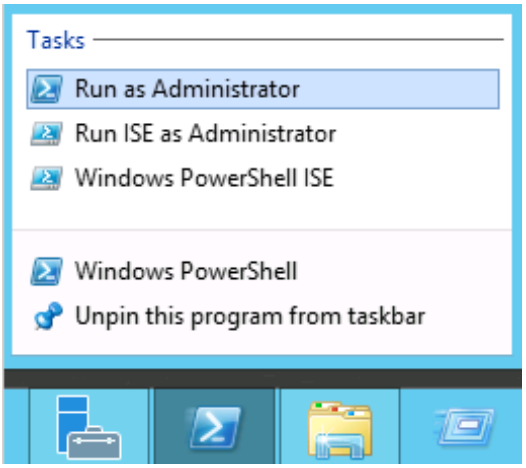
```
sdcli transport_protocol set -f
<<var_controller1>> -type https -user root -
pwd <<var_admin_passwd>>
sdcli transport_protocol set -f
<<var_controller2>> -type https -user root -
pwd <<var_admin_passwd>>
```



Create the Cluster

Create a the Windows Failover Cluster in the two Virtual Machine Manager virtual machines previsioned in the earlier step. Perform the following procedure on one of the Virtual Machine Manager virtual machines.

1. Launch a PowerShell prompt with administrative permissions, by right clicking on the PowerShell icon and selecting **Run as Administrator**.



2. Create a new cluster by executing the following command

```
New-Cluster -Name <cluster_name> -Node <Node1>, <Node2> -NoStorage -StaticAddress <cluster_ip_address>
```

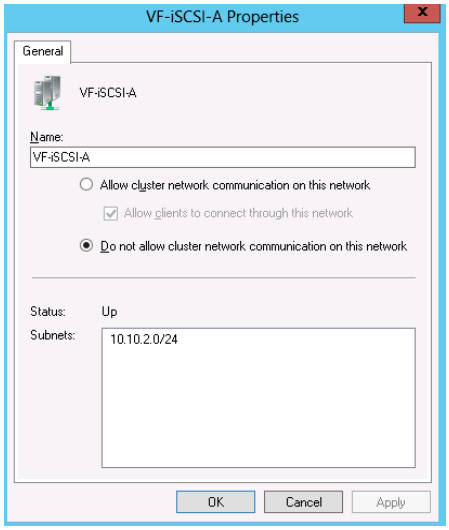
```
PS C:\Users\administrator.FLEXPOD> New-Cluster -Name SCVMM-Cluster01 -Node SCVMM01, SCVMM02 -NoStorage -StaticAddress 19
2.168.1.70
Report file location: C:\Windows\cluster\Reports\Create Cluster Wizard SCVMM-Cluster01 on 2013.04.28 At 13.01.18.mht

Name
----
SCVMM-Cluster01
```

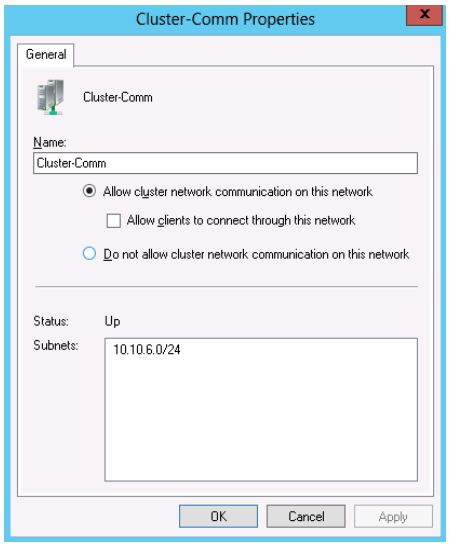
3. Rename the cluster networks to match there function.

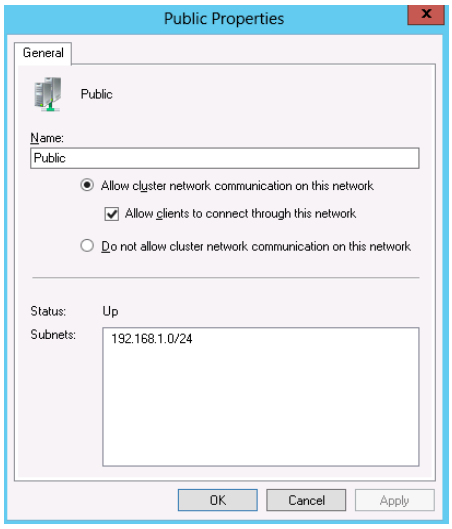
```
Get-ClusterNetworkInterface | ? Name -like *Public* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'Public'}

Get-ClusterNetworkInterface | ? Name -like *Cluster* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'Cluster-Comm'}

Get-ClusterNetworkInterface | ? Name -like *iSCSI-A* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'VF-iSCSI-A'}

Get-ClusterNetworkInterface | ? Name -like *iSCSI-B* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'VF-iSCSI-B'}
```

```
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetworkInterface | ? Name -like *Public* | Group Network| %{ (Get-ClusterN
etwork $_.Name).Name = 'Public'}
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetworkInterface | ? Name -like *Cluster* | Group Network| %{ (Get-Cluster
Network $_.Name).Name = 'Cluster-Comm'}
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetworkInterface | ? Name -like *iSCSI-A* | Group Network| %{ (Get-Cluster
Network $_.Name).Name = 'VF-iSCSI-A'}
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetworkInterface | ? Name -like *iSCSI-B* | Group Network| %{ (Get-Cluster
Network $_.Name).Name = 'VF-iSCSI-B'}
PS C:\Users\administrator.FLEXPOD>
```

4. Using Failover Cluster Manager, expand the Networks object in the left tree view. Right click each network and select properties.
    a. **Disable** cluster communication for the VF-iSCSI-A and VF-iSCSI-B networks.
    b. **Uncheck** Allow clients to comment through this network for the Cluster-Comm network.
    c. **Check** Allow clients to comment through this network for the Public network.

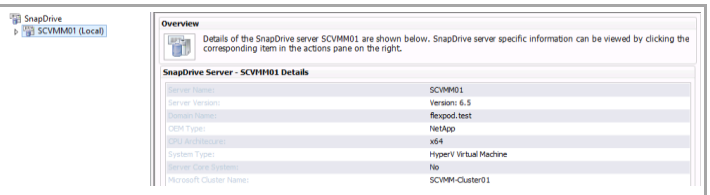
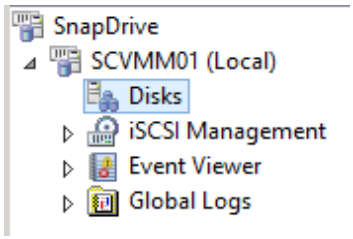
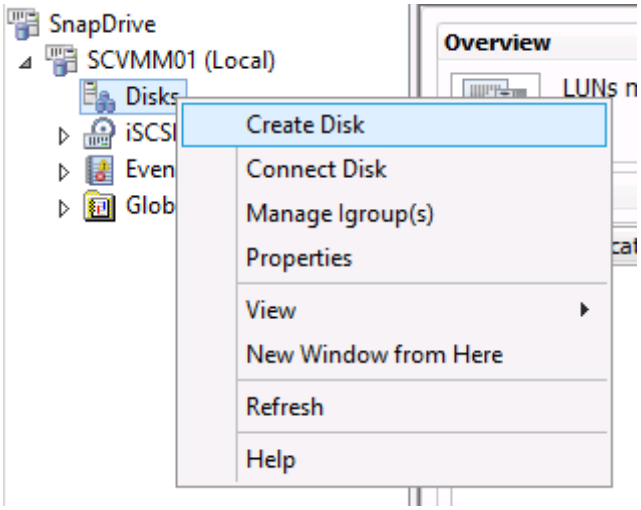
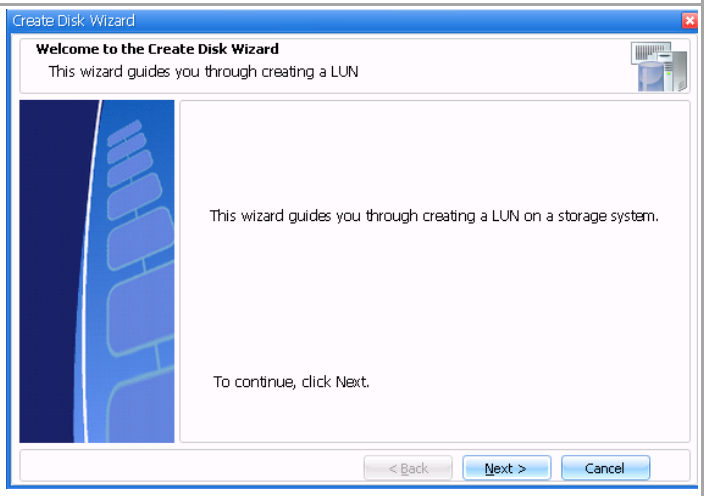


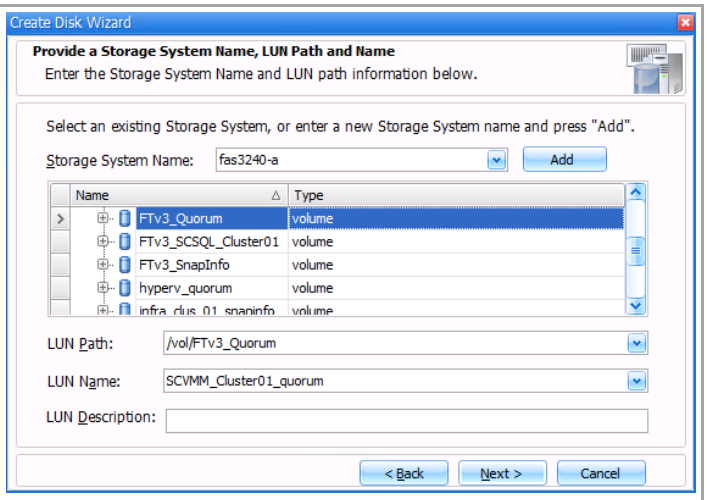
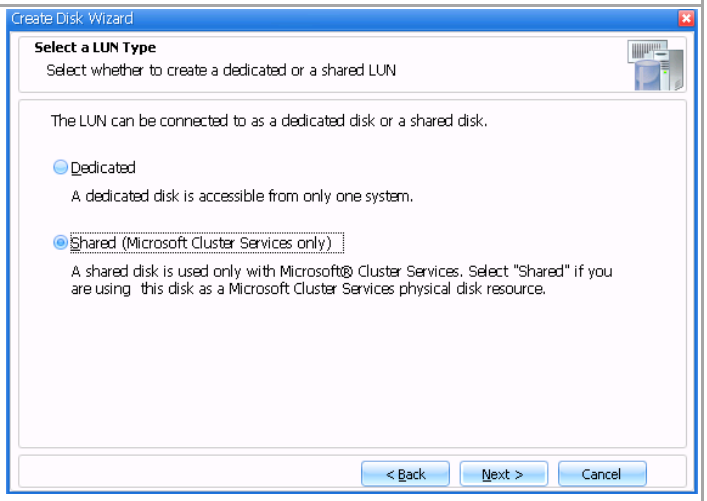
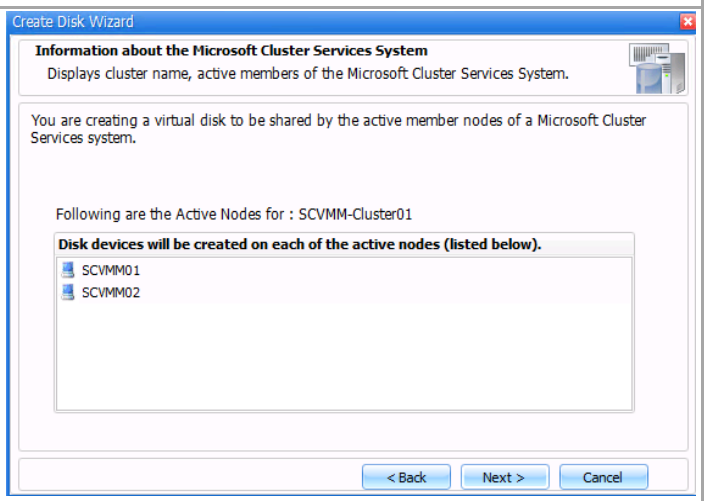


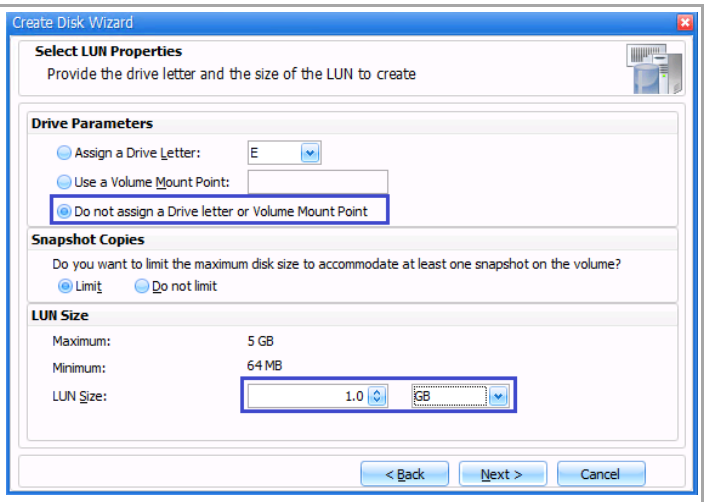
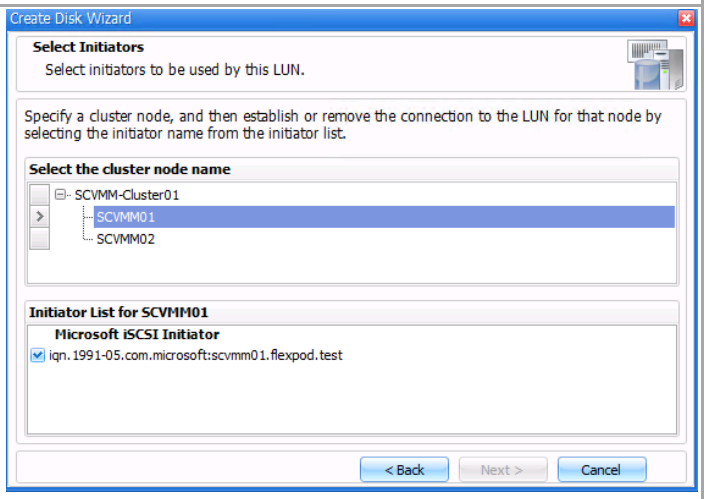
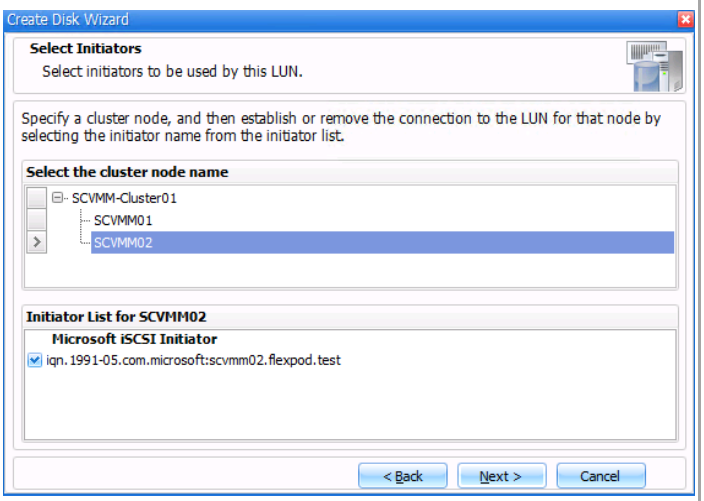


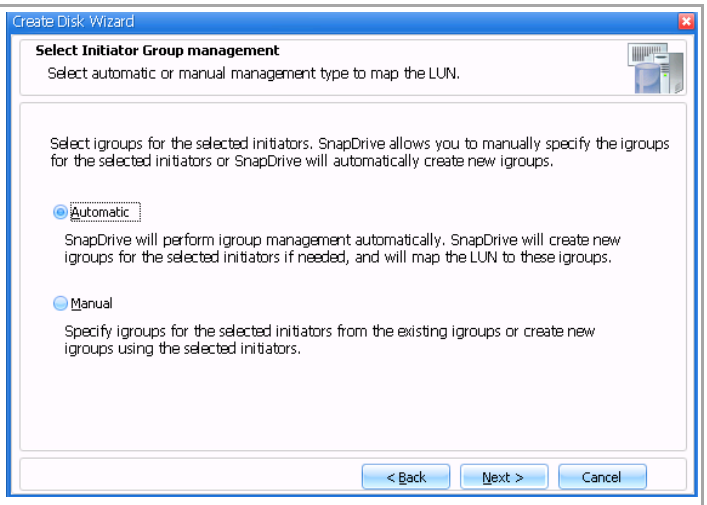
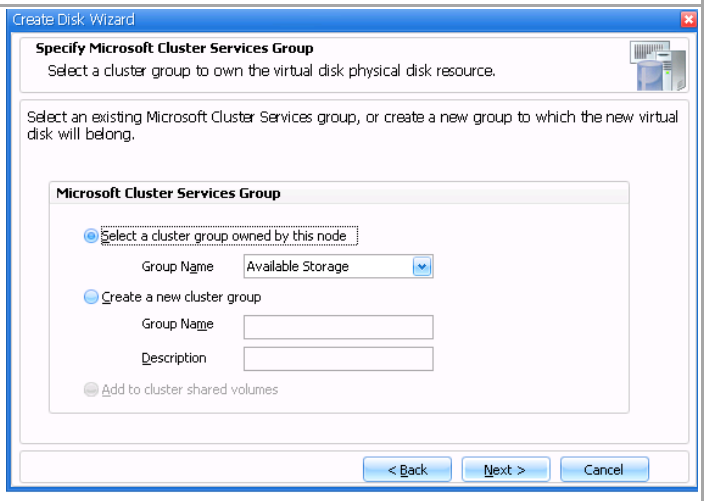
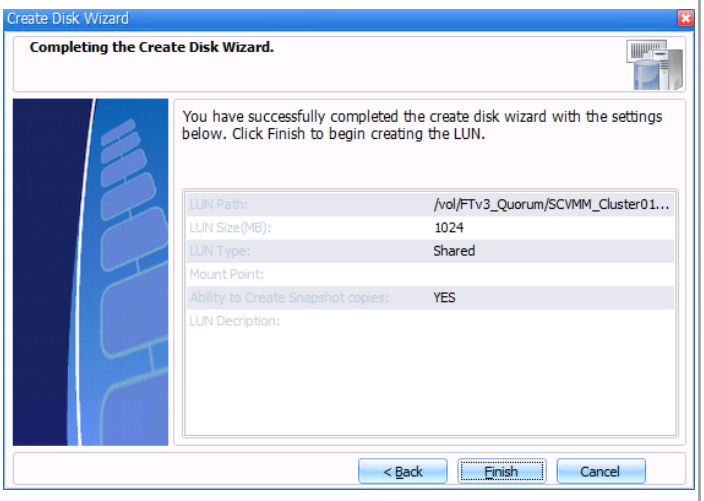
Create and Map the LUNs using SnapDrive

Create Virtual Machine Manager Cluster quorum LUN using SnapDrive. Perform this action from the one node in the Virtual Machine Manger Cluster.

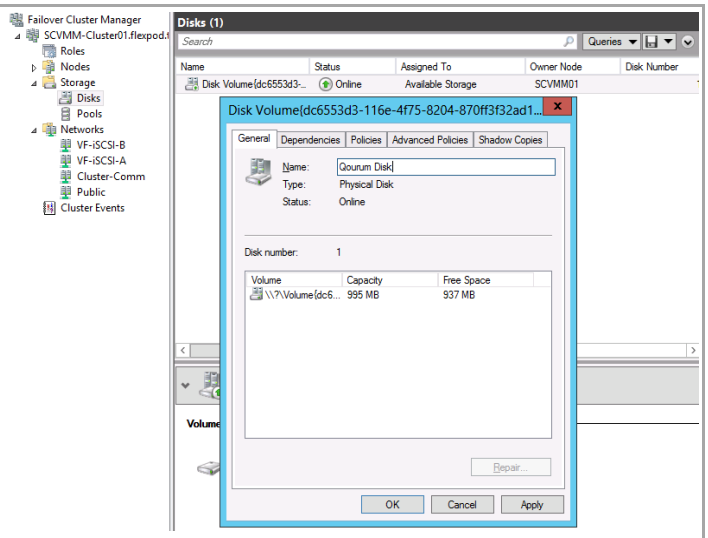
1. Open SnapDrive from the start screen to configure cluster storage.	
2. Expand server name object in the left tree view, and select the disk object.	
3. Right-click the Disks Icon and choose to Create Disk.	
4. Click Next on the welcome screen.	

5. Enter in the IP Address or host name of the controller in the Storage System Name field and click Add. 6. Select the volume from the volume list. 7. Enter the LUN name and click next.	
8. Select Shared (Microsoft Cluster Service) click Next.	
9. Review the list of cluster nodes and click Next.	

10. Do not assign the drive letter and set the LUN size to 1GB. Click Next.	
11. In the Select Initiators screen, Select each cluster node and check the Microsoft iSCSI initiator IQN to use for the LUN mapping. Click Next.	 

12. Select Automatic igroup management and Click Next.	
13. Select the cluster group owned by this node and select the Available Storage group.	
14. Review the parameters and click Finish. 15. Repeat this operation for each LUN in the table above. 16. Database and transaction log LUNs may be distributed among both storage controllers.	

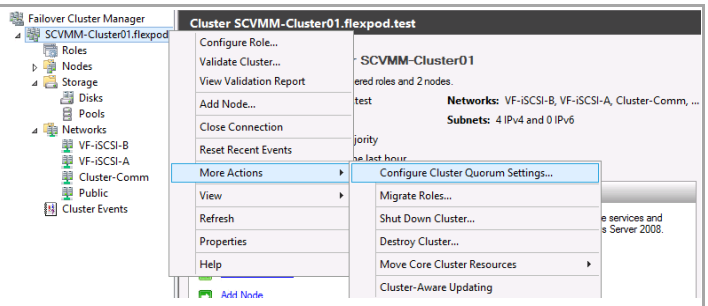
17. Use Failover Cluster Manager navigate to the Disks object under Storage. Double click the new disk to open its properties windows. Rename the disk to match its function.



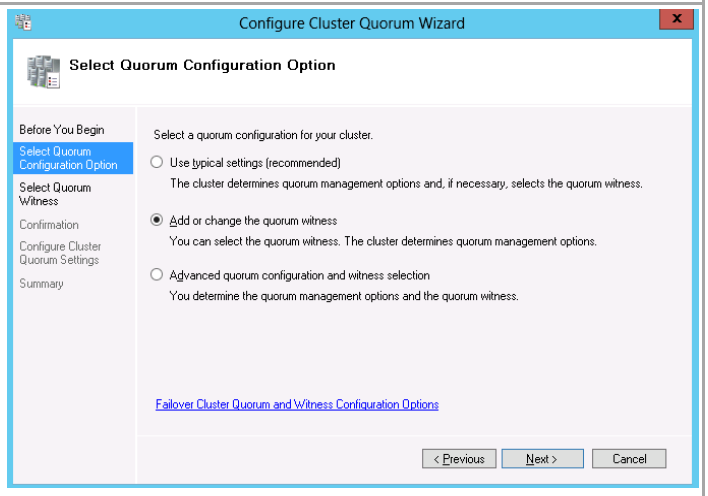
Change the VMM Server Cluster to Use a Quorum Disk

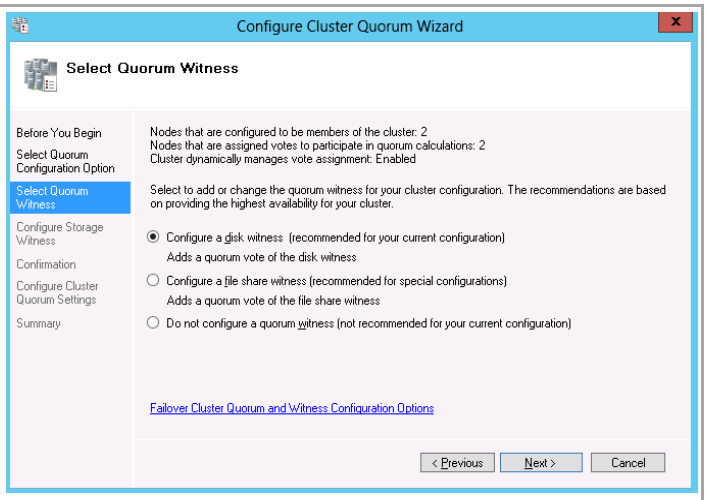
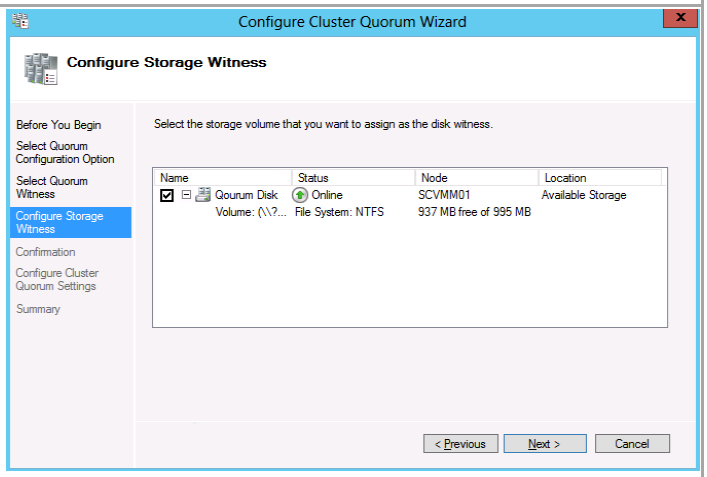
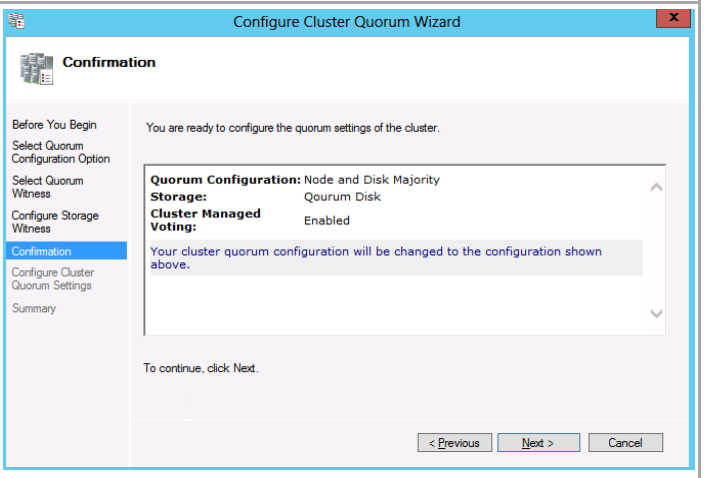
1. In failover cluster manager, select **More Actions** in the action pane and click **Configure Cluster Quorum Settings...**
2. The following comdlet can be used to assign the quorum disk as an alternative to using Failovor Cluster Manager.

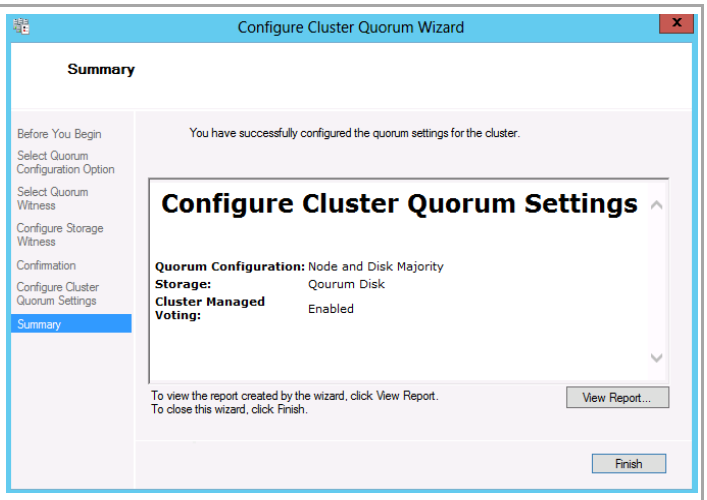
Set-ClusterQuorum -NodeAndDiskMajority <ClusterQuorumDisk>



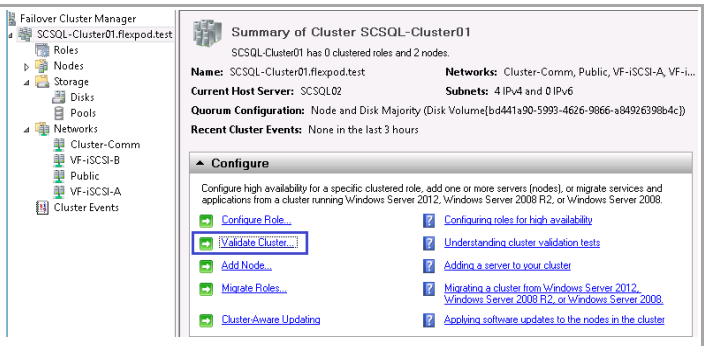
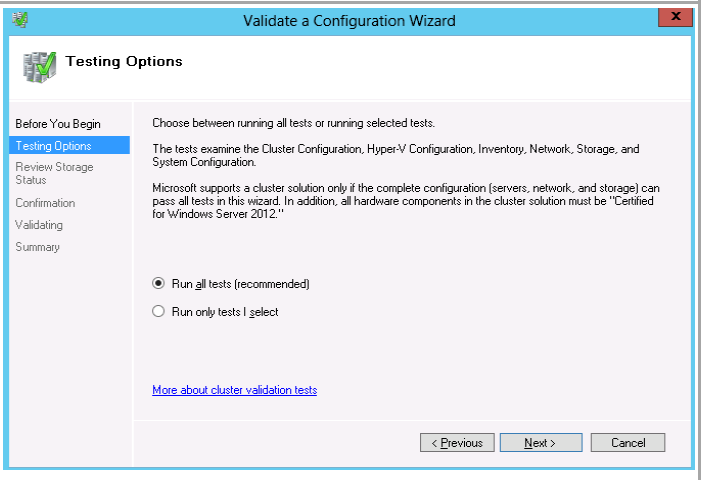
3. Select **Add or Change the quorum witness**, and click **Next**.

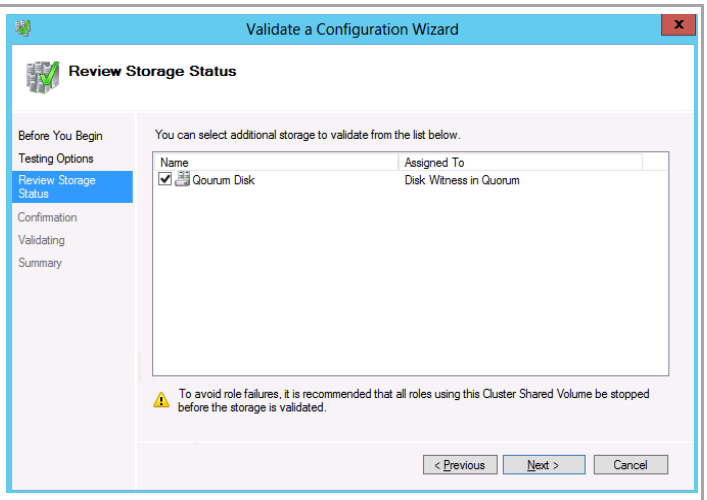
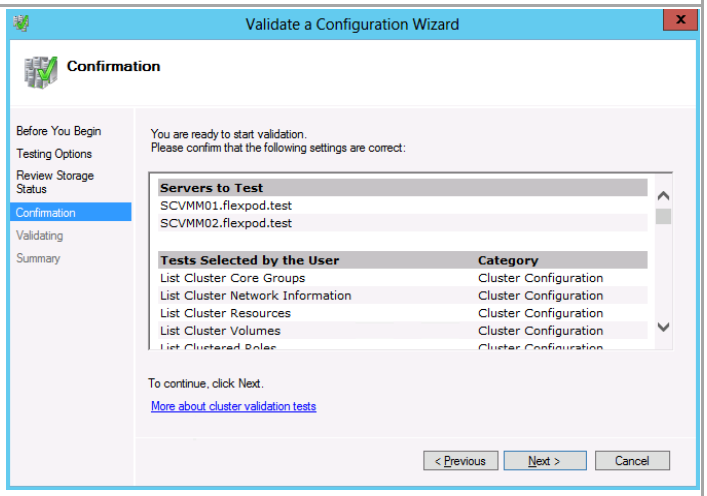
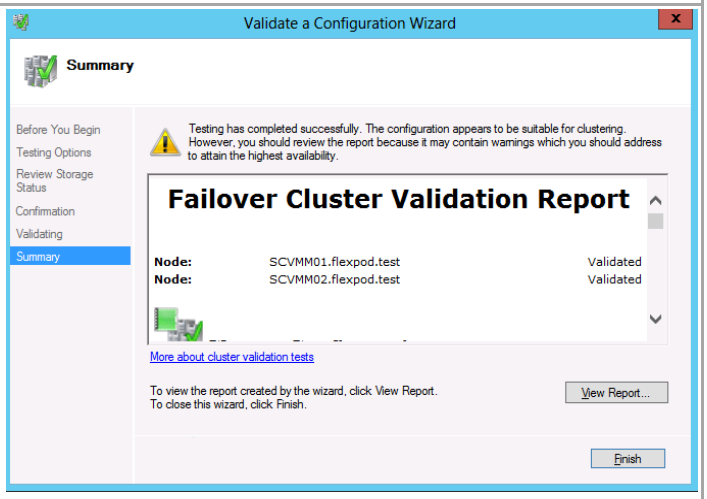


4. Select **Configure a disk witness** and click **Next**.	
5. **Select the LUN** without a drive letter that was previously created to be the quorum LUN. Click **Next**.	
6. Confirm the settings and click **Next.**	

7. **Review the results** and click **Finish to close the wizard screen.**	

Validated the VMM Server Cluster

1. Select the SQL Server cluster in the left tree view and click Validate Cluster.	
2. Select **Run all tests** and click Next.	

3. Select all the disks on the cluster and click Next.	
4. Confirm the selected options and click **Next**.	
5. Review and correct any failures that are listed in the validation report. The following warnings are expected to be reported by the validation wizard. These warning can safely be disregarded.	

Note: The following warnings are expected to be reported by the validation wizard. These warning can safely be disregarded.

Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node SCVMM01.flexpod.test.

Test Disk 0 does not support SCSI-3 Persistent Reservations commands needed to support clustered Storage Pools. Some storage devices require specific firmware versions or settings to function properly with failover clusters. Please contact your storage administrator or storage vendor to check the configuration of the storage to allow it to function properly with failover clusters.

Create the Virtual Machine Manger Distributed Key Management Container in Active Director Domain Services

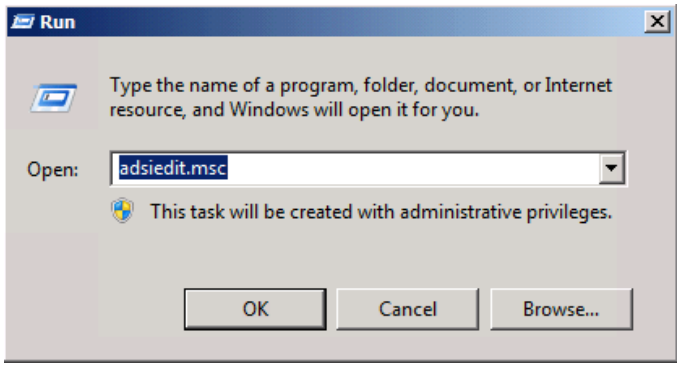
The Virtual Machine Manager installation requires that an Active Directory container be created to house the distributed key information for Virtual Machine Manager.[8]

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

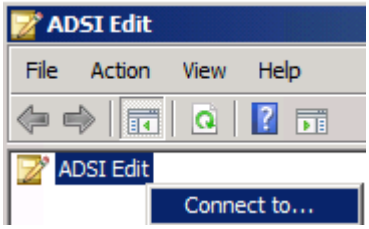
Perform the following steps to create an AD DS container to house the distributed key information. These instructions assume a Windows Server 2008 R2 domain controller is in use, similar steps would be followed for other versions of Active Directory including Windows Server 2008 and Windows Server 2012.

▶ Perform the following steps on a **Domain Controller** in the domain where Virtual Machine Manager is to be installed.

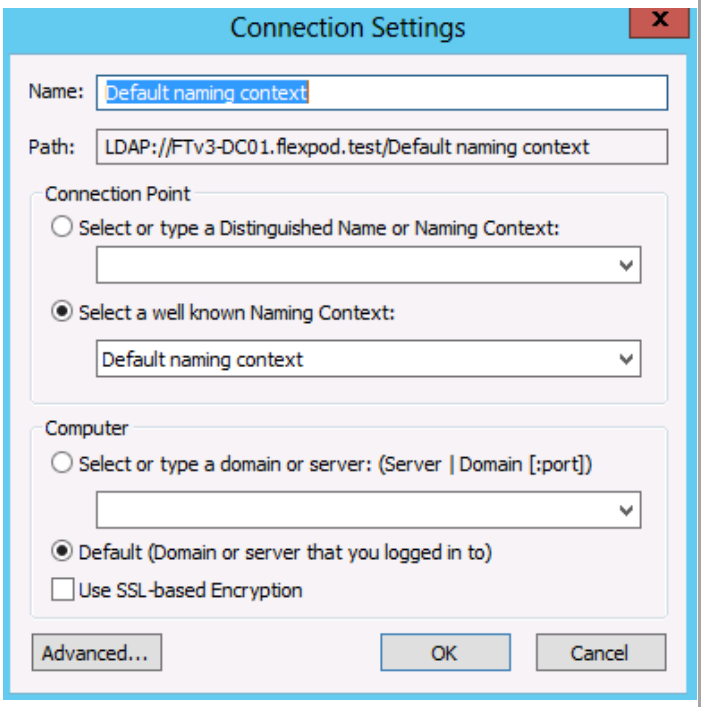
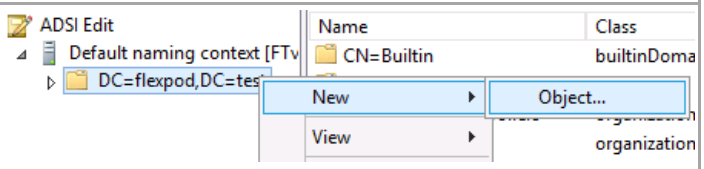
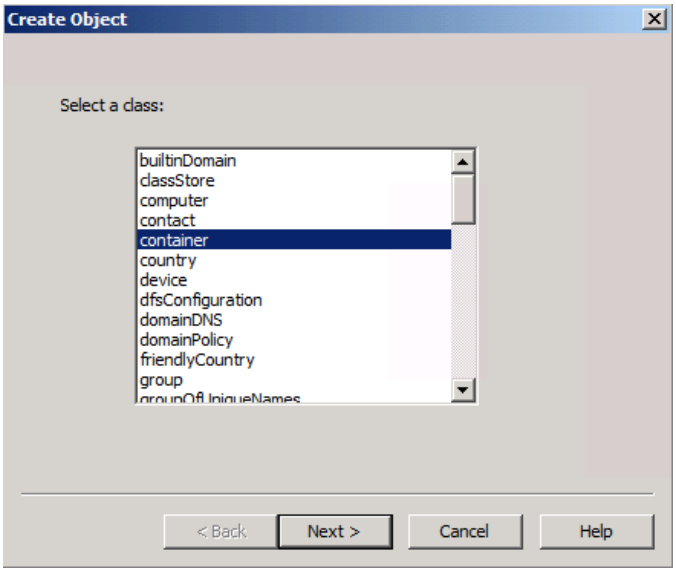
1. Log on to a Domain Controller with a user that has Domain Admin privileges and run **adsiedit.msc.**

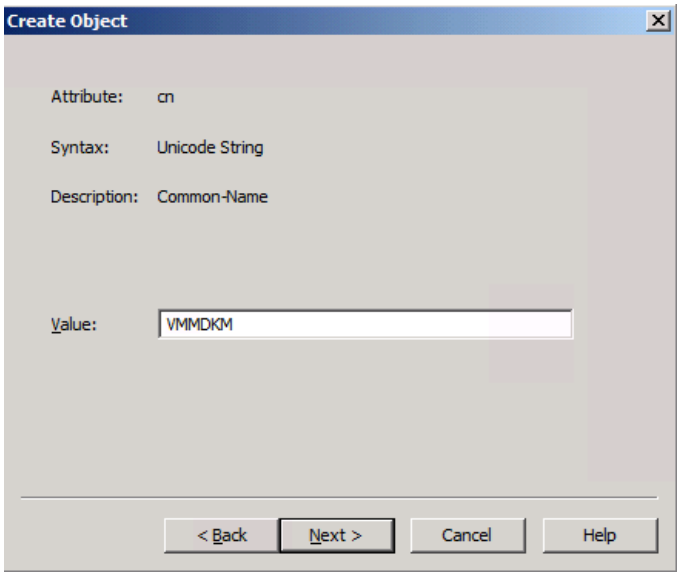
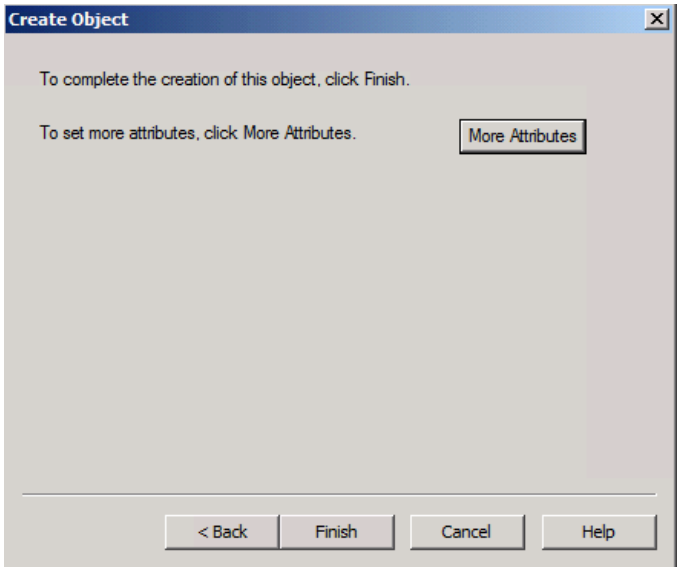


2. Right-click the **ADSI Edit** node and select **Connect to...** from the context menu.

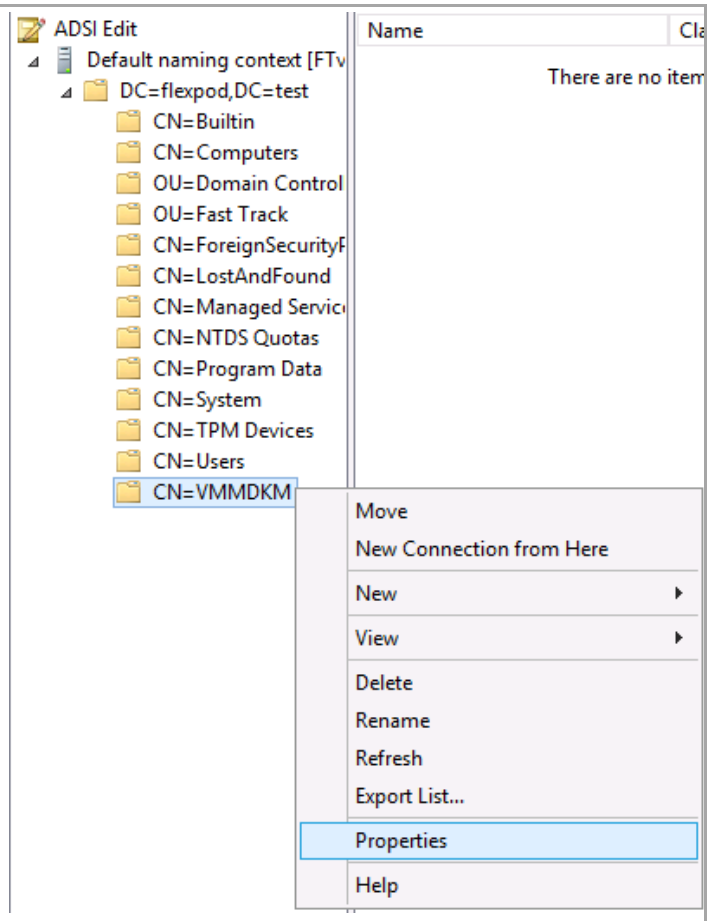


[8] Configuring Distributed Key Management in VMM - http://technet.microsoft.com/library/gg697604.aspx.

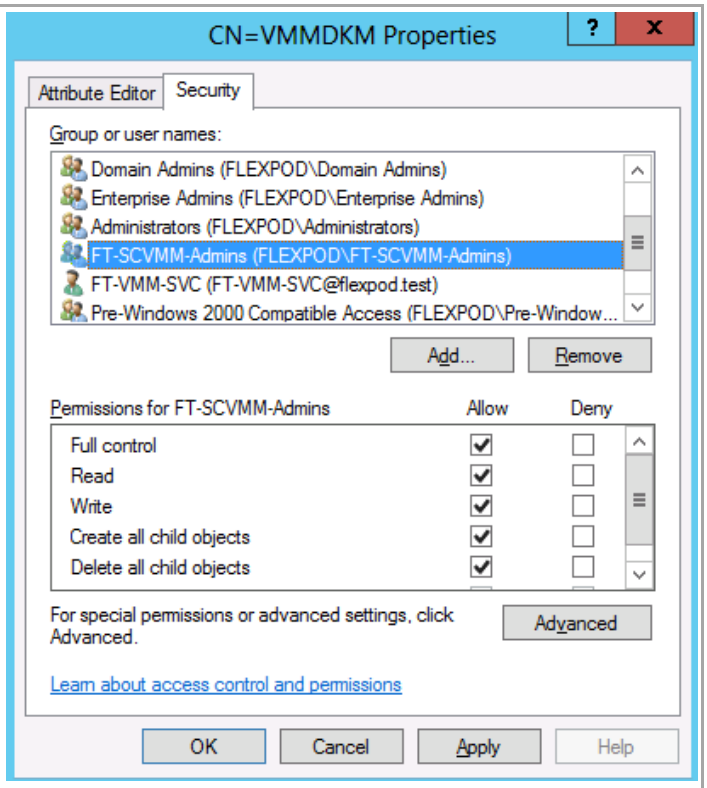
3. In the **Connections Settings dialog** in the **Connection Point** section, select the **Select a well known Naming Context** option. Select **Default naming context** from the drop-down menu and click **OK**.	
4. Expand *Domain Default naming context [<computer fully qualified domain name>]*, expand *<distinguished name of domain>*, right-click the root node and select **New – Object...** from the context menu.	
5. In the **Create Object** dialog box, select **Container** and then click **Next.**	

6. In the **Value** text box, type *VMMDKM* and then click **Next**.	
7. Click **Finish** to create the container object.	

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



9. 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.
10. Click **OK** three times and close ADSI Edit.

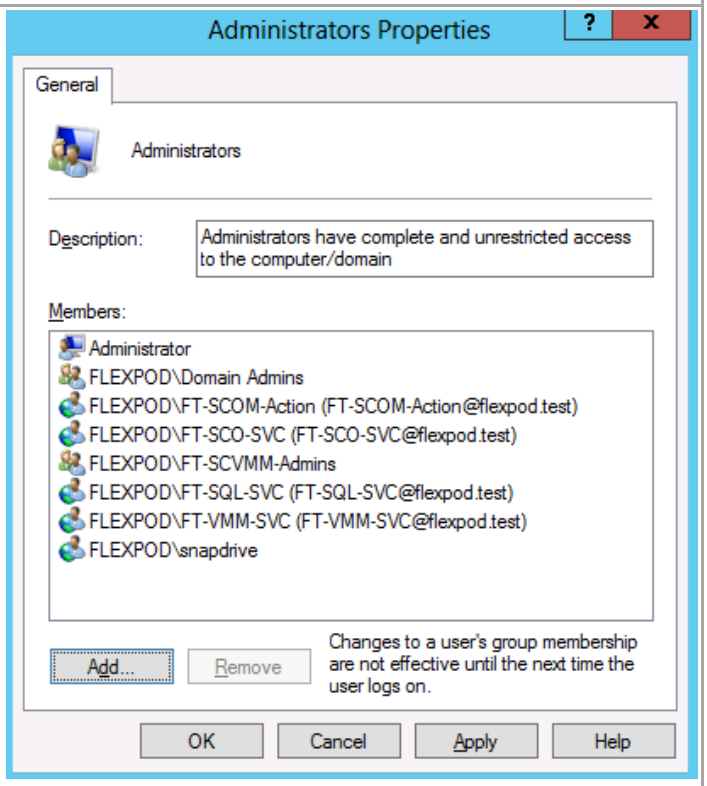


15.4 Installation

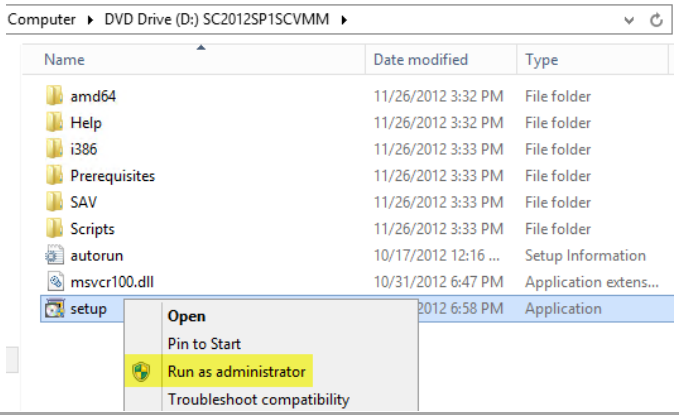
Install the Virtual Machine Manager Failover Cluster

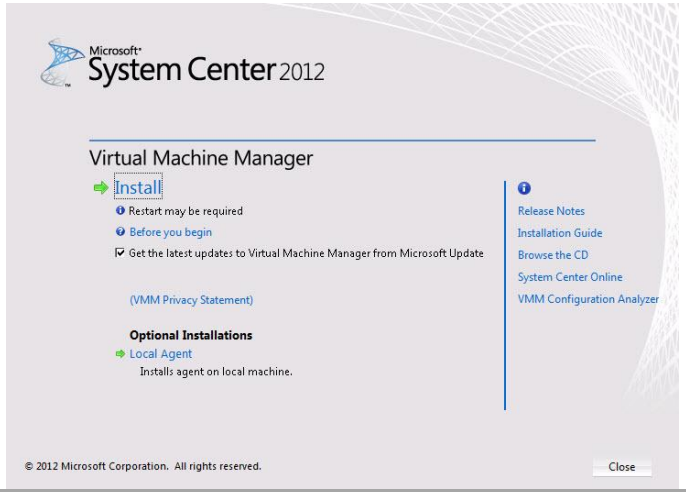
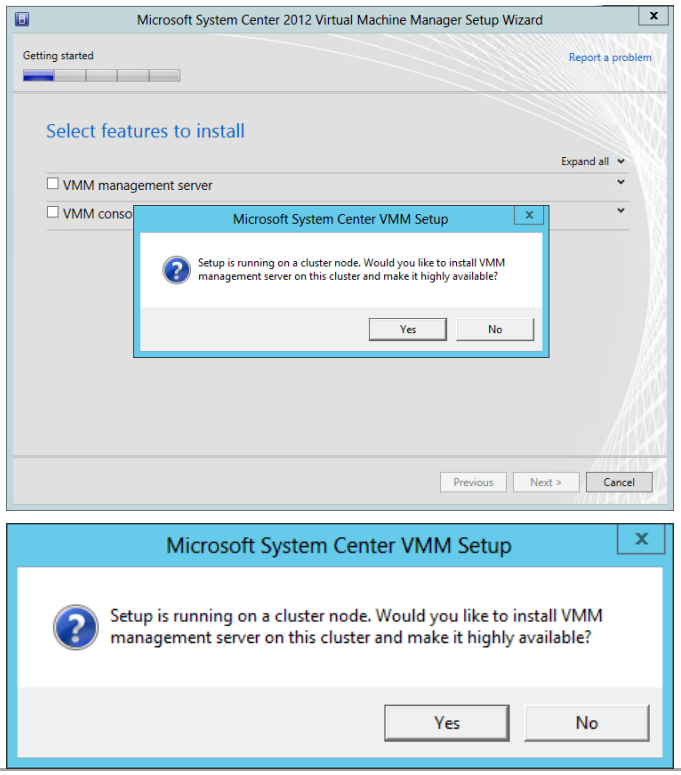
▶ Perform the following steps on the **first Virtual Machine Manager** virtual machine.

1. Log on to the Virtual Machine Manager virtual machine with a user with local admin rights.
2. 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.
   - SnapDrive Service account

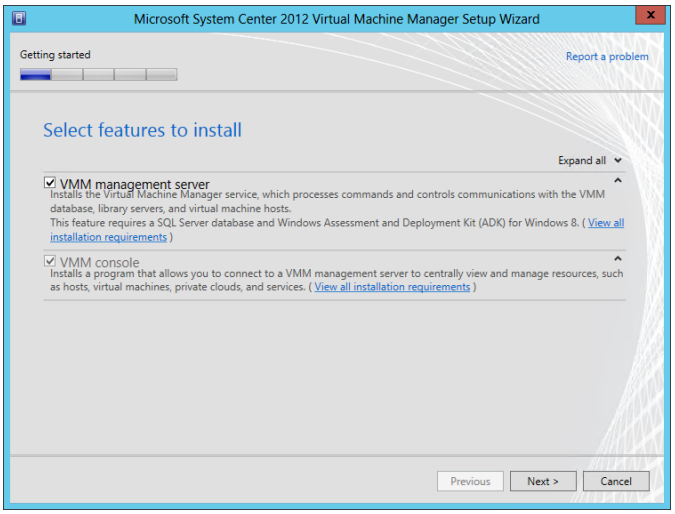


3. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.

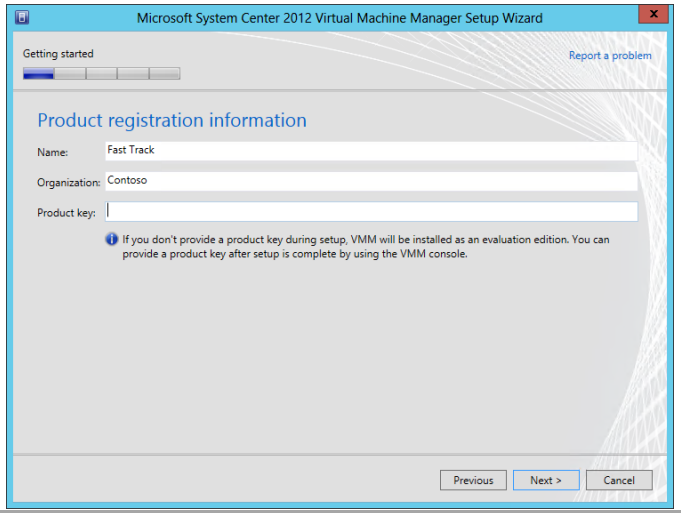


4. The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.	
5. Attempting to select any feature will cause the cluster management server notice to appear. 6. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard.	

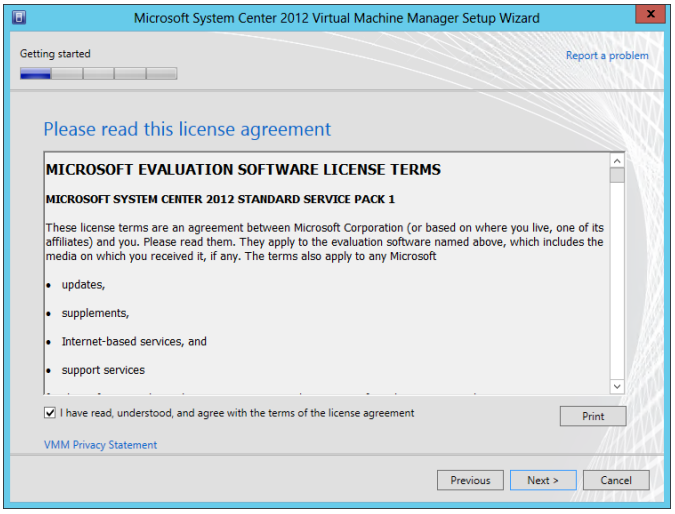
7. In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **VMM console** installation option check box will be selected by default. Click **Next** to continue.

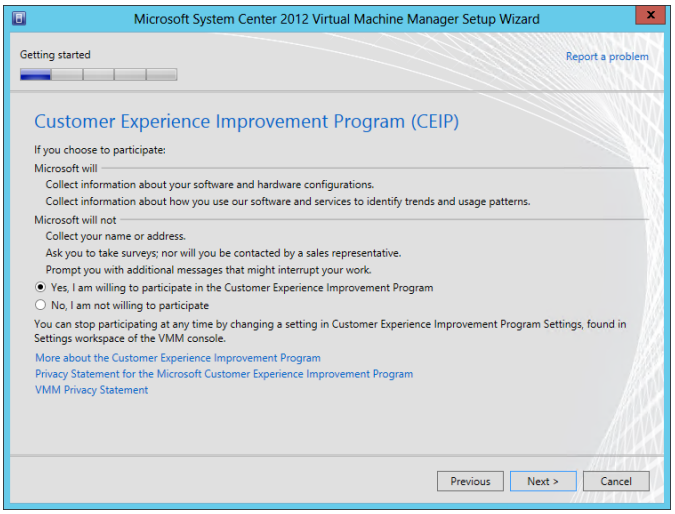
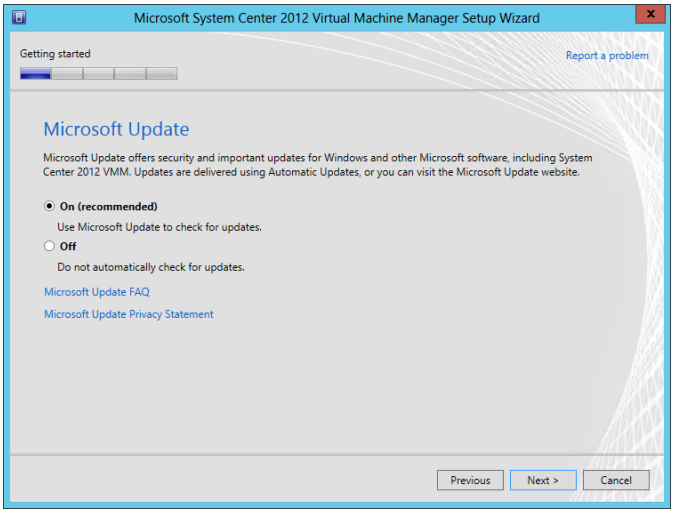
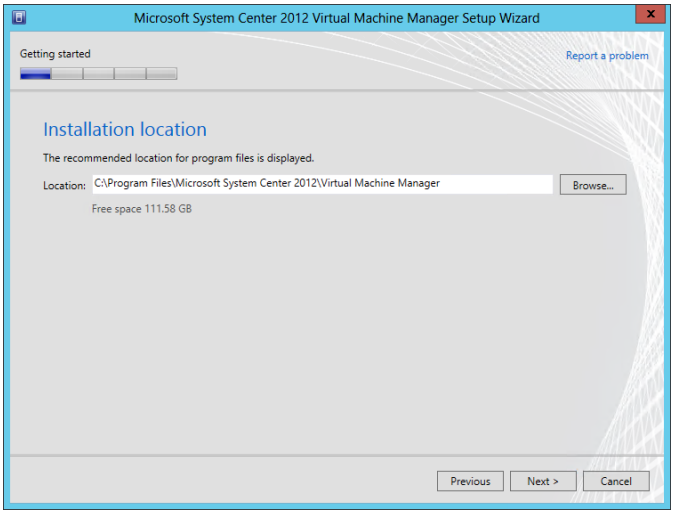


8. In the **Product registration information** dialog, enter the following information in the provided text boxes:
   a. **Name** – *specify the name of the primary user or responsible party within your organization.*
   b. **Organization** - *specify the name of the licensed organization.*
   c. **Product 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.*
9. Click **Next** to continue.

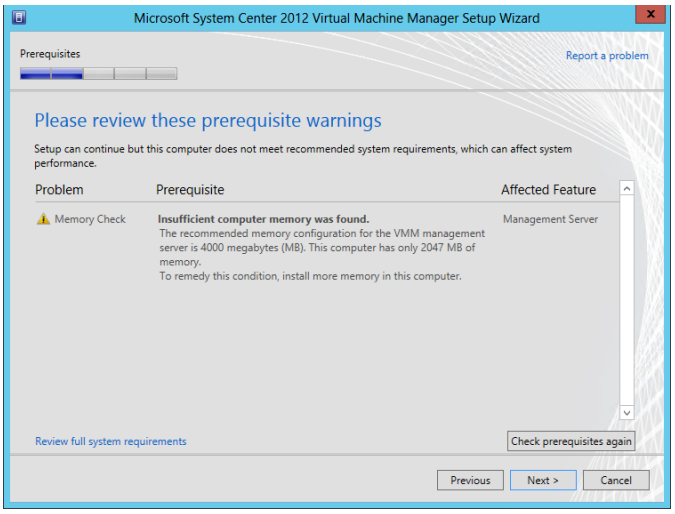


10. In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.

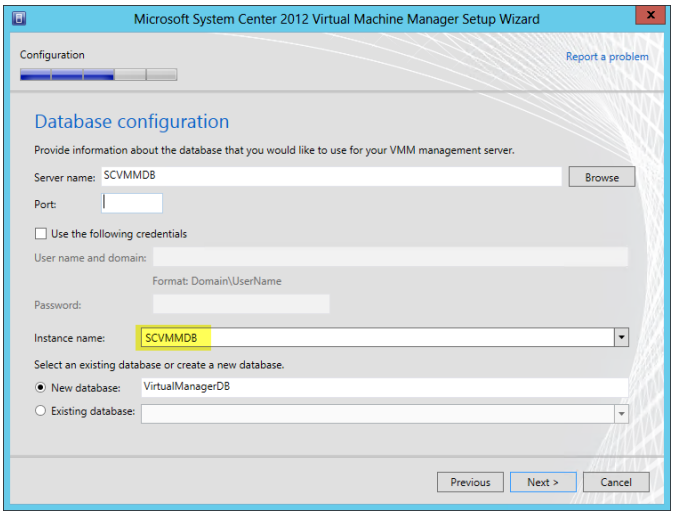


11. In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
12. In the **Microsoft Update** dialog, select the option to either 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.	
13. 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.	

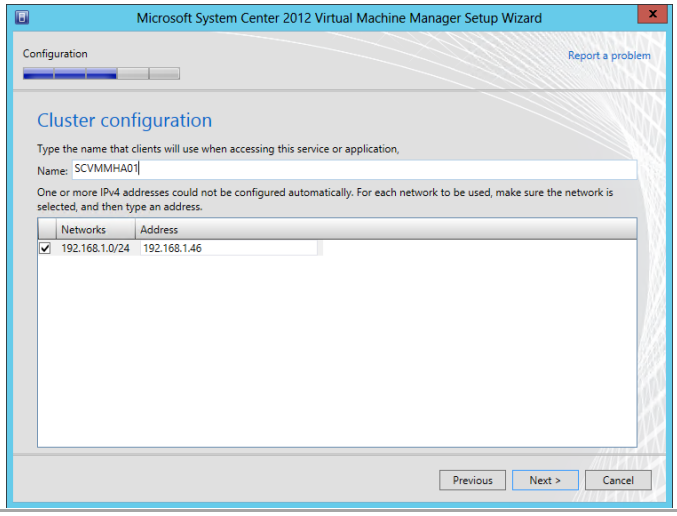
14. **Note:** The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy.
15. **The following is just an example of that UI.**
16. If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



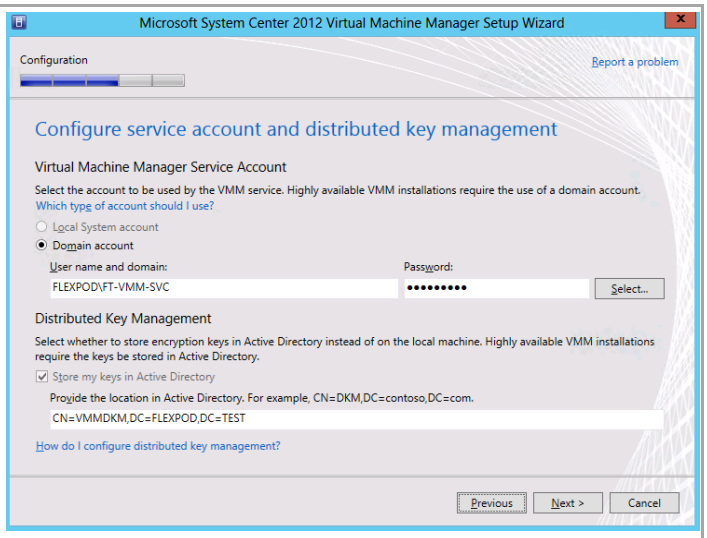
17. In the **Database configuration** dialog, enter the following information in the provided text boxes:
    a. **Server name** – *specify the name of the SQL Server cluster created in the steps above.*
    b. **Port** - *specify the TCP port used for the SQL Server, as configured in the steps above.*
18. 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.
19. 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*.
20. Click **Next** to continue.



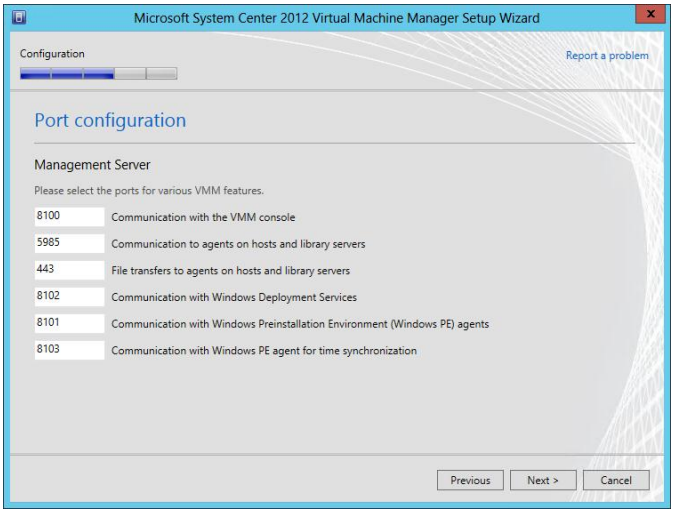
21. In the **Cluster Configuration** dialog, in the **Name** field, provide a name for the Virtual Machine Manager cluster service.
22. If the cluster node you are installing is configured with static IP addresses you will also need to provide an IP address for the Virtual Machine Manager cluster service.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



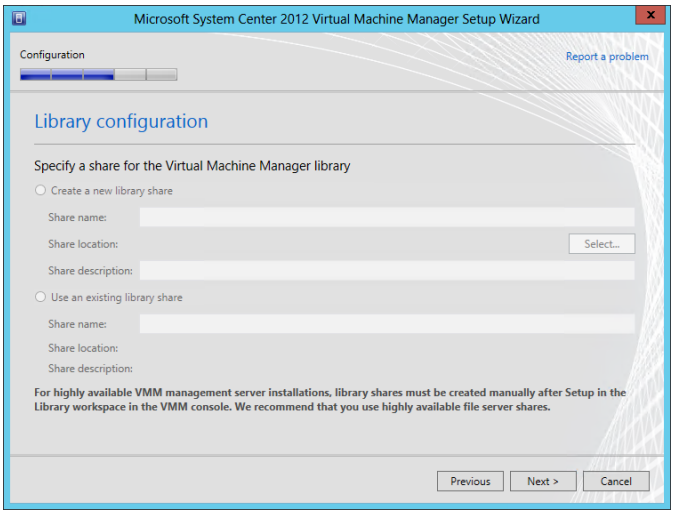
23. In the **Configure service account and distributed key management** dialog, in the **Virtual Machine Manager Service account** section, select the **Domain account** option. Enter the following information in the provided text boxes:
    a. **User name and domain** – *specify the Virtual Machine Manager service account identified in the section above in the following format: <DOMAIN>\<USERNAME>.*
    b. **Password** – *specify the password for the Virtual Machine Manager service account identified above.*
24. 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,…*
25. Click **Next** to continue.



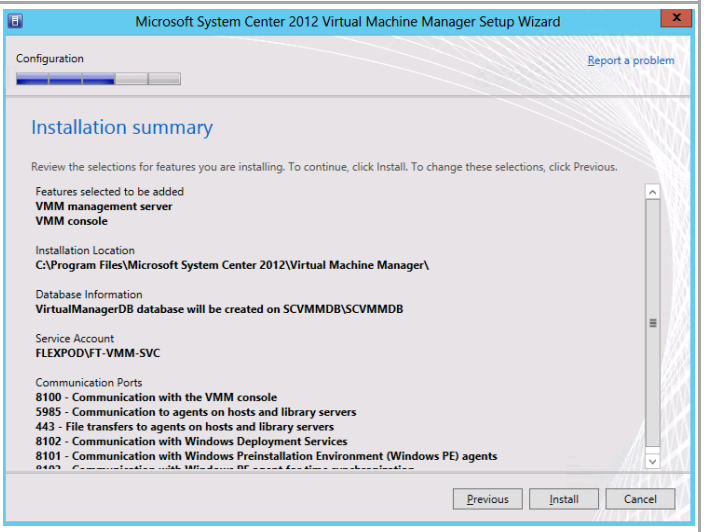
26. In the **Port configuration** dialog, accept the default values in the provided text boxes:
    a. **Communication with the VMM console** – *default: 8100.*
    b. **Communication to agents on hosts and library servers** – *default: 5985.*
    c. **File transfers to agents on hosts and library servers** – *default: 443.*
    d. **Communication with Windows Deployment Services** – *default: 8102.*
    e. **Communication with Windows Preinstallation Environment (Windows PE) agents** – *default: 8101.*
    f. **Communication with Windows PE agent for time synchronization** – *default: 8103.*
27. Click **Next** to continue.



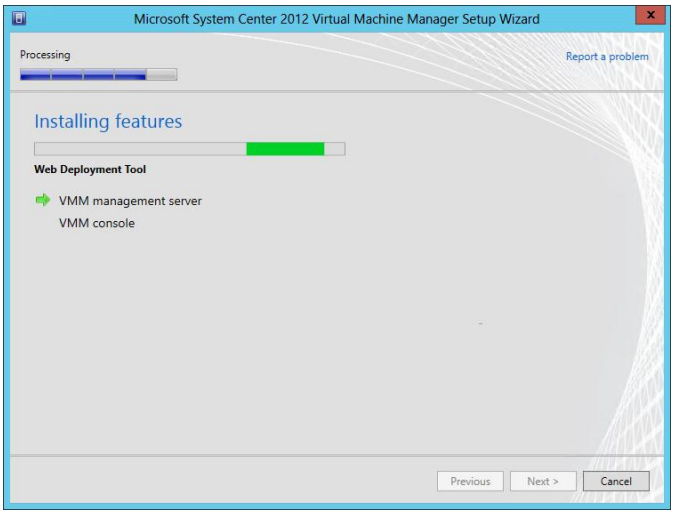
28. In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.



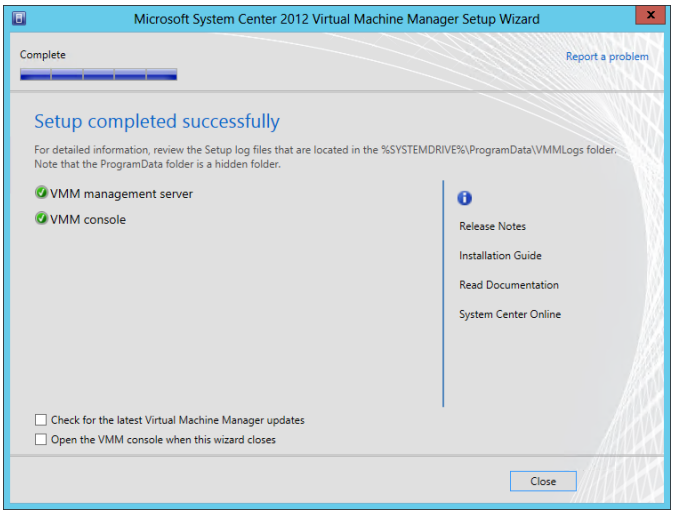
29. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



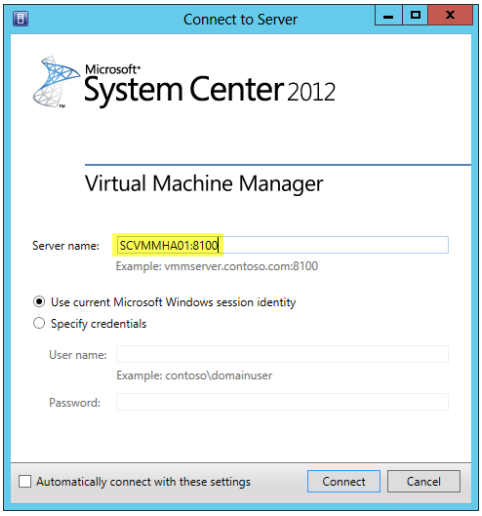
30. The wizard will display the progress while installing features.

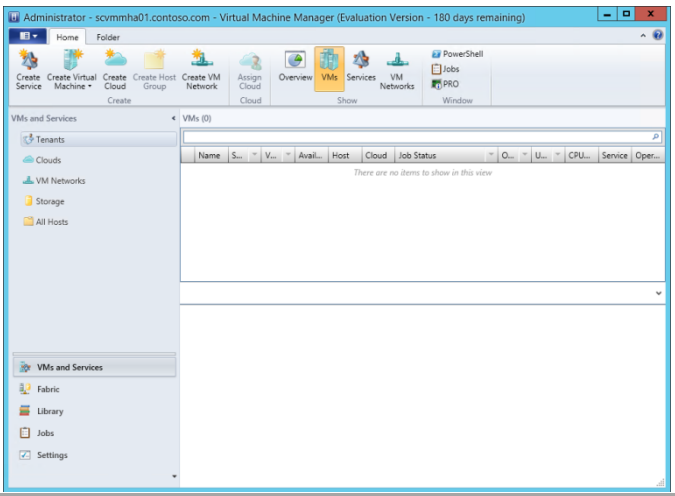


31. When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.



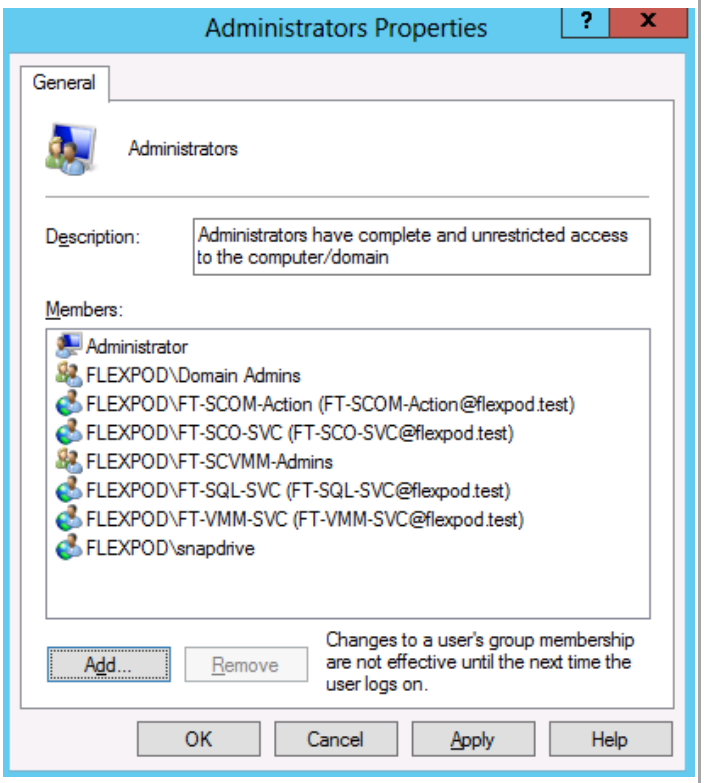
32. When complete, launch the Virtual Machine Manager console to verify the installation occurred properly. Set the **Server name** value to match the name that was provided for the **Cluster Resource** name during setup (for example, HAVMM: 8100). Verify that the console launches and connects to the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



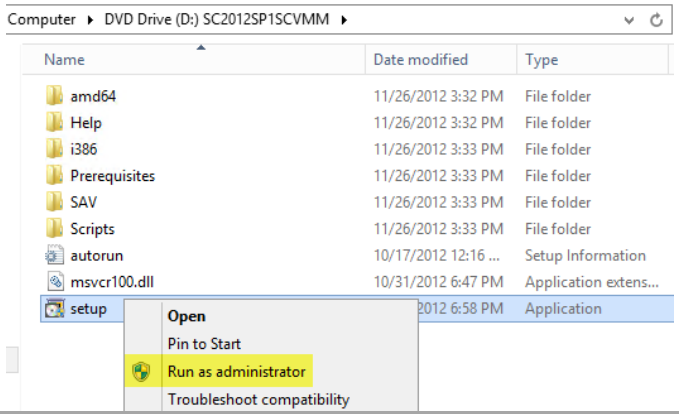


▶ Perform the following steps on the **second Virtual Machine Manager** virtual machine.

1. Log on to the **second** Virtual Machine Manager virtual machine with a user with local admin rights.
2. 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.



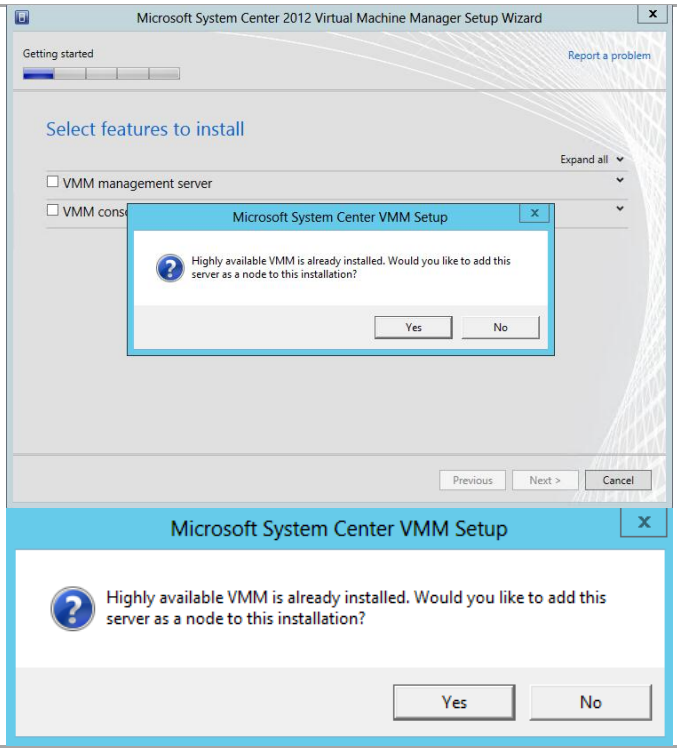
3. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



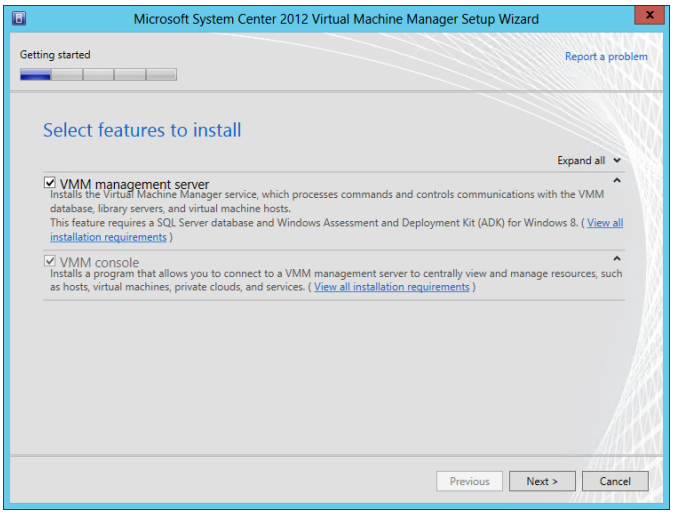
4. The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.

5. Attempting to select any feature will cause the cluster management server notice to appear.
6. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard and add the second node.

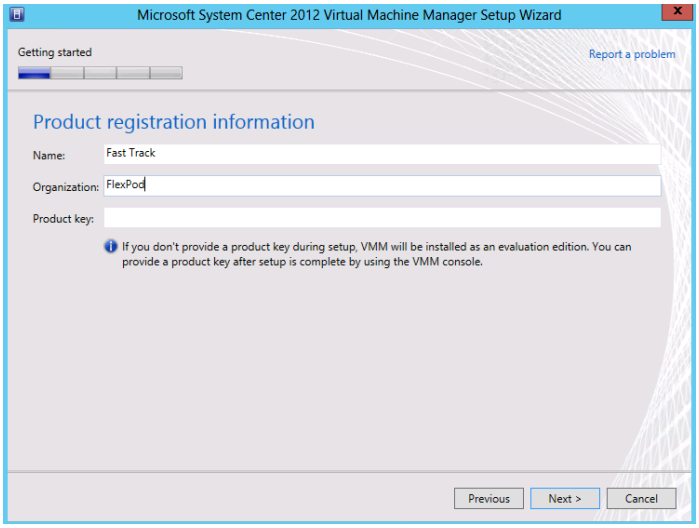
Note: Virtual Machine Manager can be deployed on up to 16 cluster nodes but only a single node can be active at any time.



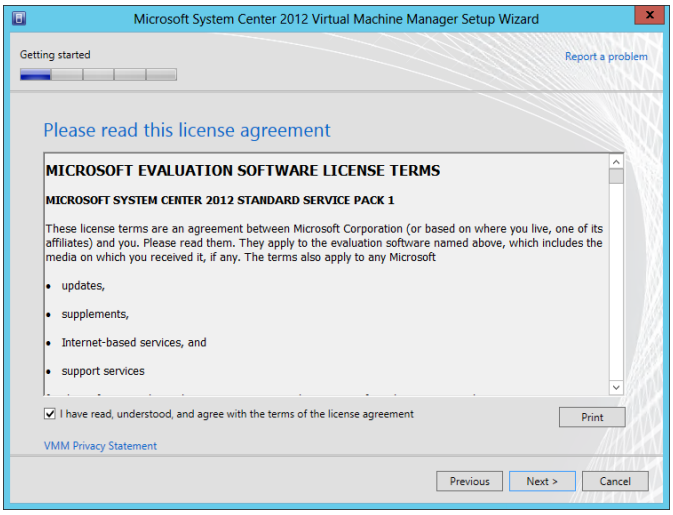
7. In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **Virtual Machine Manager console** installation option check box will be selected by default. Click **Next** to continue.



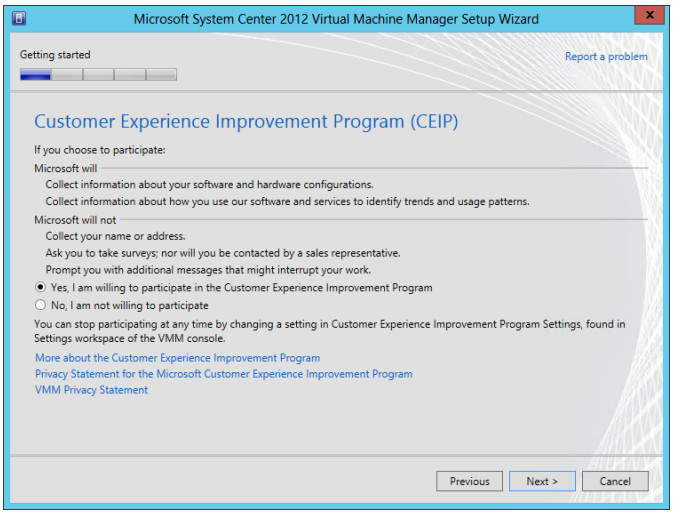
8. In the **Product registration information** dialog, enter the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** – *specify the name of the licensed organization.*
    c. **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.*
9. Click **Next** to continue.



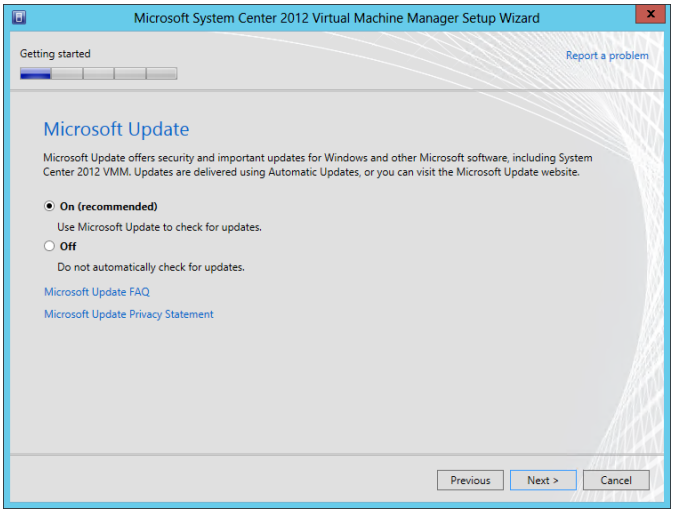
10. In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



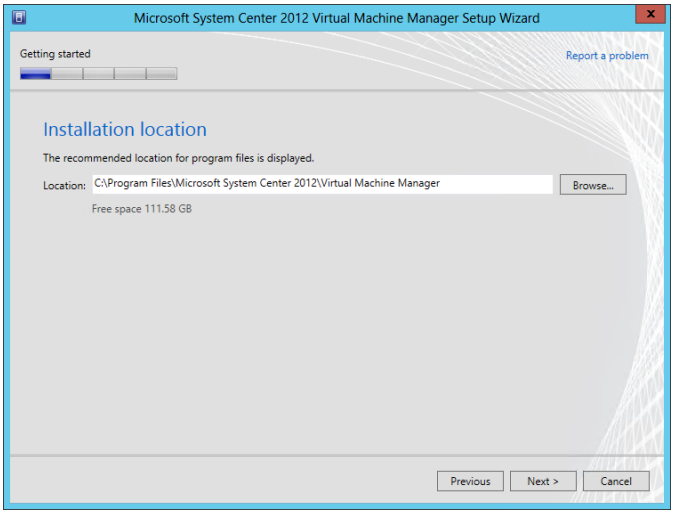
11. In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



12. 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.

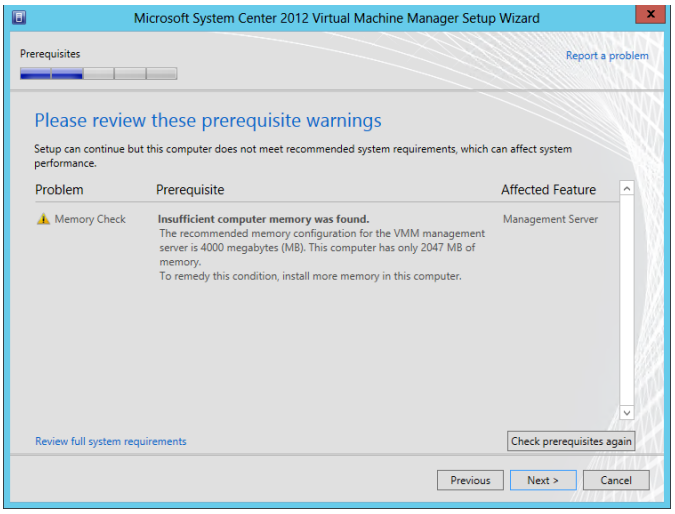


13. In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.

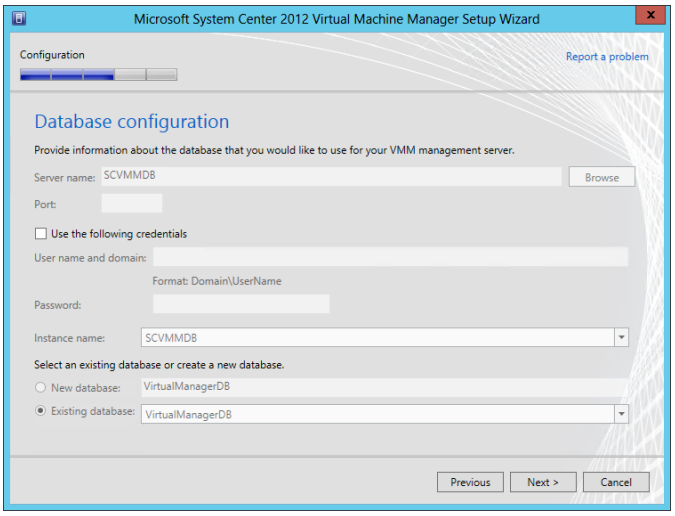


Note: The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy.

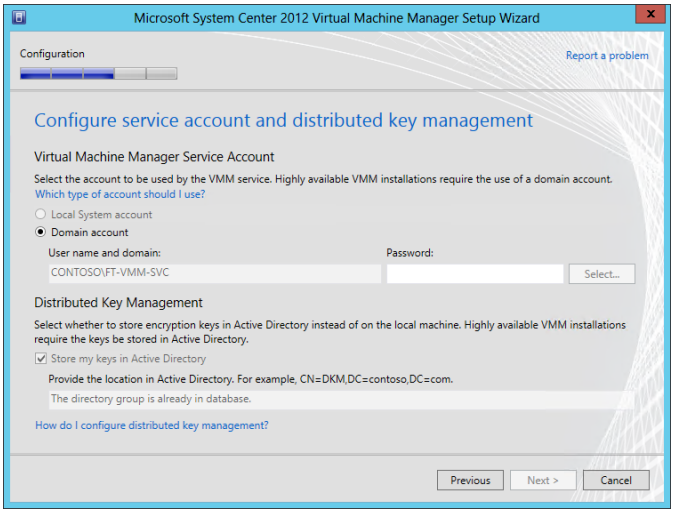
14. **The following is just an example of that UI.**
15. If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



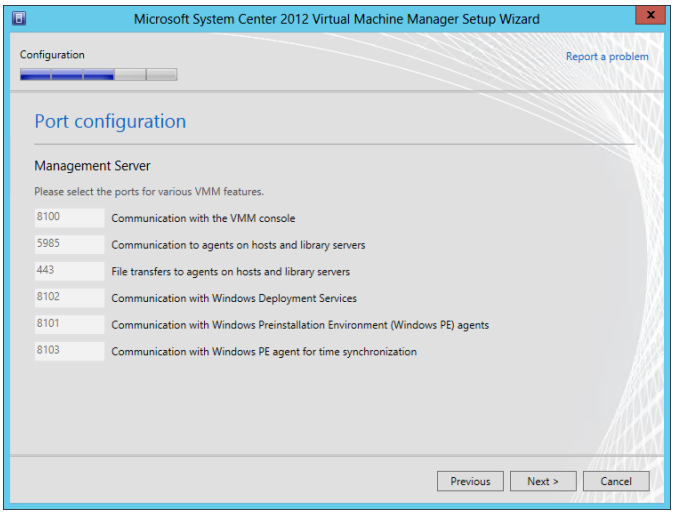
16. In the **Database configuration** dialog, all options are greyed out when adding an additional node to an existing Virtual Machine Manager cluster.
17. Click **Next** to continue.



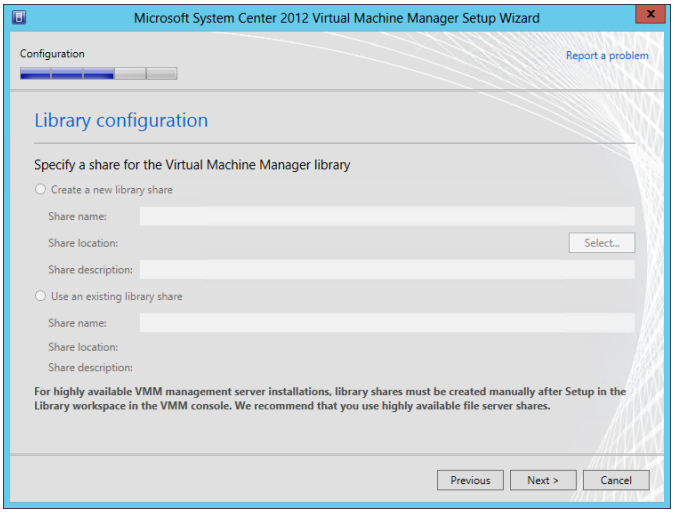
18. In the **Configure service account and distributed key management** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields other than **Password** are greyed out.
    a. **Password** – *specify the password for the Virtual Machine Manager service account identified above.*
19. Click **Next** to continue.



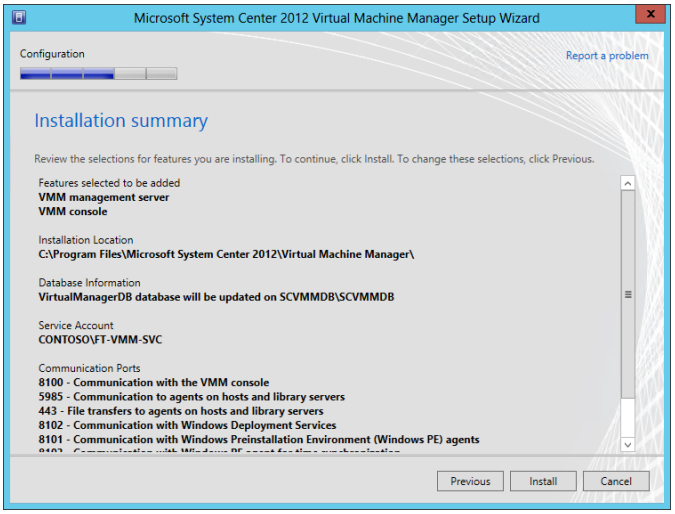
20. In the **Port configuration** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields are greyed out.
21. Click **Next** to continue.

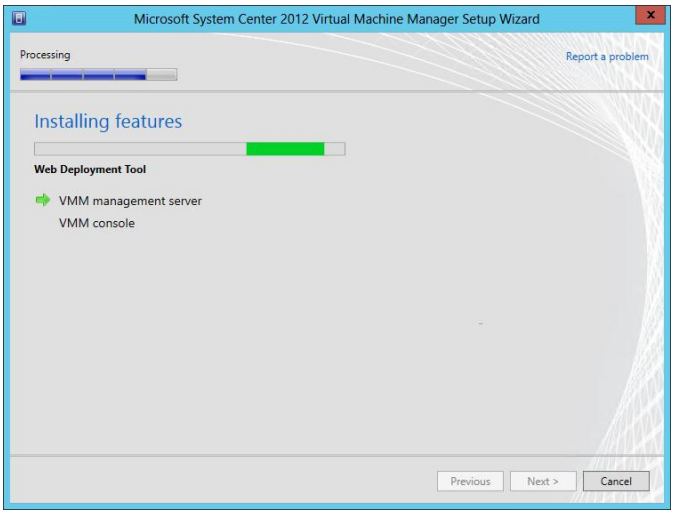
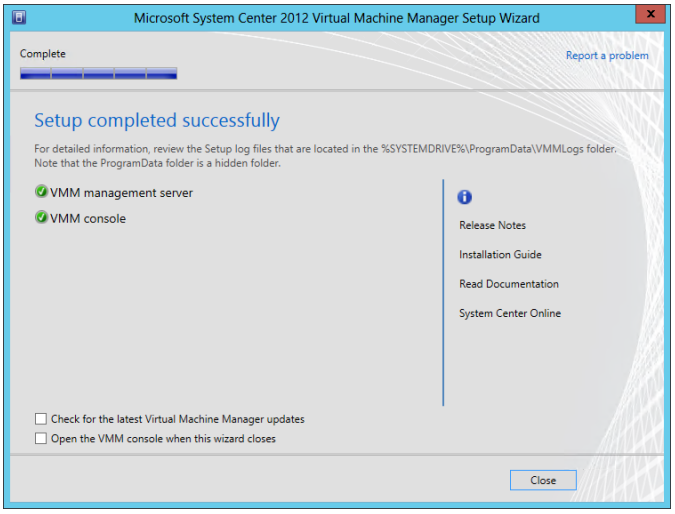


22. In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.

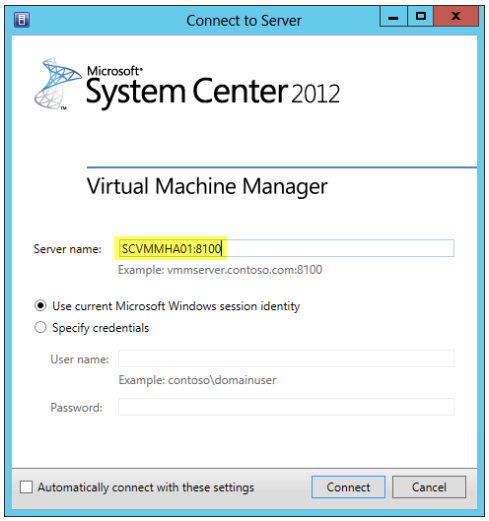


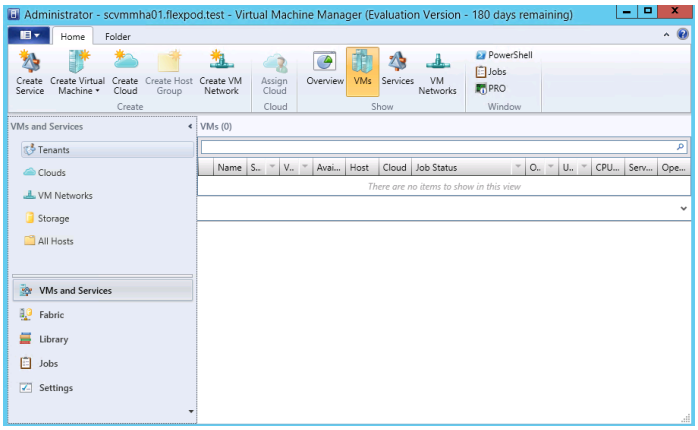
23. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



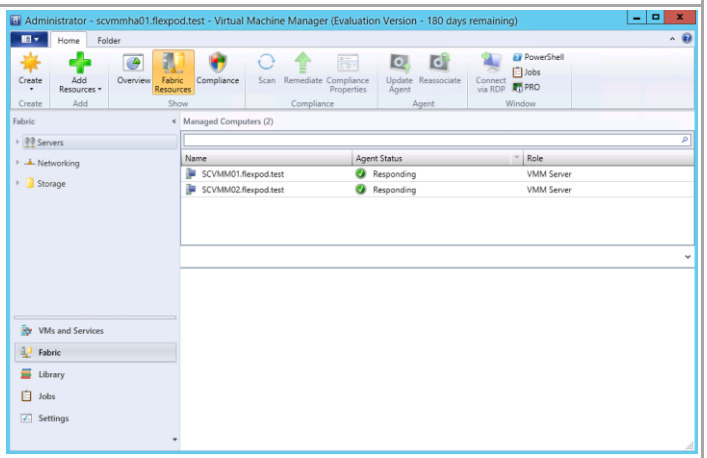
24. The wizard will display the progress while installing features.	
25. When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.	

26. 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.





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



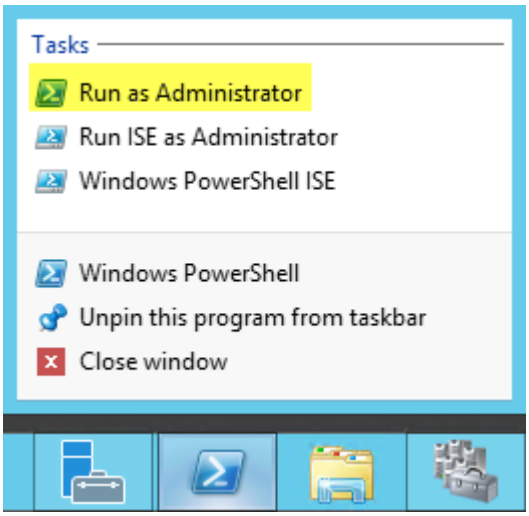
Creating Virtual Machine Manager Library Share on a Failover Cluster

In a highly available installation of Virtual Machine Manager, the Virtual Machine Manager Library must reside on a 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

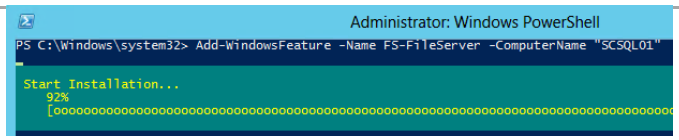
given that the Virtual Machine Manager servers themselves are highly available. While any file server cluster will suffice, this document will detail the steps required to host the Virtual Machine Manager Library upon the SQL Server Cluster created in earlier portions of this document.

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

1. Open a PowerShell session as an administrator.



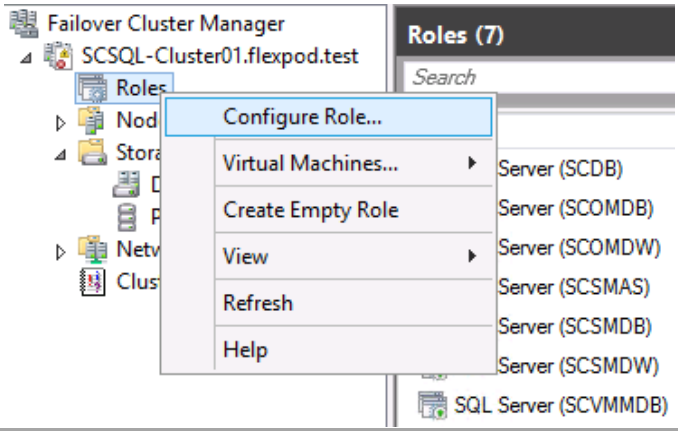
2. From the administrator PowerShell session run the following command once for each SQL cluster node changing the ComputerName value each time to that of a different SQL cluster node.
3. Add-WindowsFeature -Name FS-FileServer –ComputerName "SCSQL01"

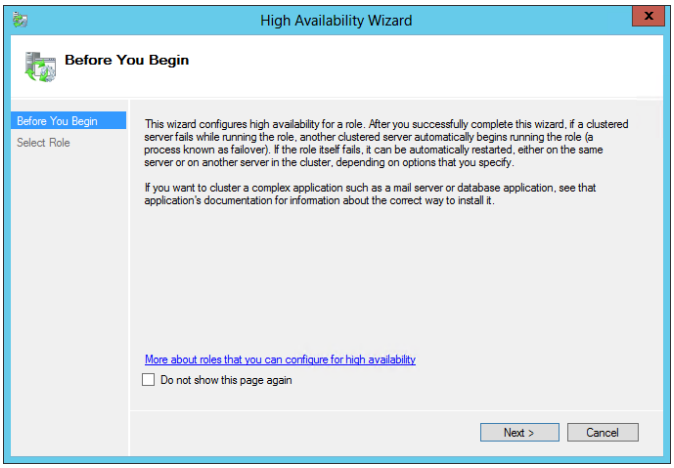
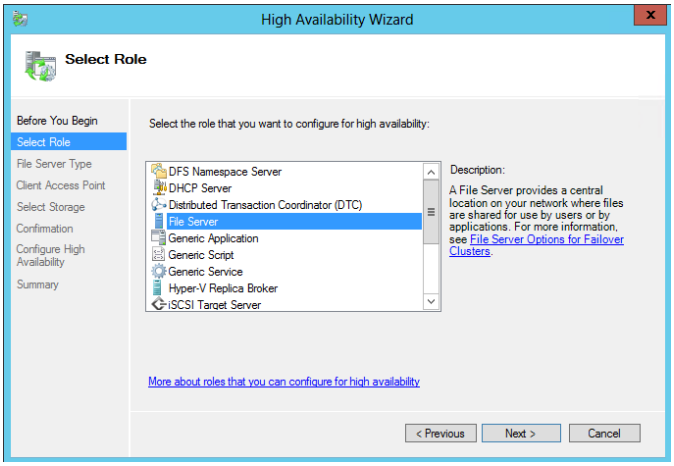
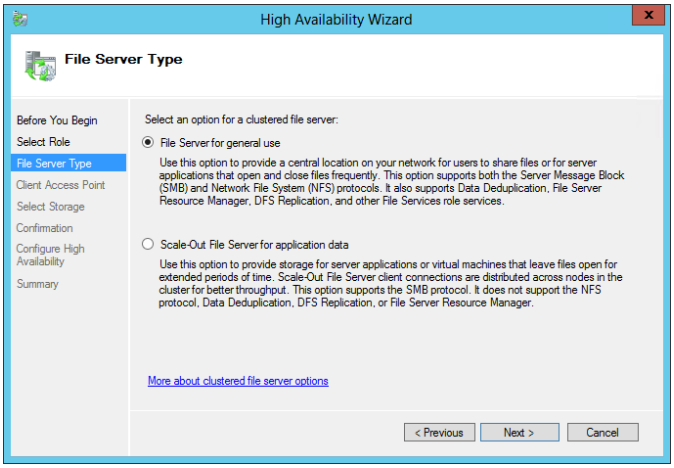


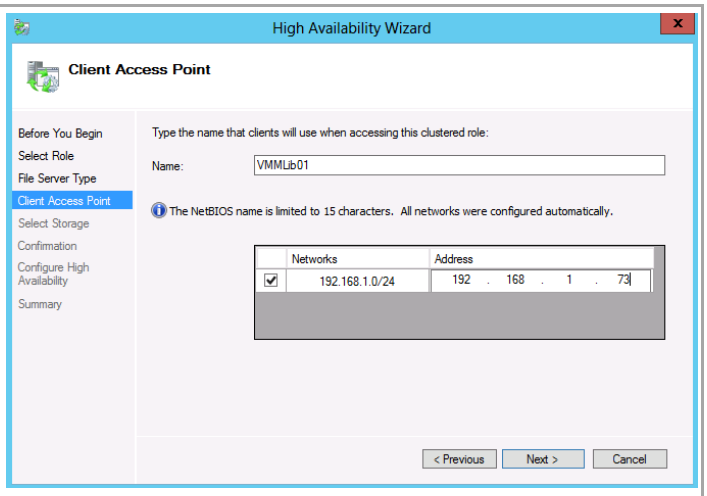
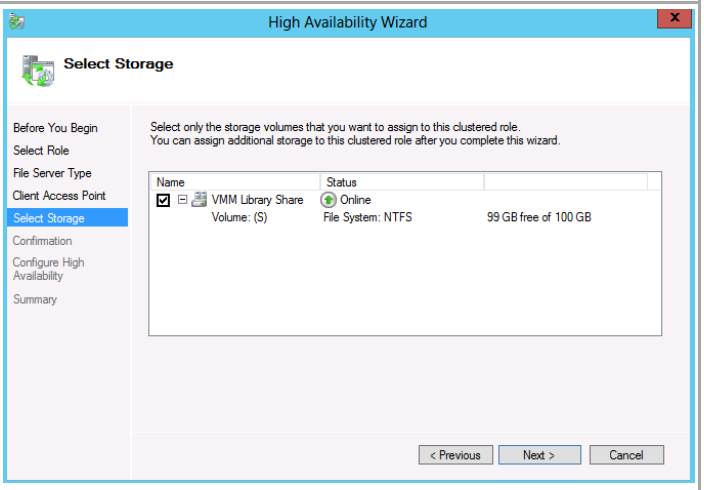
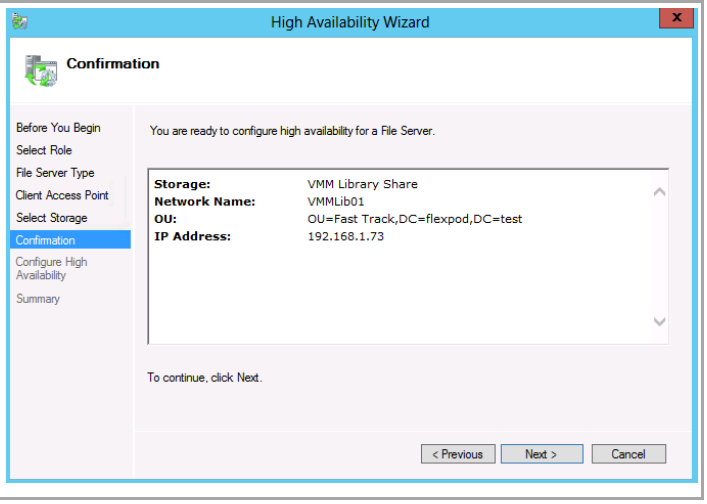
4. Add an additional iSCSI or Fibre Channel LUN and prepare it as described in previous steps. This should appear as available storage in the Failover Cluster Manager Storage node.

▶ Perform the following steps on the **first SQL Server** cluster node.

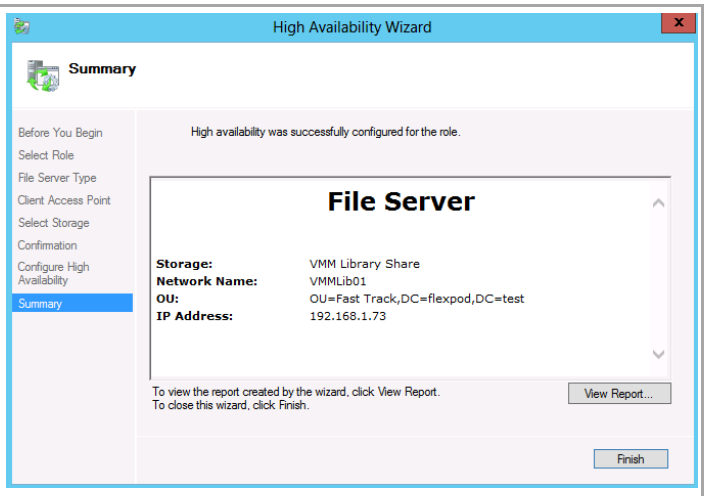
1. Within Failover Cluster Manager, right-click on Services and applications and select Configure Role… from the context menu.



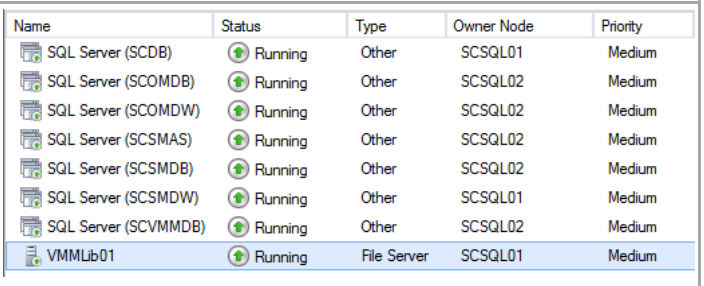
2. The High Availability Wizard will appear. In the Before You Begin dialog click Next to begin the wizard.	
3. In the Select Role dialog, from the available services and applications, select File Server and click Next to continue.	
4. In the File Server Type dialog, select the File Server for general use radio button and click Next to continue.	

5. 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.	
6. 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.	
7. In the Confirmation dialog, verify the options selected and click Next to continue.	

8. 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.

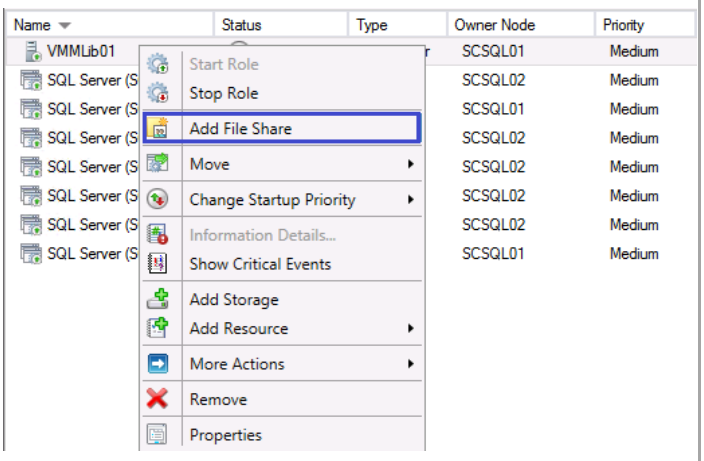


Note: The new highly available file server is available as a new service in Failover Cluster Manager.

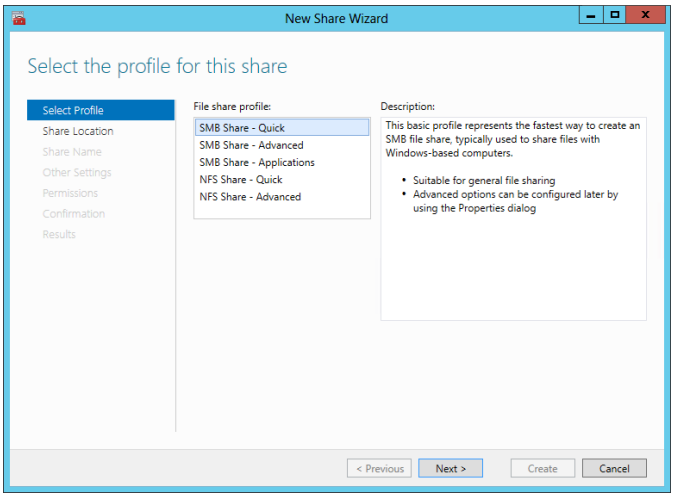


Name	Status	Type	Owner Node	Priority
SQL Server (SCDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDB)	Running	Other	SCSQL02	Medium
SQL Server (SCOMDW)	Running	Other	SCSQL02	Medium
SQL Server (SCSMAS)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDB)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCVMMDB)	Running	Other	SCSQL02	Medium
VMMLib01	Running	File Server	SCSQL01	Medium

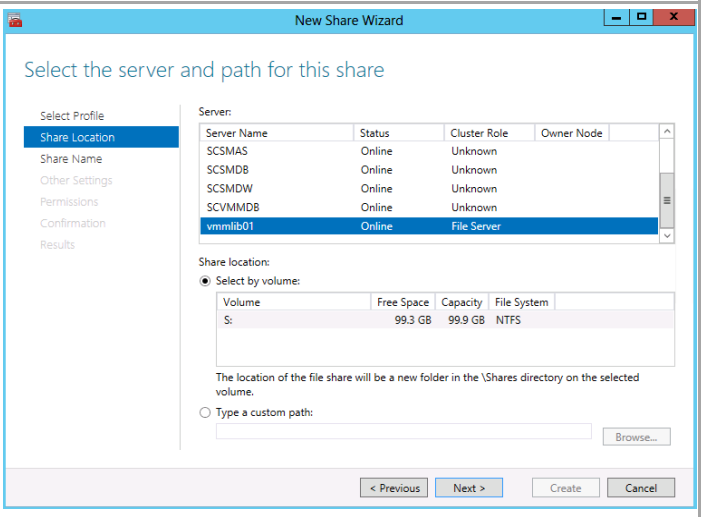
9. Within Failover Cluster Manager, right-click the newly created file server service and select Add File Share from the context menu.



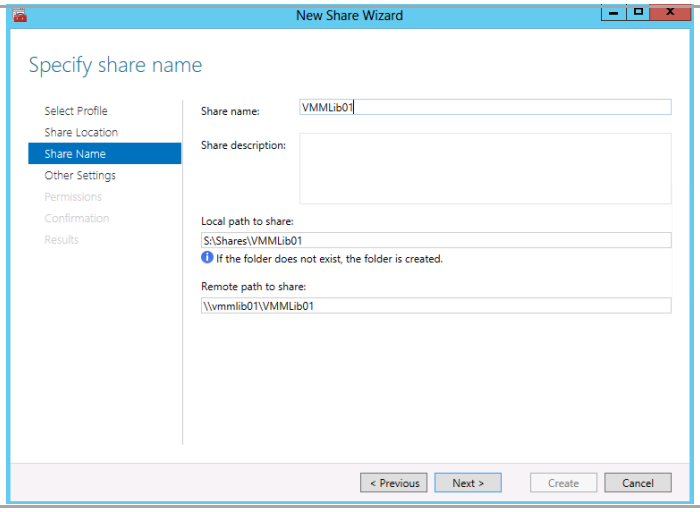
10. The New Share Wizard will appear. In the Select Profile dialog, select SMB Share – Quick and click Next to continue.



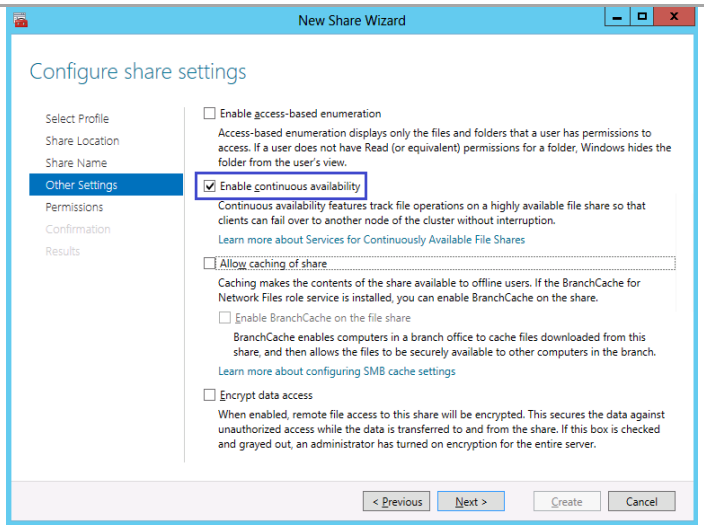
11. In the Shared Folder Location dialog, in the Server pane select the File Server cluster role object name created earlier. In the Share location pane, choose the Select by volume radio button option and click Next to continue.



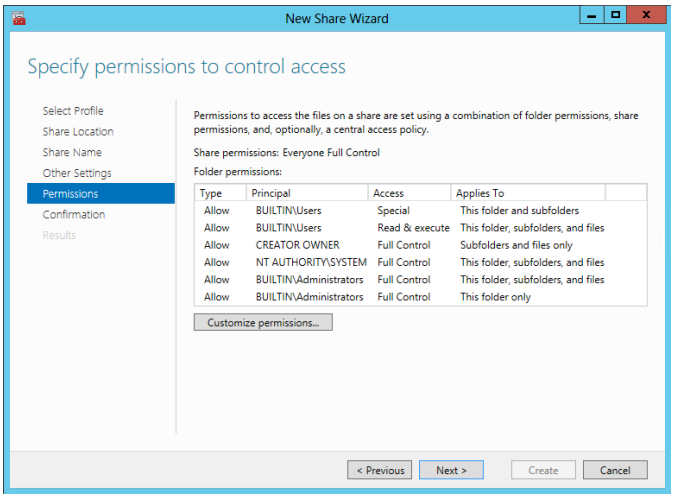
12. In the Share Name dialog, type the value of "VMMLibrary" in the Share name field and then click Next to continue.



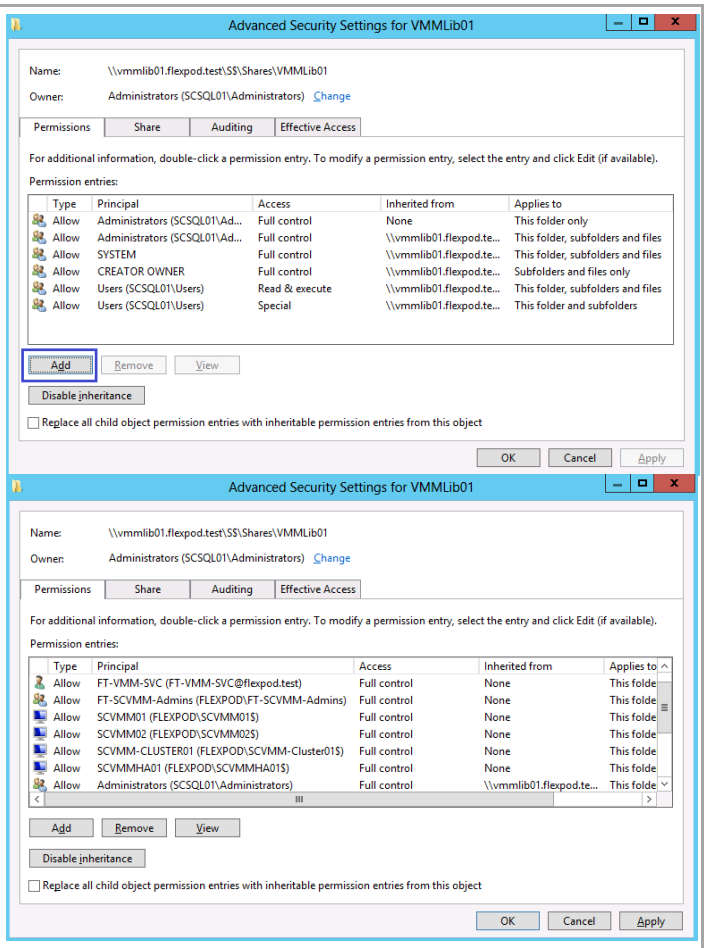
13. On the Other Settings page, select only the Enable continuous availability option and then click Next.



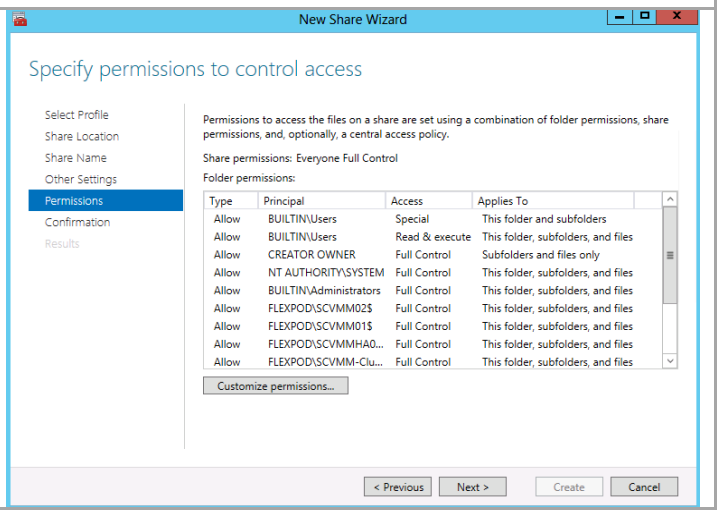
14. In the Permissions dialog, click the Customize Permissions... button.



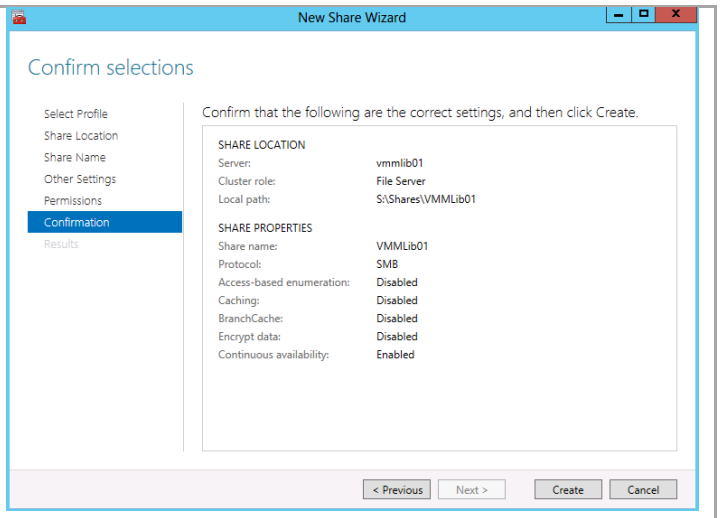
15. In the Permissions for VMMLibrary dialog, add the following accounts with NTFS Full Control permissions over the folder:
    a. The VMM service account.
    b. The VMM Admins group.
    c. Both VMM computer accounts.
    d. The VMM CNO computer account.
    e. The VMM VCO computer account.
16. Click OK to save the changes.



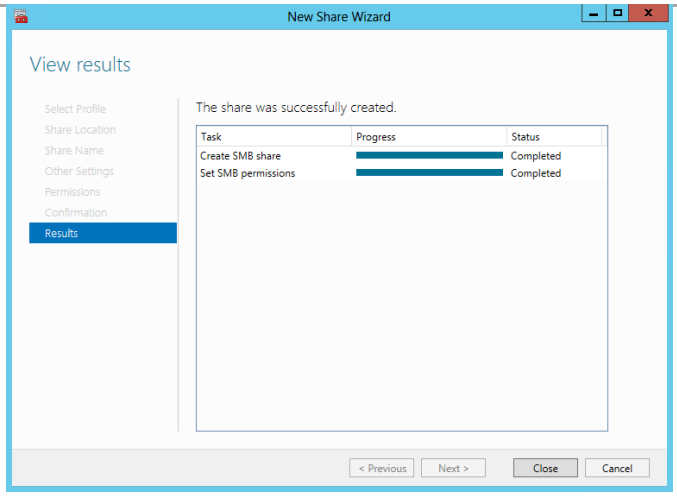
17. Click Next to continue in the wizard.



18. Review the settings on the Confirmation dialog and click Create.

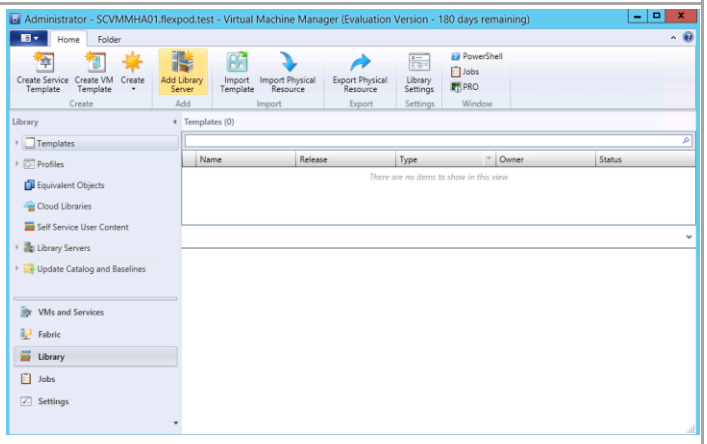


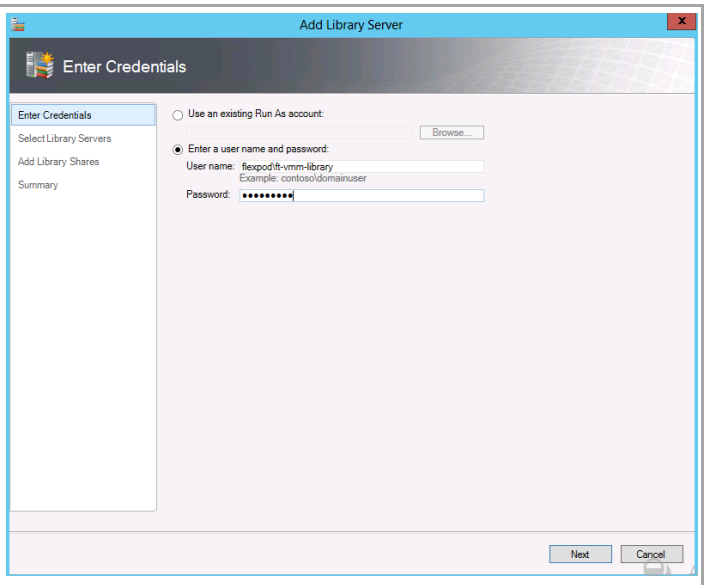
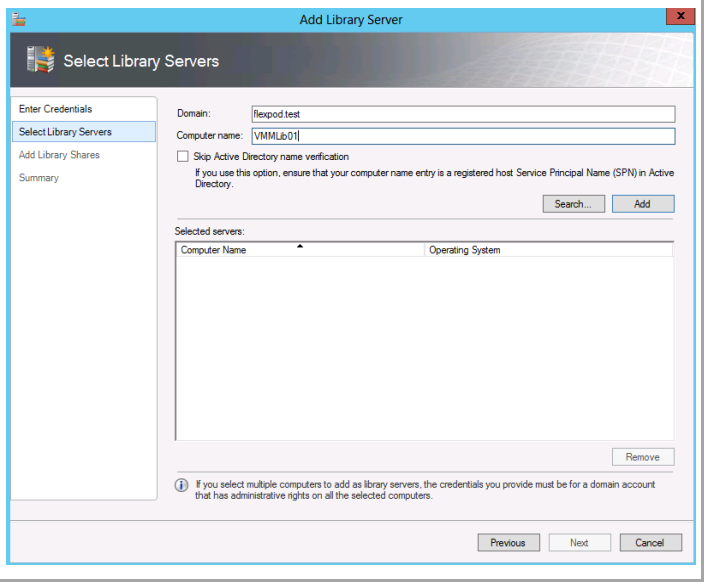
19. In the Results dialog, verify that the shared folder was provisioned properly and click Close.

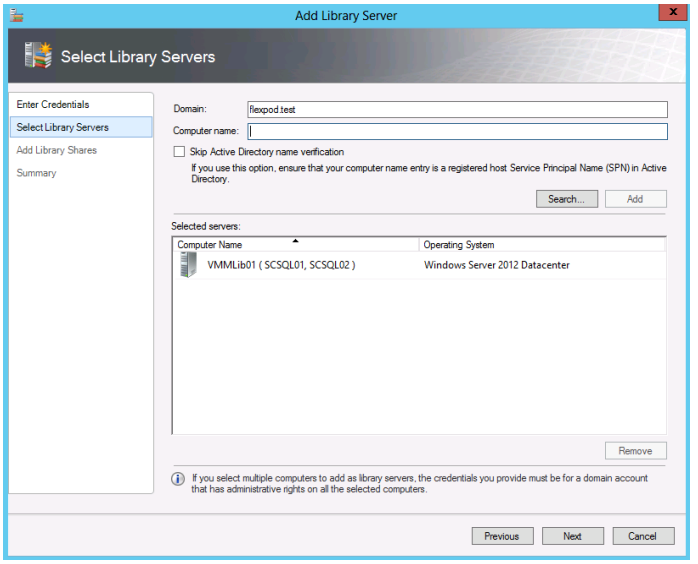
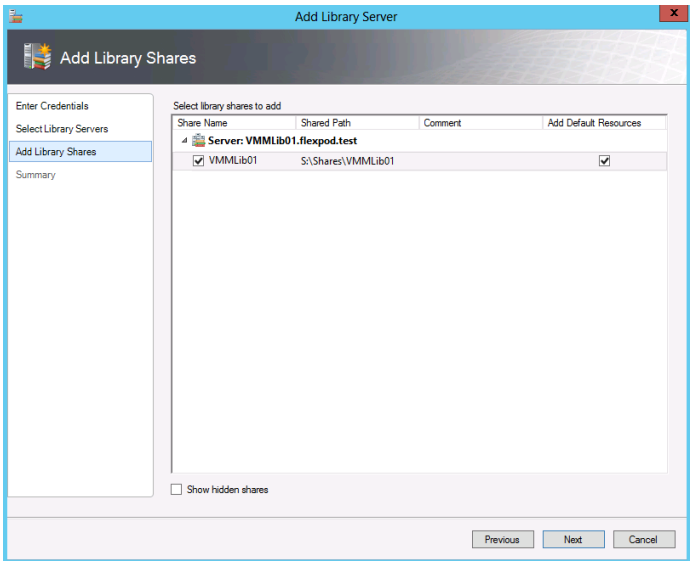


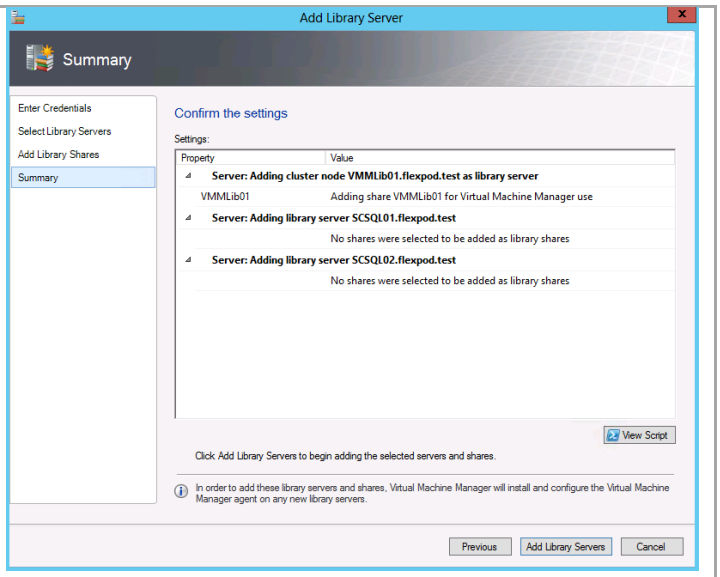
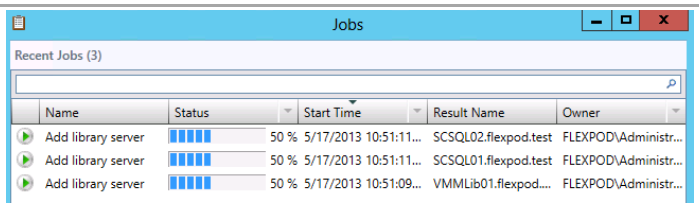
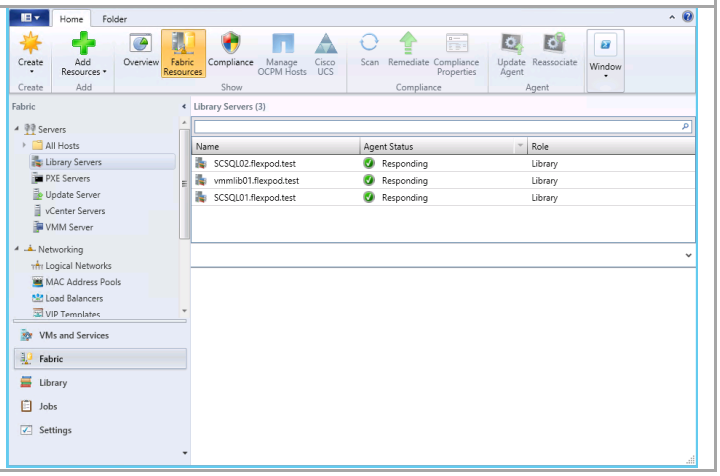
▶ Perform the following steps on the **Virtual Machine Manager** virtual machine.

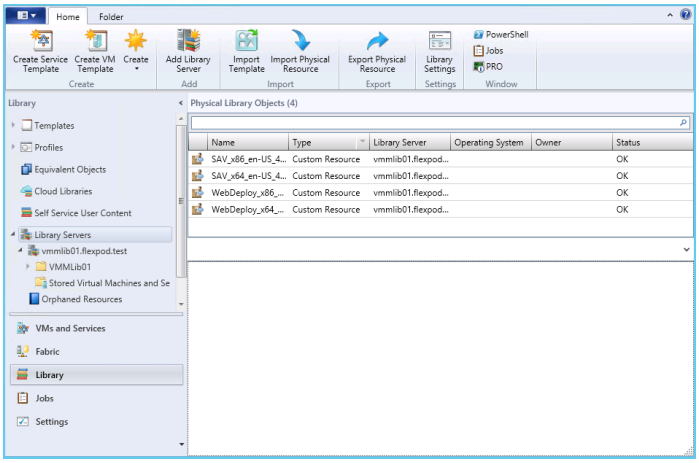
1. In the **Virtual Machine Manager** console, select the **Library** node. In the **Home** tab, click the **Add Library Server** button from the ribbon.



2. 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.	
3. 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**.	

4. In the **Specified Servers** pane, the cluster object will appear in the dialog. Click **Next** to continue.	
5. 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.	

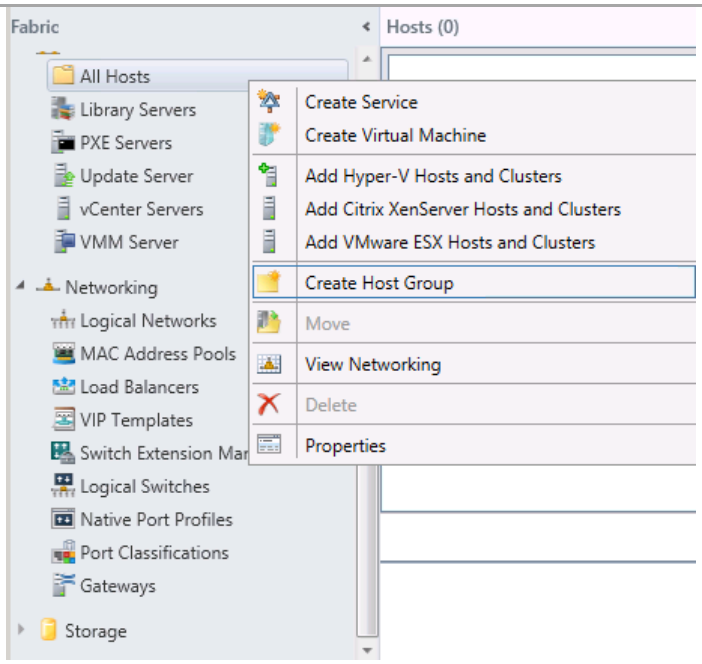
6. Review the **Summary** dialog and click **Add Library Servers** to continue.	
7. The **Jobs** dialog will appear showing the progress of the Add Library Server action. In the **Jobs** dialog, verify that all steps have completed.	
8. In the **Virtual Machine Manager** console, expand, select Fabric, 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**.	

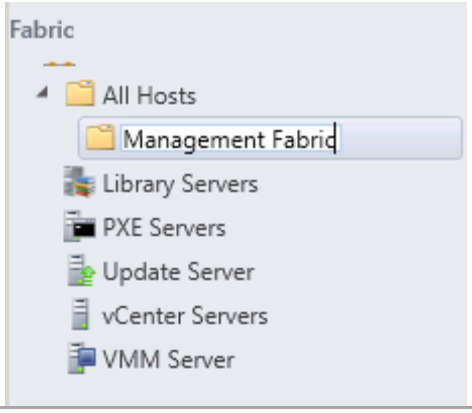
9. In the **Virtual Machine Manager** console, navigate to the **Library Servers** node and verify that all of the correct objects are created. When verified, exit the console.	

15.5 Add Fabric Management Resources Virtual Machine Manager

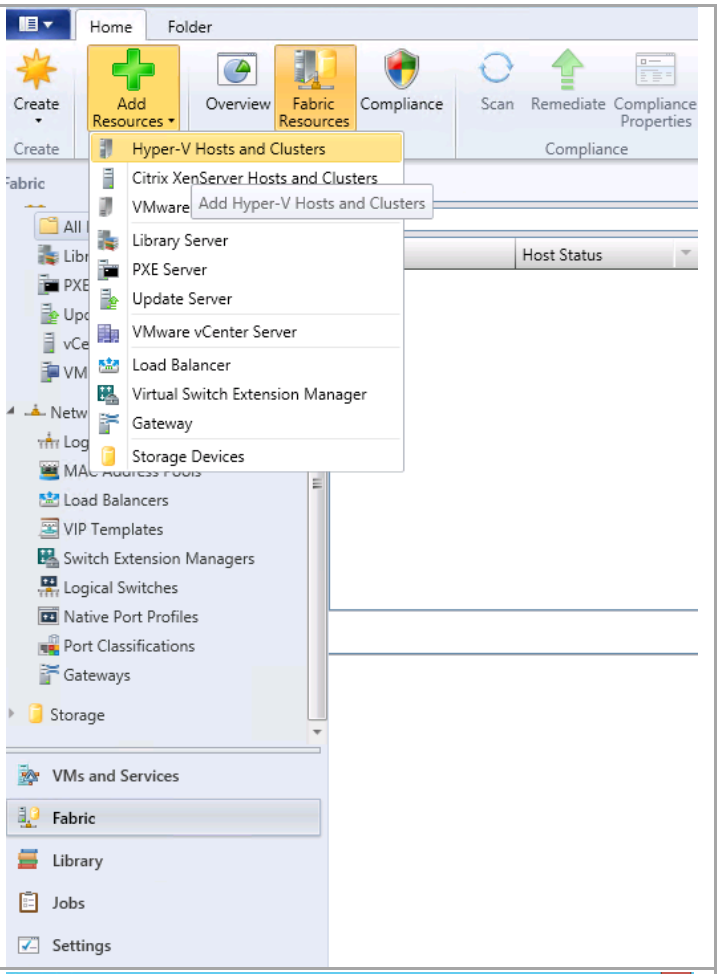
Complete the following steps to add the Fabric Management Hyper-V hosts to VMM.

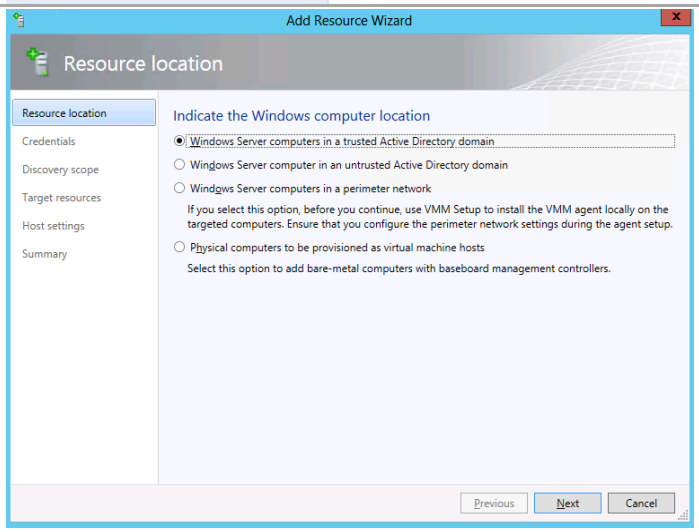
▶ Perform the following steps on the **Virtual Machine Manager** virtual machine.

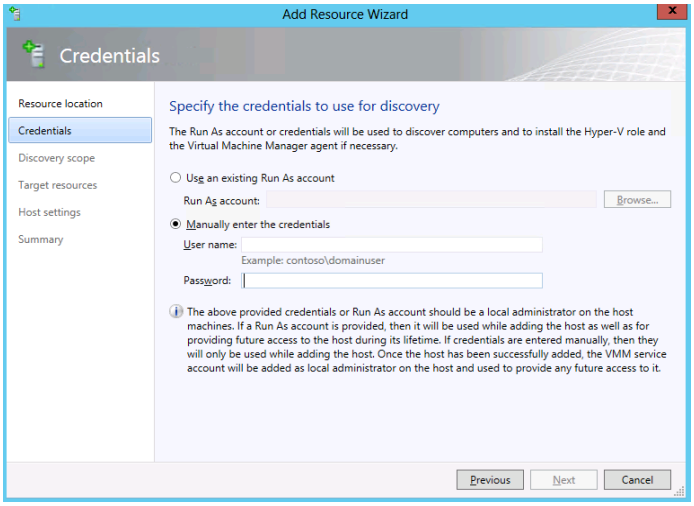


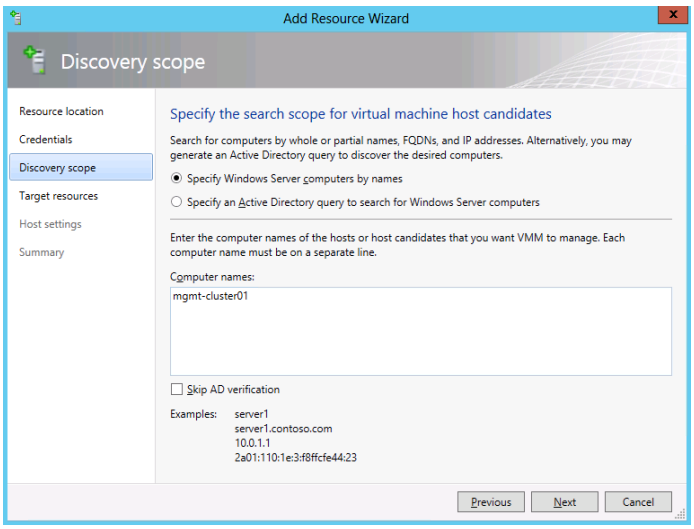


1. Select Fabric and All Hosts. Click Add Resources.

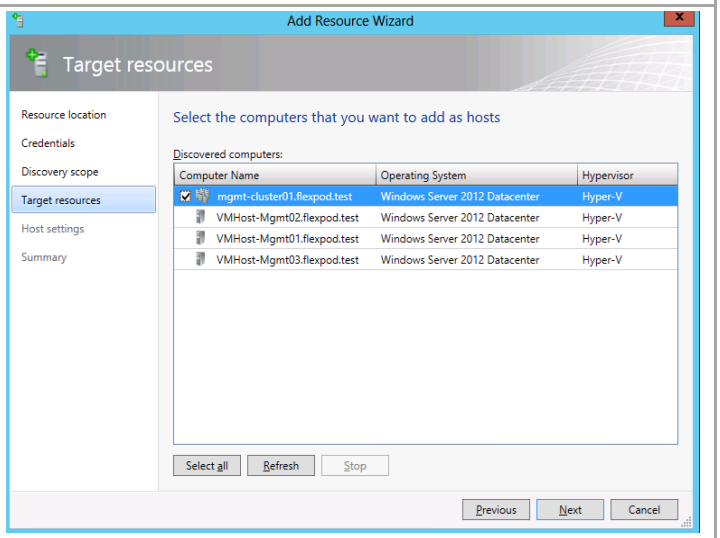


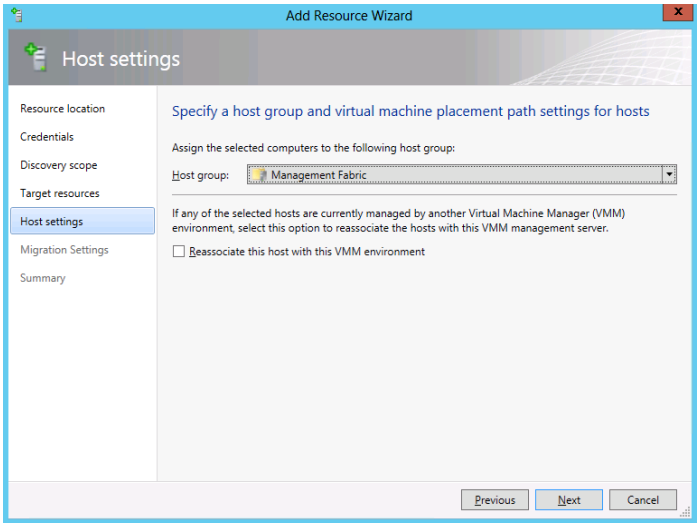




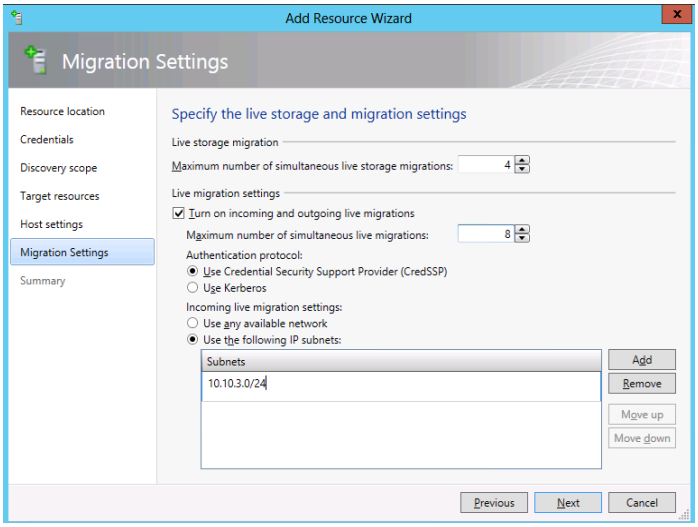


2. Click Select All and click Next.

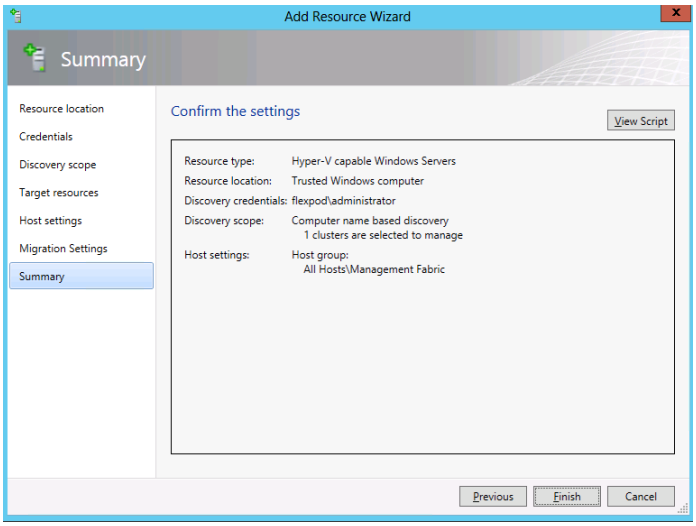


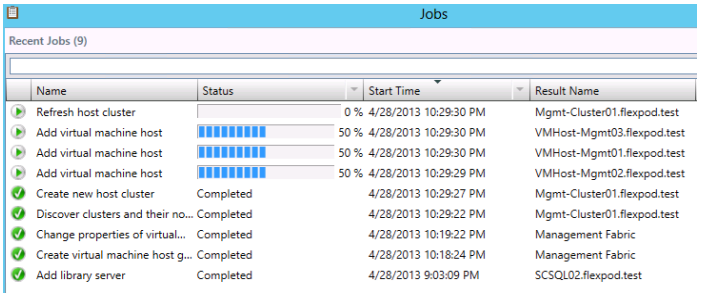
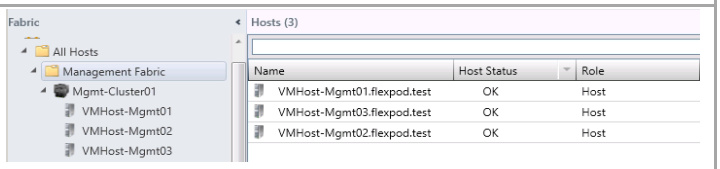


3. Set live migration settings. Default is 2 for each. Set the IP subnet for live migration network.

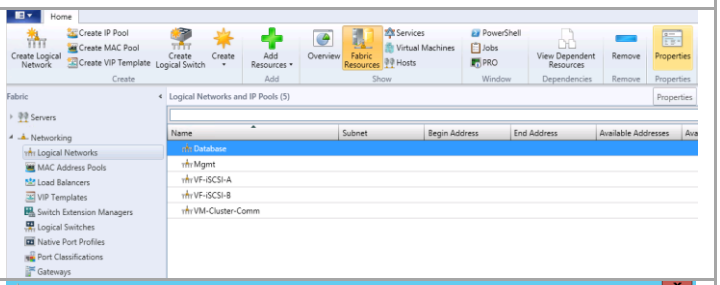
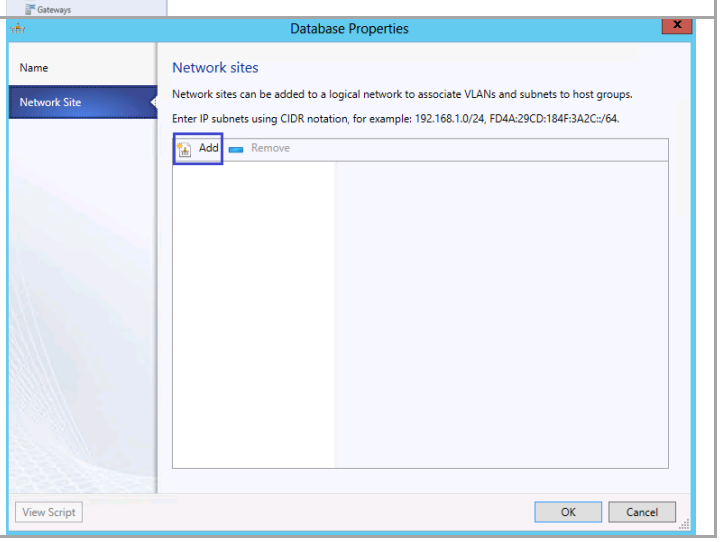


4. Click Finish.

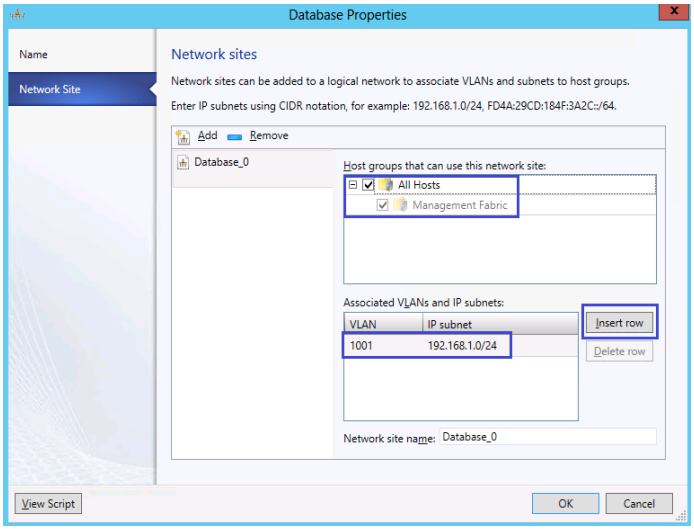


5. Verify job completion.	
6. Hosts are added.	

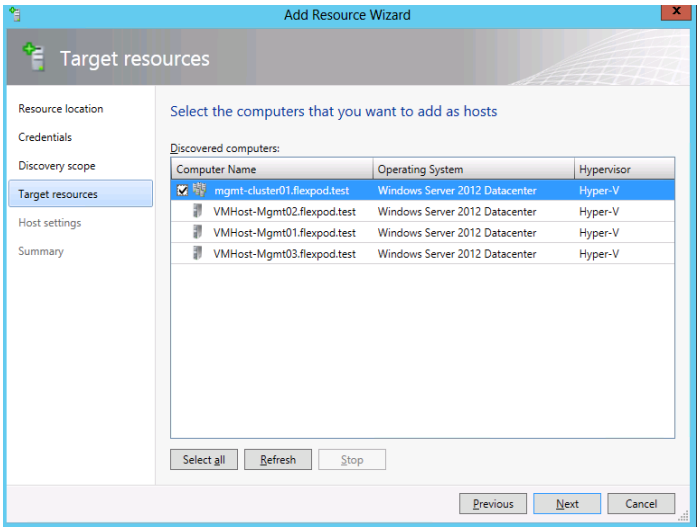
15.6 Configure Logical Networks

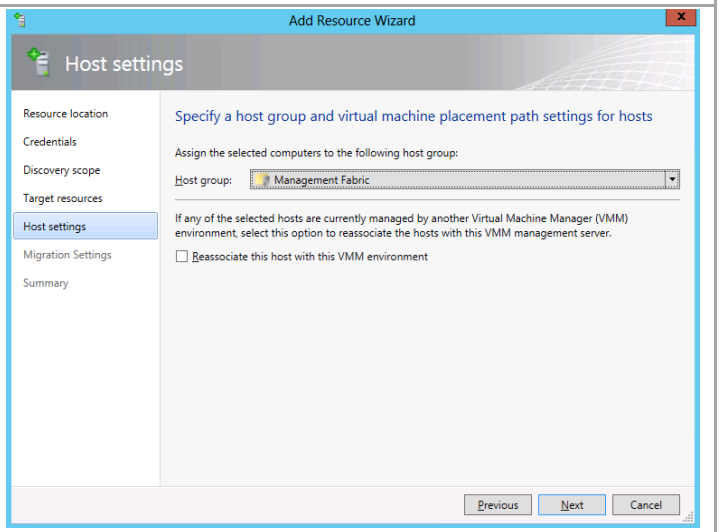
▶ Perform the following steps on the **Virtual Machine Manager** virtual machine.	
1. Select Fabric and Networking. Select Logical Networks and click Properties.	
2. Select Network Site and click Add.	

3. Check All Hosts. Click Insert row. Enter the VLAN ID and IP subnet the network site. Click OK.
4. Repeat this procedure for each Logical Network.
5. Enter 0 for the VLAN ID for the native VLAN.



6. Click Select All and click Next.





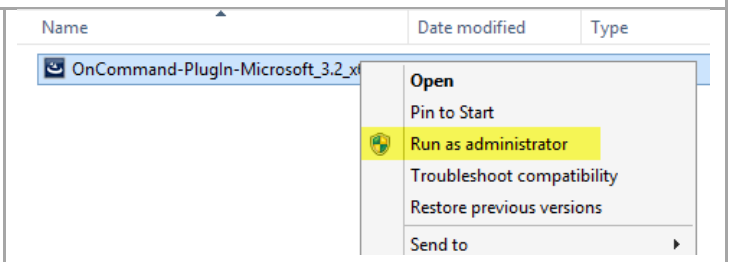
15.7 Install the NetApp SCVMM GUI Extension

This section describes the steps that must be completed to install and configure the NetApp OnCommand SCOM Management Pack.

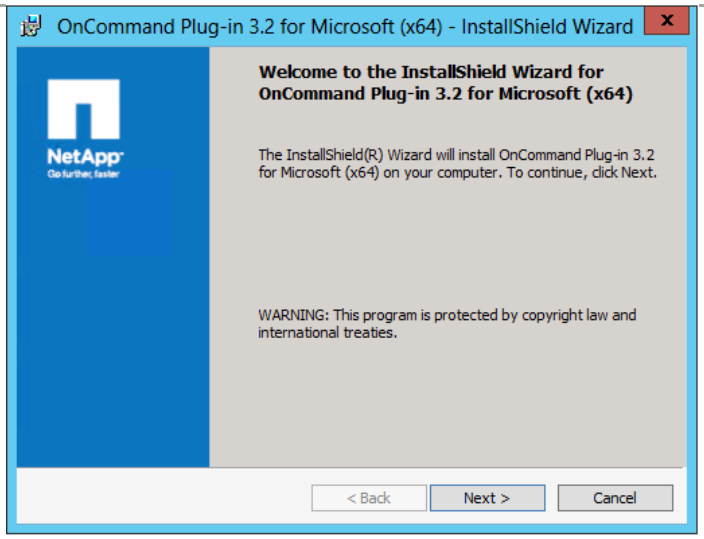
Install the NetApp OnCommand Plug-In GUI Extension

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

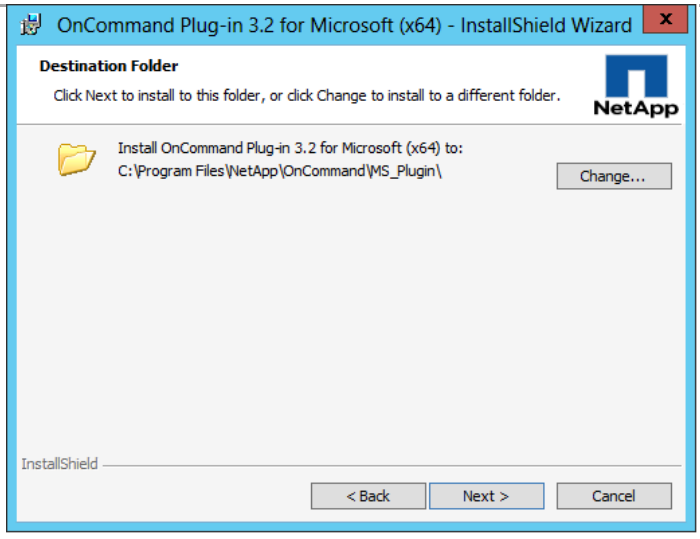
1. Log in to the SCO management server, right-click the OCPM 3.2 installation package, and select Run as Administrator to start the OCPM installation wizard.



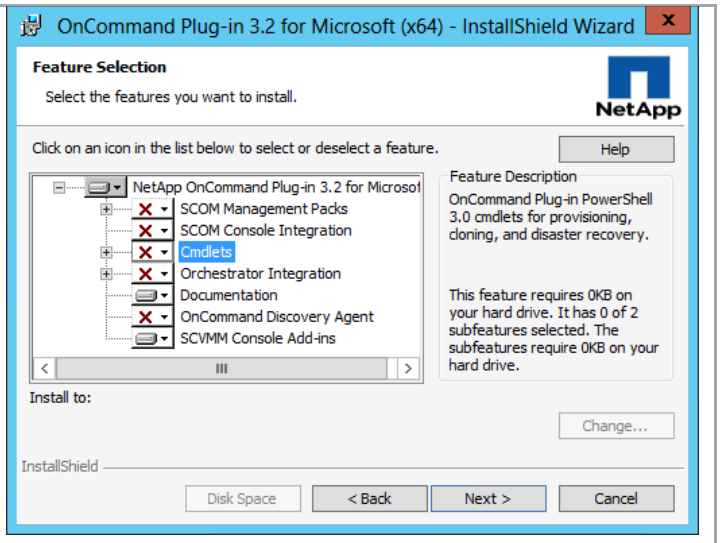
2. In the Welcome screen, click Next.



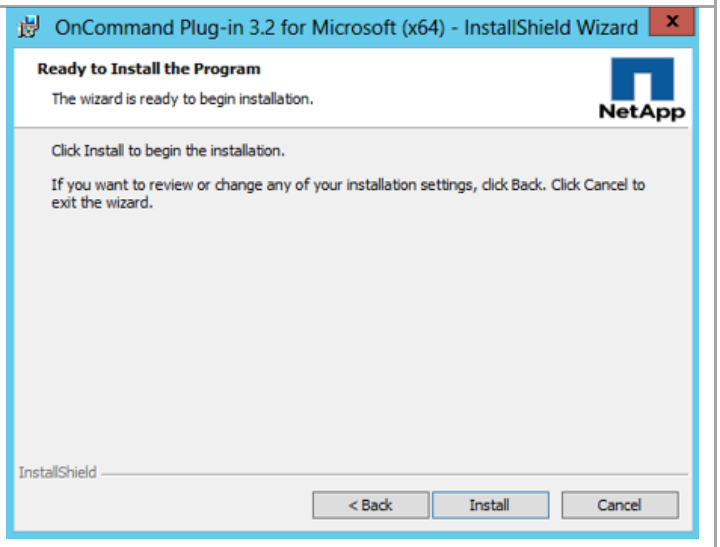
3. In the Destination Folder screen, click Next to keep the default installation folder.



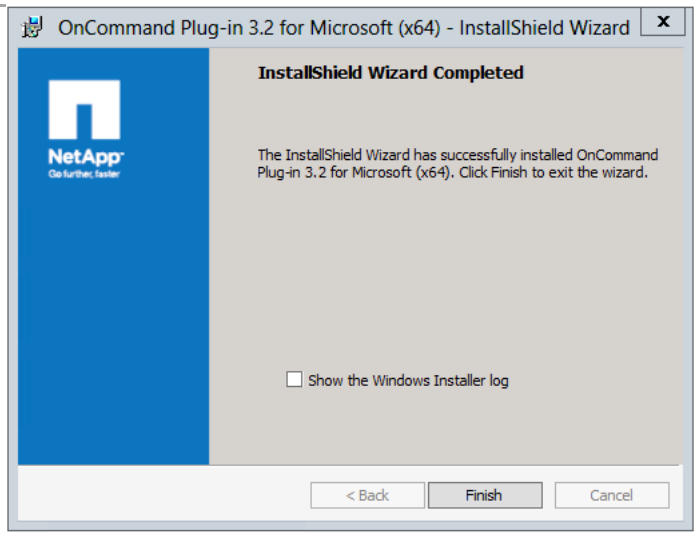
4. In the Feature Selection screen, select the following features and click Next:
    a. Documentation
    b. SCVMM Console Add-ins



5. Click Install to continue the installation.



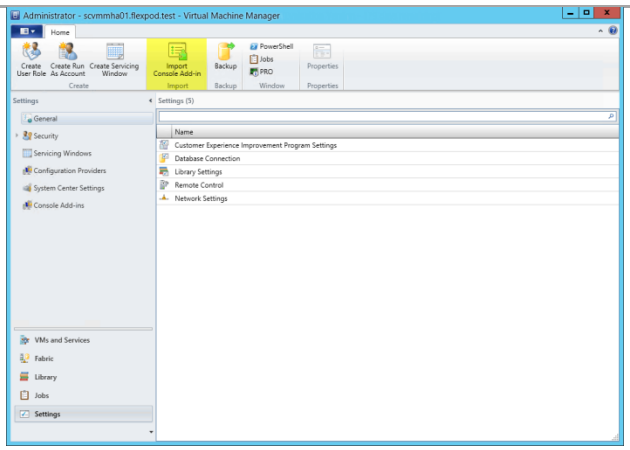
6. In the InstallShield Wizard Completed screen, click Finish to complete the installation.
7. It may be necessary to reboot the server to completely register the Management Pack and its associated tasks.



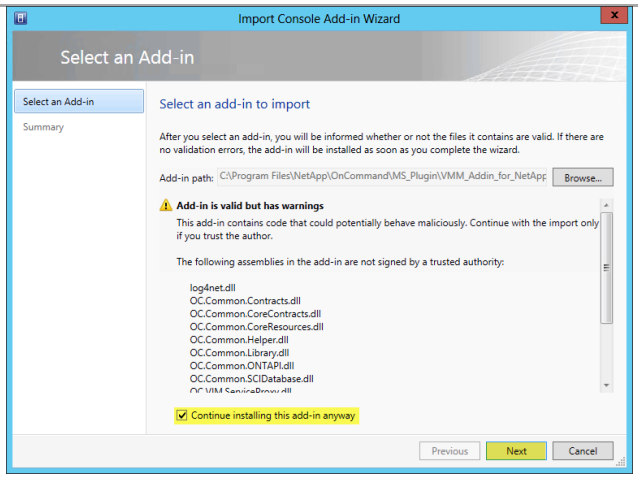
Register the NetApp OnCommand Plug-In GUI Extension

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

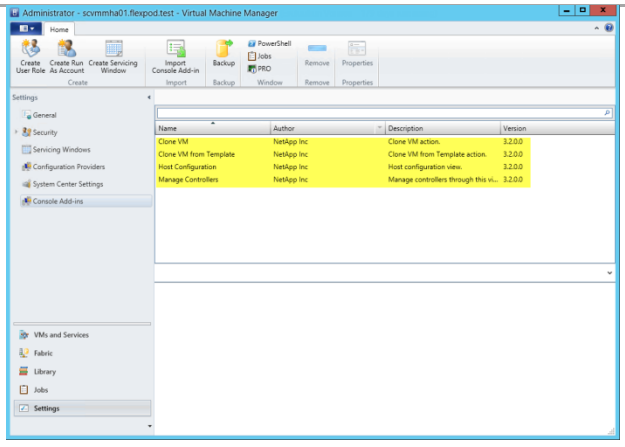
1. In the Virtual Machine Manager console, navigate to the Settings pane and select Import Console Add-in.



2. In the Import Console Add-in Wizard, click the Browse button next to Add-in Path.
3. Browse to the OCPM install path: %ProgramFiles%\NetApp\OnCommand\MS_Plugin
4. Select CloneVM_3.2.zip and click Open.
5. Select the "Continue installing this add-in anyway" checkbox and click Next.
6. Click Finish,
7. Repeat for the following add-ins:
    a. Clone VM from Template
    b. Host Configuration
    c. Manage Controllers



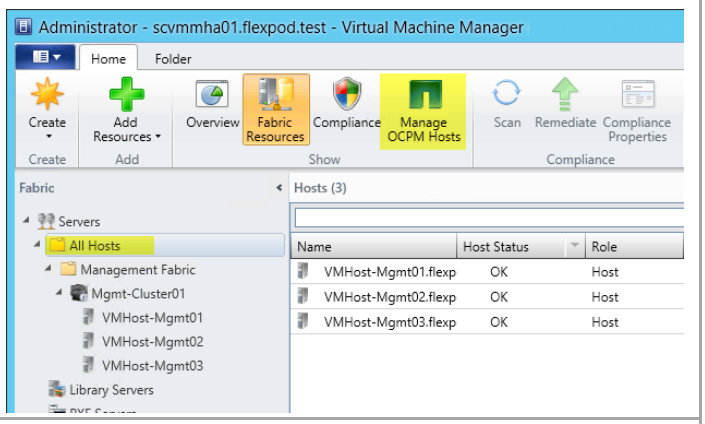
8. In the Virtual Machine Manager console, select Console Add-ins and verify that the add-ins are listed.



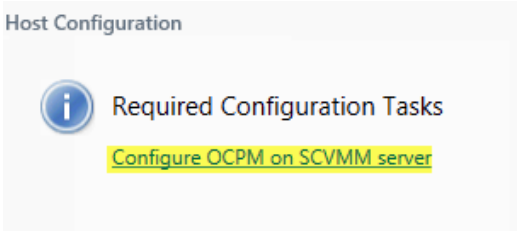
Configure NetApp OnCommand Plug-In SCVMM GUI Extension

▶ Perform the following steps on the **Operations Manager** virtual machine.

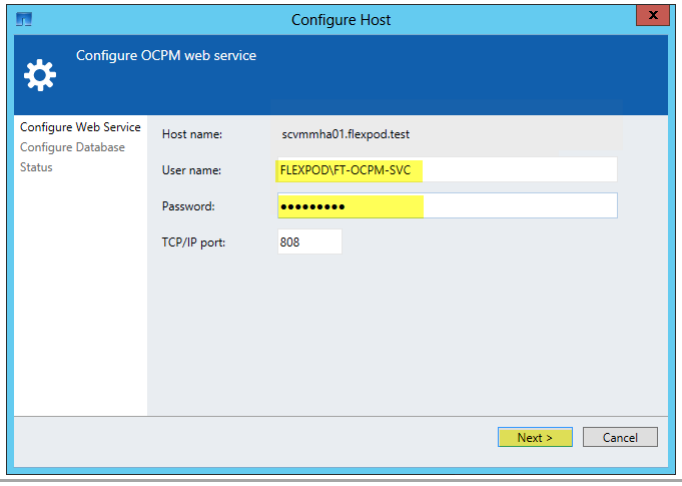
1. In the Virtual Machine Manager console, navigate to the Fabric pane, expand the Servers node, and select All Hosts.
2. In the ribbon, click Manage OCPM Hosts.



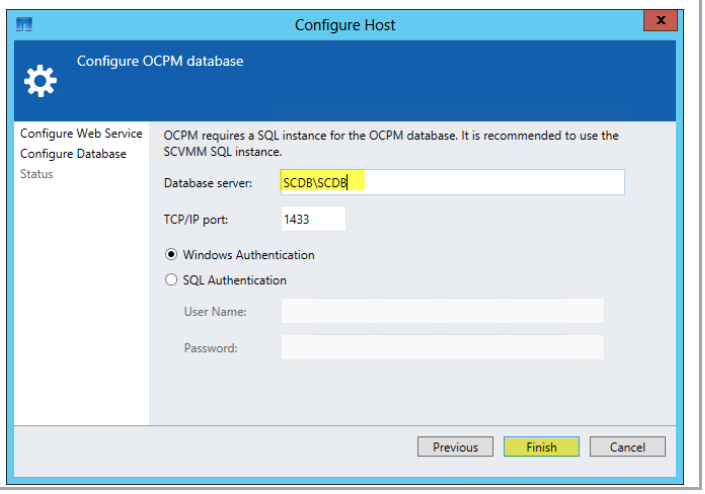
3. Click the Configure OCPM on SCVMM Server link.



4. In the Configure Host screen, enter the OCPM SVC account name and password, then click Next.



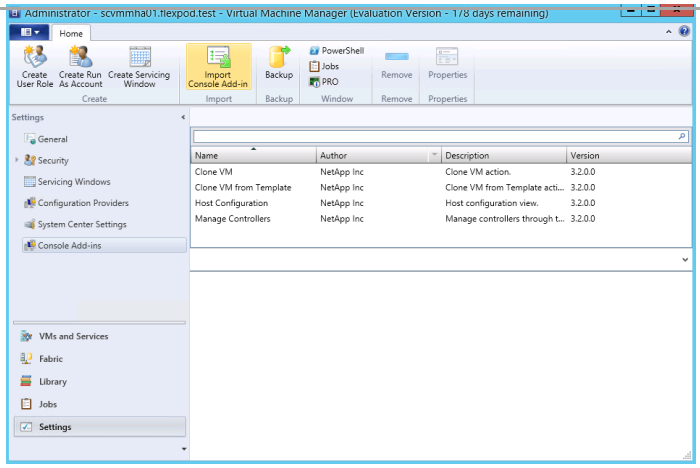
5. Enter the database server path and click Finish.
6. When the configuration wizard has finished, click Close.



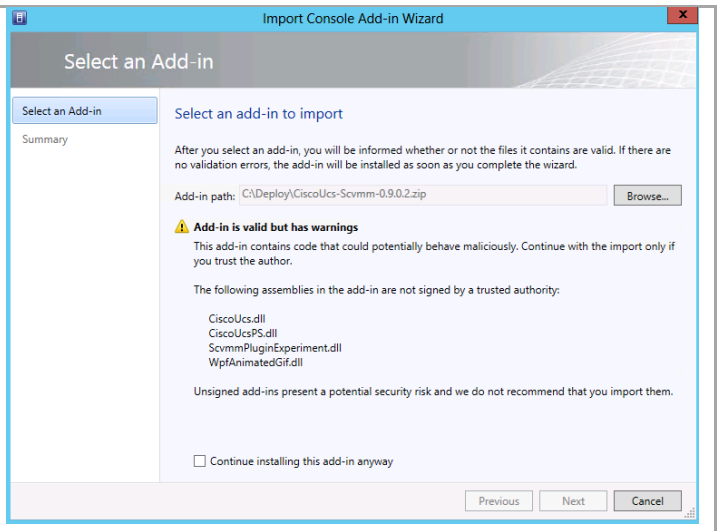
15.8 Install Cisco UCS User Interface Extensions for Virtual Machine Manager

▶ Perform the following steps on both **Virtual Machine Manger** virtual machine.

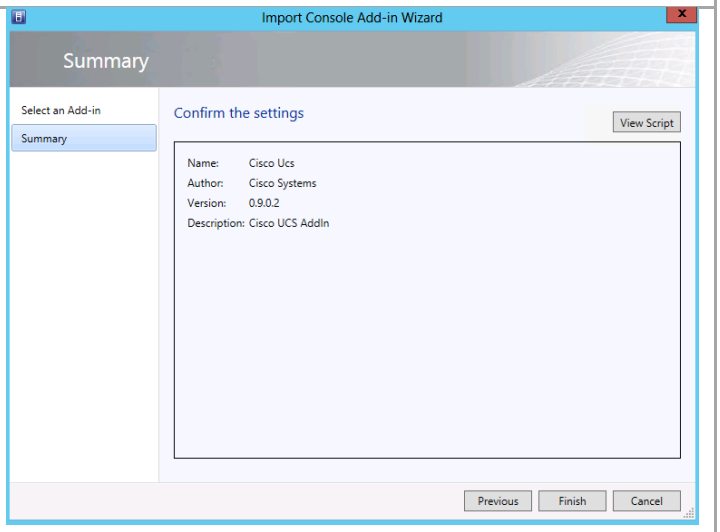
1. In the **Virtual Machine Manger** console, navigate to the **Settings** pane and select the **Import Console Add-in**.

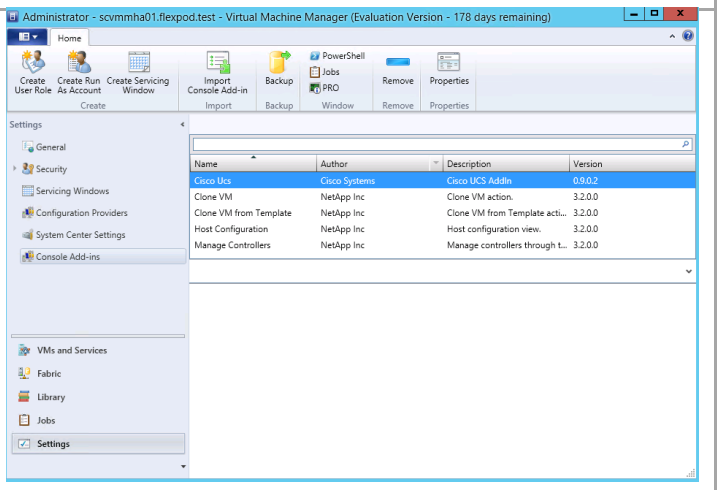


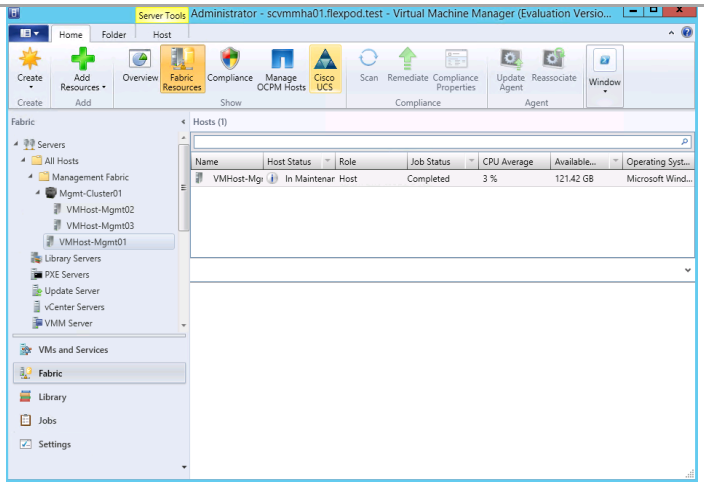
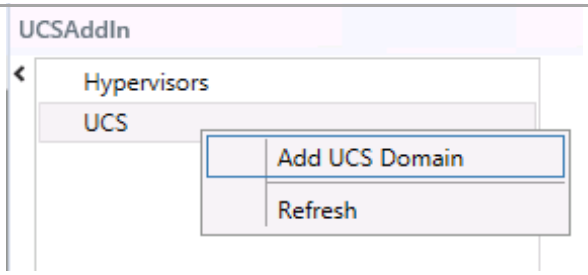
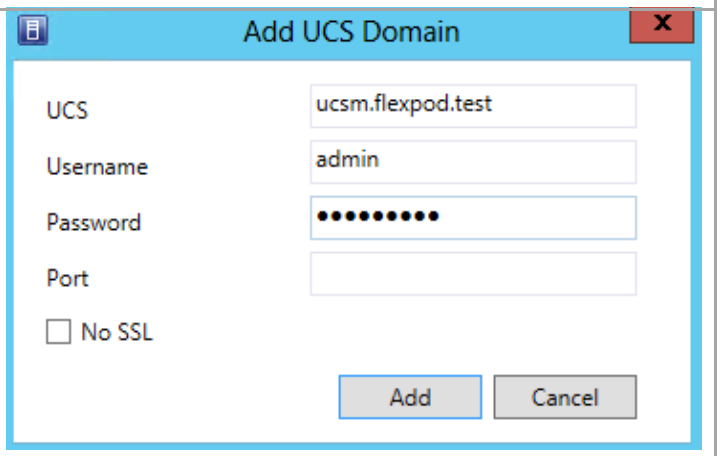
2. On the Import Console Add-in Wizard, click **Browse** on the Add-in Path. Select the **Cisco UCS UI Extensions for Virutal Machine Manager** package and click **Open**.
3. Click **Next** to continue.

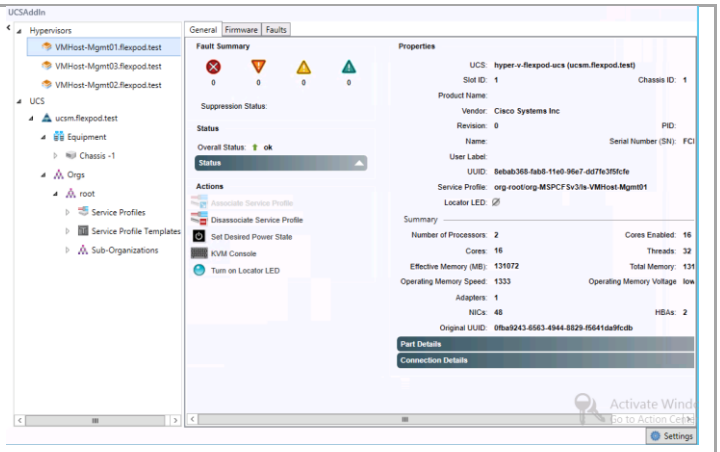


4. Review the summary information and click **Finish**.





5. Select **Fabric** in the left pane and click the **Cisco UCS** icon.	
6. Right-click **UCS** and select **Add UCS Domain**.	
7. Enter the Cisco UCS Manager host name, admin account, and password. Click Add.	

8. The Cisco UCS Manager objects are displayed in the review view pane.	

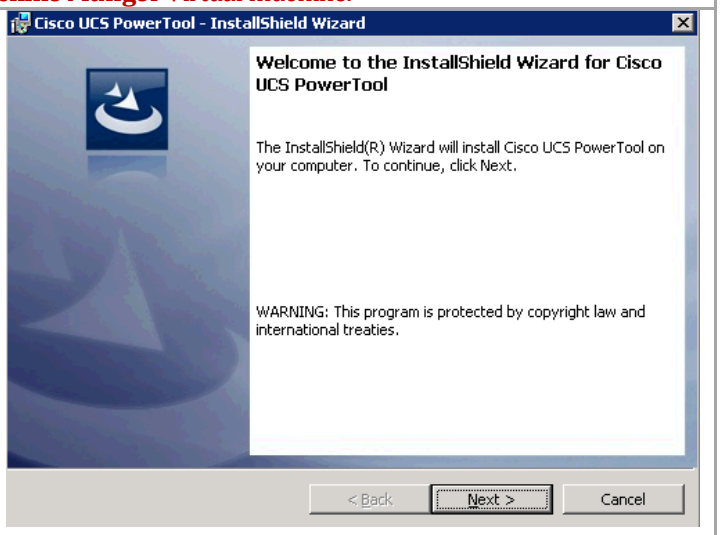
15.9 Install Cisco UCS PowerTool

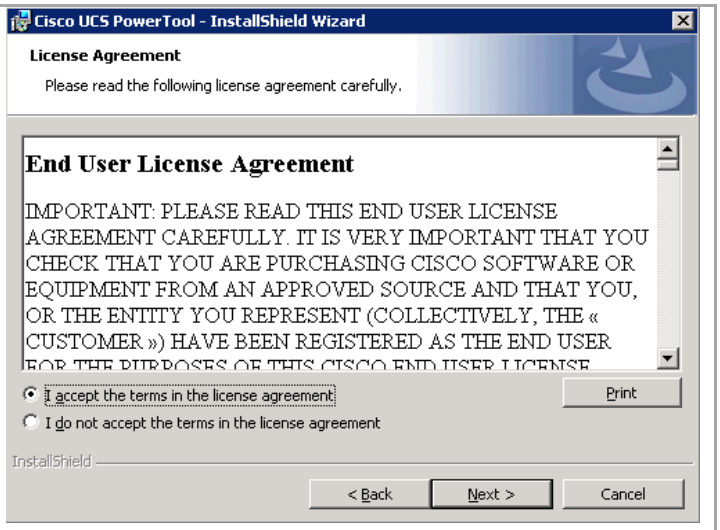
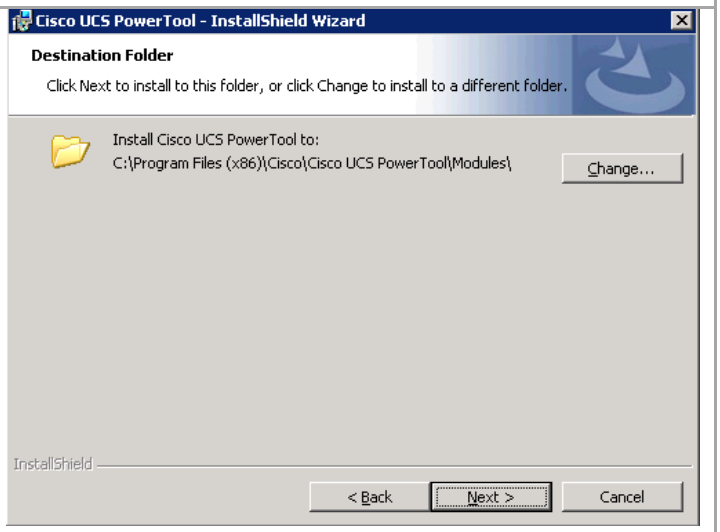
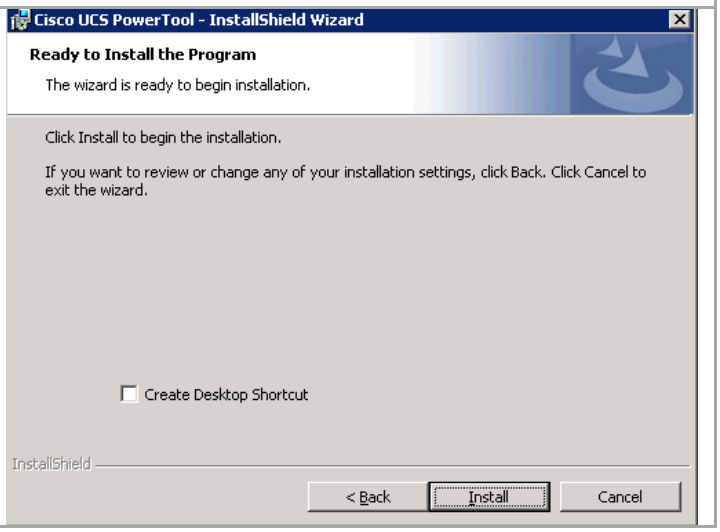
The Cisco UCS PowerTool should be installed on the FlexPod Management server.

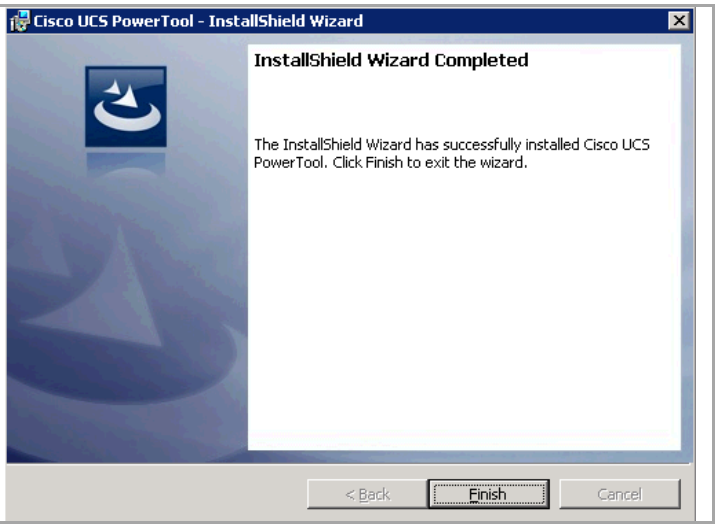
Download the Cisco UCS PowerTool version 0.9.9.0 or newer from the Cisco Developer Network. It can be found in the Microsoft Management section - http://developer.cisco.com/web/unifiedcomputing/microsoft.

Extract the zip file and execute the extracted exe file.

▶ Perform the following steps on both **Virtual Machine Manger** virtual machine.

1. Launch the Cisco UCS PowerTool Installer. The **Setup Wizard** screen appears.	

2. **Read and accept** the end user license agreement. Click **Next** to continue.	
3. Select the **Destination Folder** and click **Next** to continue.	
4. Cisco UCS PowerTool is ready to install. Click **Next** to complete the installation.	

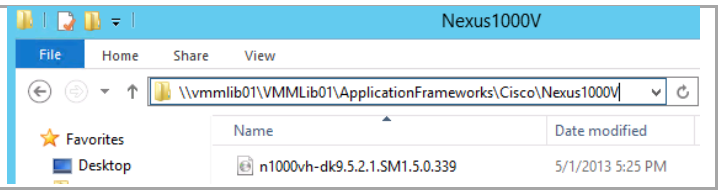
5. After the installation completes successfully click **Finish** to close the installation wizard.	

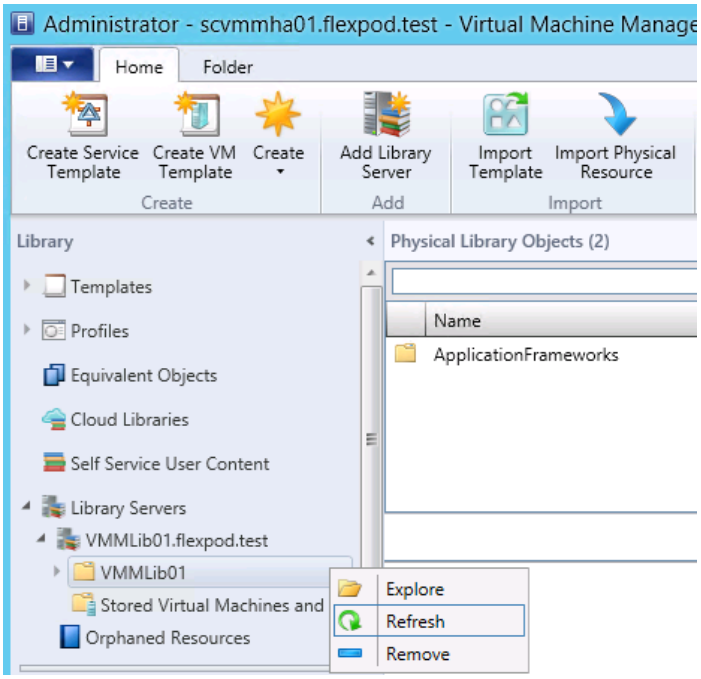
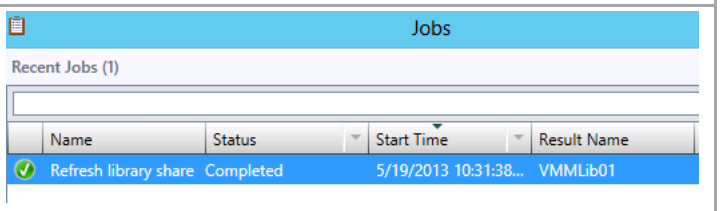
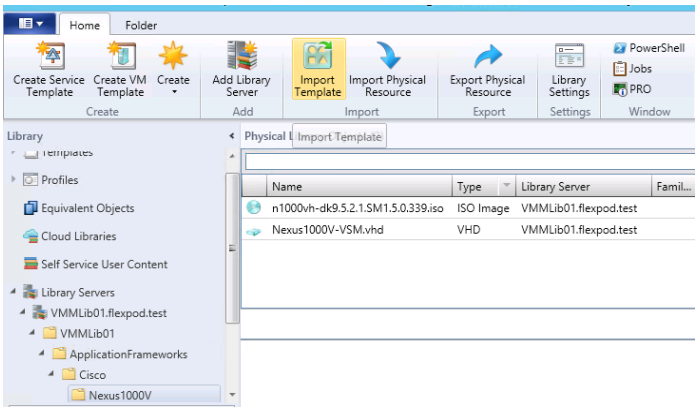
16 Install and Configure Nexus 1000V for Hyper-V

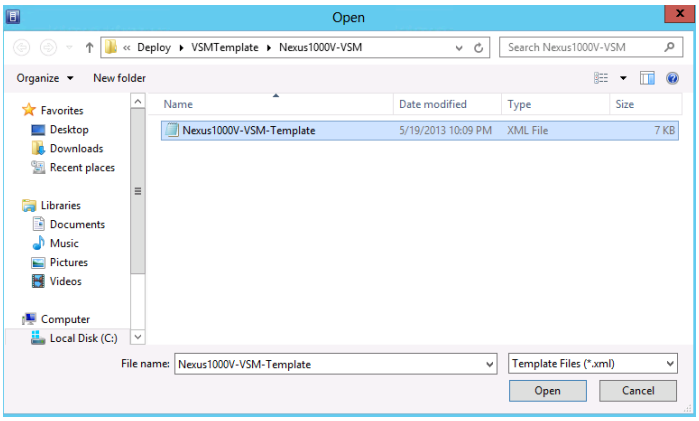
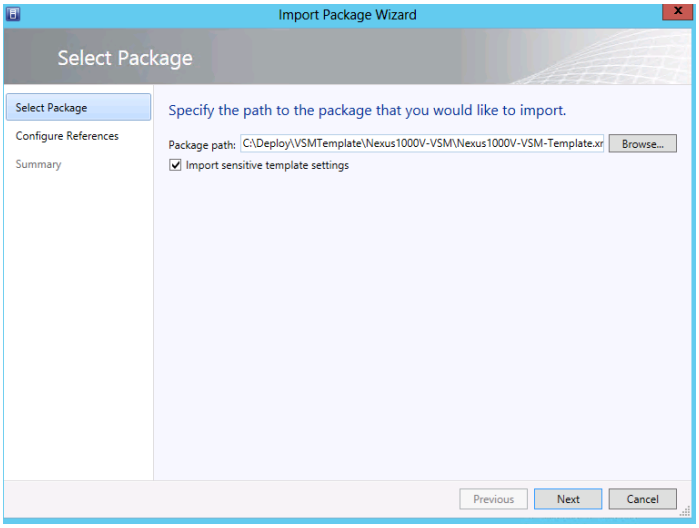
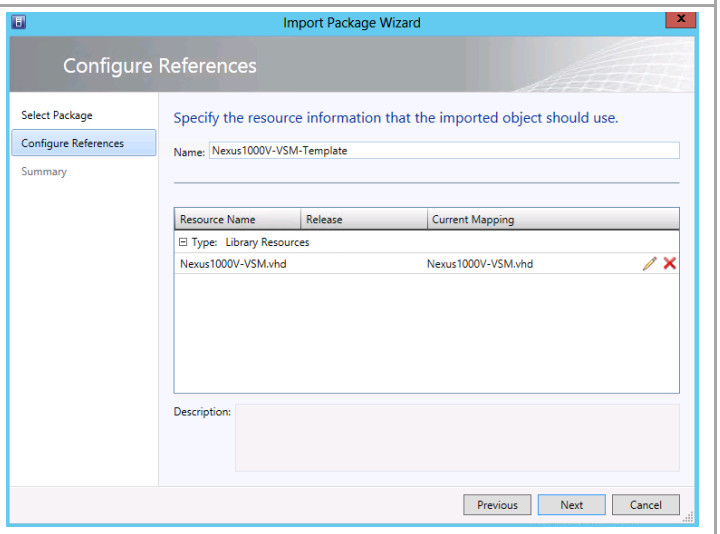
The Cisco Nexus 1000V for Microsoft Hyper-V package (a zip file) is available at the download URL location provided with the software. Complete the following steps to download the Cisco Nexus 1000V for Microsoft Hyper-V package.

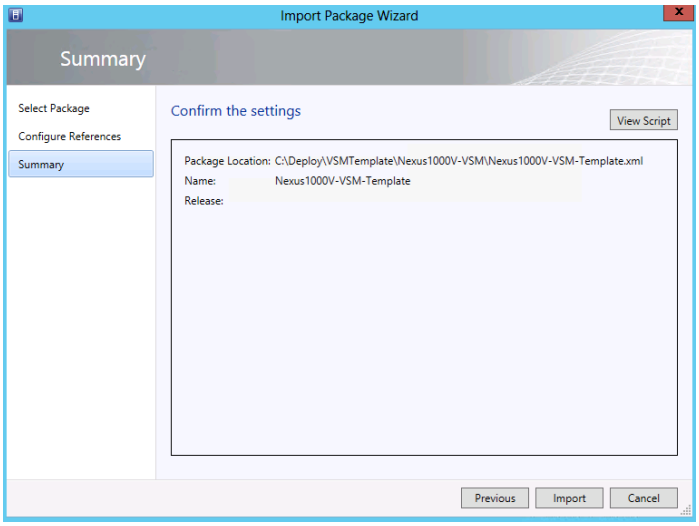
- Virtual Supervisor Module (VSM) ISO (N1000vh-dk9.5.2.1.SM1.5.0.1.iso)
- Virtual Ethernet Module (VEM) MSI package (Nexus1000V.msi)
- Cisco VSEM Provider MSI package (CiscoProviderInstaller.msi)
- Nexus 1000V Virtual Machine Template(Nexus1000V-VSM-Template.xml)
- Nexus 1000V VSM Virtual Hard Drive (Nexus1000V-VSM.vhd)

16.1 Intall the Virtual Supervisor Modules Virtual Machine Template

1. Copy the Nexus 1000V ISO imange to the VMM Library share created earlier.	

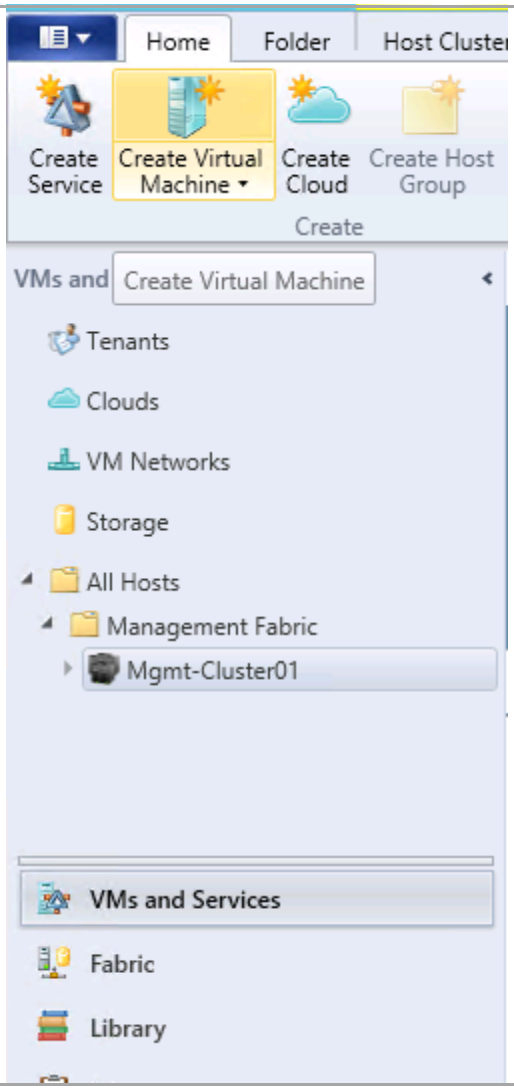
2. In Virtual Machine Manager, click Library and select the library share. Right-click the share and select Refresh.	
3. Verify that the refresh operation completed succesufully.	
4. Navigate the library share structure and verify the location of the Nexus 1000V VSM ISO image and VHD. 5. Click Import Library.	

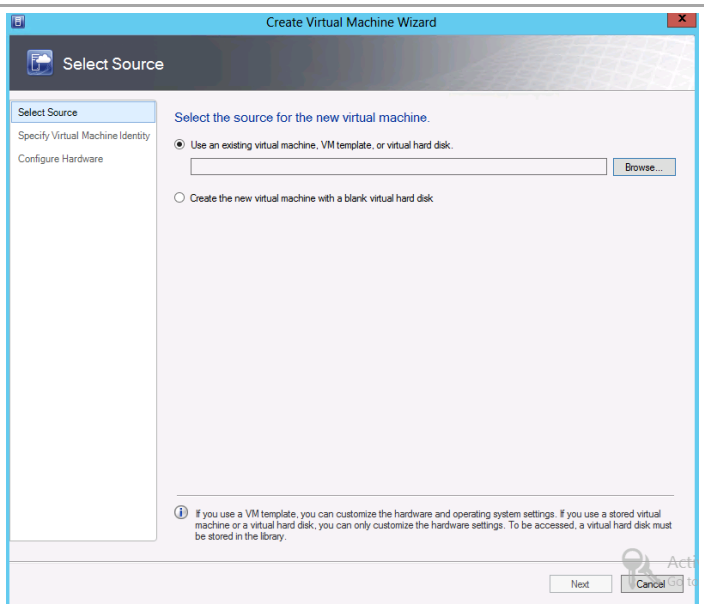
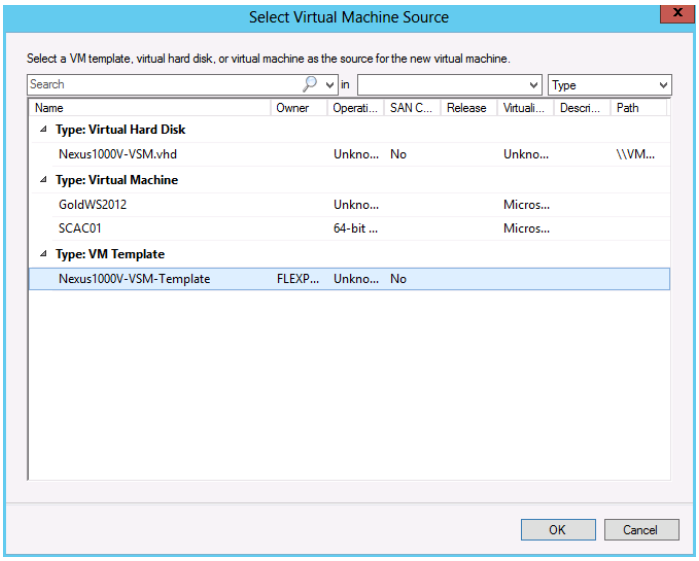
6. Browes to the location of the Nexus 1000V VSM virtual machine template and click Open.	
7. Click Next to proceede.	
8. Review the configuraiotn refrences and click Next to proceed.	

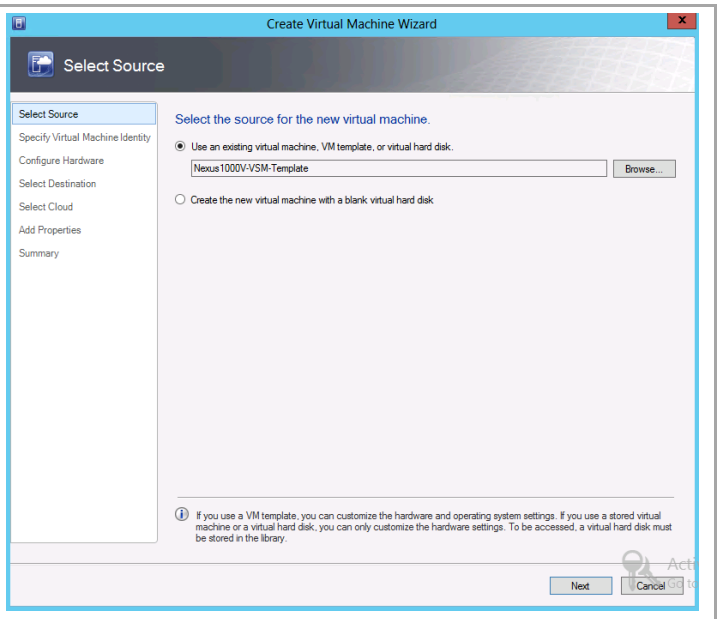
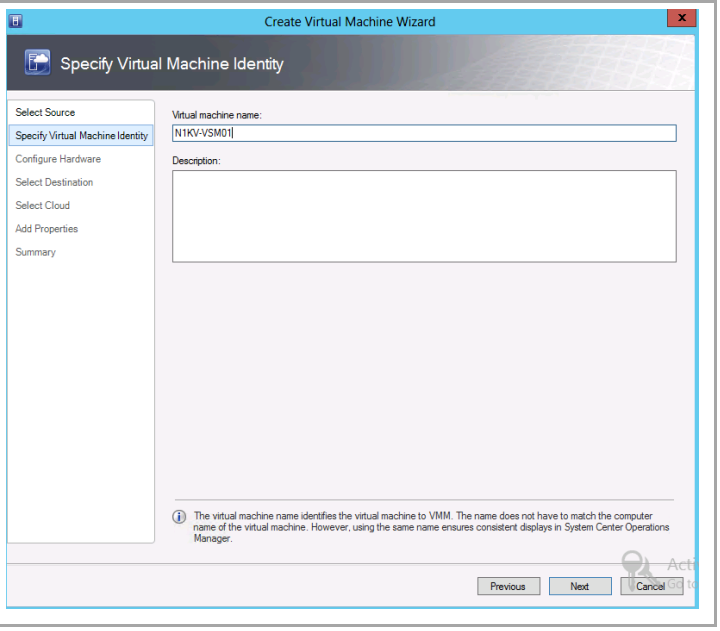
9. Review the summary and click Import.	

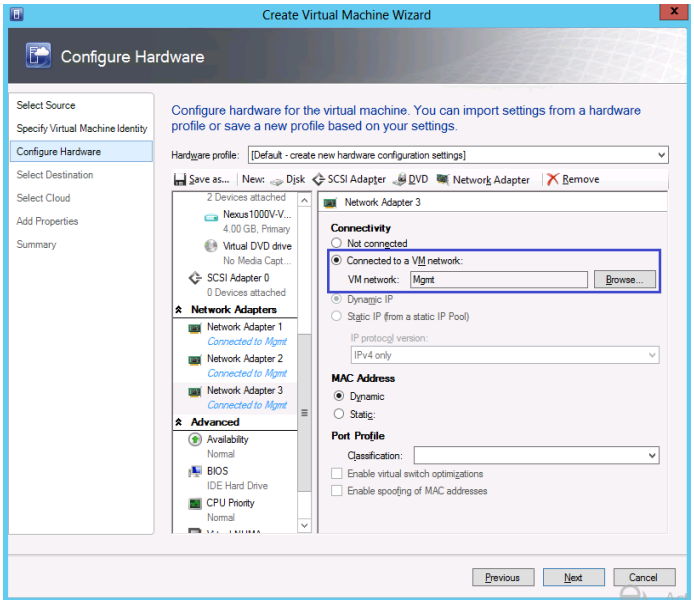
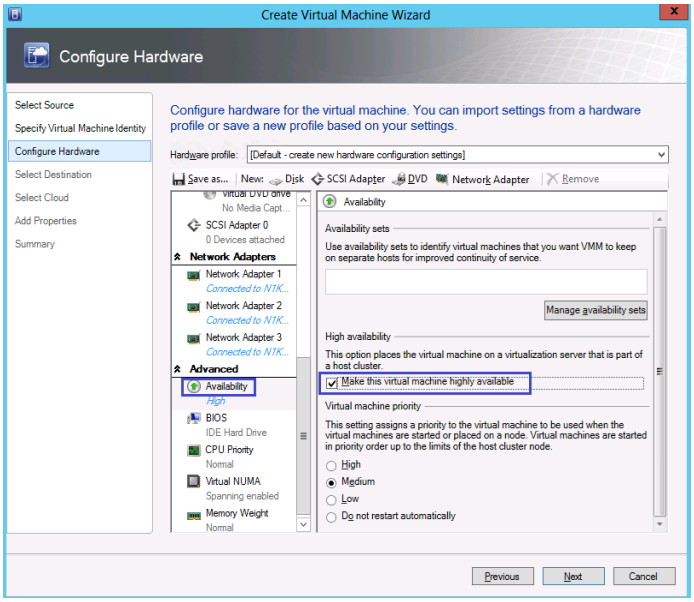
16.2 Creat the Virtual Supervisor Modules in the VMS Virtual Machines

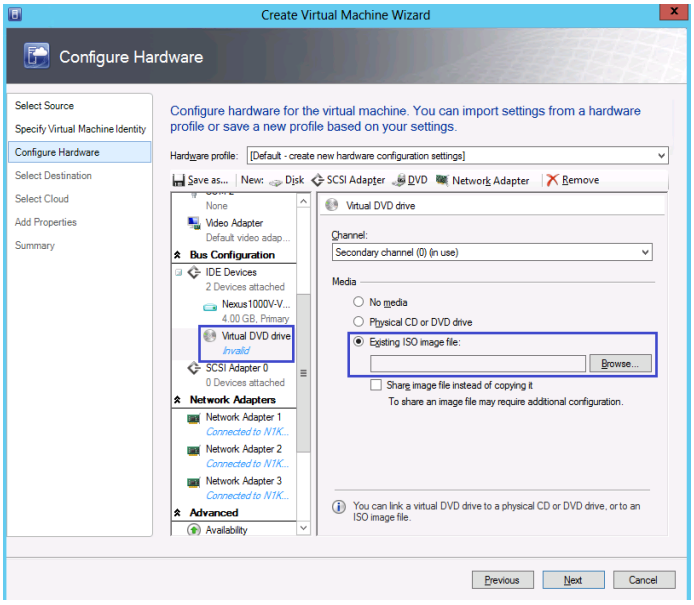
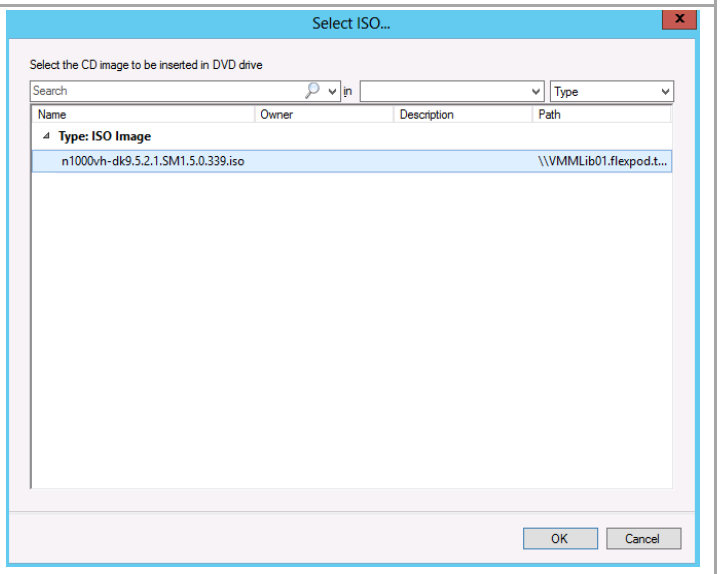
1. Select VMs and Services and click Create Virtual Machine.

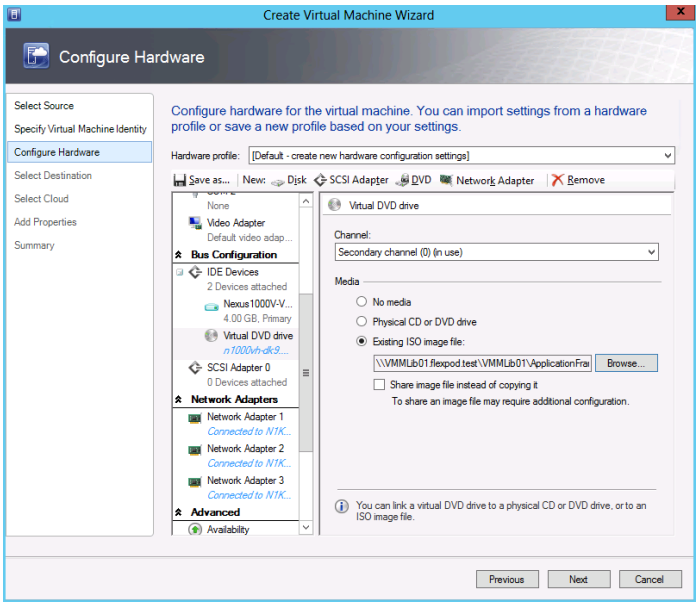
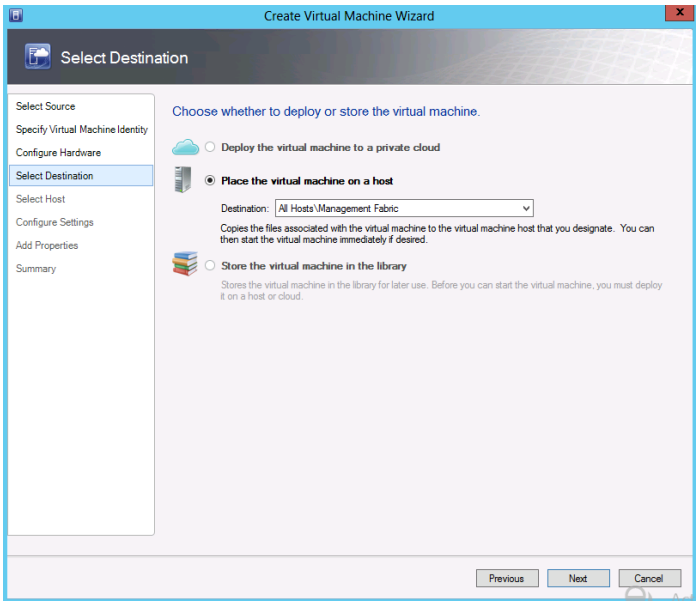


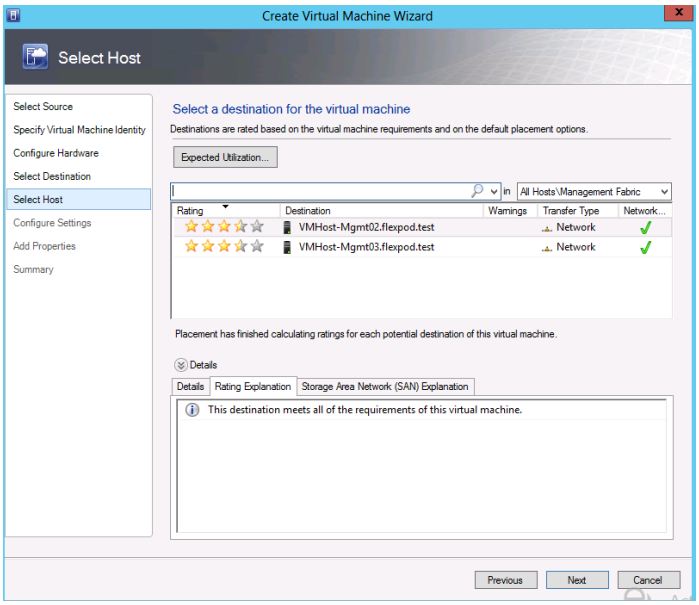
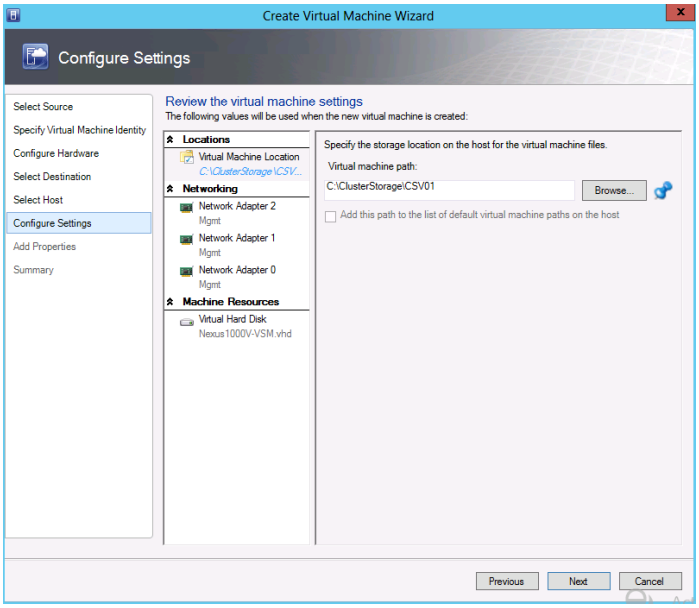
2. Select the default option Use and existing virtual machine, VM template, or virtual hard disk. Click Browse.	
3. Select the Nexus 1000V-VSM-Template and click OK.	

4. Click Next to proceed.	
5. Enter the virtual machine name and click Next.	

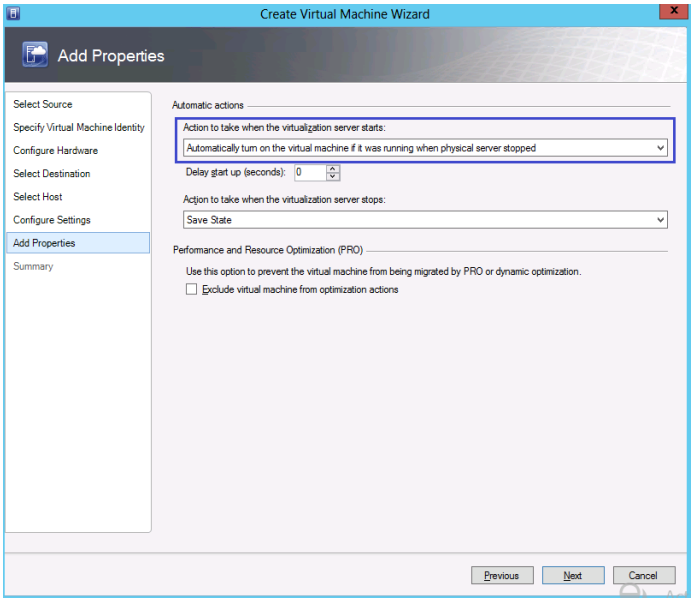
6. Navigate the the three network adapters in the center pane. Configure all three adapaters to connect to the Mgmt VM Network.	
7. Scroll down to the Advance objects in the middle pane and select Availability. Check the box Make this virtual machine highly available.	

8. Scroll up to the Bus Configuration objects in the middle pane and select Virtual DVD drive. In the righ pane select Existing DVD and click Browse…	
9. Select the Nexus 1000V VMS ISO and click OK.	

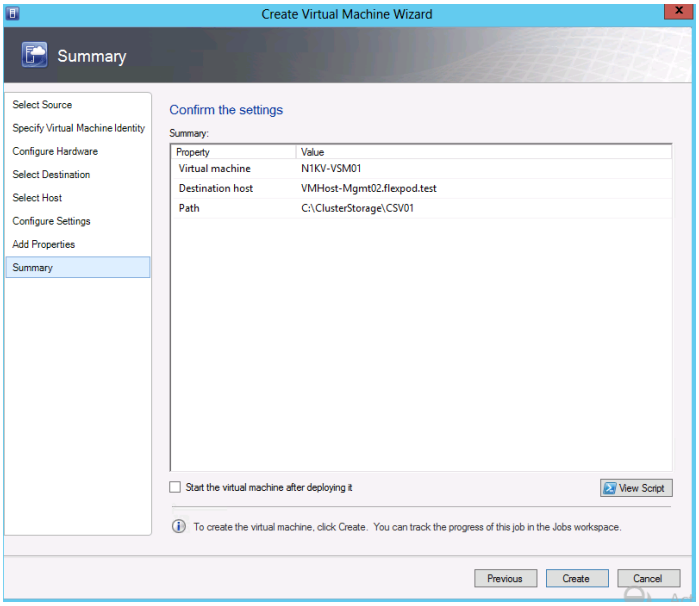
10. Click Next to proceed.	
11. Select the default placement option to place the virtual machine on all hosts and click Next.	

12. In the Select Host window, click Next.	
13. Select one of the CSV volumes to store the virtual machine configuration and VHD. Click Next to proceed.	

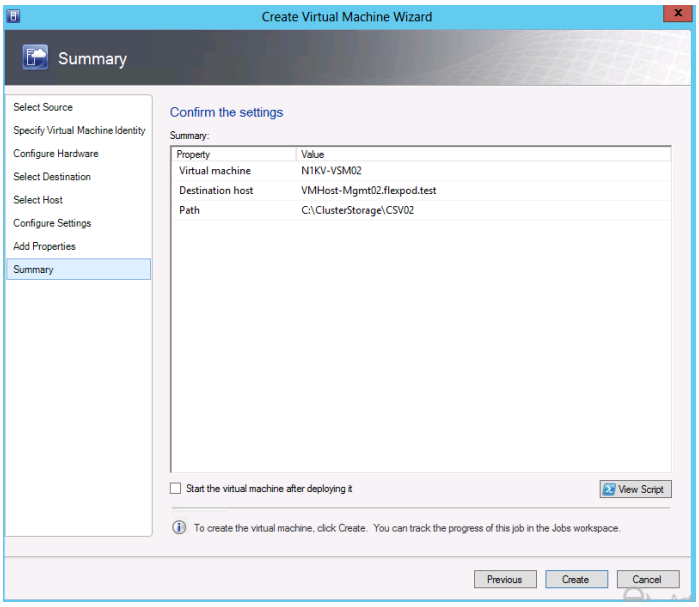
14. In the add properties window, select the server start action "Automatically turn on the virtual machine if it was running when physical server stopped." Click Next to proceed.



15. Review the summary and click Create.



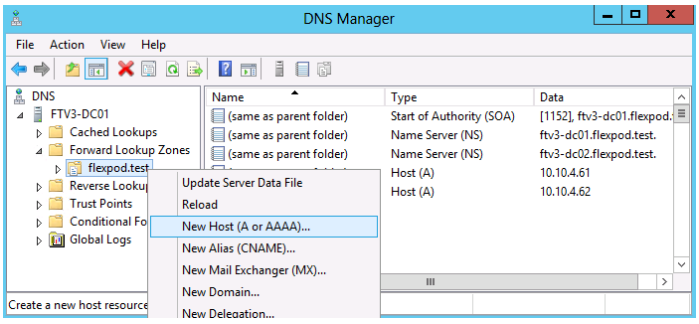
16. Repeat this procedure to create the second VSM virtual machine. Place the second VSM virtual machine configuration files and VHD on a different CSV volume.



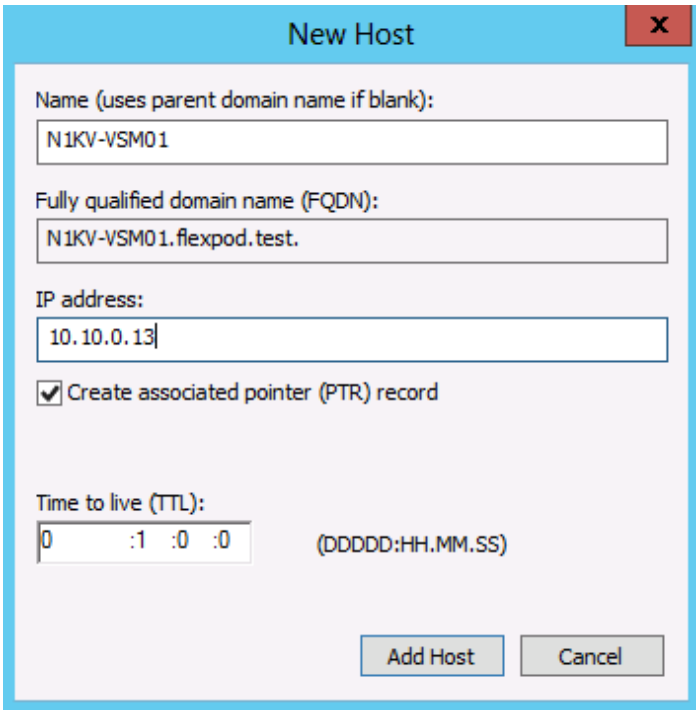
16.3 Add a Domain Name Service Record for the Virtual Supervisor Module

▶ Perform the following configuration operation on the server running Domain Name Service.

1. Open DNS Manager and navigate the forward lookup zone for the domain. Righ-click the forward lookup zone and select New Host (A or AAAA) ...



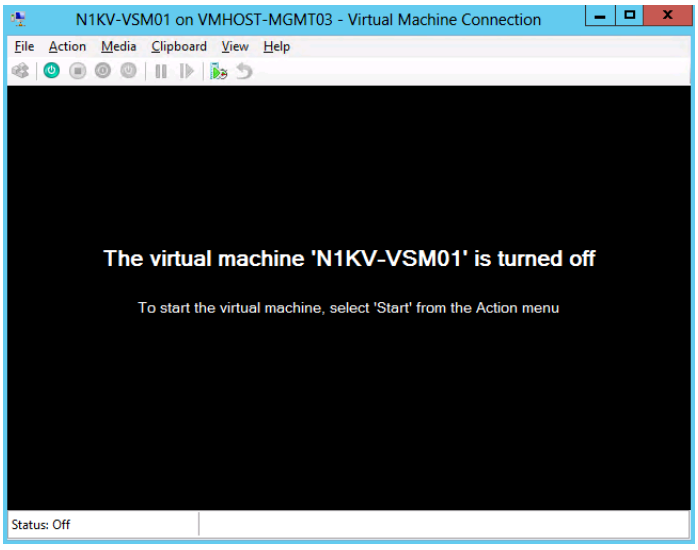
2. Enter the VMS host name and IP address. Click Add Host.
3. Click OK to achnology the DNS record creation.
4. Click Done to cluse the New Host window.

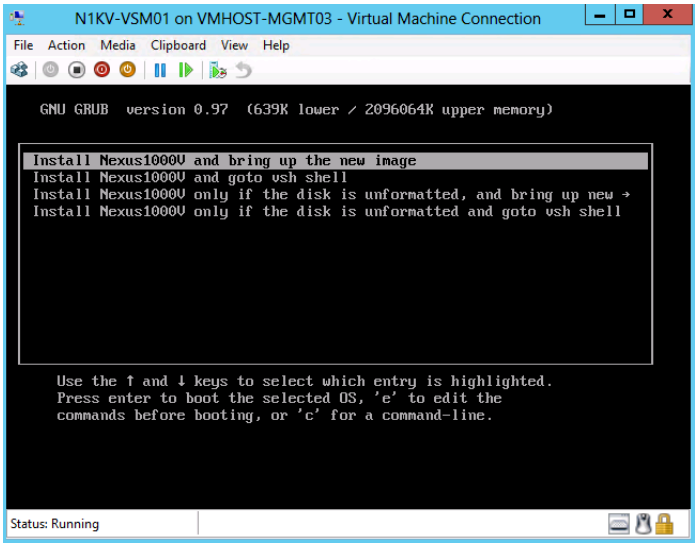


16.4 Configure Virtual Supervisor Modules in the VMS Virtual Machines

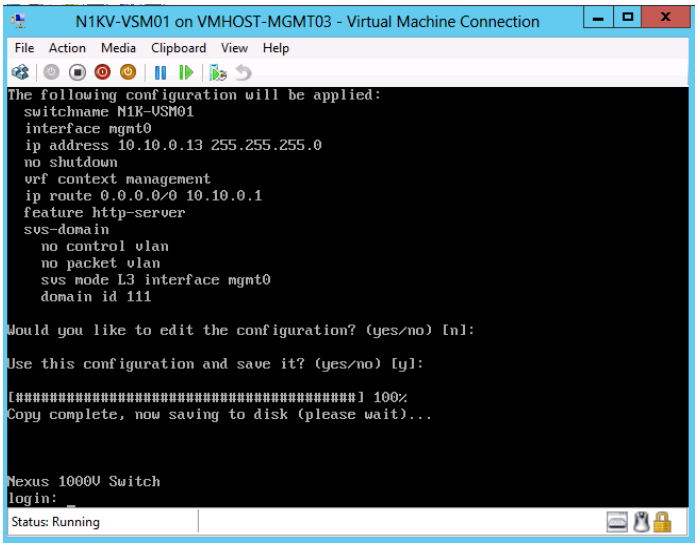
▶ Perform the following configuration operation on the first VSM virtual machine.

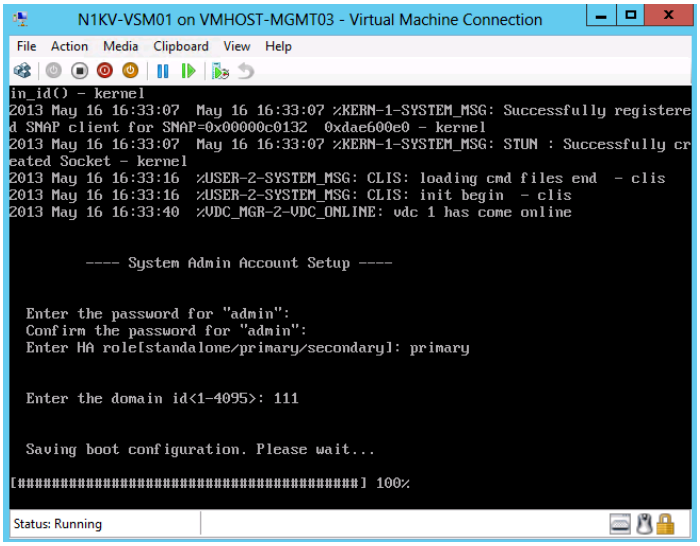
1. In VMM, connect to the first VSM01 VM and power it on.



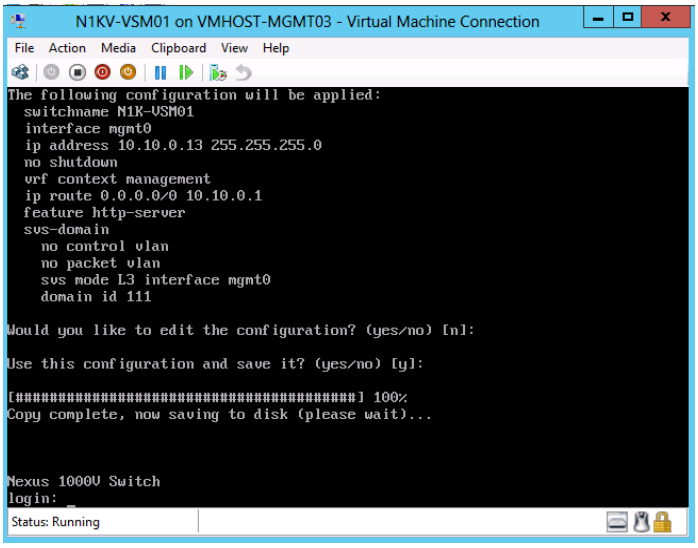
2. Select Install Nexus 1000V and bring up the new image. Hit Return.	

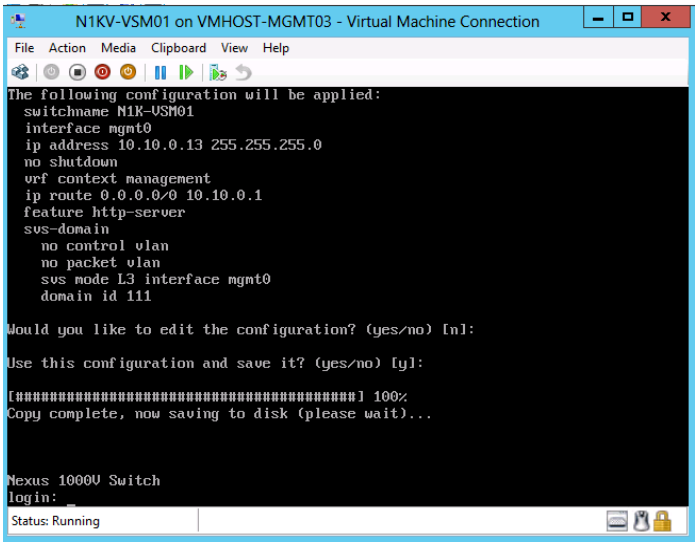
3. The Virtual Machine Viewer window opens up. While it processes, it stops at the command prompt with the following message: Do you want to format it? (y/n). **Enter Y for yes at the prompt.**
4. At the next command prompt, the following message is displayed: Perform r/w tests (takes very long time) on target disks? (y/n). **Enter Y for yes at the prompt.**
5. You are prompted to enter the System Administrator Account Setup. At the Enter the password for "admin": prompt, enter the password. At the Confirm the password for "admin": prompt, re-enter the password.
6. Enter the high availability (HA) role at the next prompt; enter **Primary.**

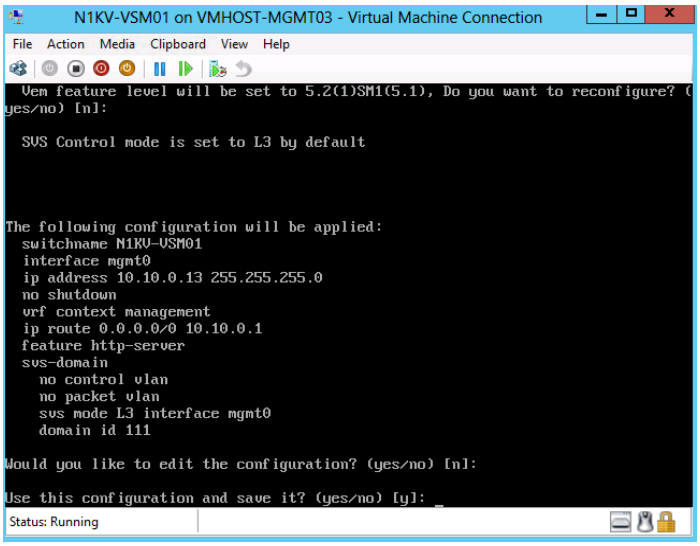




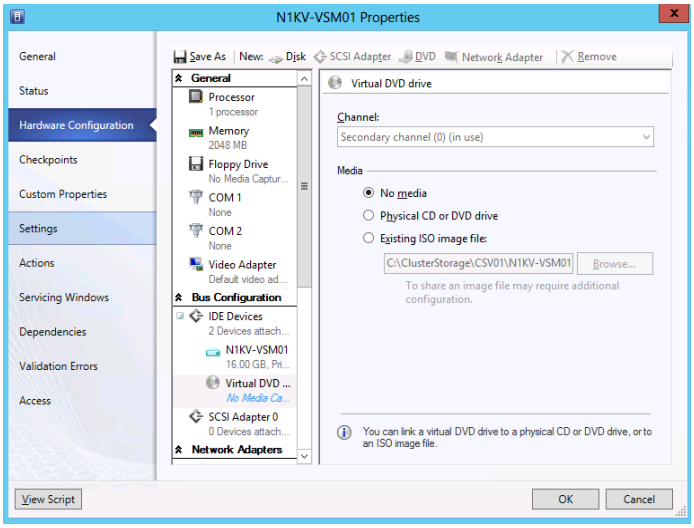
7. Enter **Y** to enter the basic configuration.
8. Enter **N** to creating and another login account.
9. Eneter the switch name : N1KV-VSM01
10. Enter **Y** to configurure Out-of-Band management interface.
11. Enter the Mgmt0 IPv4 address: 10.10.0.13
12. Enter the IPv4 netmask: 255.255.255.0
13. Enter **Y** to configure the default gateway.
14. Enter **Y** to configure advance options.
15. Enter **Y** to configure advanced IP options.
16. Enter **N** not to configure a static route.
17. Enter **N** not to configure the default network.
18. Enter **Y** to configure DNS IP Address: 10.10.4.61
19. Enter **Y** to configure default domain name: flexpod.test
20. Enter **N** not to configure read-only SNMP community string.
21. Enter **N** not to configure read-write SNMP community string.
22. Enter **N** not to enable telnet service.
23. Enter **Y** to enable ssh service.
24. Enter **Y** to configure NTP server address.
25. Enter **N** to reconfigure option.
26. Enter **N** not to edit the configuration.
27. Enter **Y** to save the configuration and use it.







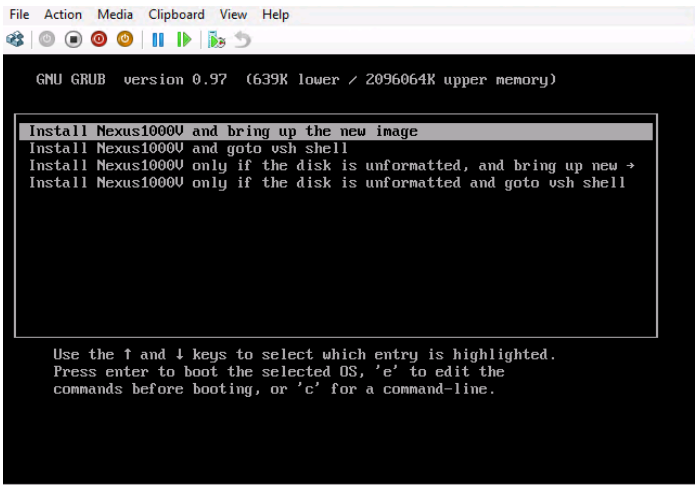
28. Remove ISO from the first VSM02 Virtual Machine if there is an ISO image connected to the virtual machine.



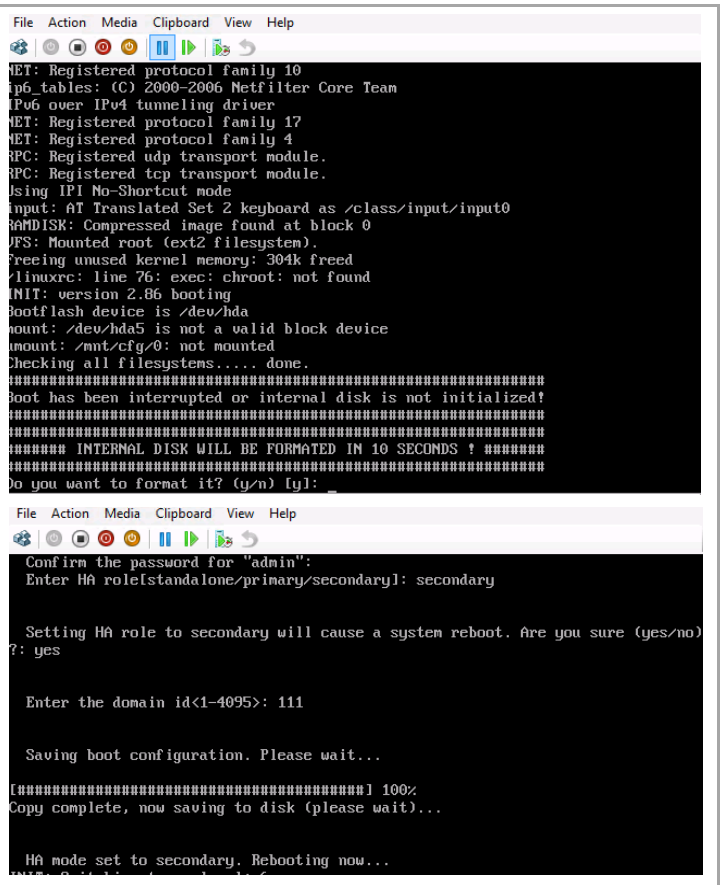
▶ Perform the following configuration operation on the SecondVSM virtual machine.

1. In VMM, connect to the first VSM02 VM and power it on.

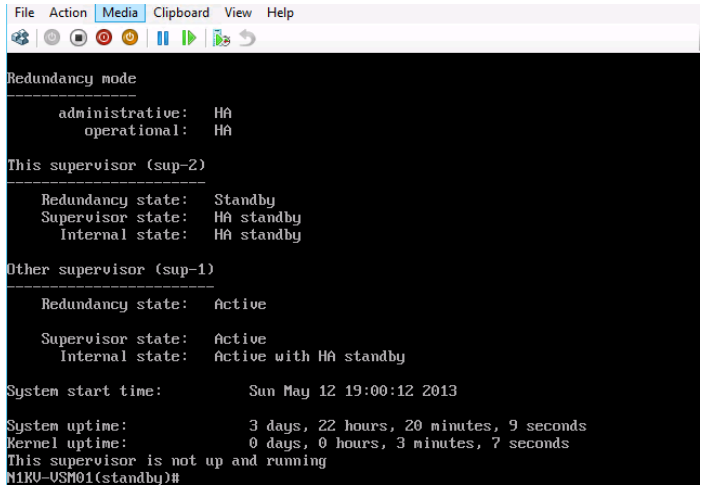
2. Select Install Nexus 1000V and bring up the new image. Hit Return.



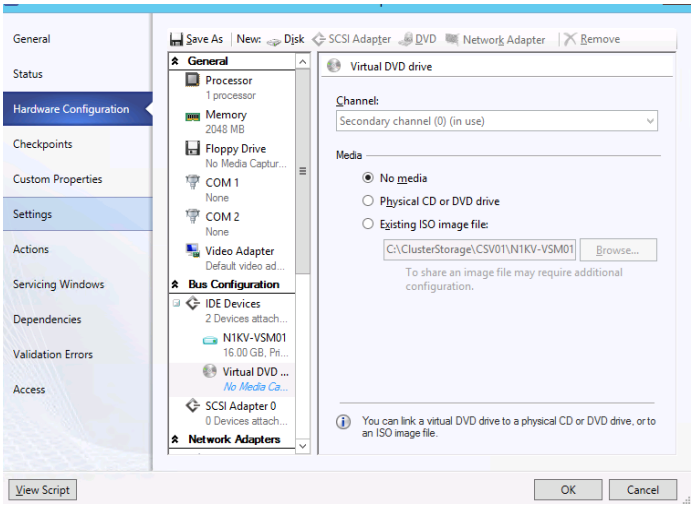
3. The Virtual Machine Viewer window opens up. While it processes, it stops at the command prompt with the following message: Do you want to format it? (y/n). **Enter Y for yes at the prompt.**
4. At the next command prompt, the following message is displayed: Perform r/w tests (takes very long time) on target disks? (y/n). **Enter Y for yes at the prompt.**
5. You are prompted to enter the System Administrator Account Setup. At the Enter the password for "admin": prompt, enter the password. At the Confirm the password for "admin": prompt, re-enter the password.
6. Enter the high availability (HA) role at the next prompt enter **secondary.**
7. Enter the domain ID: 111
8. Acknologe that the system will reboot.



9. Login to the VMS and verify the redundancy status:
    a. Show redundancy status



10. Remove ISO from the first VSM 02 Virtual Machine if there is an ISO image connected to the virtual machine.



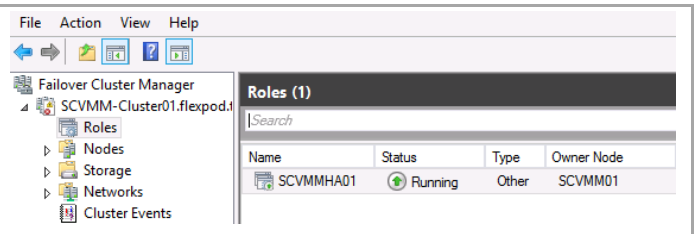
16.5 Configure Nexus 1000V VSM For Use with Virtual Machine Manager

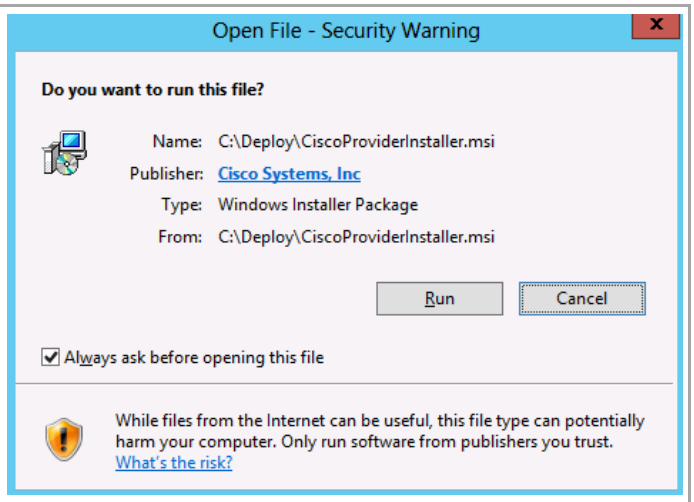
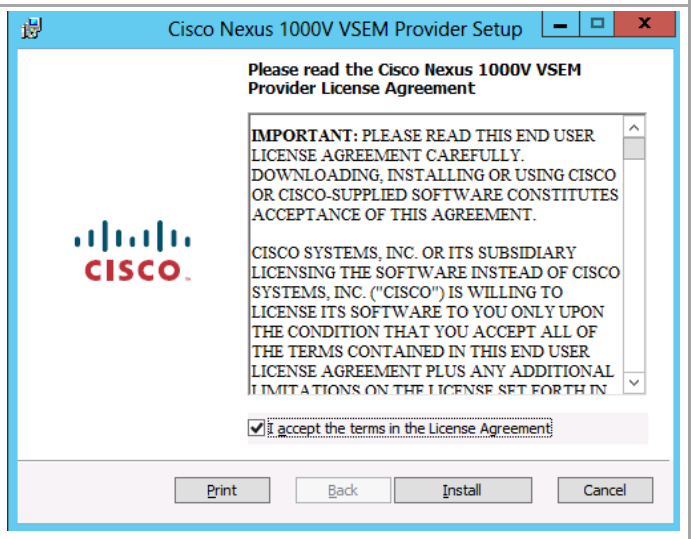
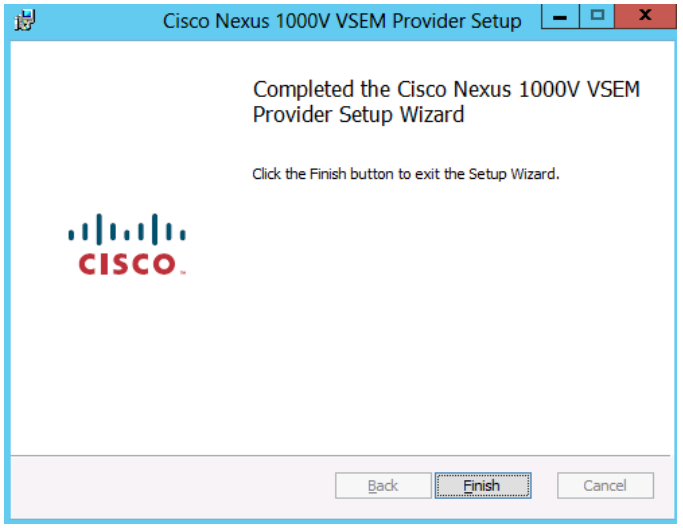
1. Enther the following configuration commands on the primary VSM:

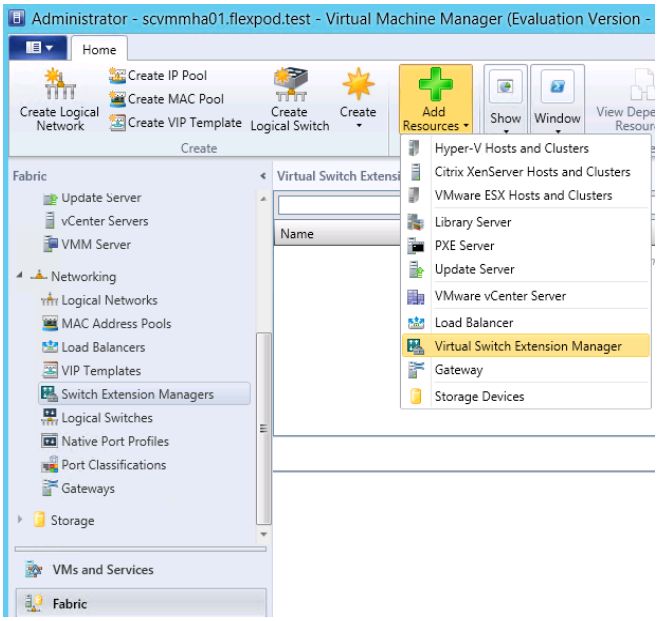
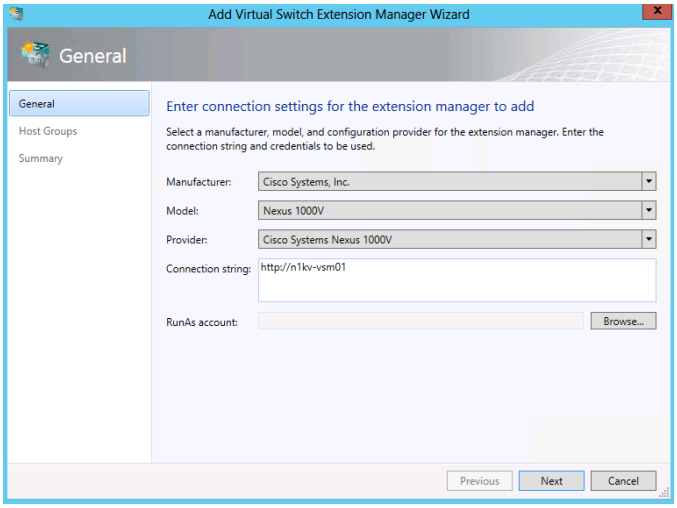
```
nsm logical network FastTrack
exit

nsm network segment pool Mgmt-Fabric
 member-of logical network  FastTrack
 exit


nsm ip pool template N1KV-FM-Public-IP-Pool
  ip address 192.168.2.90 192.168.2.99
  network 192.168.2.0 255.255.255.0
  default-router 192.168.2.1
  exit

nsm network segment N1KV-MF-Public
  member-of network segment pool Mgmt-Fabric
  switchport access vlan 1002
  ip pool import template N1KV-FM-Public-IP-Pool
  publish network segment
  exit

port-profile type vethernet AllAccess1
 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 Mgmt-Fabric
 system network uplink
 publish network uplink
 exit

Copy running-config startup-config
```

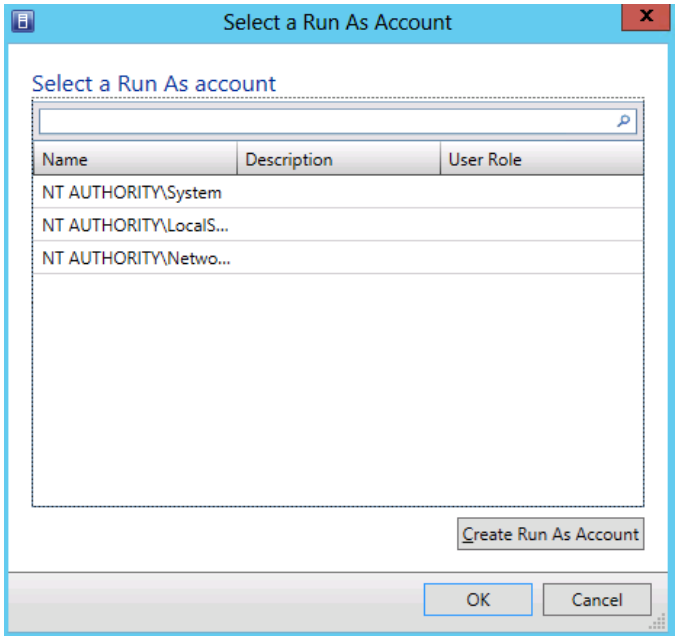
16.6 Configure Virtual Switch Extension Manager in Virtual Machine Manager.

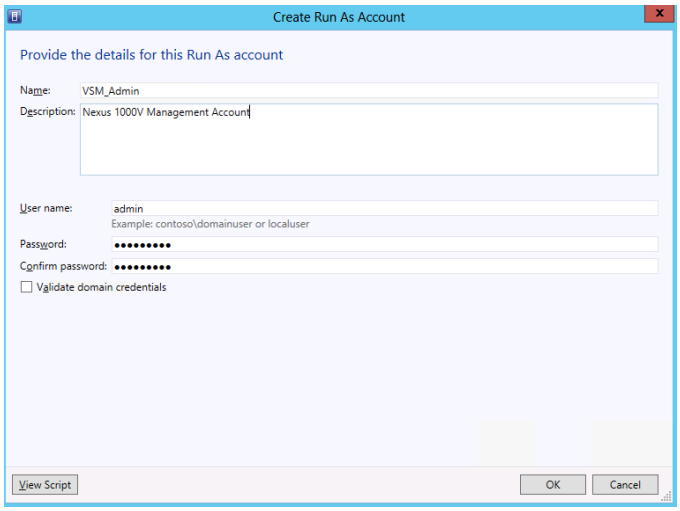
1. On the Virtual Machine Manager virtual machine, verify that it owns the highly available Virtula Machine Mnager instance. Move the instance to this node if it is currenly owned by the other Virtual Machine Manager node.



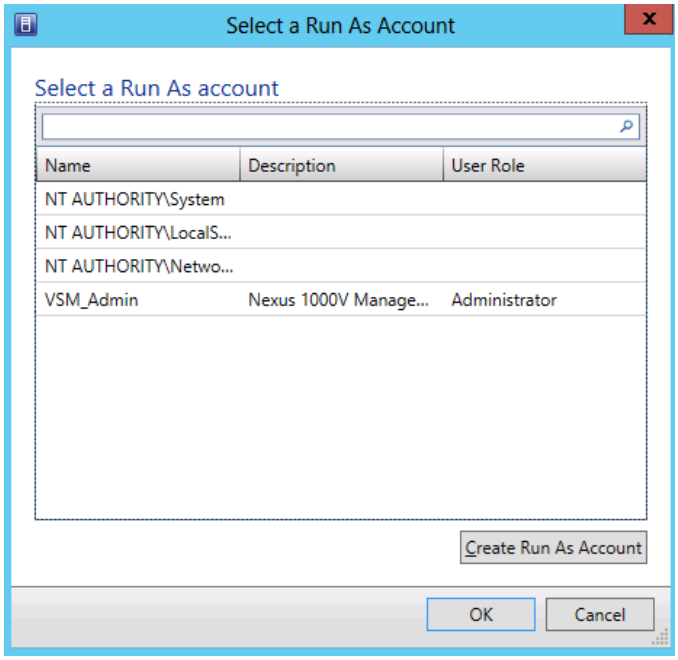
2. Install the Cisco Nexus 1000V switch extensions by running CiscoProviderIntaller.msi. In the security warning window, click Run.	
	
	

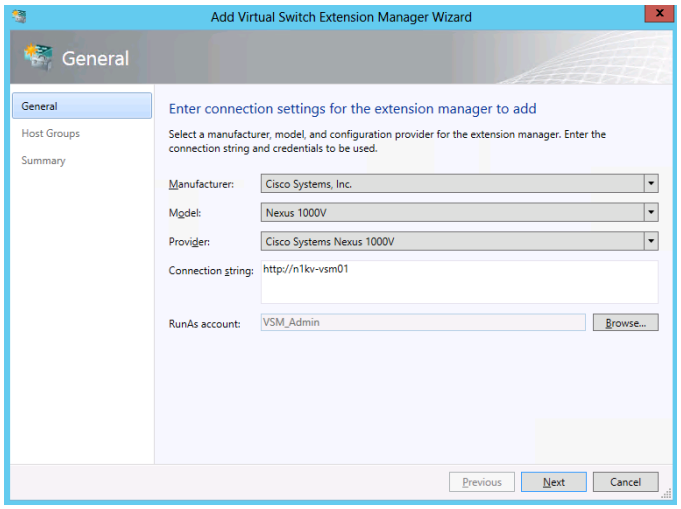
	
3. Enter connection string. Click Browse.	


Select a Run As Account
Select a Run As account
Name
Description
User Role
NT AUTHORITY\System
NT AUTHORITY\LocalS...
NT AUTHORITY\Netwo...
Create Run As Account
OK
Cancel

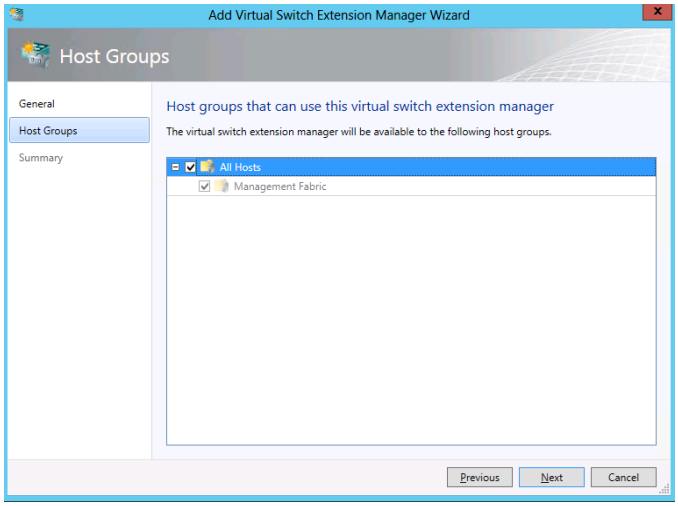

Create Run As Account
Provide the details for this Run As account
Name:
VSM_Admin
Description:
Nexus 1000V Management Account
User name:
admin
Example: contoso\domainuser or localuser
Password:
Confirm password:
Validate domain credentials
View Script
OK
Cancel

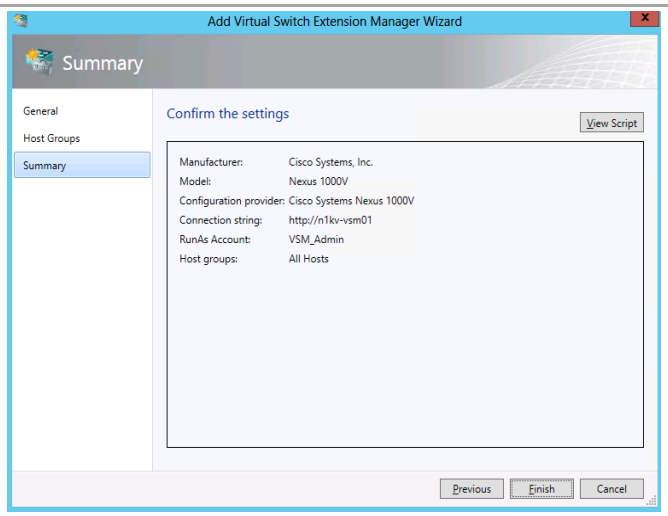
4. Select VSM_Admin account and click OK.

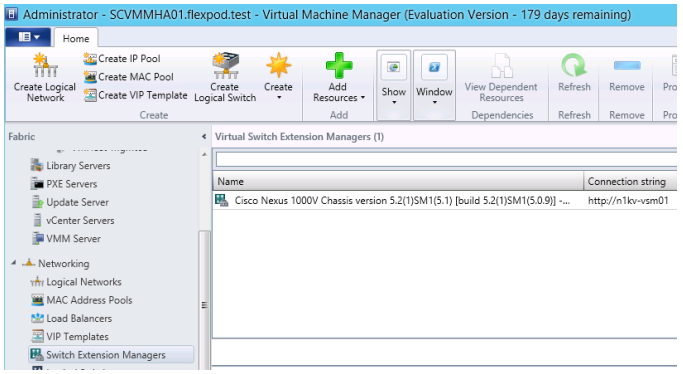




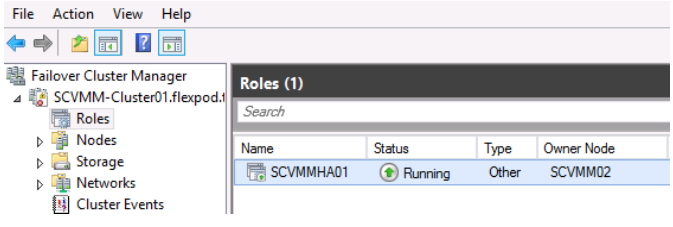
5. Select All Hosts group.

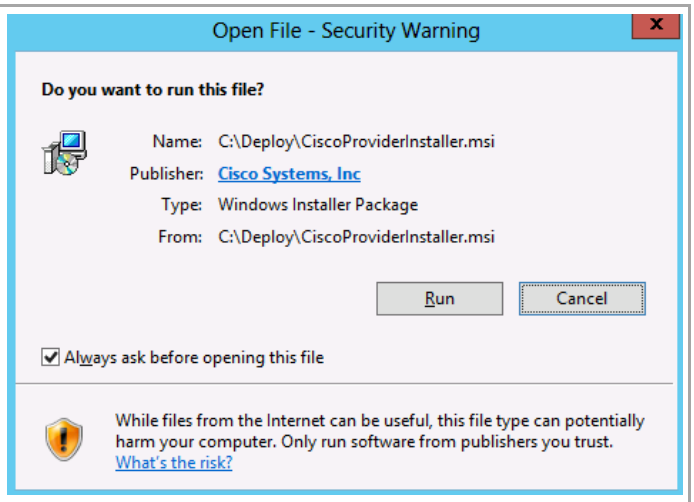
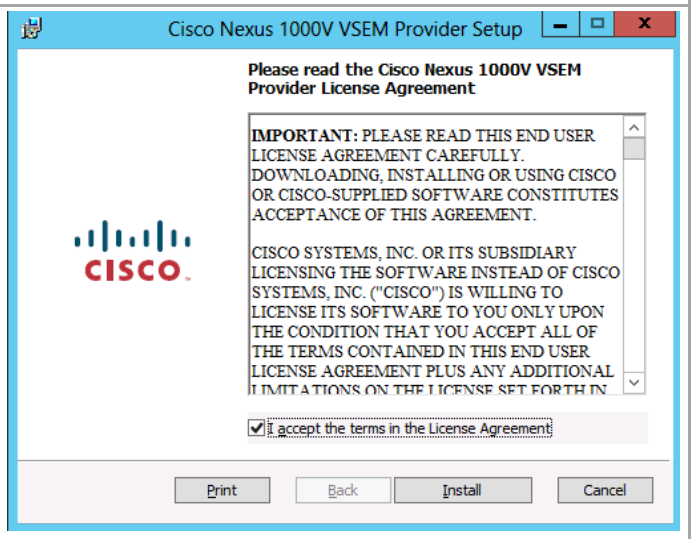
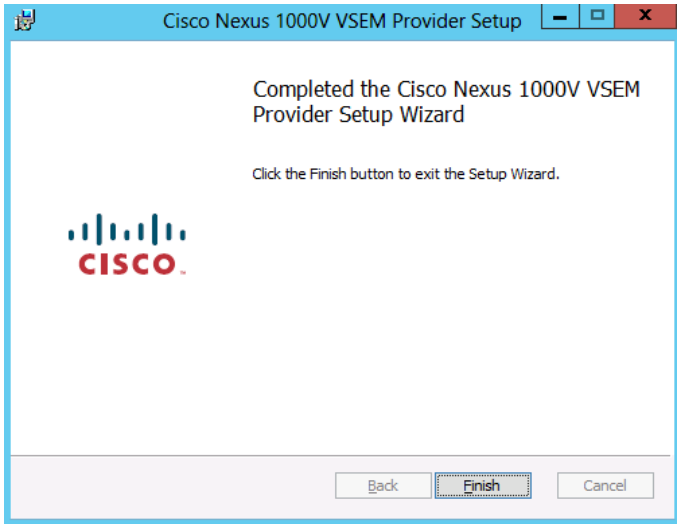






6. Using Cluster Failover Manager, move the highly available Virtual Machine Manager instance to the second Virtual Machine Manager node.



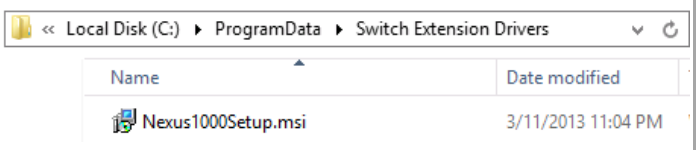
7. Connect to the second Virtual Machine Manager node. Install the Cisco Nexus 1000V switch extensions by running CiscoProviderIntaller.msi. In the security warning window, click Run.	
	
	

16.7 Copy Virtual Ethernet Module Installation Packager to the Virtual Machine Manager Virtual Machines

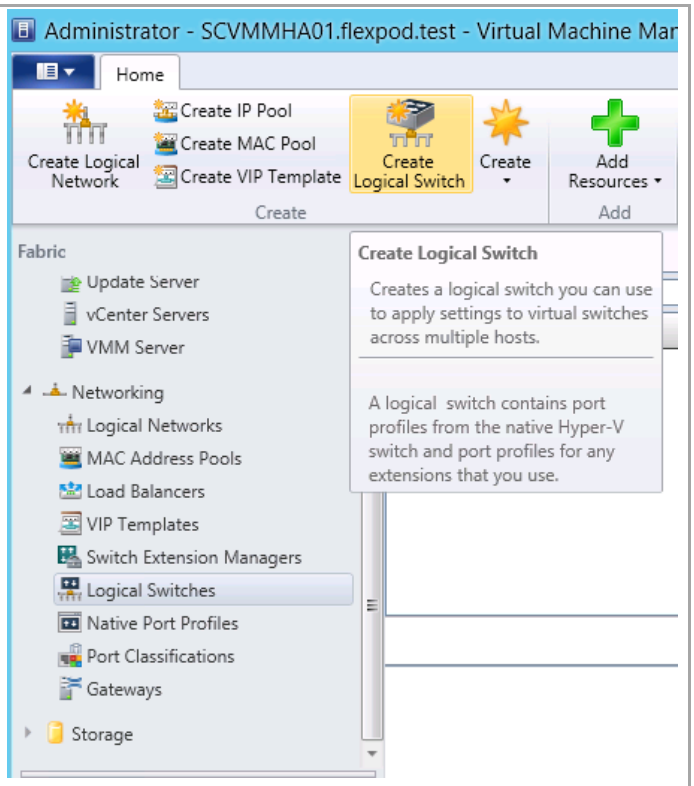
▶ Perform the following procedure on each Virtual Machine Manager node.

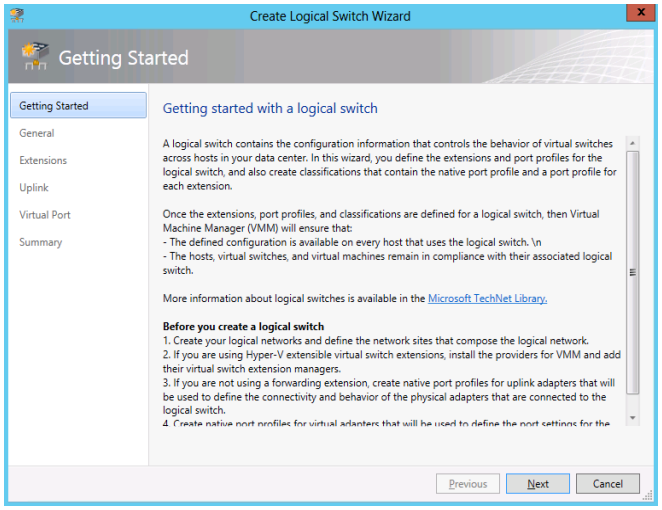
1. Copy Nexus1000Setup.msi to the following directory on each Virtual Machine Manager server:

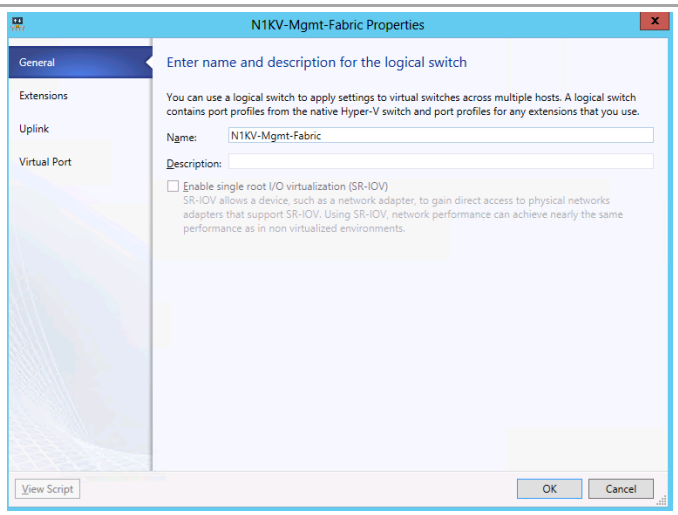
C:\ProgramData\Switch Extensions Drivers



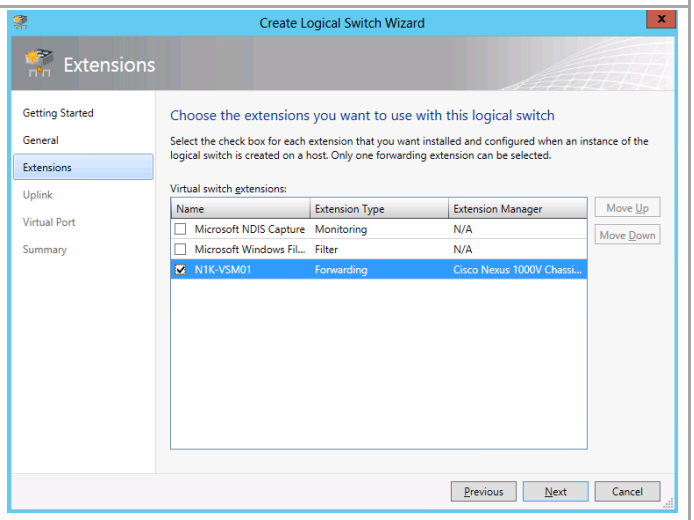
16.8 Configure a Logical Switch In Virtual Machine Manager

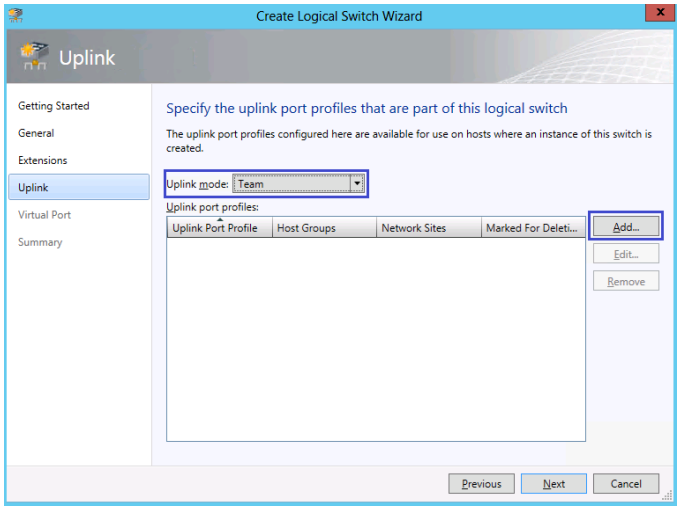
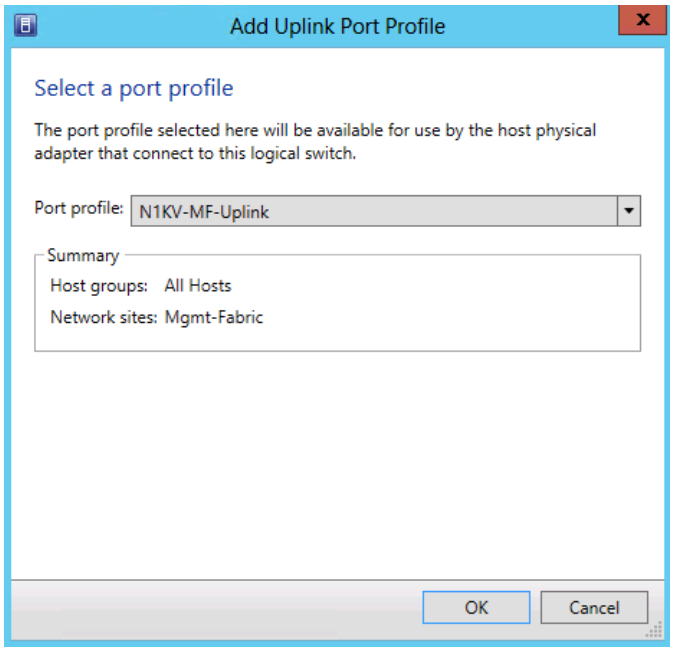


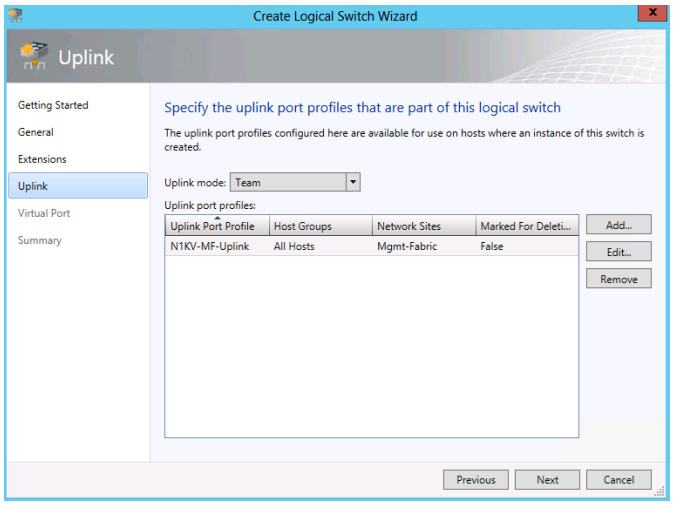
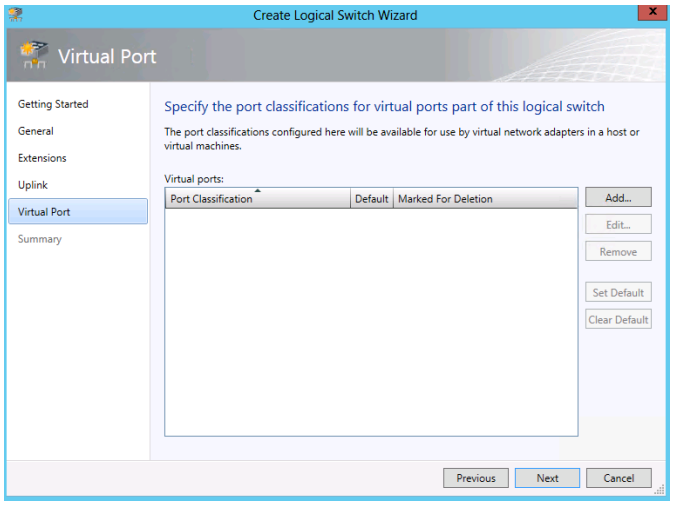


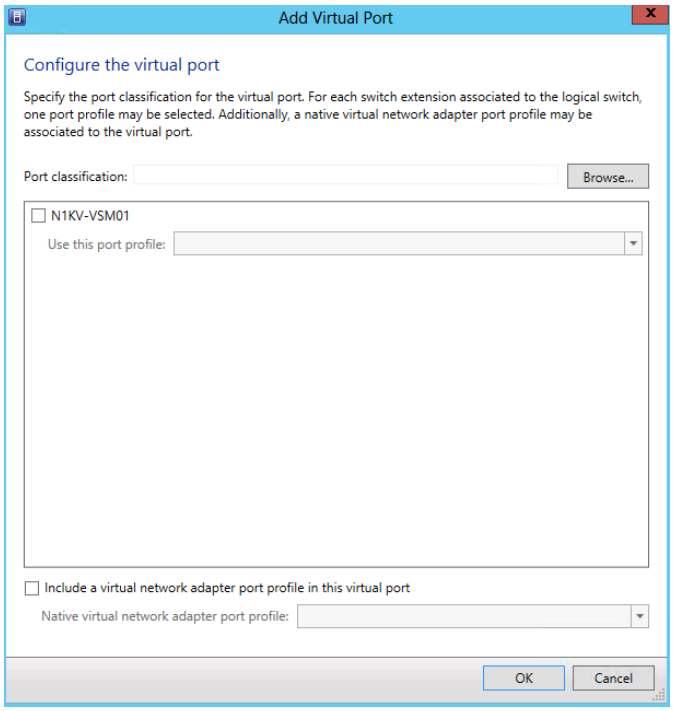
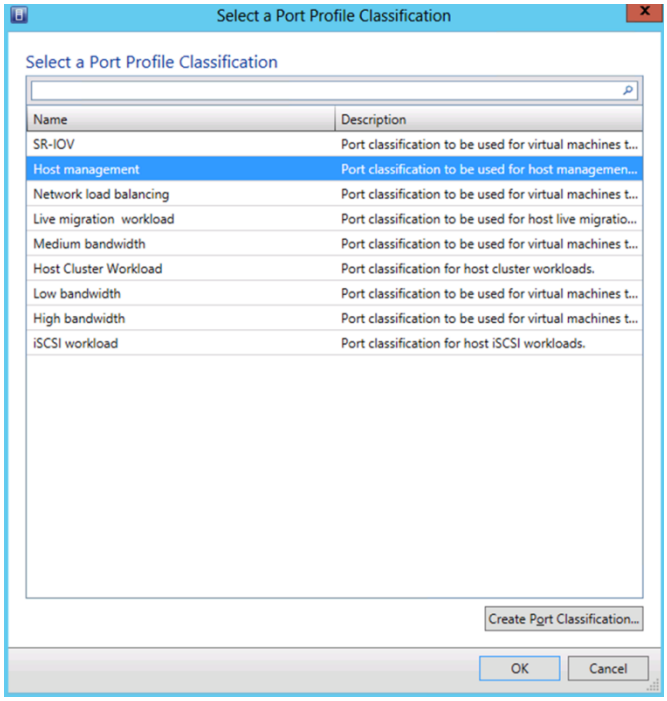


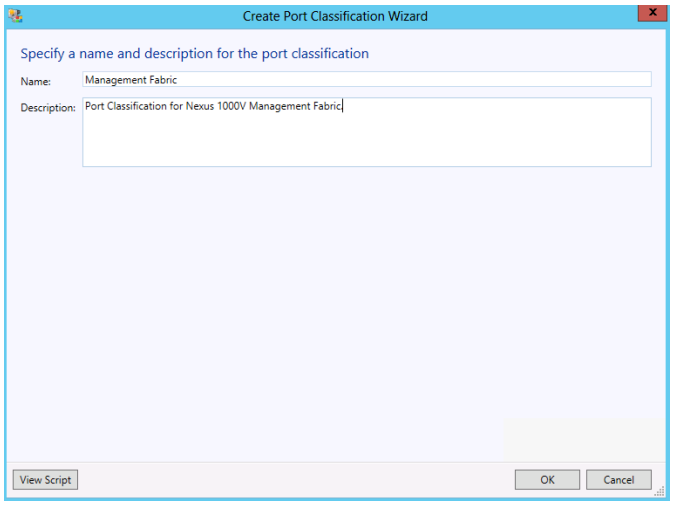
1. Uncheck Microsoft Windows Filtering Platform. Check N1KV-VSM01 forwarding extension type.



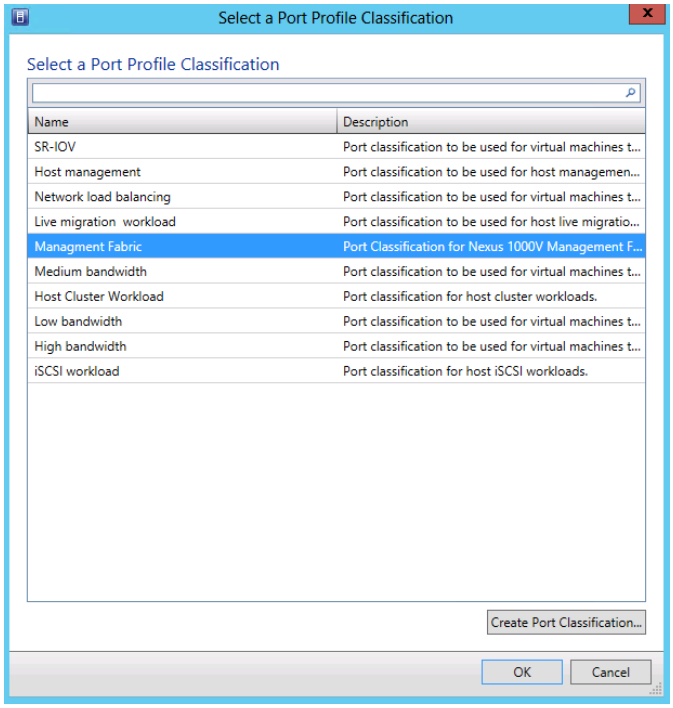
2. Select the Team Uplink mode in the dropdown text box. Click Add to add the uplink port profile.	
3. Select the **Port Profile** and click **OK**.	

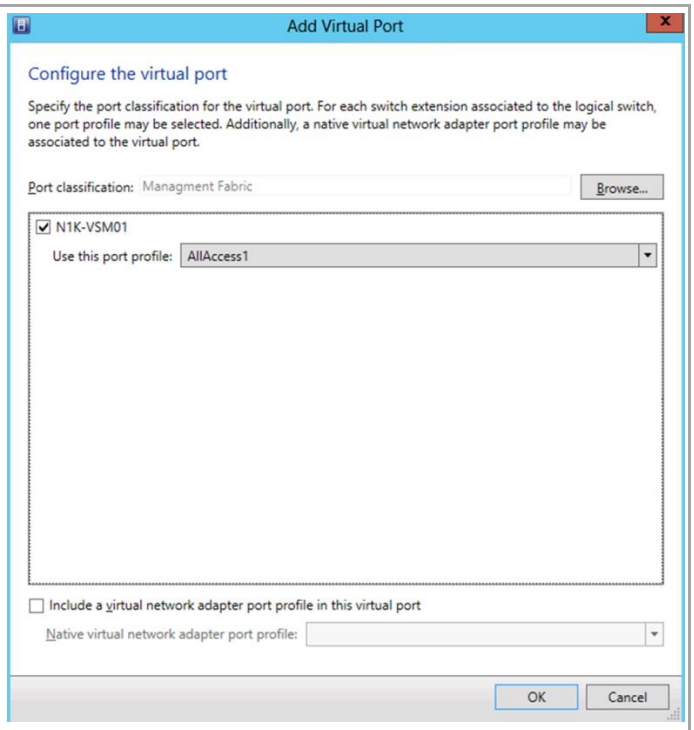
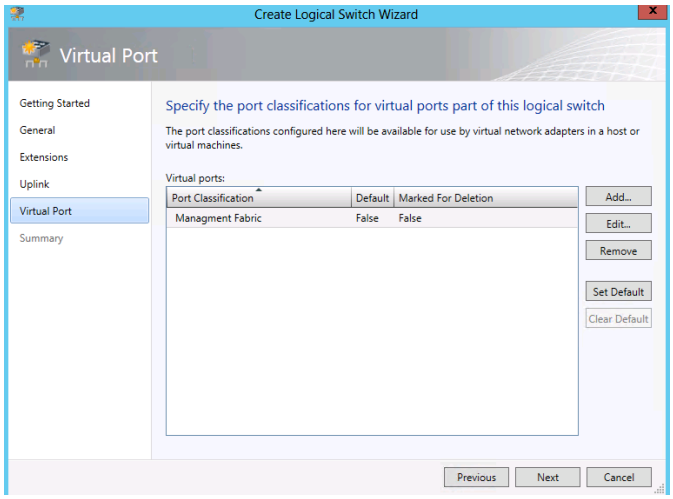
4. Review the added uplink port profile and click **Next** to continue.	
5. Click Add to add the virtual port clasifiction.	

6. Click Browse.	
7. Click Create Port Classification.	

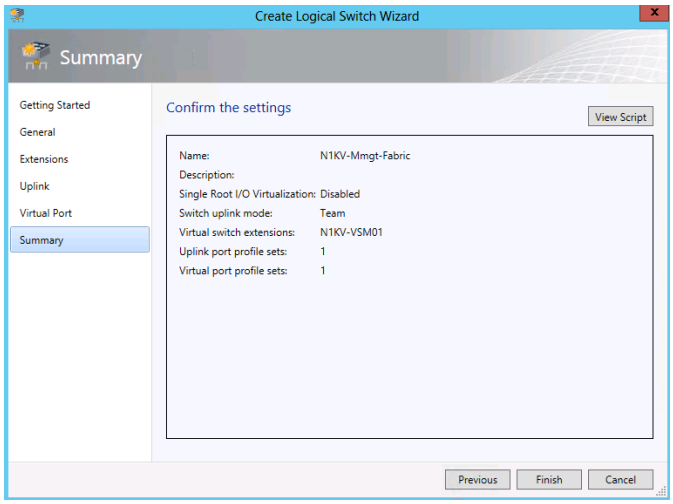


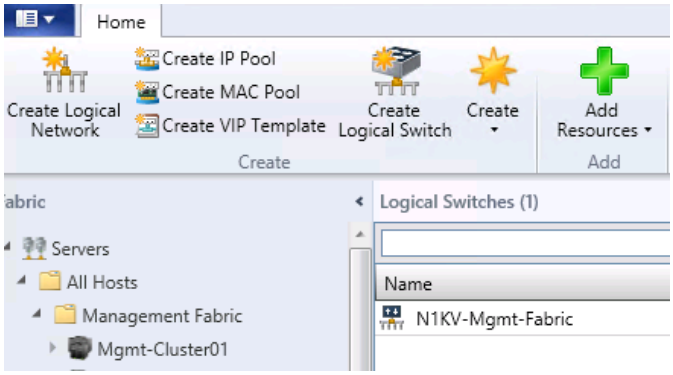
8. Select the new **Management Fabric** port classification and click **OK**.



9. Check N1KV-VSM01 and select the port profile from the dropdown text box. Click OK.	
10. Click Next to proceed.	

11. Confirm the configuration setting and click finish to create the logical switch.

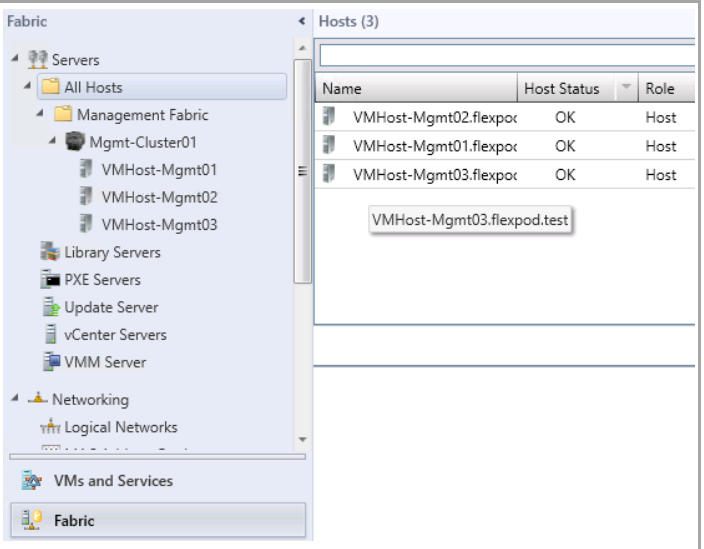




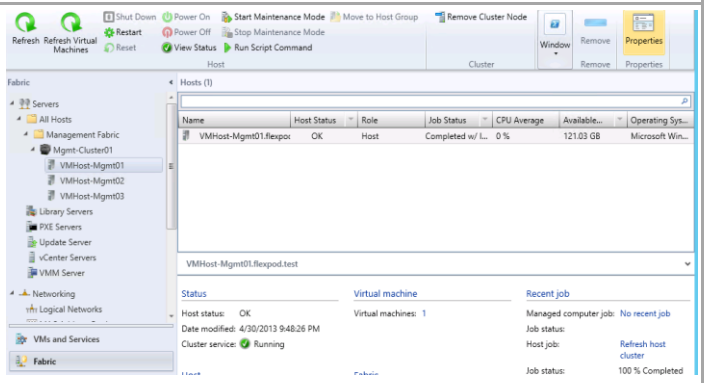
16.9 Creating the Logical Switch on the Hyper-V Hosts

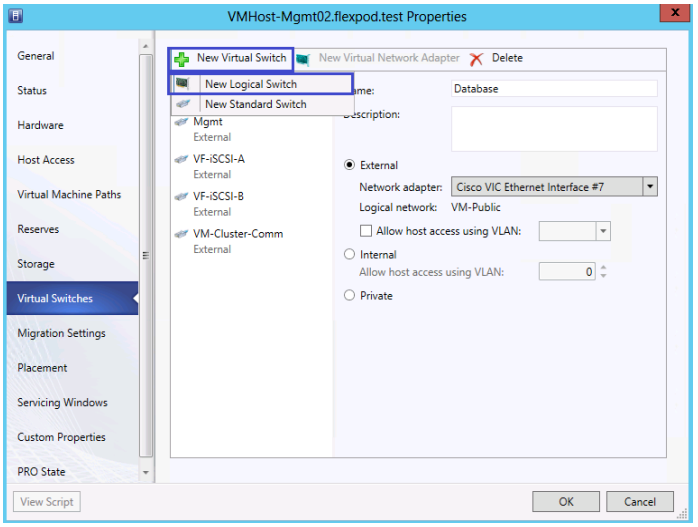
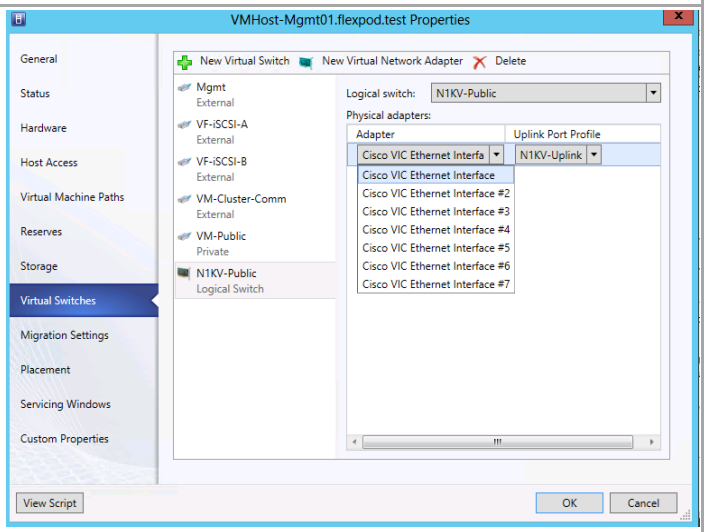
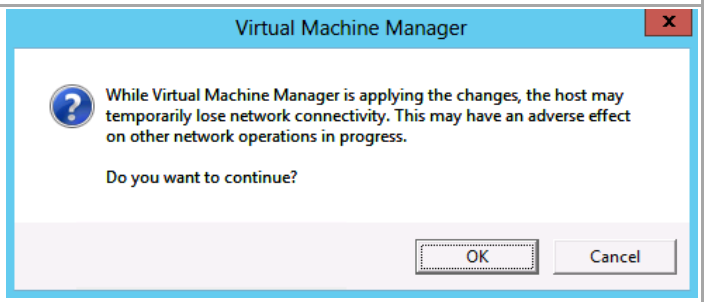
▶ Perform the following procedure on each Management Fabric Cluster node.

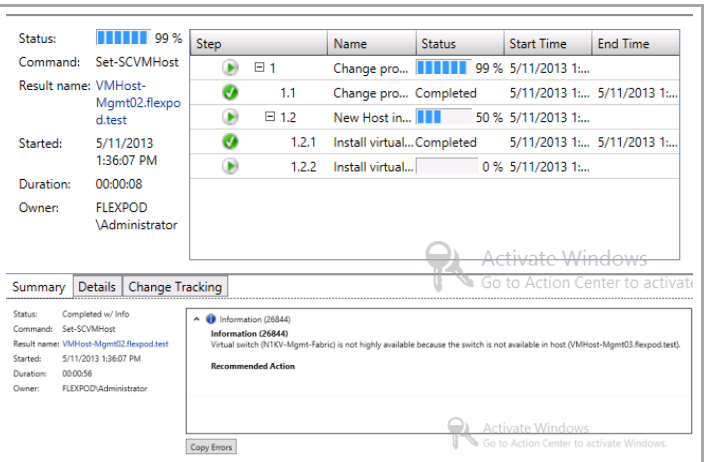
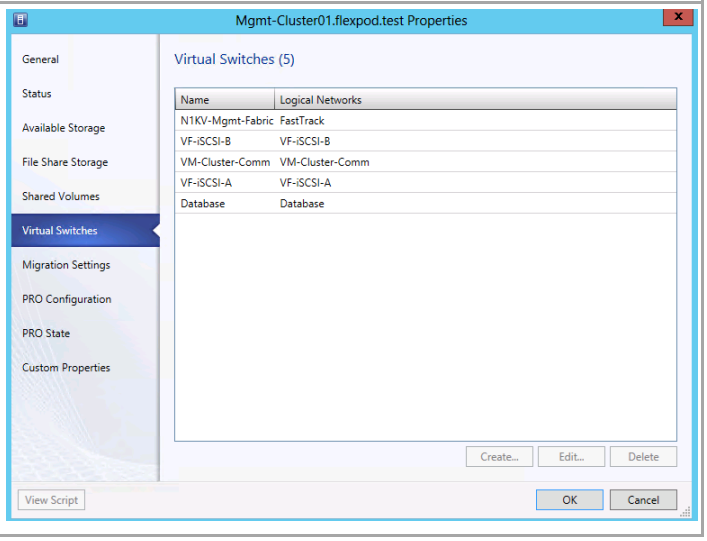
1. In the active Virtual Machine Manager instance, select Fabric. Expand All Hosts and Management Fabric.



2. Select the first management fabric host and click **Properties**.



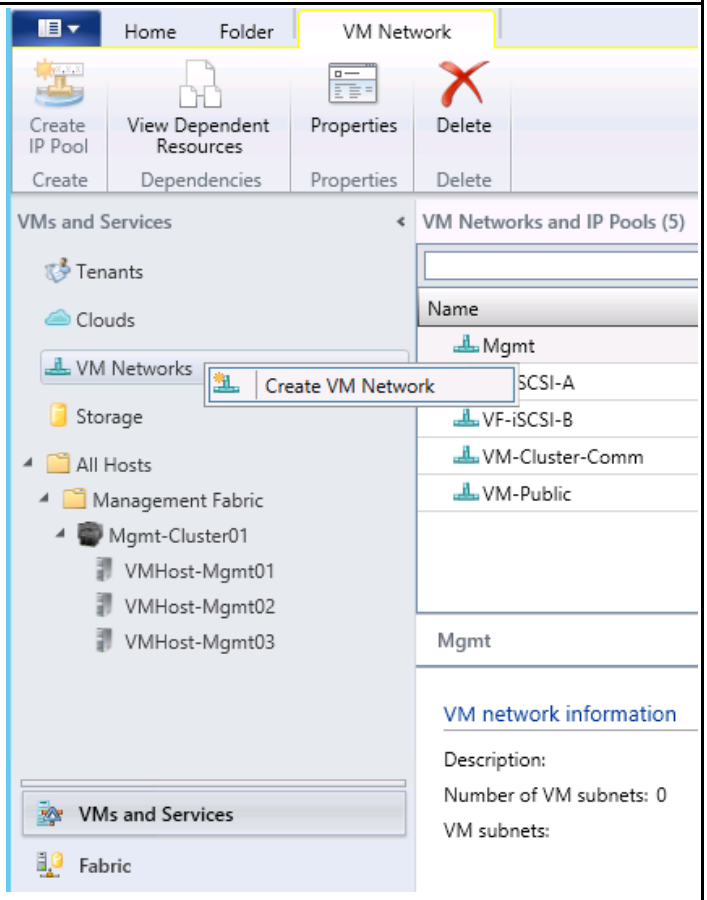
3. Select Virtual Switch in the left pane and New Virtual Switch. Select New Logical Switch.	
4. Select the new logical switch in the middle pane and in the right pane select the Ethernet adapter for the N1KV-Mgmt-Fabric network. Click OK.	
5. Click OK to invoke the configuration change. 6. Repeat this procedure on the remaining management fabric hosts.	

7. Click Jobs and monitor the job progress. The job will complete with info until the logical swith is installed on all of the hosts in the cluster. 8. Repeat this procedure on all cluster nodes.	
9. Open the Mgmt-Cluster01 properties and verify that the N1KV-Mgmt-Fabric Switch is in the list of switch installed on all cluster nodes.	

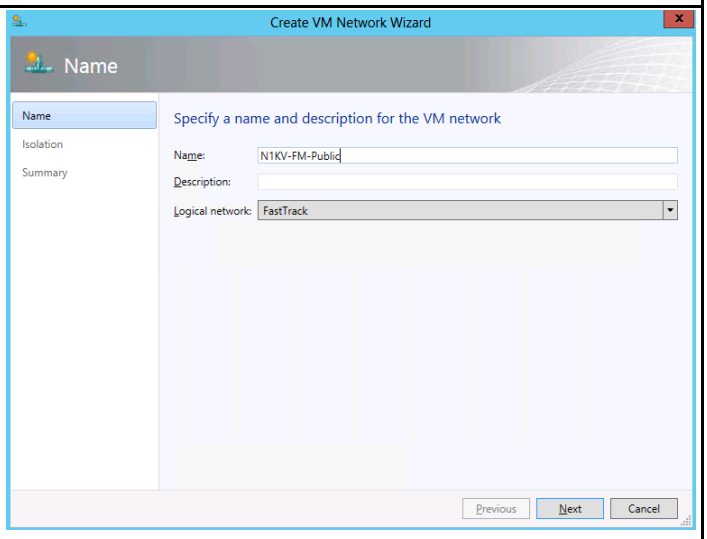
16.10 Create a VM Network

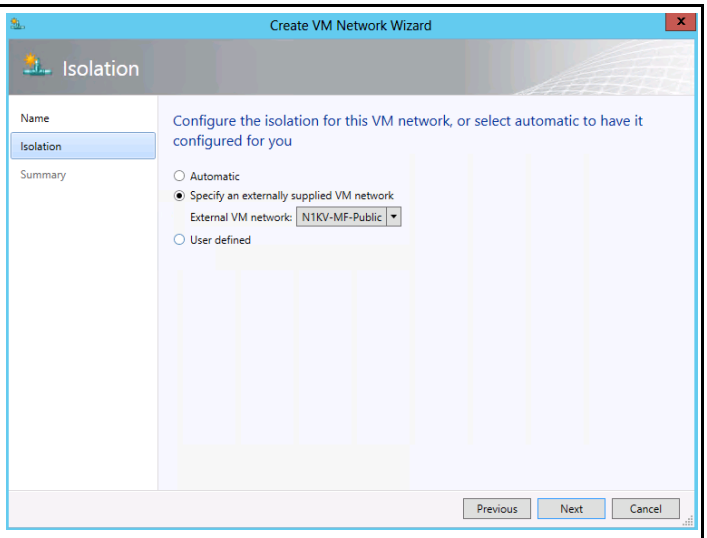
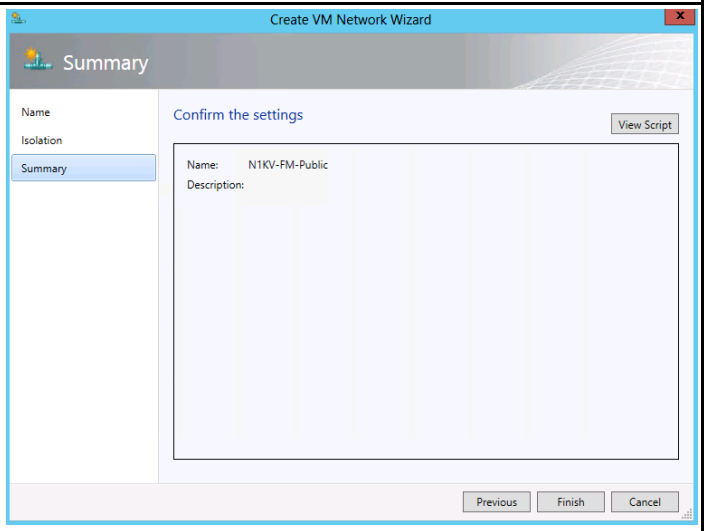
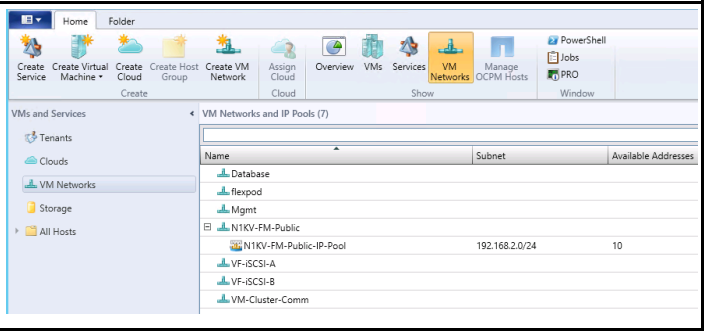
▶ Perform the following procedure.

1. In Virtual Machine Manager, select VMs and Services. Right-click VM Networks and click Create VM Network.



2. Enter the network name. Verfy that the logical network FastTrack is selected and click Next.

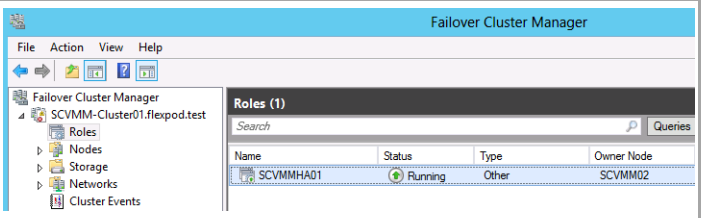


3. In the Isolation window, select Specify an externally supplied VM Network and select the External VM network N1KV-MF-Public. Click Next.	
4. In the Summary window, click Finish.	
5. The VM Network is created.	

16.11 Configure the Virtual Machine Manager Virtual Manchine Properties

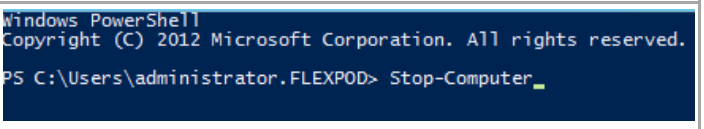
▶ Perform the following steps on the Virtual Machone Manager virtual machine.

1. Login to the first Virtual Machine Manager virtual machine. Using Failover Cluster Manager 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.



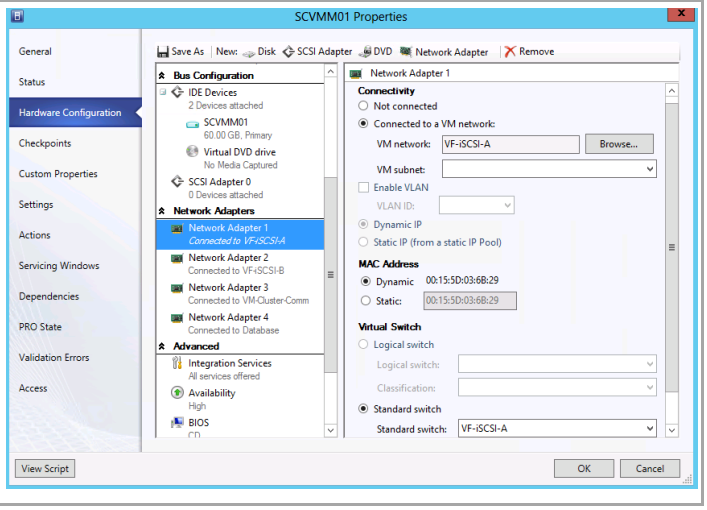
2. Shutdown the first Virtual Machine Manager virtual machine by running following powershell command:

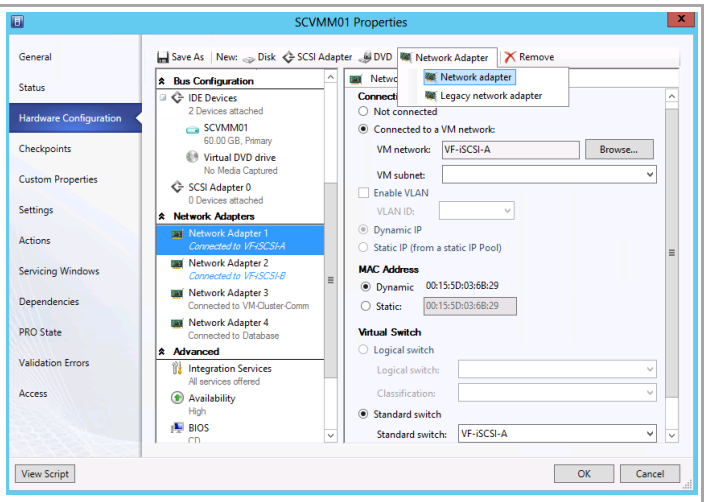
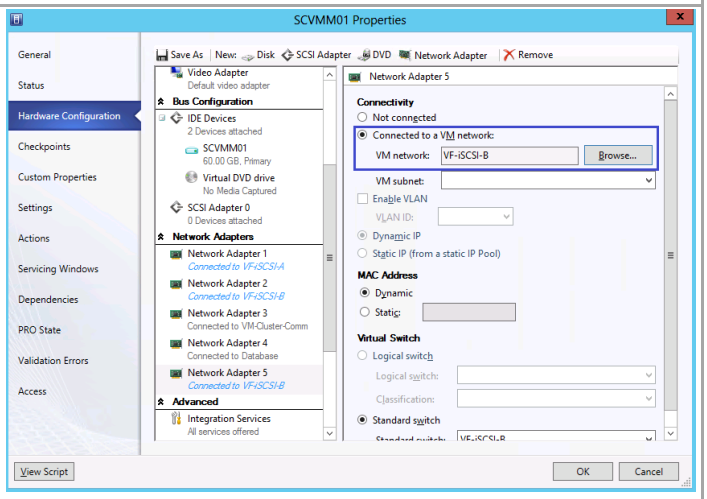
Stop-computer

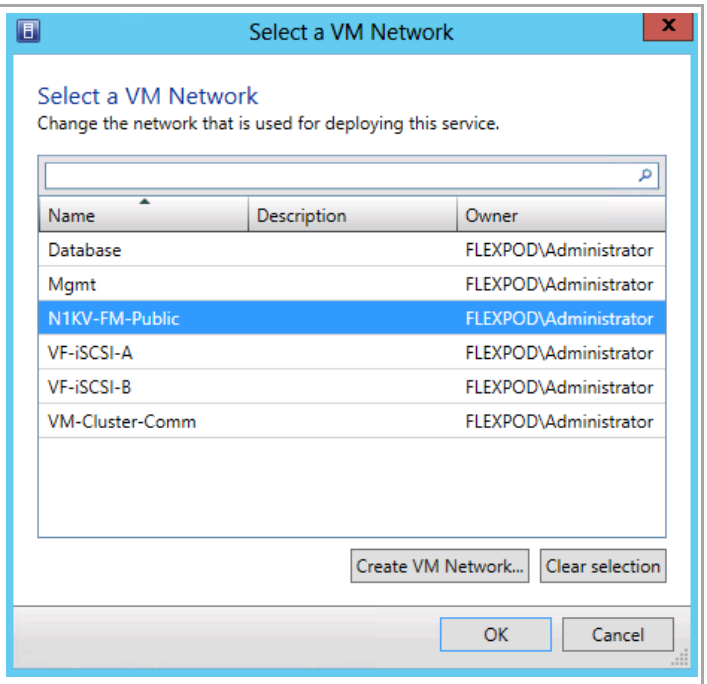
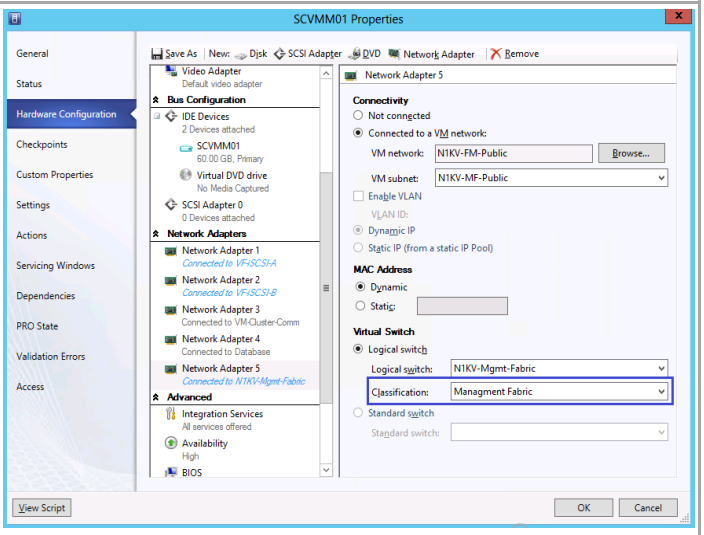
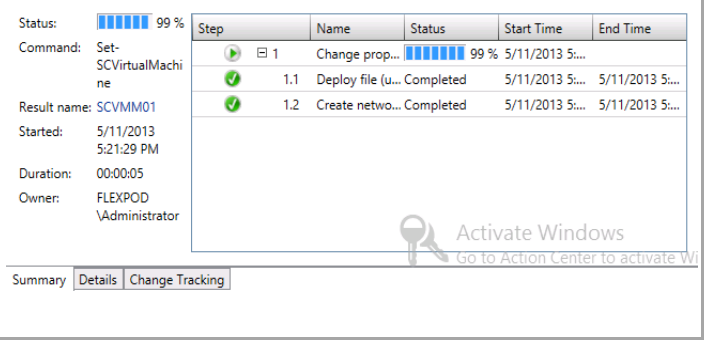


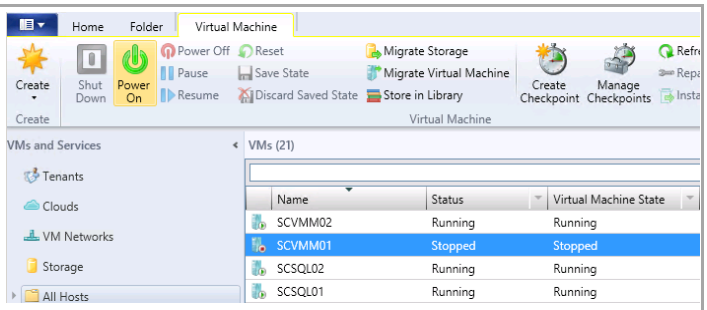
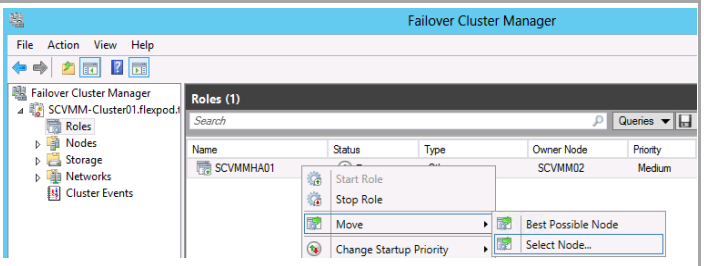
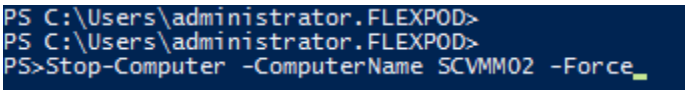
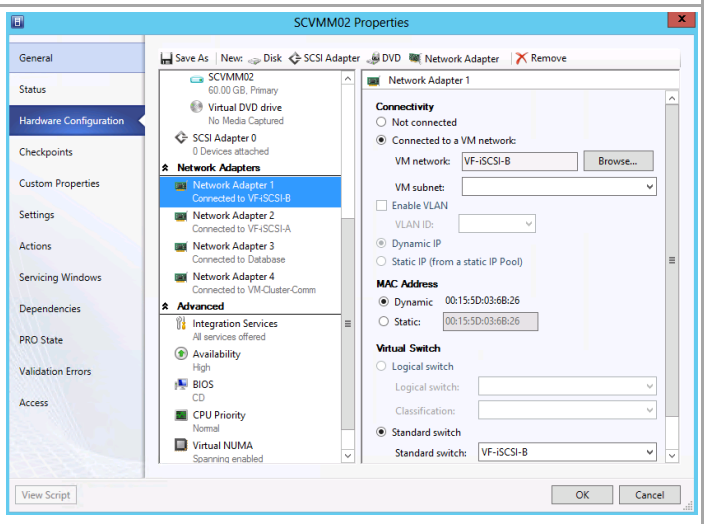
3. Log into the second Virtual Machine Manager virtual machine and start the Virtual Machine Manager console. Select VMs and Services. Click all hosts. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select properties.

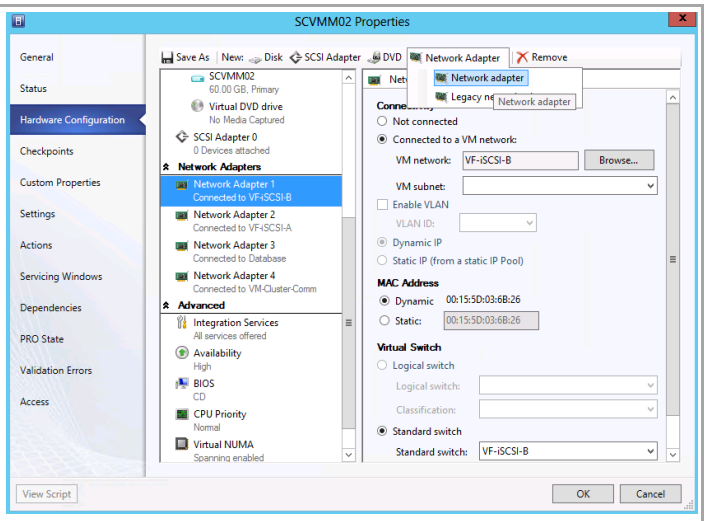
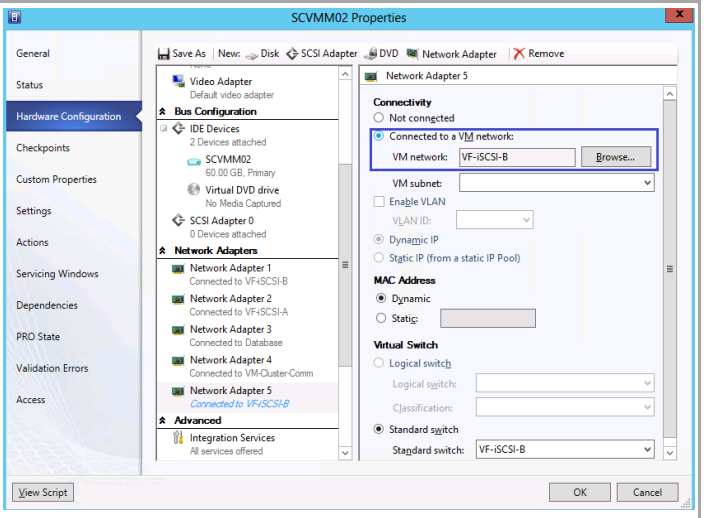
4. Select Hardware Configuraiton in the left pane and scroll down to the Network adapaters in the middle pane. Verify the all adapaters have the correct VM Networks specified. If any VM networks are listed as Not Specified, click browes and select the correct VM Network.



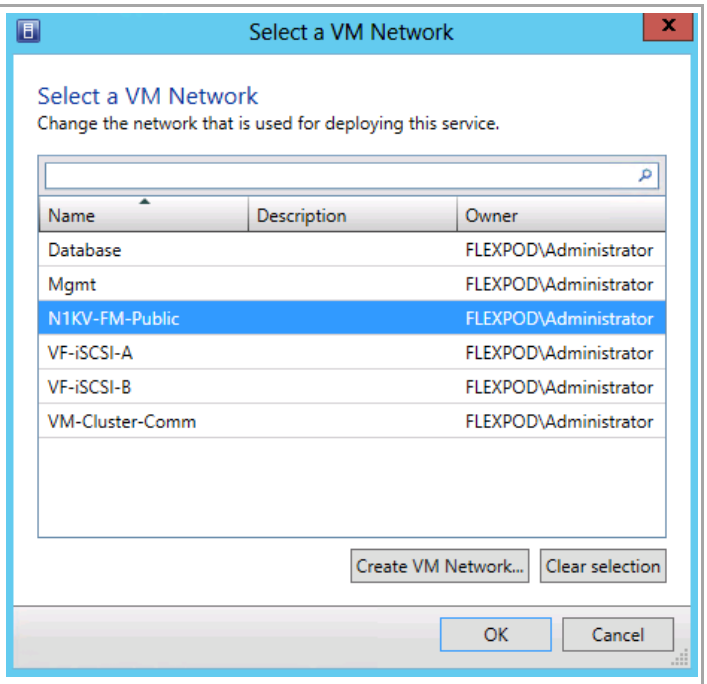
	
5. Select Connect to VM network radial button and click Browse.	

6. Select the N1KV-FM-Public VM Network and click OK.	
7. Select the Management Fabric Classification in the dropdown text box and click OK.	
8. Select Jobs and monitor the job completion progress.	

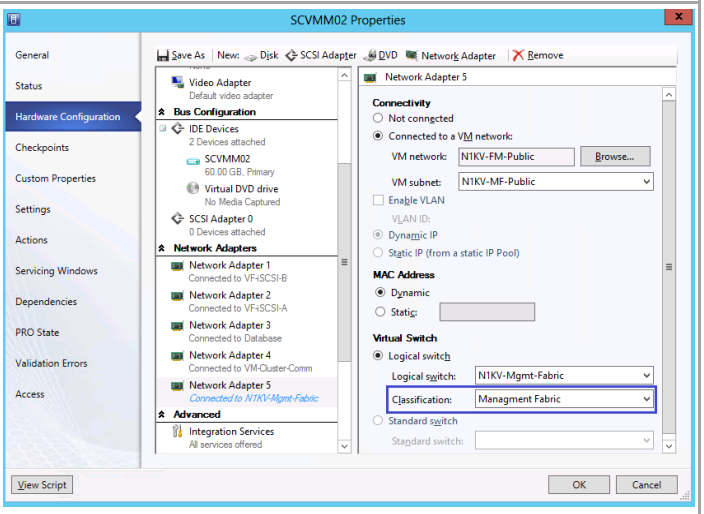
9. Start the Virtua Machine Manager virtual machine.	
10. Login to the first Virtual Machine Manager virtual machine. Using Failover Cluster Manager, move the Virtual Machine Manager instance to the first node.	
	
11. Start the Virtual Machine Manager console. Select VMs and Services. Clickall hosts. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select properties.	
12. Select Hardware Configuraiton in the left pane and scroll down to the Network adapaters in the middle pane. Verify the all adapaters have the correct VM Networks specified. If any VM networks are listed as Not Specified, click Browse and select the correct VM Network.	

	
13. Select Connect to VM network radial button and click Browse.	

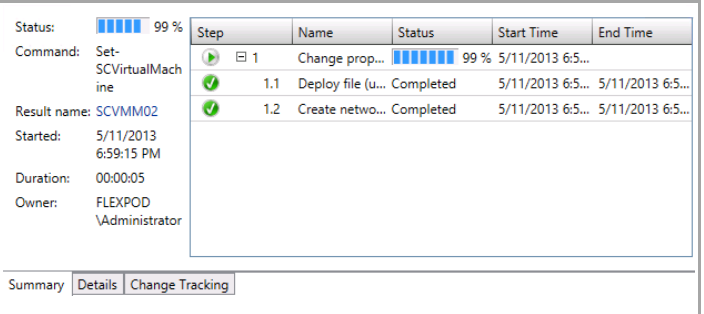
14. Select the N1KV-FM-Public VM Network and click OK.

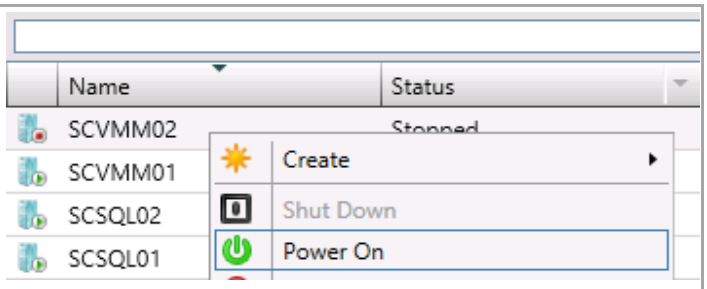
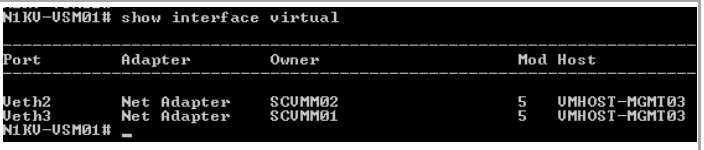


15. Select the Management Fabric Classification in the drop-down text box and click OK.



16. Select Jobs and monitor the job completion progress.

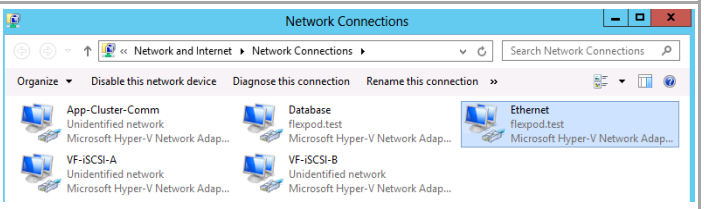


17. Start the second Virtual Machine Manager virtual Machine.	
18. Login to the Cisco Nexus 1000V VSM and verify that the virtual adapaters are connected to the Virtual Machine Manager virtual machines. 19. Show interfrace virtual.	

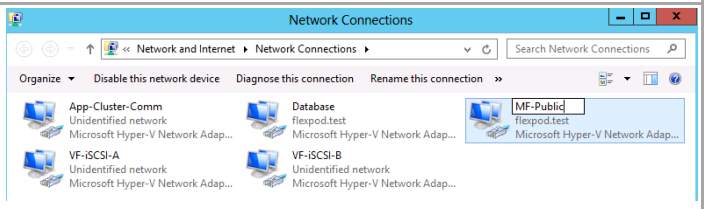
16.12 Configure Virtual Machine Manager Network Interfaces

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

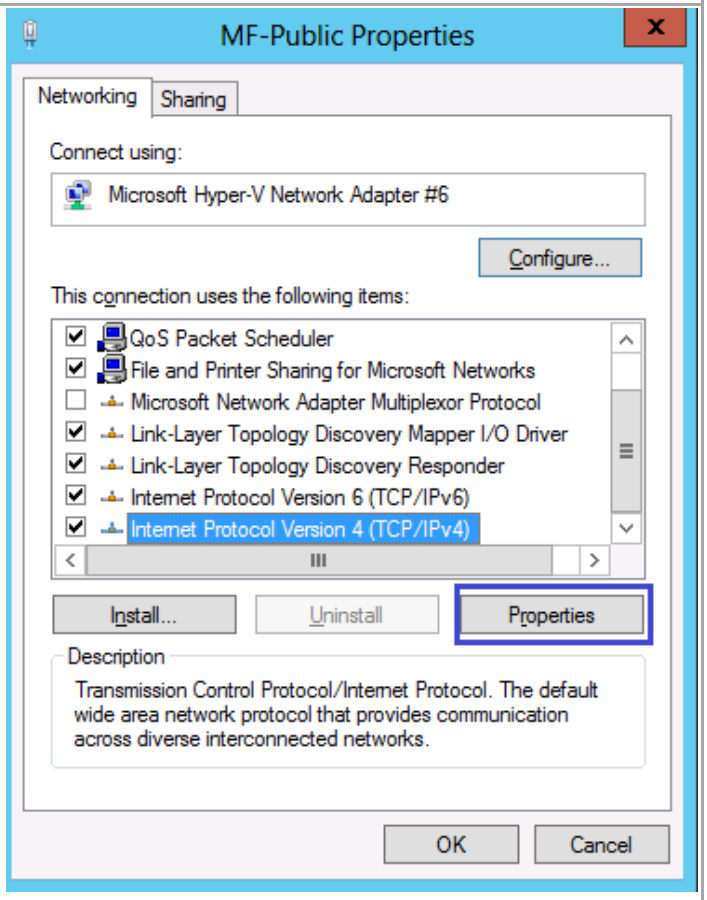
1. Open Network Connections.



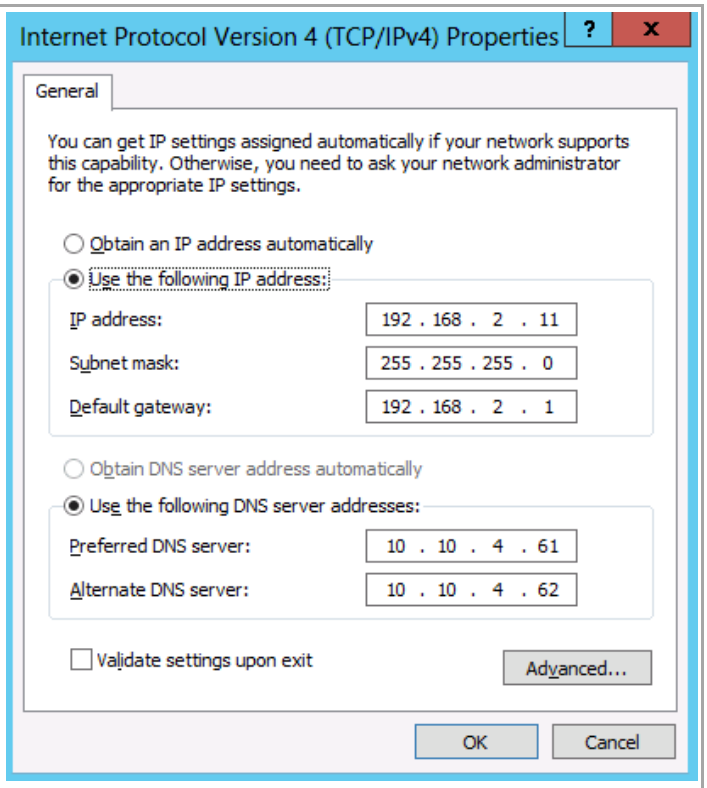
2. Rename the new network interface to match the network infrace connection.



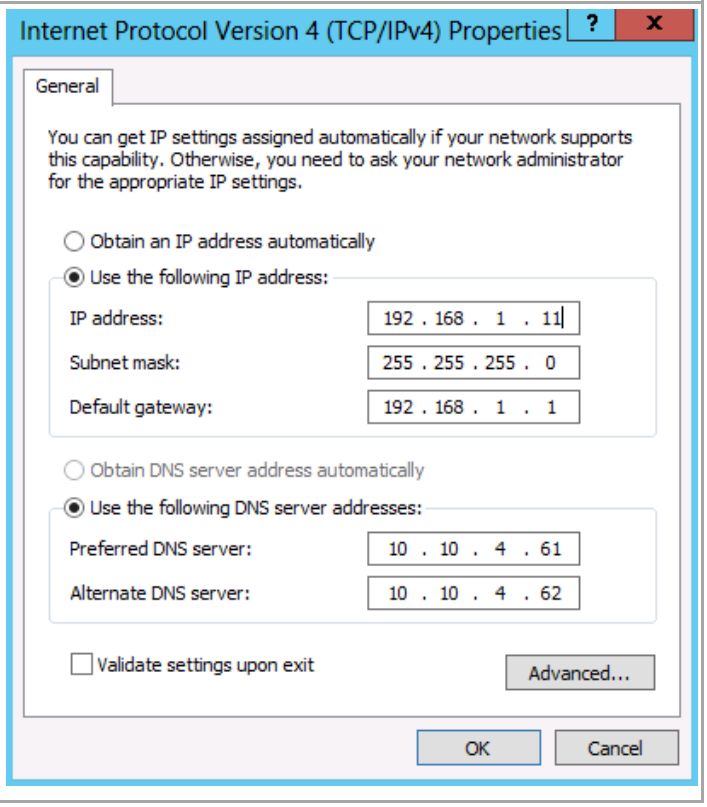
3. Right-click on the new network interace, select properites. Select the TCP/IPv4 item and click Properties.



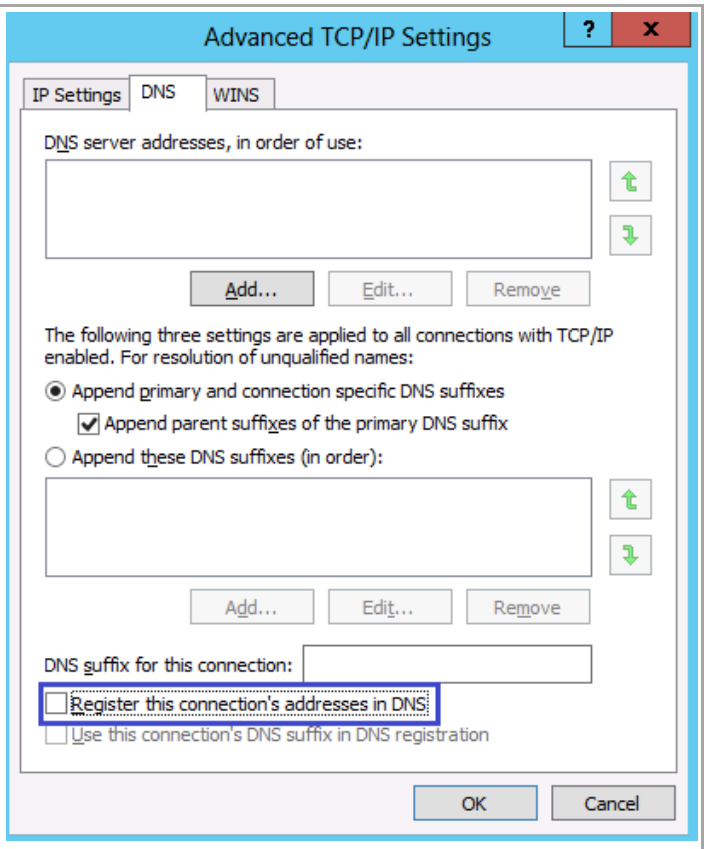
4. Configure the TCP/IP perperties. Specify the IP Address, Subnetmask, Default gateway, and Prefered DNS servers. Click OK to save changes.



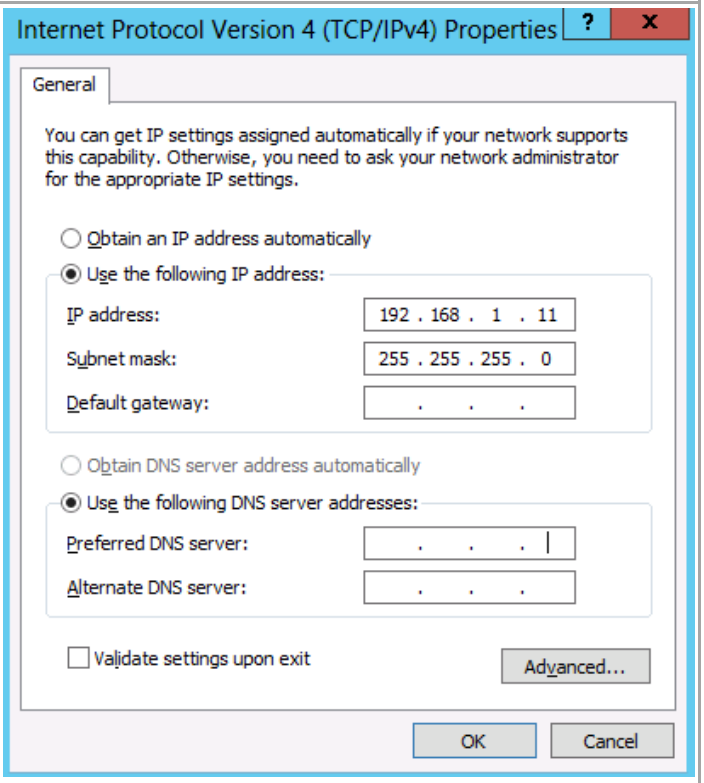
5. Right-click on the previously created **Databases** network interace, select properites and click Advanced...

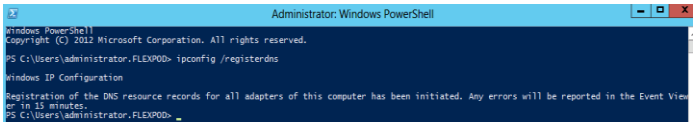


6. Select the DNS tab. Uncheck Register this connection's address in DNS. Click OK to save the configuration.

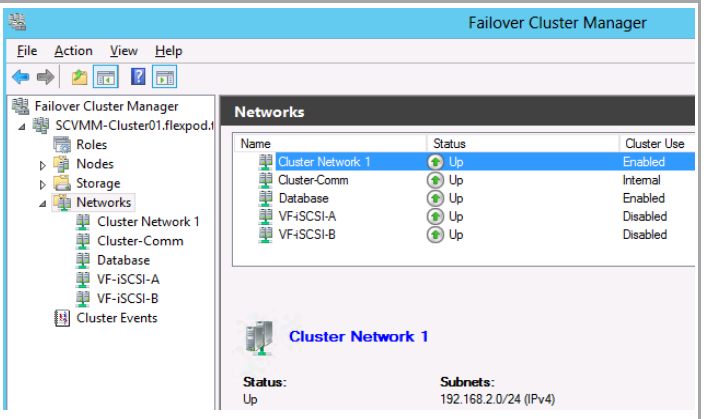
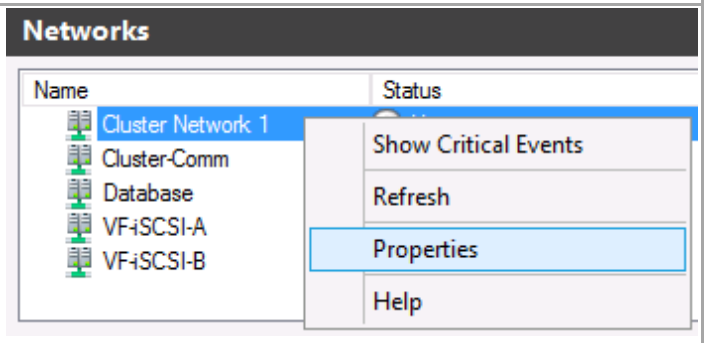


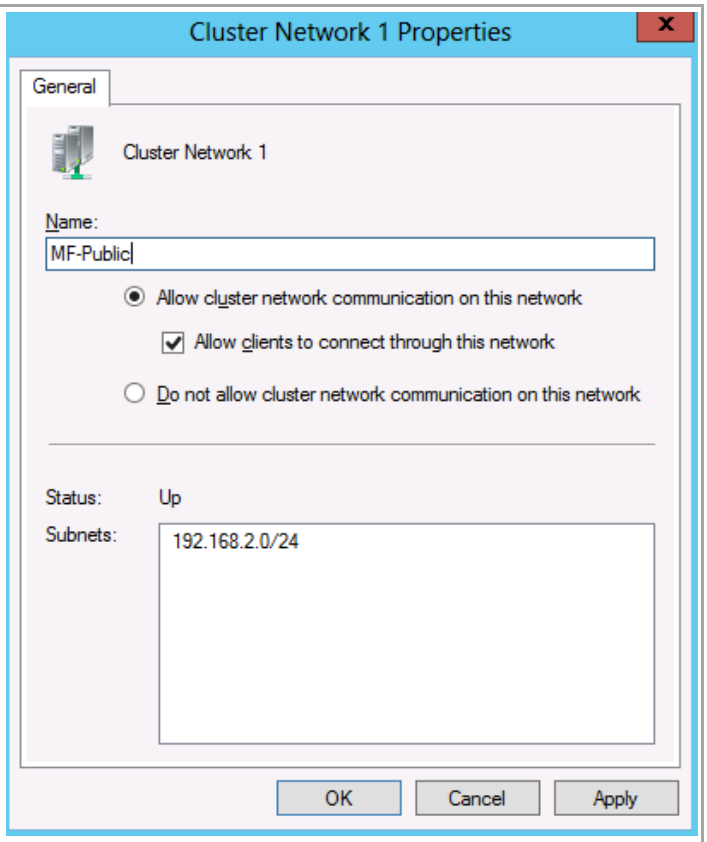
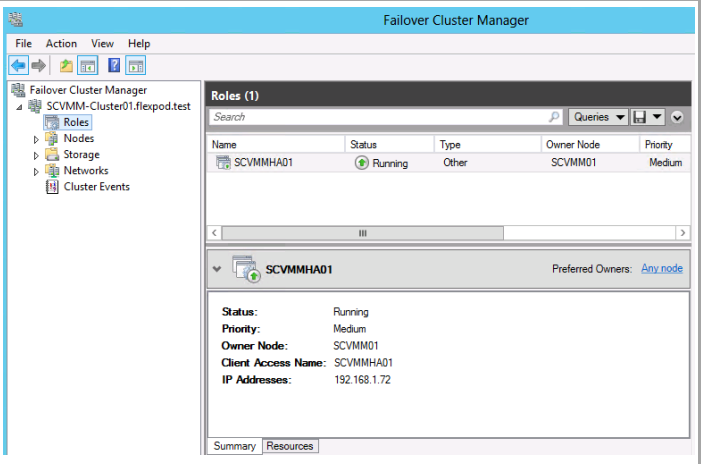
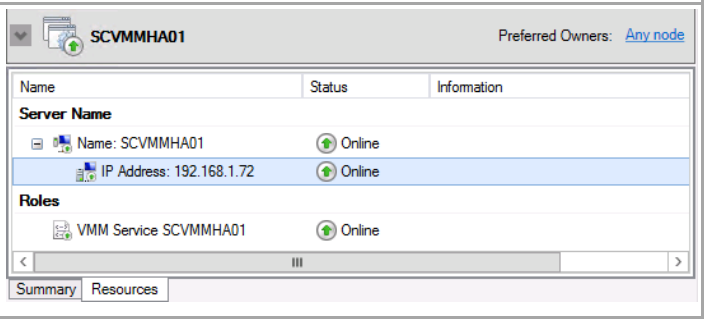
7. In the general IPv4 TCP/IP oproperties clear the default gateway and perfered DNS entries. Click OK to save the changes.

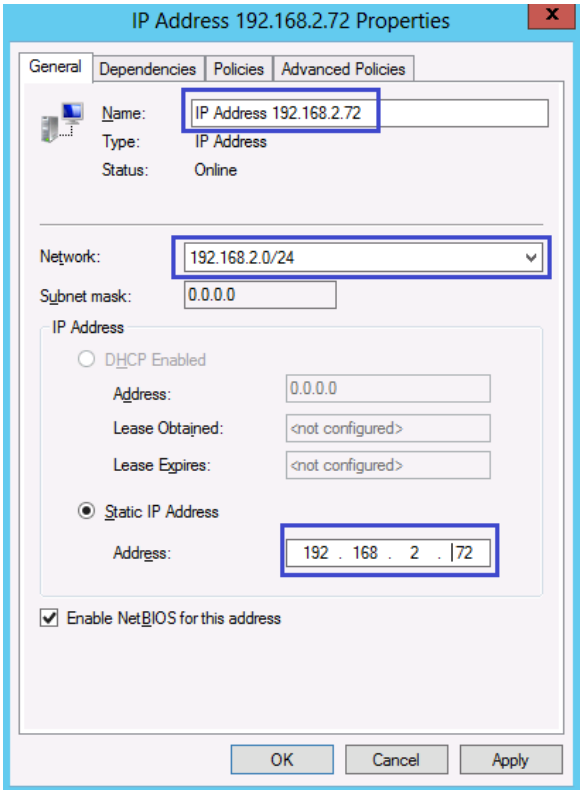


8. Open a command prompt. Run the following command: Ipconfig /registerdns	

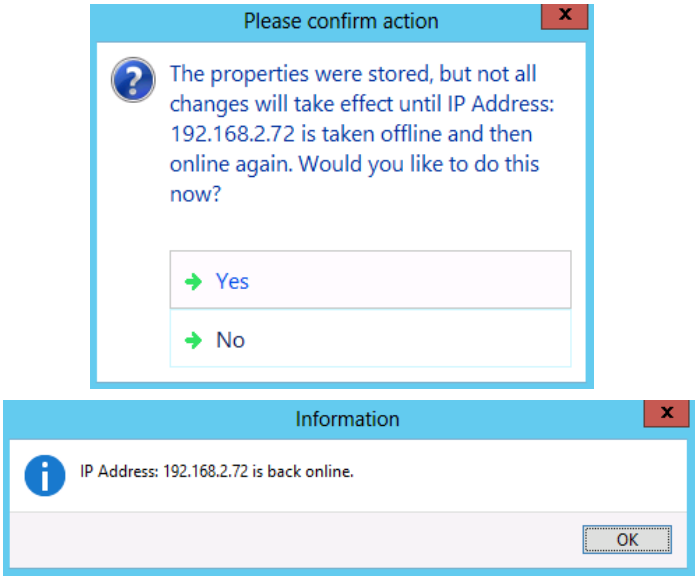
16.13 Rename the New Cluster Network

▶ **Perform the following operation on both Virtual Machine Manager virtual machines.**	
1. Open Failover Cluster Manager. Select the Virtual Manchine Manager Cluster and expand the Networks object.	
2. Right-click Cluster Network 1 and open Properties.	

3. **Rename** the network name to match the connected network. Click **OK** to save changes.	
4. Select Roles in the left pane and select the highly available Virtual Machine Manager instance in the top middle pane.	
5. In the middle lower pane click the resource tab and double-click the IP address to open its Properties page.	

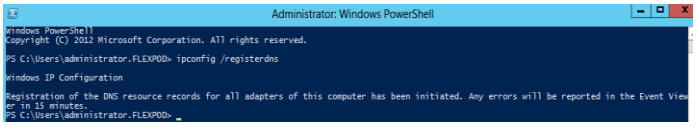


6. Click Yes to take the IP Adress resource offline, apply the changes. Click OK to bring the IP Address resource back online.

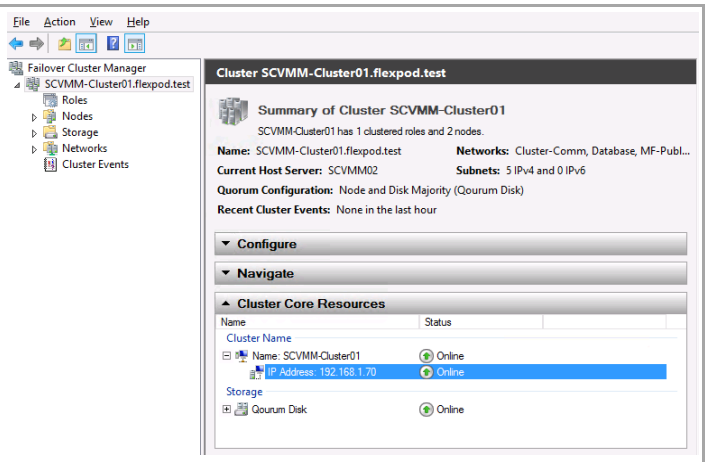


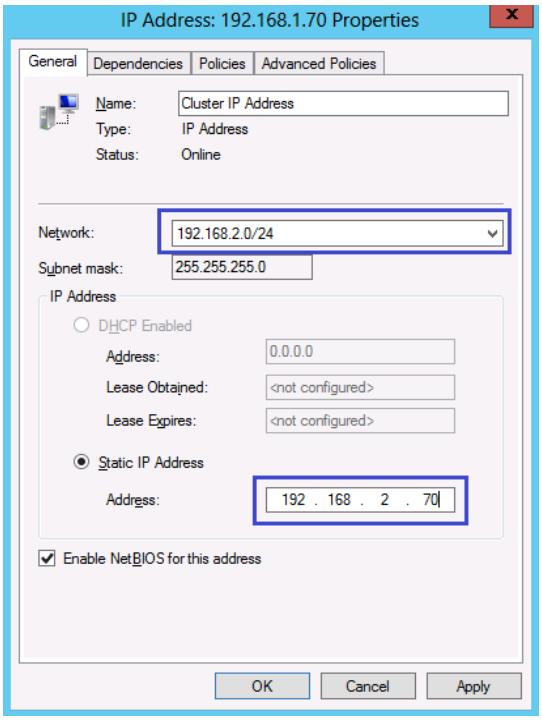
7. Open a command prompt. Run the following command.

Ipconfig /registerdns



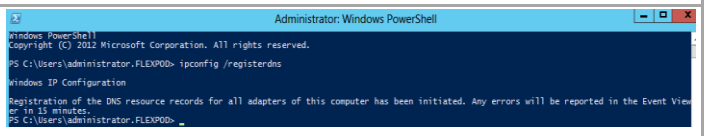
8. Select the Virtula Machine Manager cluster in the top left pane and double click the cluster core resource IP Address to open its property page.





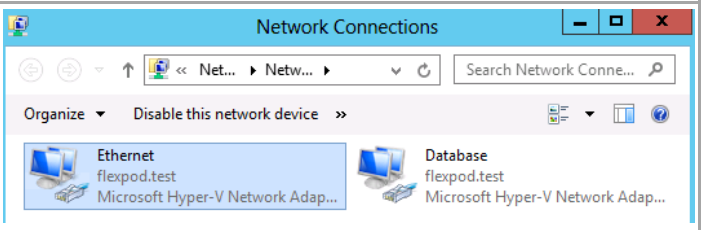
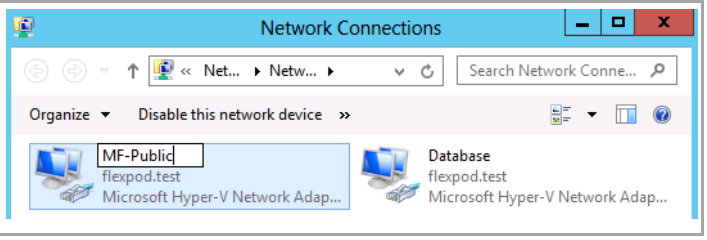
9. Allow the IP Address resource to be brought offine. Bring the IP Address resource back online.
10. Open a command prompt. Run the following command:

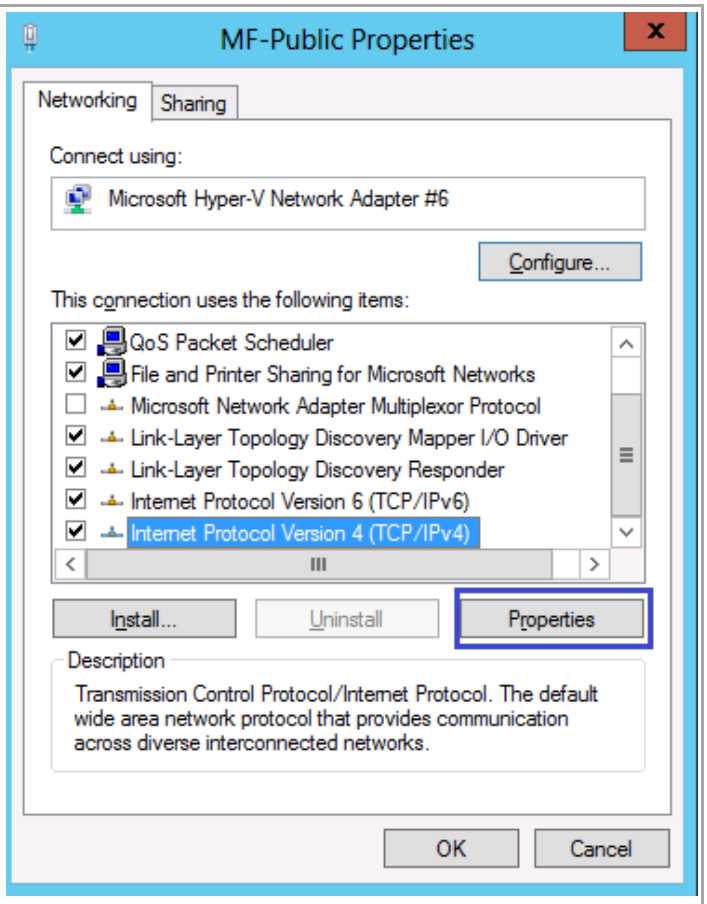
Ipconfig /registerdns

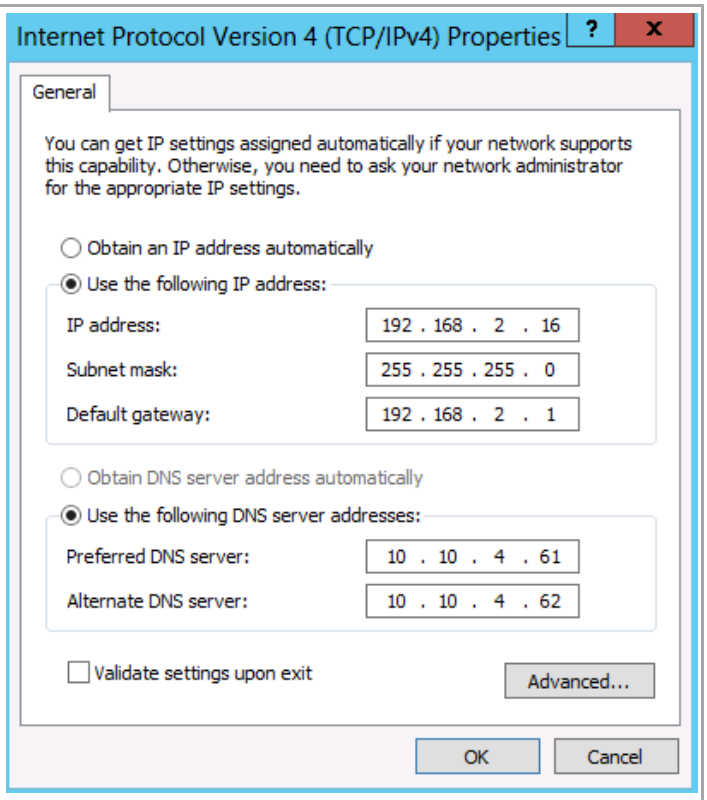
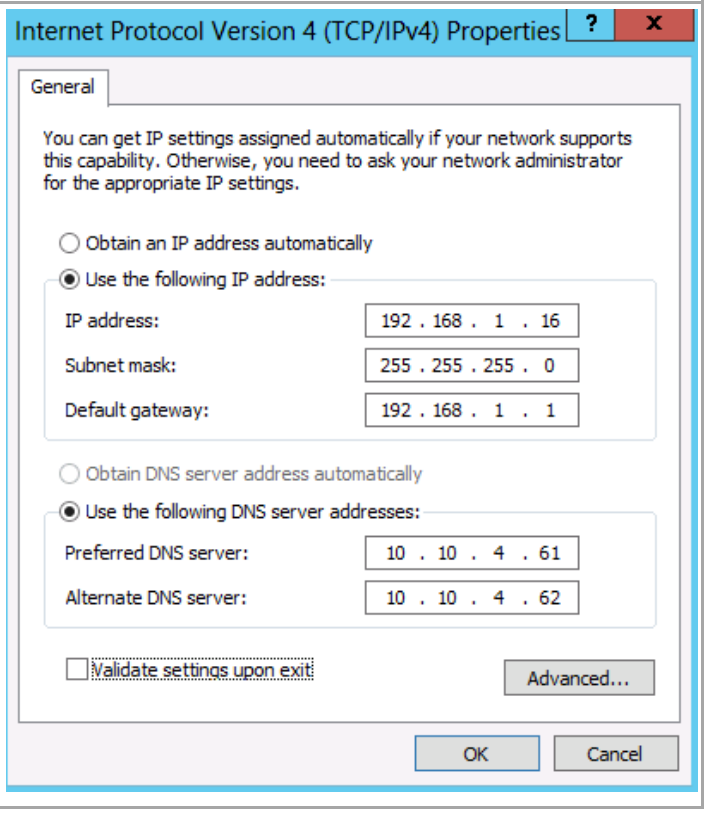


16.14 Configure System Center Application Virtual Machine Network Interfaces

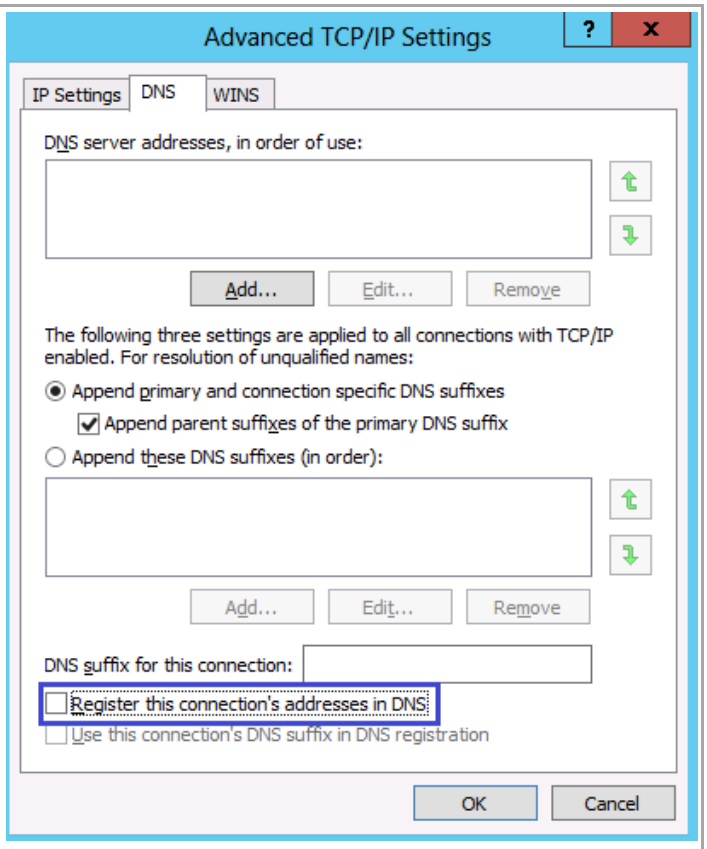
- **Perform the following operation on the following System Center virtual machines.**
  - Operations Manager
  - Operations Manager Reporting Services
  - Service Manager
  - Orchestrator
  - Application Controller

1. Open Network Connections.	
2. Rename the new network interface to match the network infrace connection.	

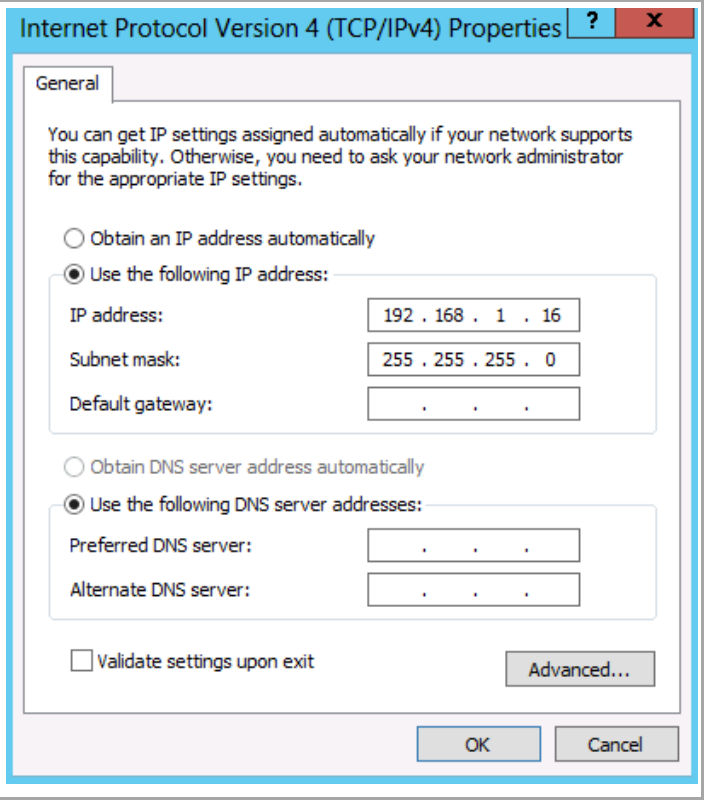
3. Right-click the new network interace, select Properites. Select the TCP/IPv4 item and click Properties.	

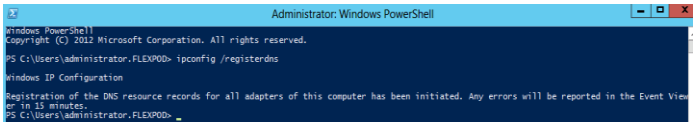
4. Configure the TCP/IP perperties. Specify the IP Address, Subnetmask, Default gateway, and Prefered DNS servers. Click OK to save changes.	
5. Right-click on the previously created **Databases** network interace, select properites and click Advanced...	

6. Select the DNS tab. Uncheck Register this connection's address in DNS. Click OK to save the configuration.



7. In the general IPv4 TCP/IP oproperties clear the default gateway and perfered DNS entries. Click OK to save the changes.



8. Open a command prompt. Run the following command: Ipconfig /registerdns	

17 Install and Configure the SMI-S Provider

17.1 Install the SMI-S Provider

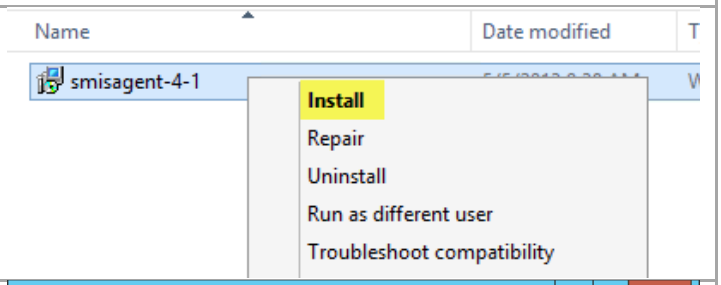
Complete the following steps to install the NetApp SMI-S provider.

- Download the installer from:

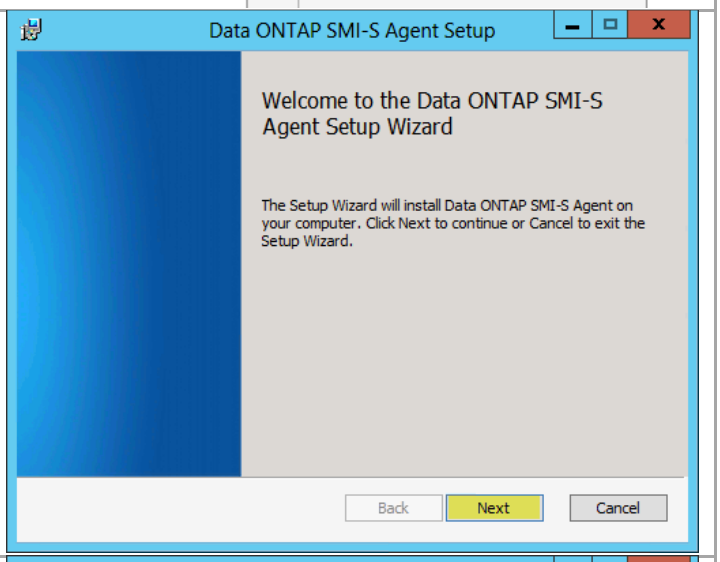
  http://support.netapp.com/NOW/download/software/smis/Windows/4.1/smisagent-4-1.msi.

▶ Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

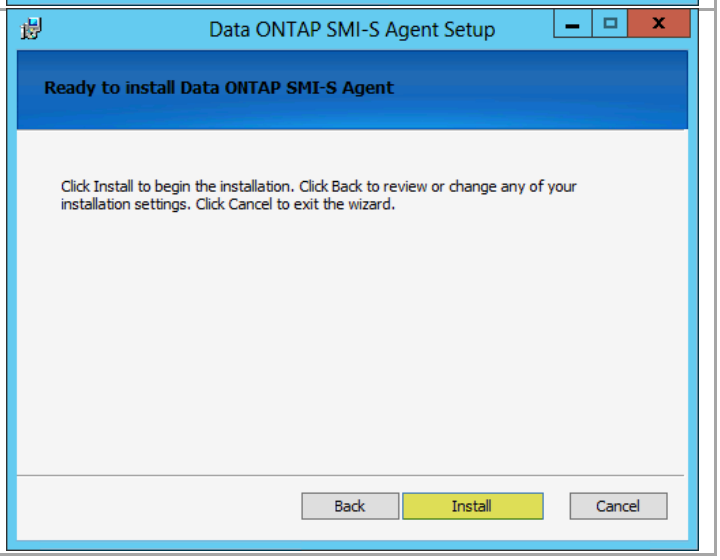
1. Right-click **smisagent-4-1** and select **Install** to begin setup.



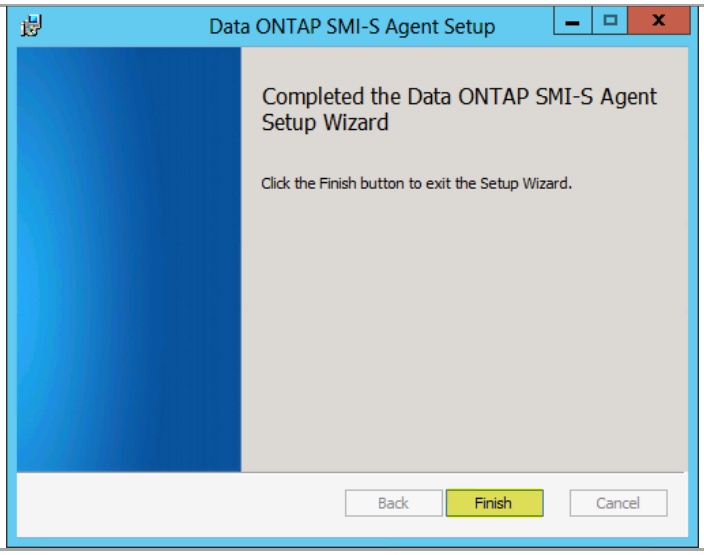
2. On the Welcome to the Data ONTAP SMI-S Agent Setup Wizard page, click **Next**.



3. On the Ready to install Data ONTAP SMI-S Agent page, click **Install**.



4. On the Completed the Data ONTAP SMI-S Agent Setup Wizard page, click **Finish** to complete the installation.

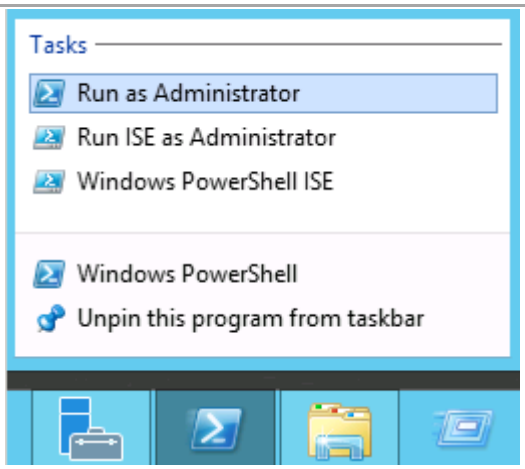


17.2 Configure the SMI-S Provider

Complete the following steps to configure the NetApp SMI-S provider.

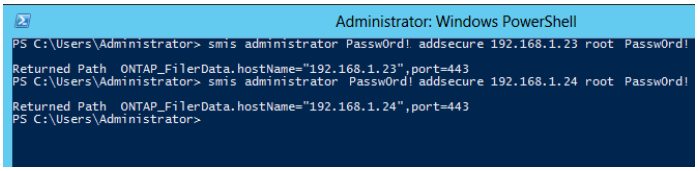
▶ Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

1. Launch a PowerShell prompt with administrative permissions: Right-click the PowerShell icon and select **Run as Administrator.**



2. Add both NetApp controllers to the SMIS configuration.

```
Smis <SMIUser> <SMISPass> addsecure
<controller ip address> <FASUser> <FASPass>
```

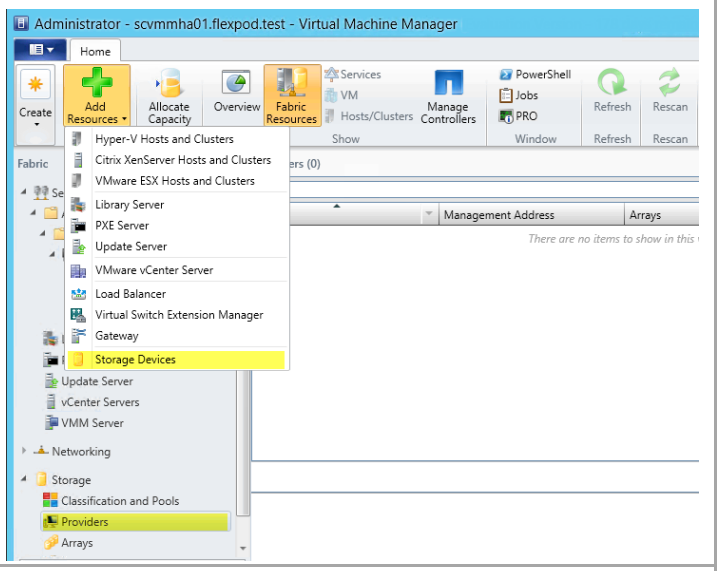


17.3 Register SMI-S in SCVMM

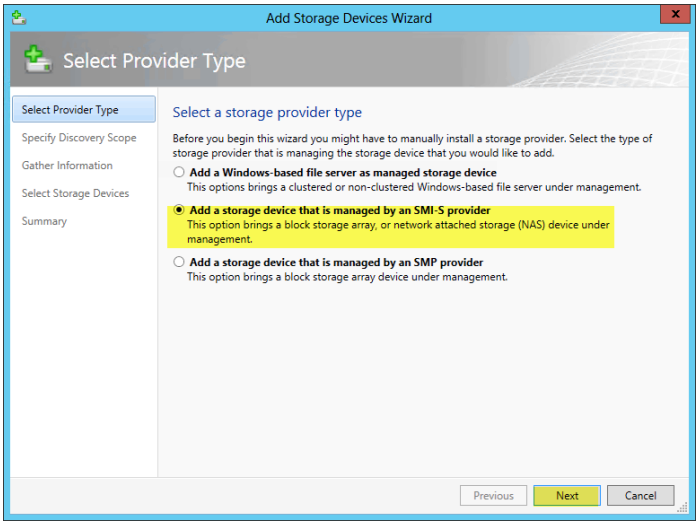
Complete the following steps to register the NetApp SMI-S provider in SCVMM.

▶ Perform the following steps on both **Virtual Machine Manger** virtual machine.

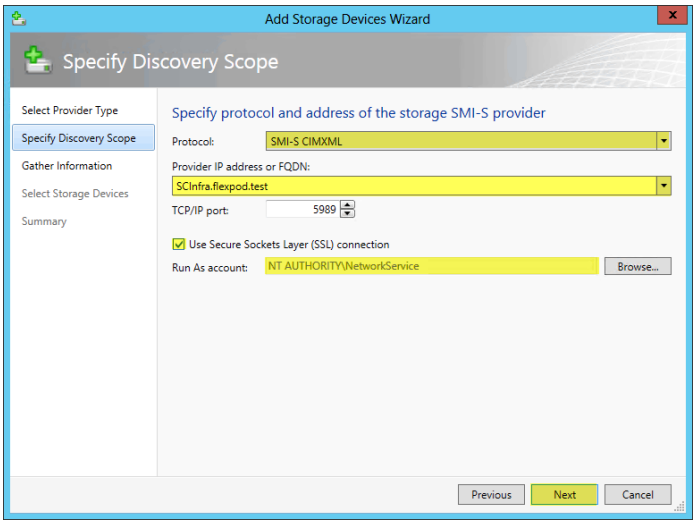
1. In the **Virtual Machine Manger** console, navigate to the **Fabric** pane and expand the **Storage** node. Select the **Providers** subnode.
2. From the ribbon, click **Add Resources** and select **Storage Devices** from the drop-down list.



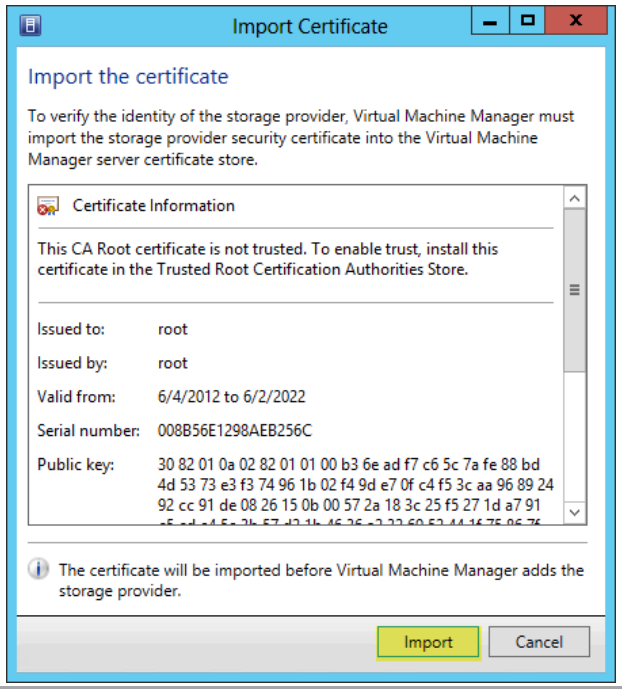
3. In the Add Storage Devices Wizard, select **Add a storage device that is managed by an SMI-S provider** and click **Next**.



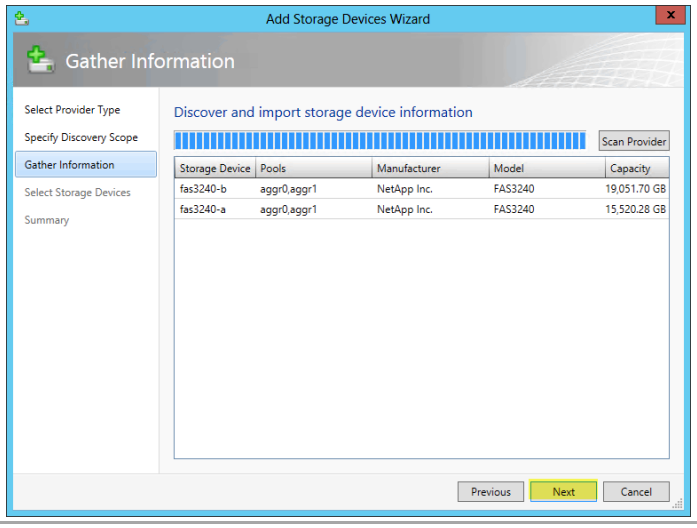
4. On the Specify Discovery Scope page.:
    a. Select **SMI-S CIMXML** for the protocol.
    b. Enter the **IP** or **FQDN** for the SMI-S provider.
    c. Select the **Use Secure Sockets Layer** checkbox.
    d. Click **Browse,** and in the resulting pop-up select **NT AUTHORITY\NetworkService.**
5. Click **Next**.



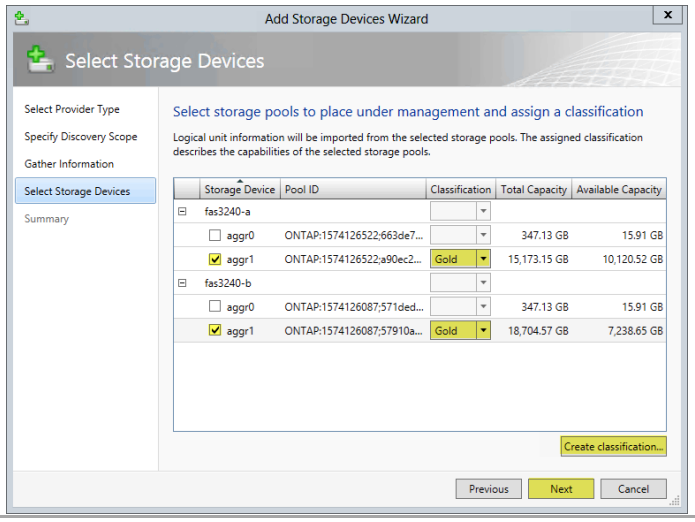
6. During the discovery phase, a pop-up opens asking to import the SMI-S provider security certificate.
7. Click **Import**.



8. When discovery is complete, the wizard shows every storage controller that is registered with the SMI-S provider.
9. Click **Next**.

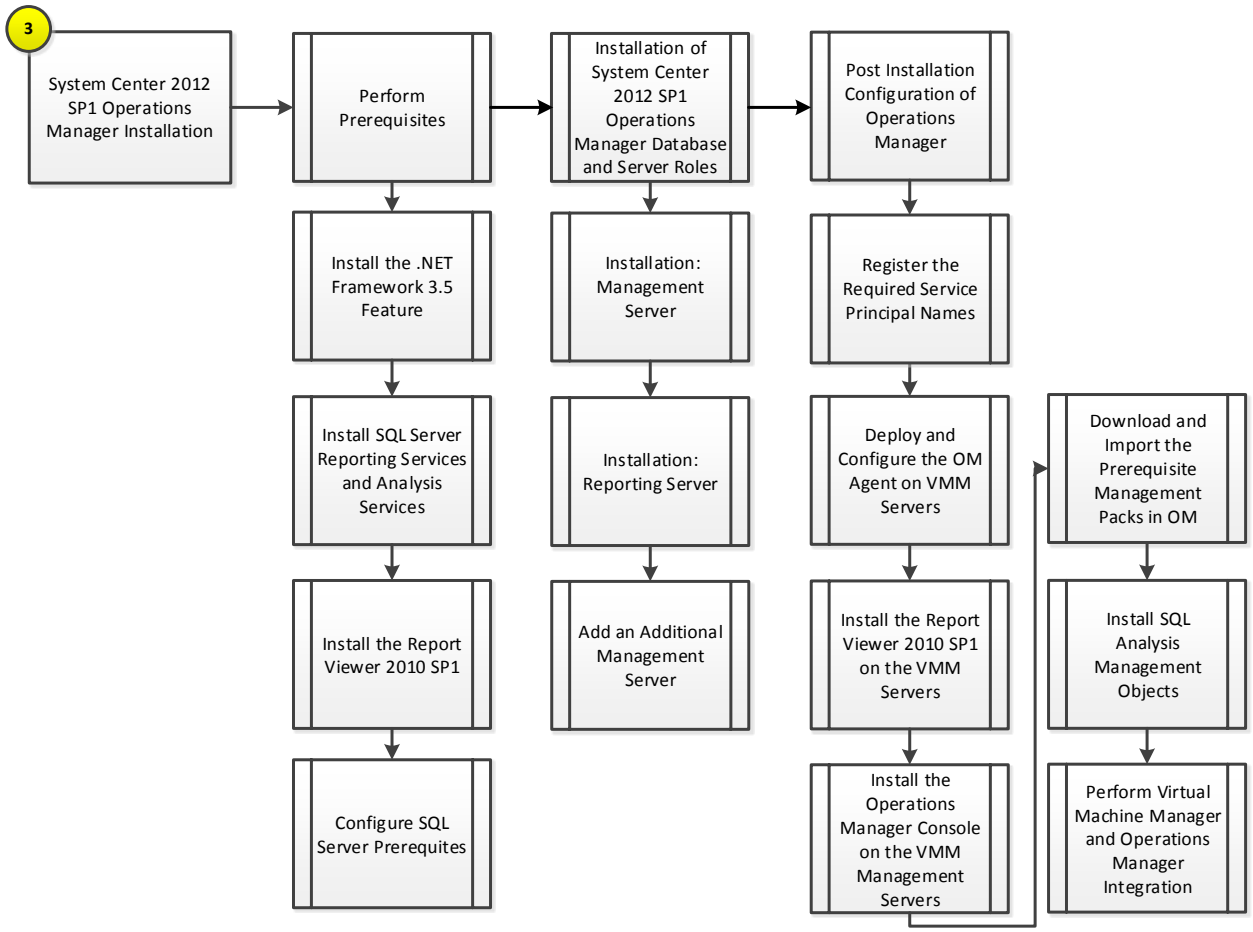


10. On the Select Storage Devices page.:
    a. Click the **Create Classification** button. In the resulting pop-up, enter a name for the storage pool.
    b. Select **aggr1** on both storage controllers and set the **classification**.
    c. Click **Next** and then close the wizard.



18 Operations Manger

The Operations Manager installation process includes the following high-level steps:



18.1 Overview

This section provides high-level walkthrough on deploying Operations Manager into the 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.

18.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created:[9]

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:

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 Operations Manager computer account <DOMAIN>\FT-VMM-SVC

[9] Specific rights for Operations Manager are outlined in http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin.

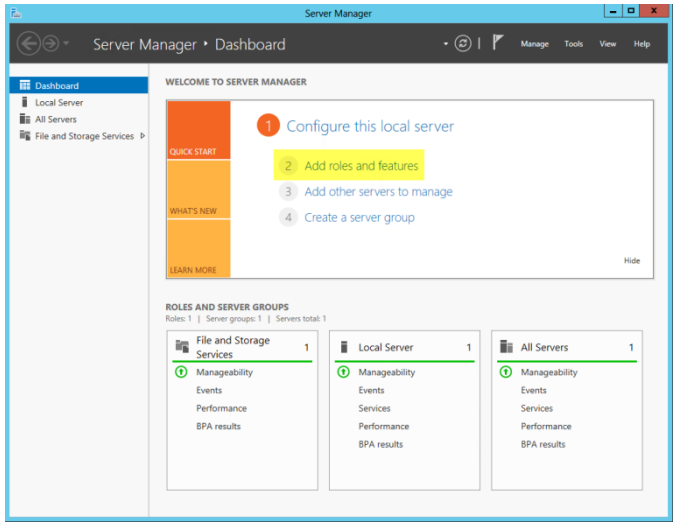
Security group name	Group scope	Members
<DOMAIN>\FT-OM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>\FT-OM-AdvOperators	Global	Operations Manager Advanced Operators privileged admin accounts

Add the .NET Framework 3.5 Feature

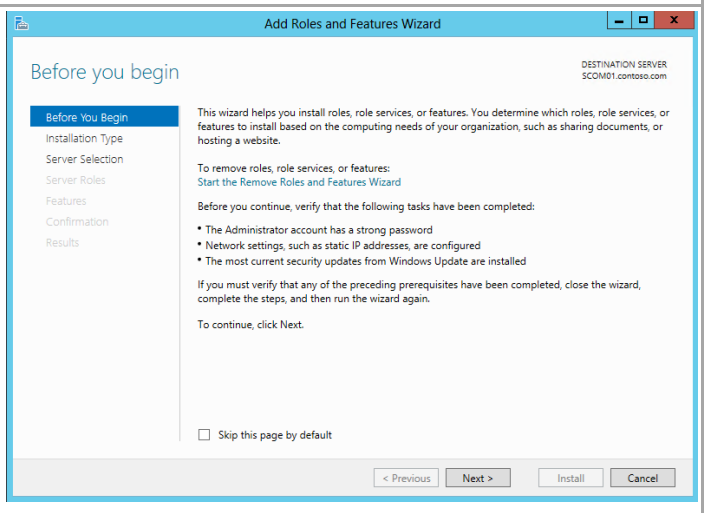
The Operations Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on all **Operations Manager** virtual machines.

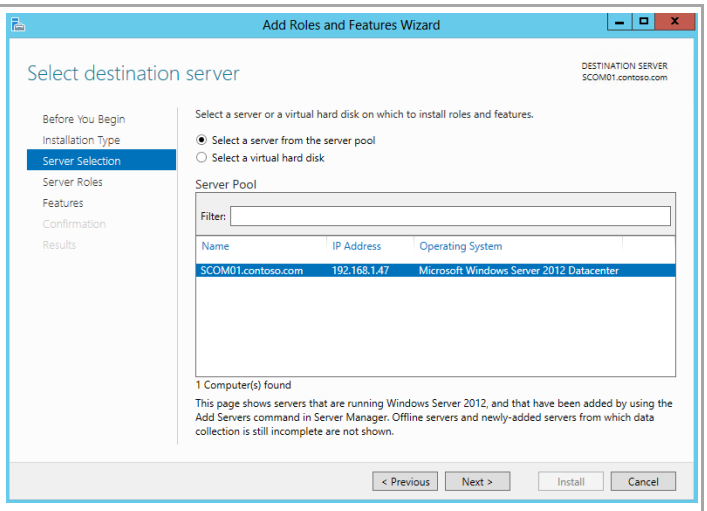
1. Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



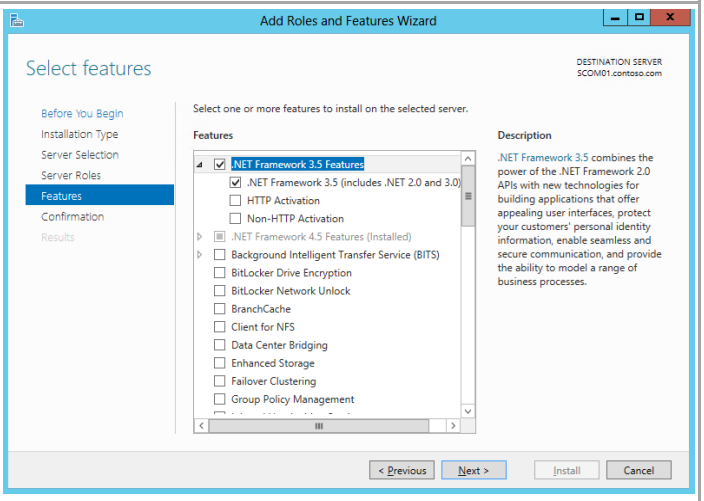
2. The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



3. 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.

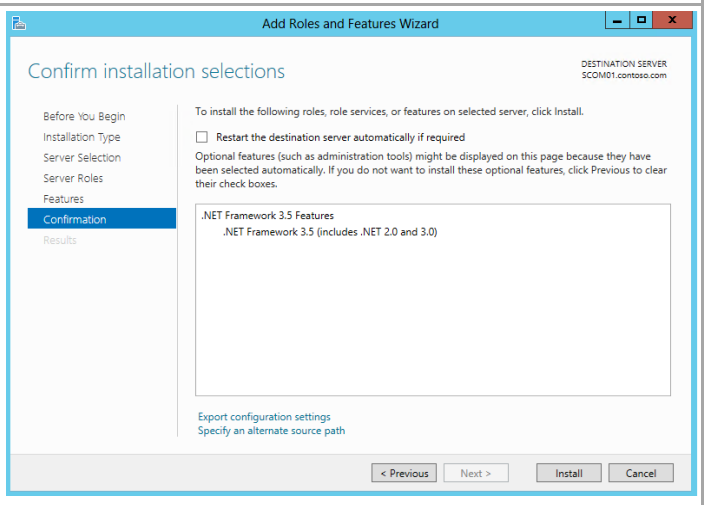


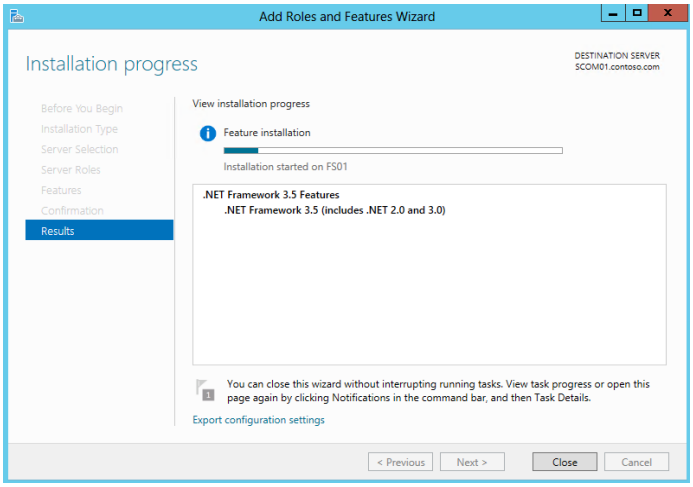
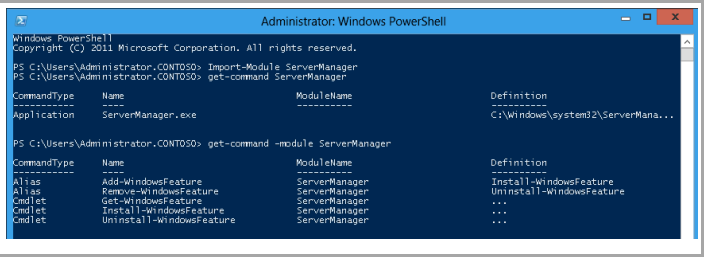
4. To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



5. 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. When exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.



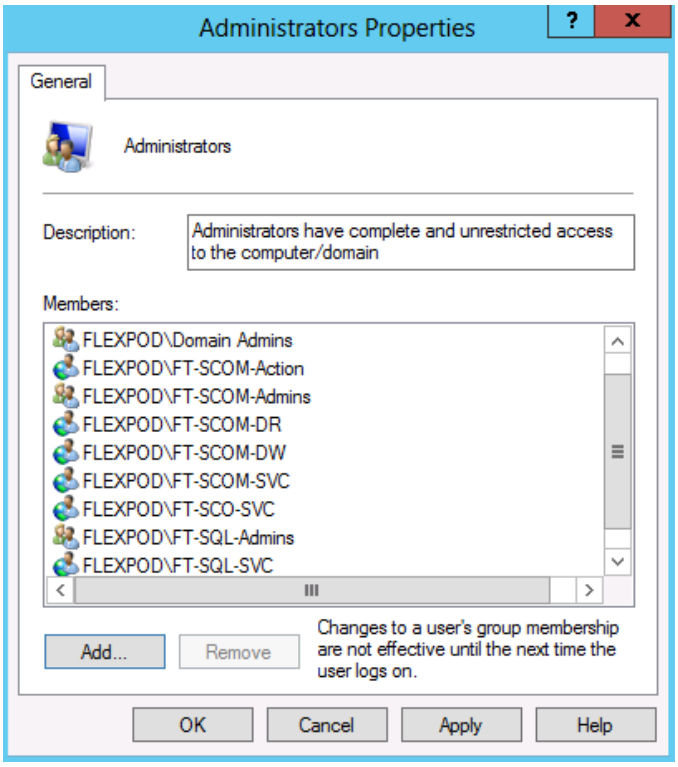
6. The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.	
Note: While the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.	

Install the SQL Server Reporting Services and Analysis Services (Split Configuration)

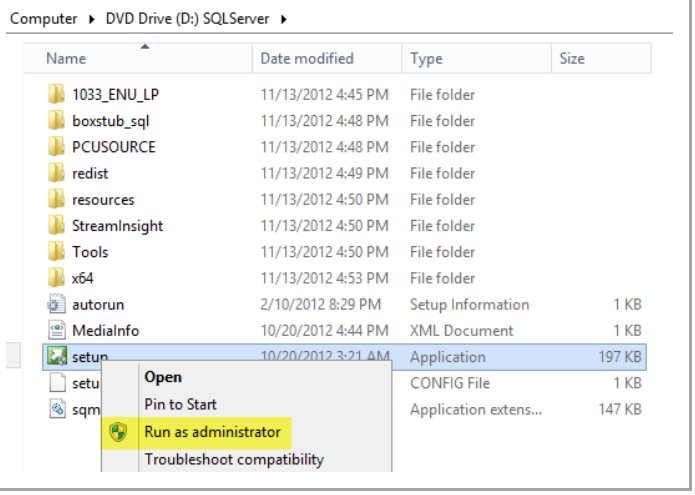
The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the provided steps to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

▶ Perform the following steps on the **Operations Manager Reporting Server** virtual machine only.

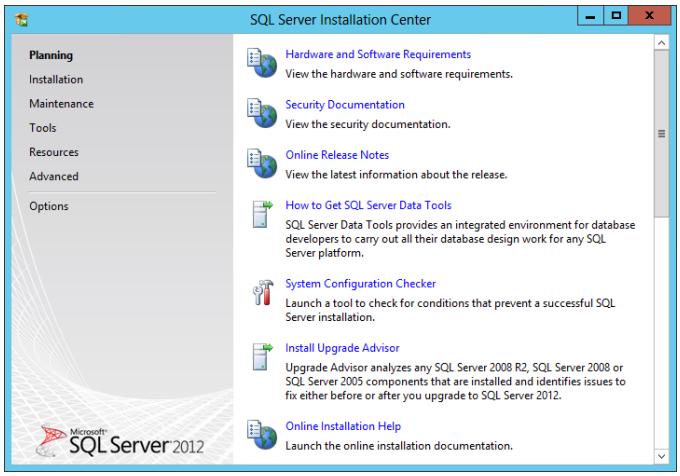
1. Log on to the Operations Manager Reporting Server virtual machine with a user with local admin rights.
2. Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager reporting server virtual machine:
   a. Orchestrator service account.
   b. Operations Manager action account.
   c. Operations Manager Admins group.
   d. Operations configuration service and data access service account.
   e. SQL Server service account.
   f. SQL Server Admins group.



3. From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

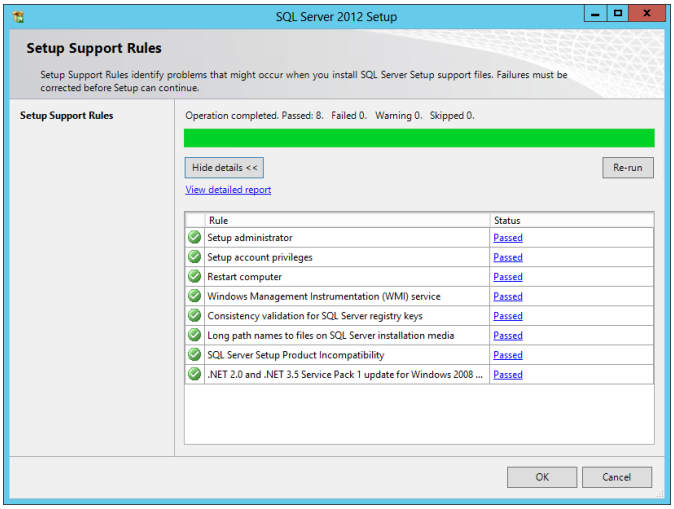


4. The **SQL Server Installation Center** will appear. Select the **Installation** menu option.

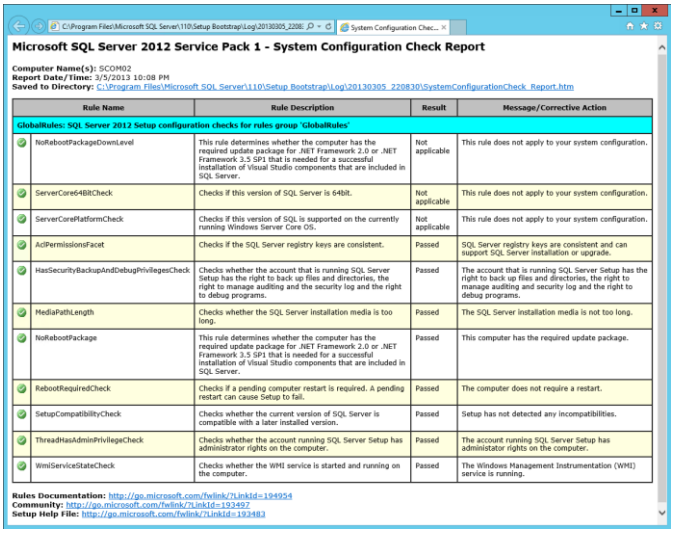


5. From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.

6. 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.

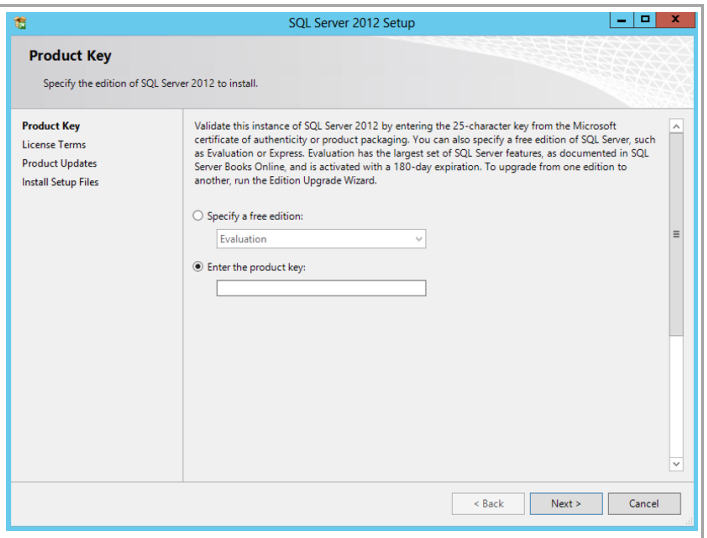


7. If the **View detailed report** link is selected, the following report is available.

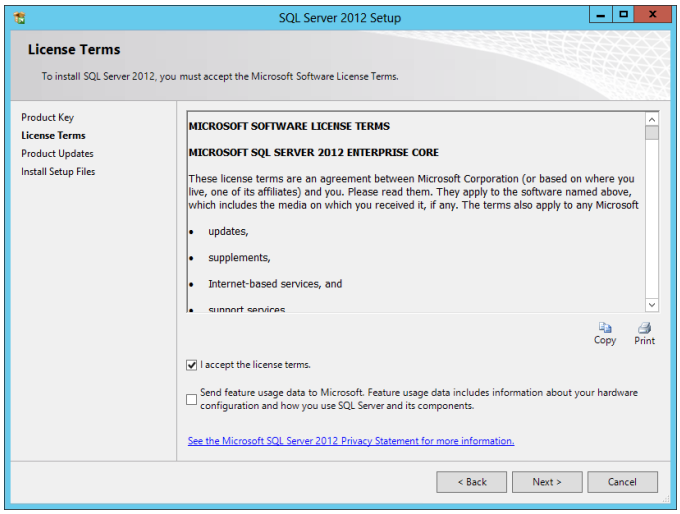


8. In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

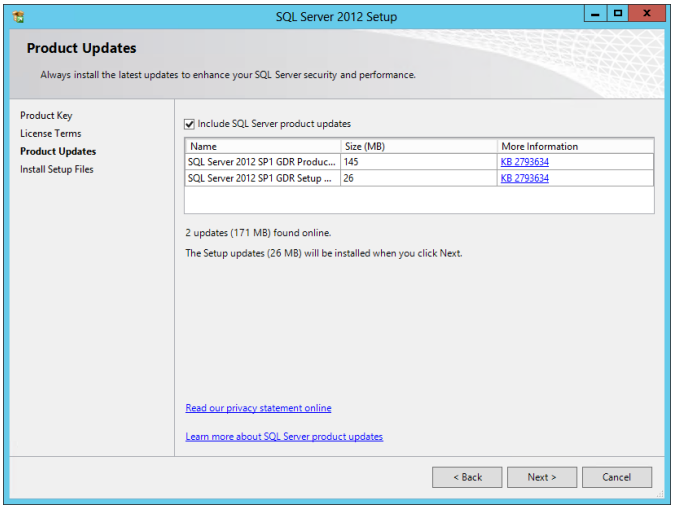
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



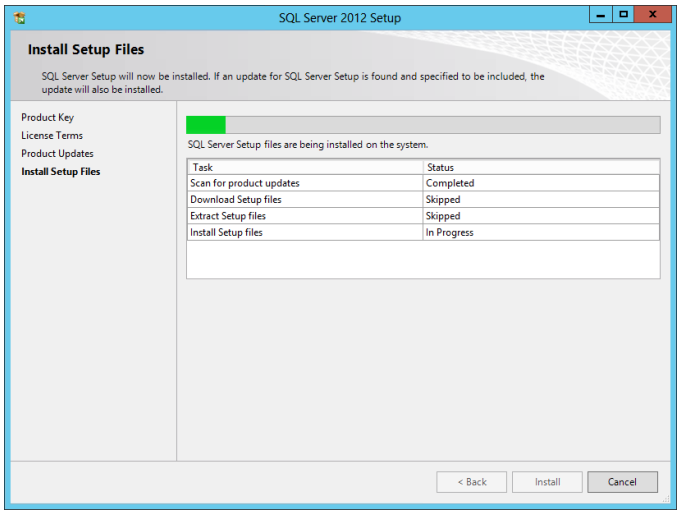
9. In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.



10. In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.



11. In the **Install Setup Files** dialog, click **Install** and allow the support files to install.

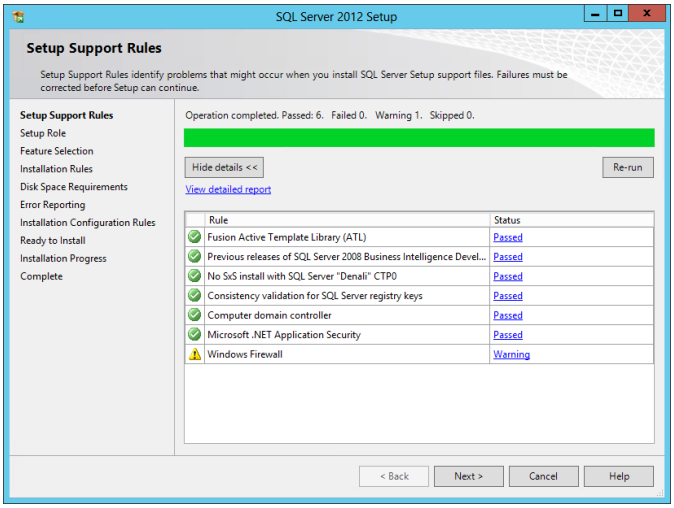


12. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check.

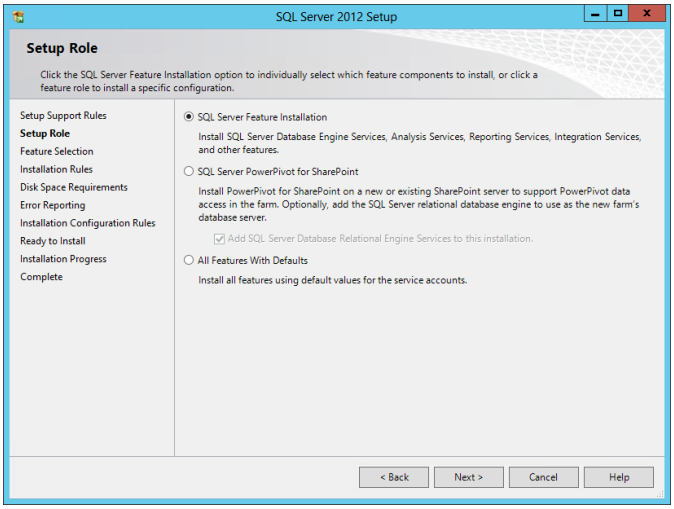
Note: The common issues include MSDTC, MSCS, and Windows Firewall warnings.

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

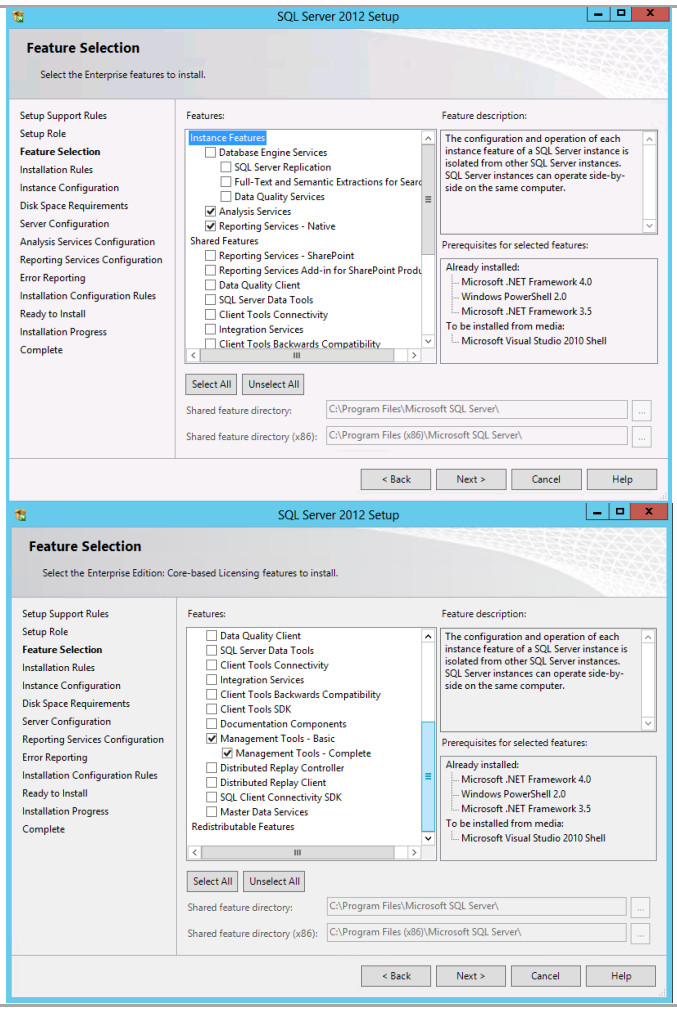
13. Click **Next** to continue.



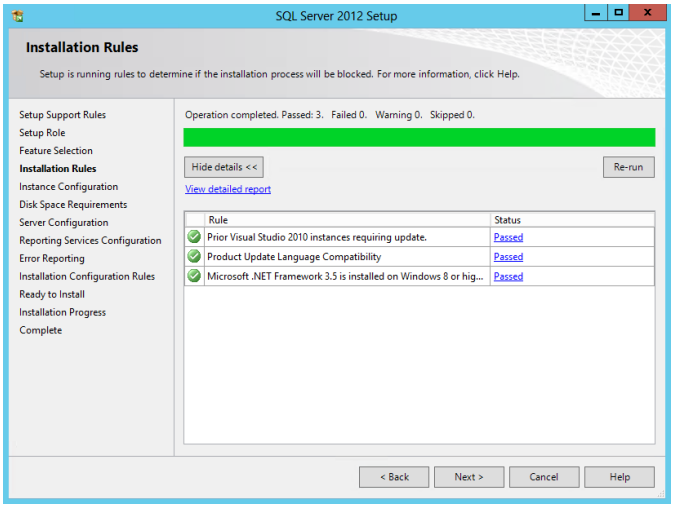
14. In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.



15. In the **Feature Selection** dialog, select the following features:
    a. Analysis Service
    b. Reporting Services – Native
    c. Management Tools – Basic
    d. Management Tools – Complete
16. When all selections are made, click **Next** to continue.



17. 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.



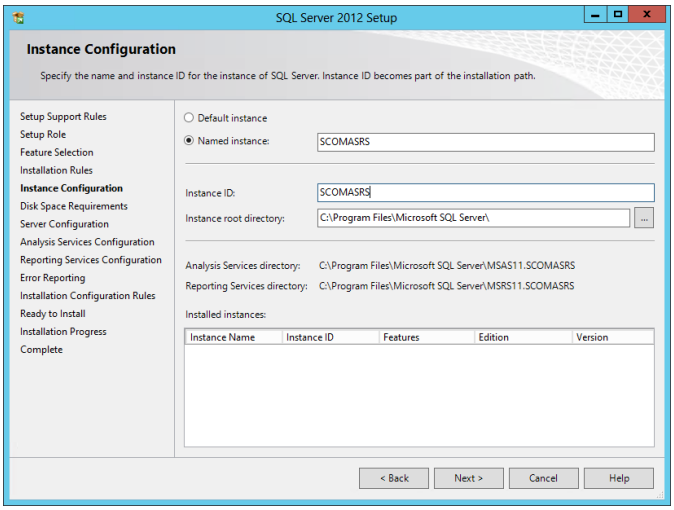
18. In the **Instance Configuration** dialog, select the **Named instance** option. In the provided text box, specify the instance name being installed.

    a. **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.*

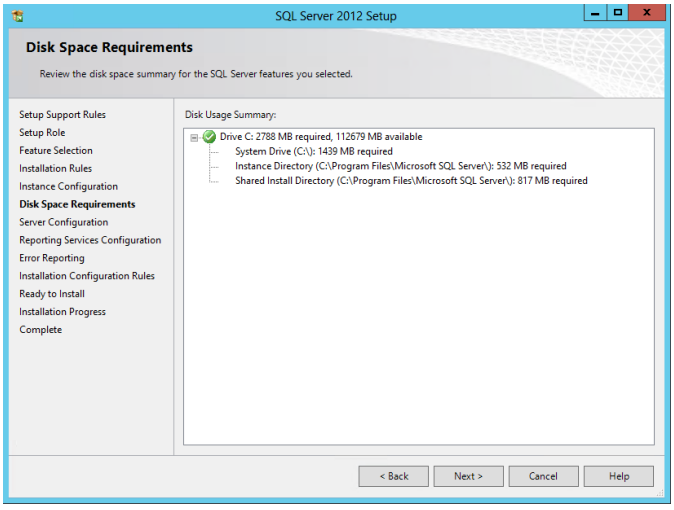
Note: A post-installation configuration process will occur to configure the reporting server database within the Operations Manager SQL Server instance.

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

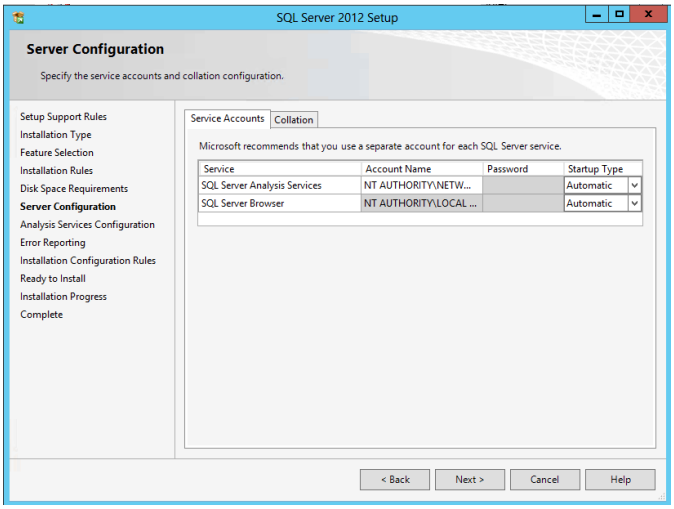
Note: A post-installation configuration process will occur to configure the reporting server database within the Operations Manager Data Warehouse SQL Server instance.



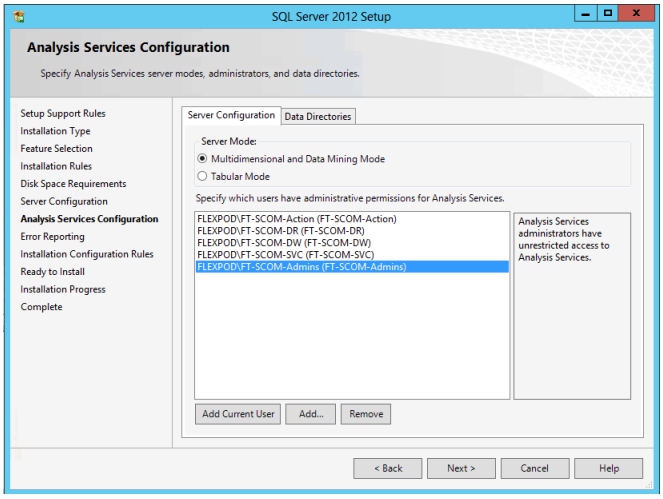
19. In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.



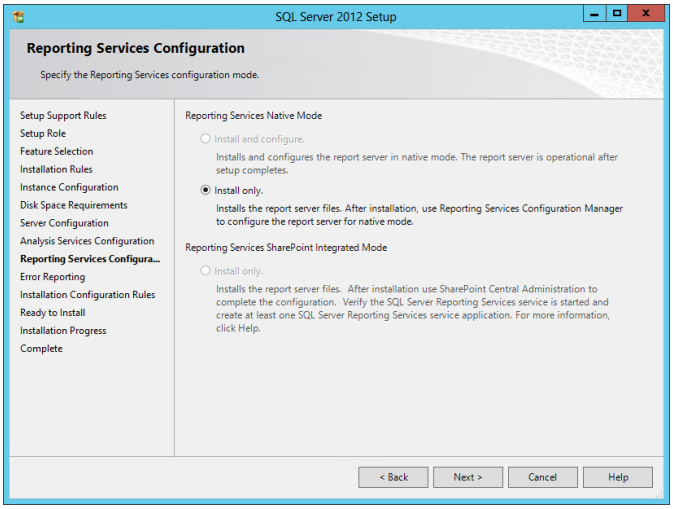
20. In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NETWORK SERVICE** account for both the **SQL Server Reporting Services** and **SQL Server Analysis Services** service, . Click **Next** to continue.



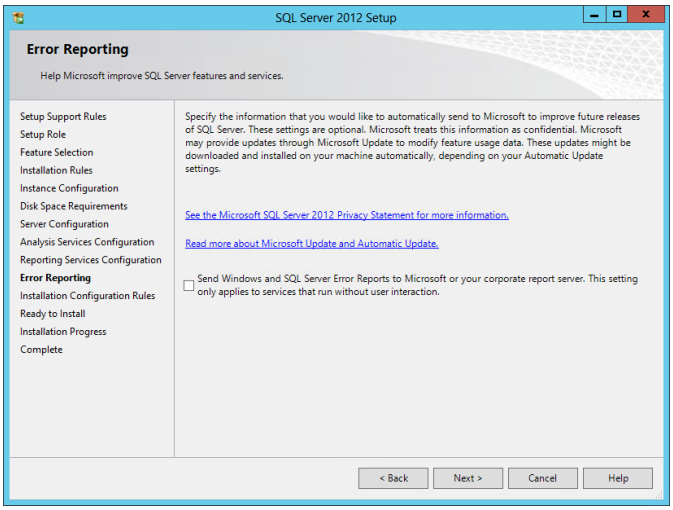
21. In the **Analysis Services Configuration** dialog, Click **Add**, Verify that the following accounts and/or groups are granted access to the Analysis Services:
    a. Operations Manager action account.
    b. Operations Manager Admins group.
    c. Operations Manager service account.
    d. Operations Manager data reader account
    e. Operations Manager, Data Warehouse write account
22. Click **Next** to continue.



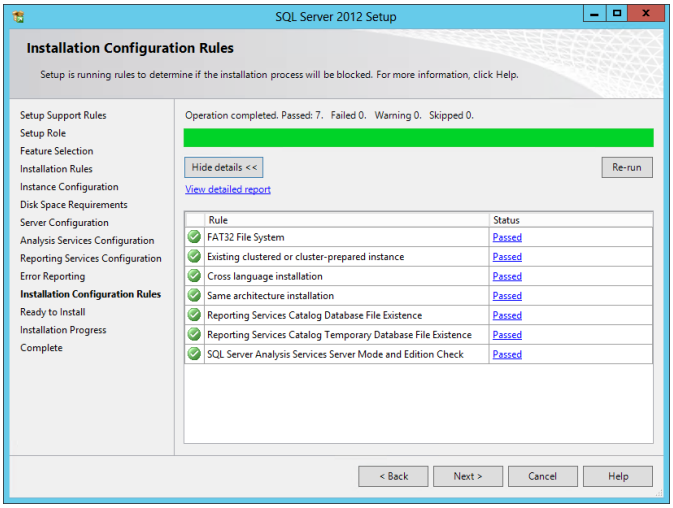
23. In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.



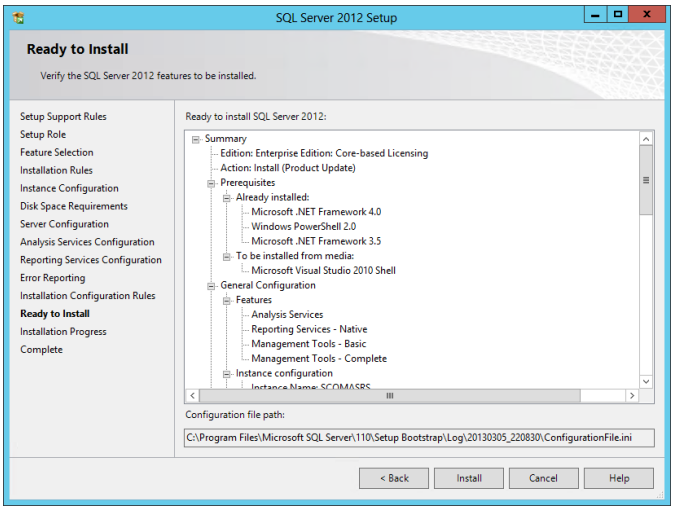
24. In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



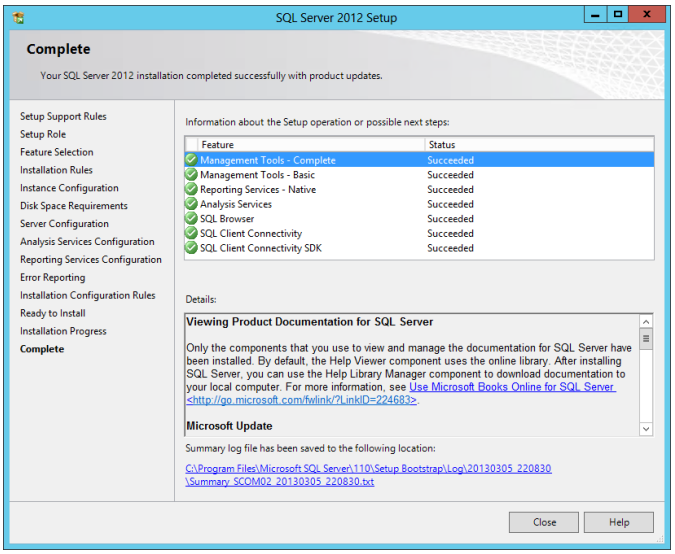
25. In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



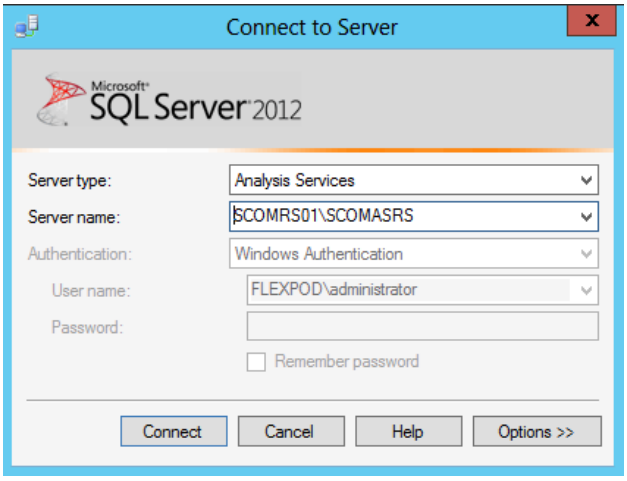
26. In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



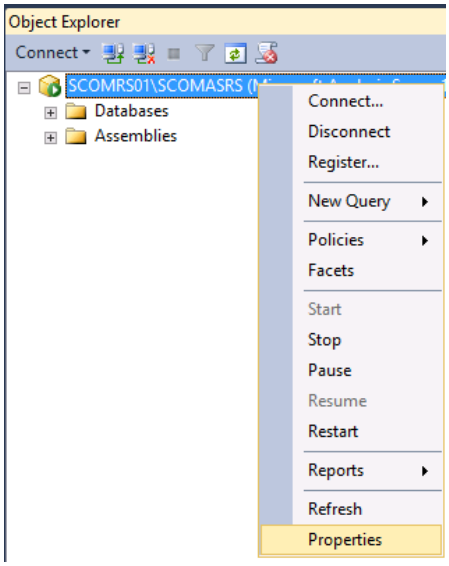
27. When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



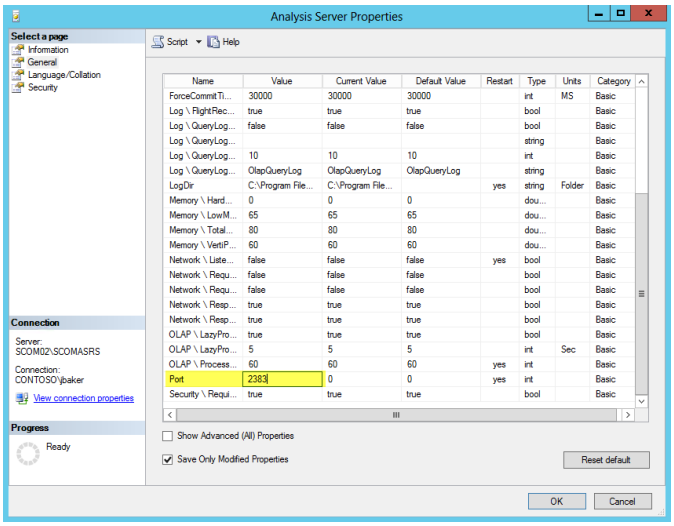
28. Verify the installation in SSMS prior to moving to the next step of installation. Launch **SQL Server Management Studio** and connect to Analysis Services at **ServerName\InstanceName**.



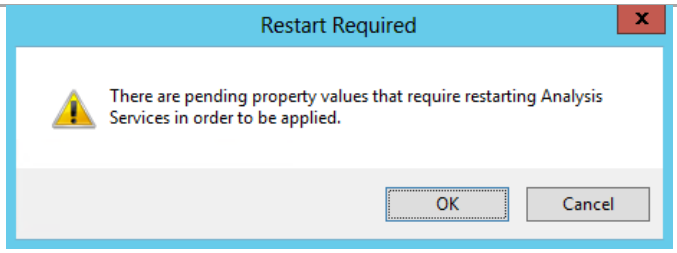
29. By default, named instances will use dynamic ports. In order to achieve better compatibility with firewalls the instance port should be set to static. Select the SSAS instance. Right-click on the instance and select **Properties**.



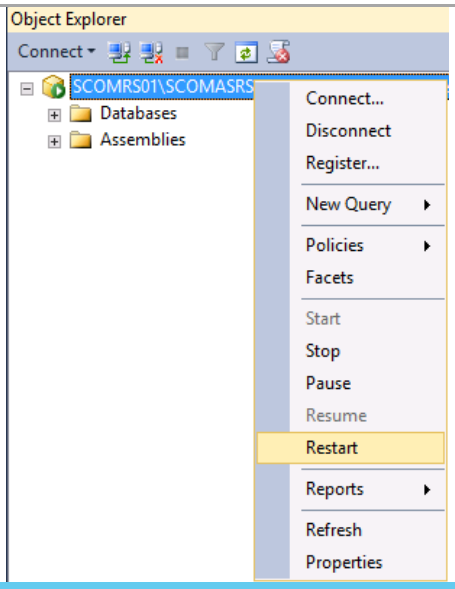
30. In the **Properties** dialog select the **General** tab. Scroll down to the **Port** value under the **Name** column. Select the value and change the value of 0 (zero) to 2383 or a port value of your choice. When complete, click **OK** to continue.



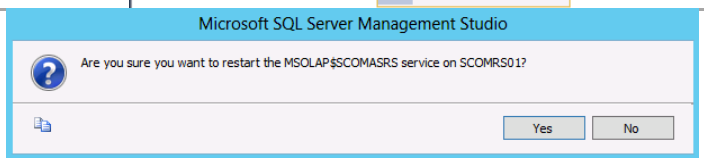
31. When prompted by the Restart Required dialog, click **OK**.



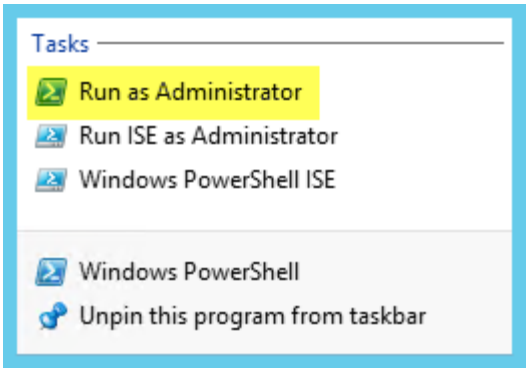
32. Within **SQL Server Management Studio**, in **Object Explorer**, select the SSAS instance, right-click and select **Restart** from the context menu.



33. On the confirmation screen, click **Yes**. Close **SQL Server Management Studio**.



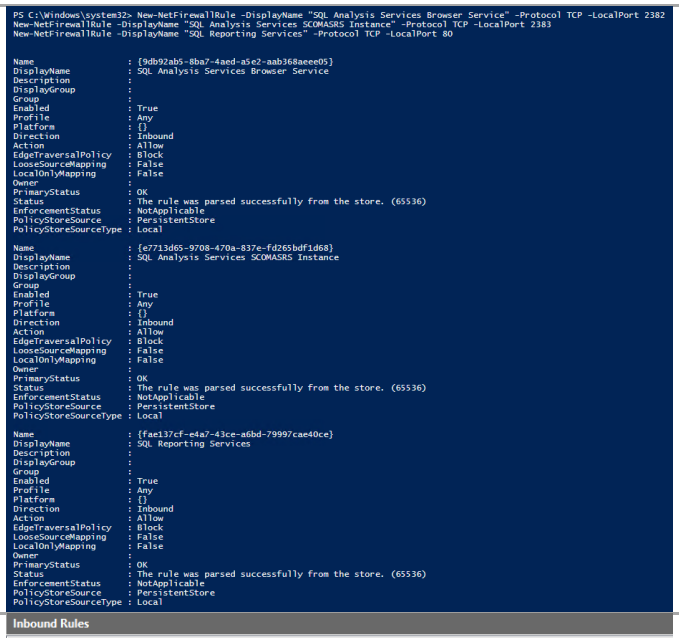
34. By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled.
35. Open an administrative session of PowerShell.



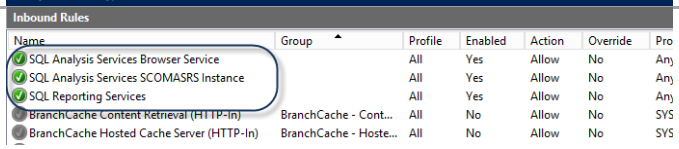
36. Execute the following commands to create the needed Firewall Rules:

```
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
```

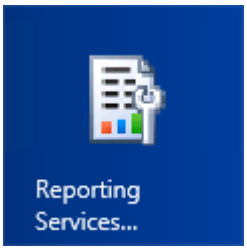
37. Adjust the display names and ports based on organizational requirements.



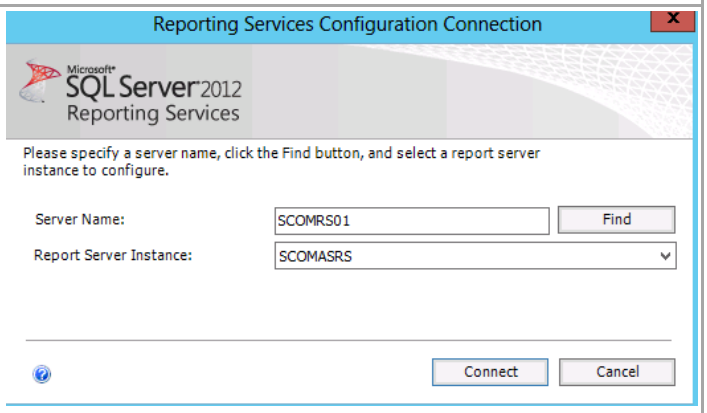
38. Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.



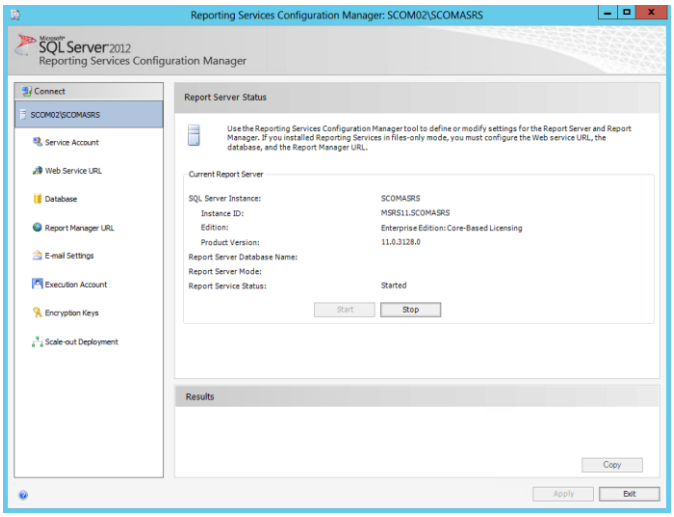
39. When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start Menu**, navigate and select the **Reporting Services Configuration Manager** tile.



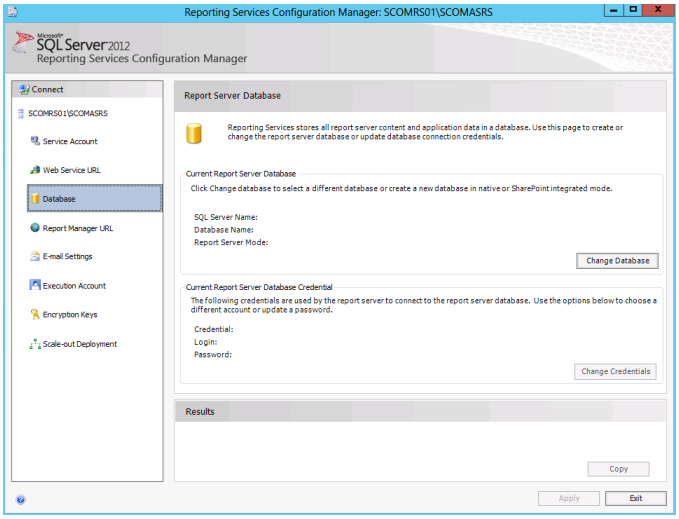
40. The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Operations Manager server. In the **Report Server Instance** text box, use the default **SCOMASRS** drop-down menu value. Click **Connect**.



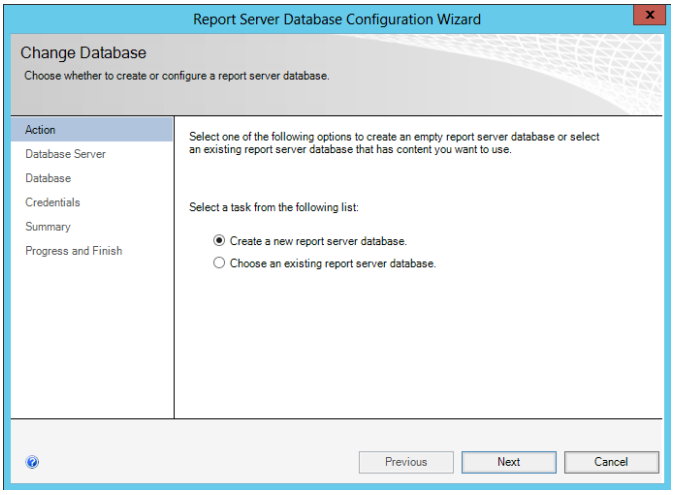
41. The **Reporting Services Configuration Manager** tool will appear.



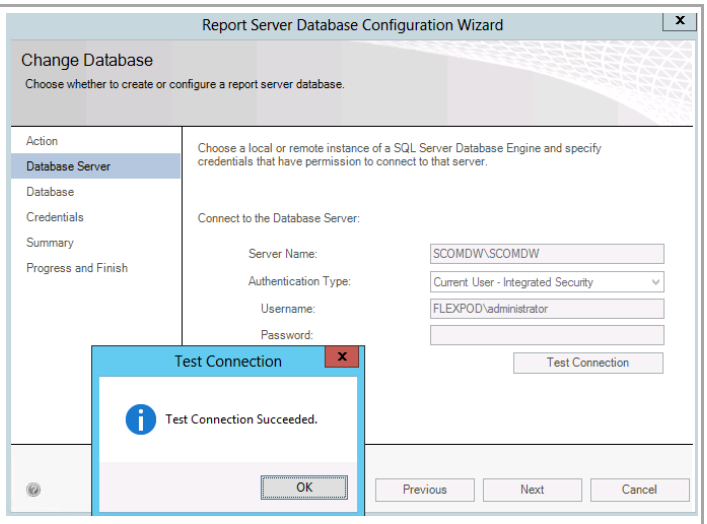
42. In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.



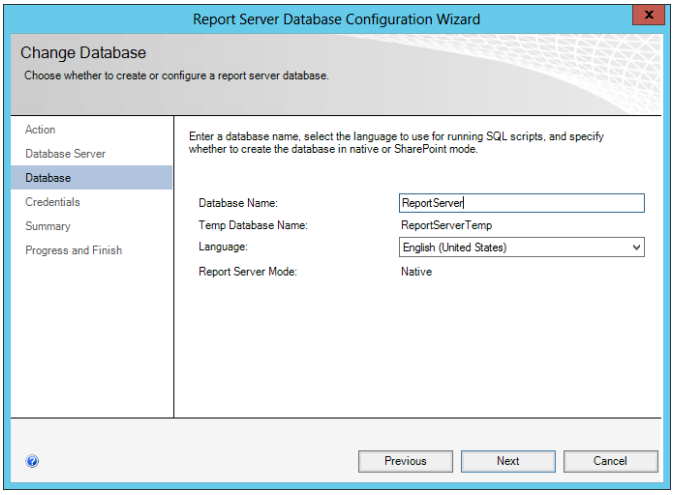
43. The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



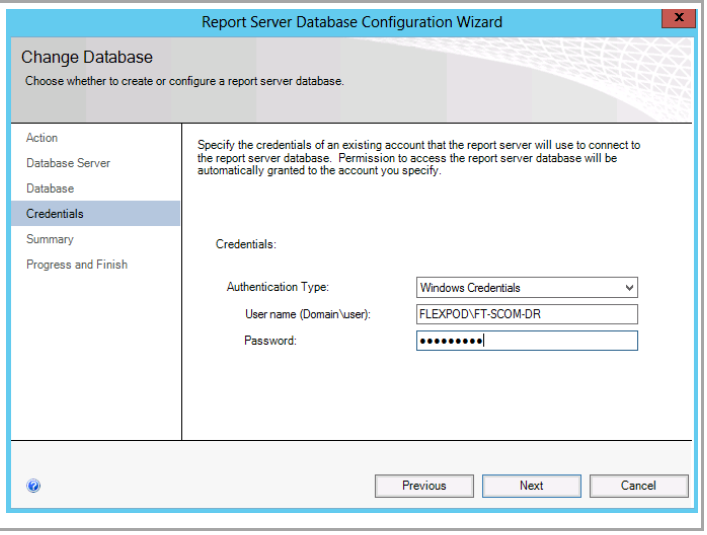
44. In the **Database Server** section, specify the following values:
    a. **Server Name** – *specify the name of the SQL Server CNO and the database instance created for the Operations Manager Data warehouse instance.*
    b. **Authentication Type** – *specify **Current User – Integrated Security** from the drop-down menu.*
45. Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



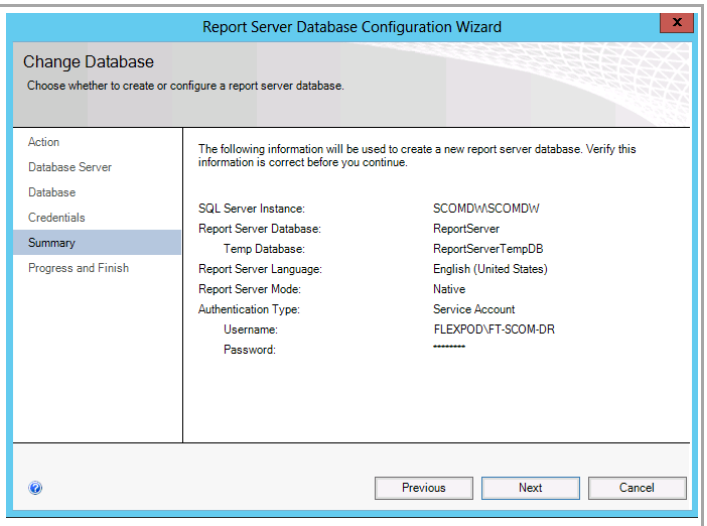
46. In the **Database** section, specify the following values:
    a. **Database Name** – accept the default value of ReportServer.
    b. **Language** – specify the desired language option from the drop-down menu.
    c. **Report Server Mode** – select the Native Mode option.
47. Click **Next** to continue.



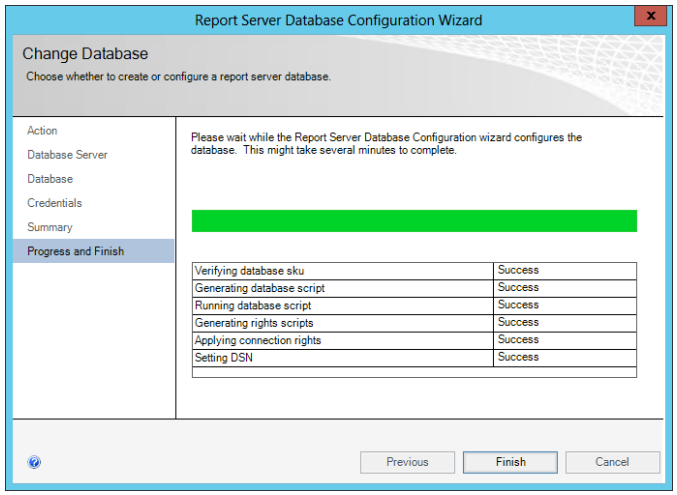
48. In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.



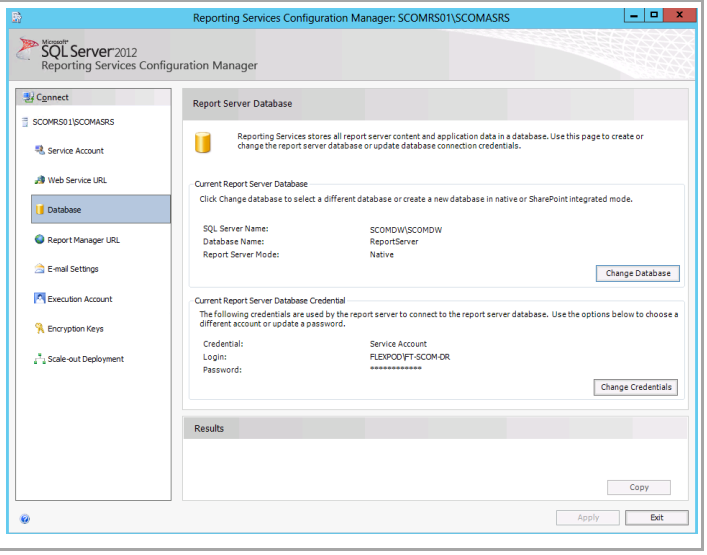
49. In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.



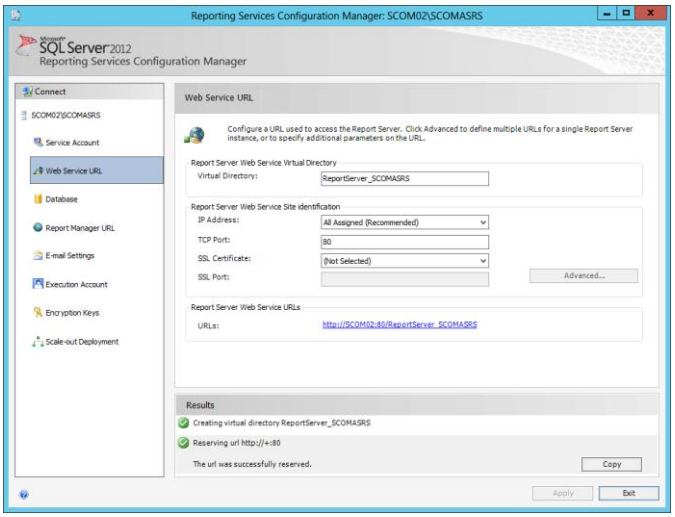
50. The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.



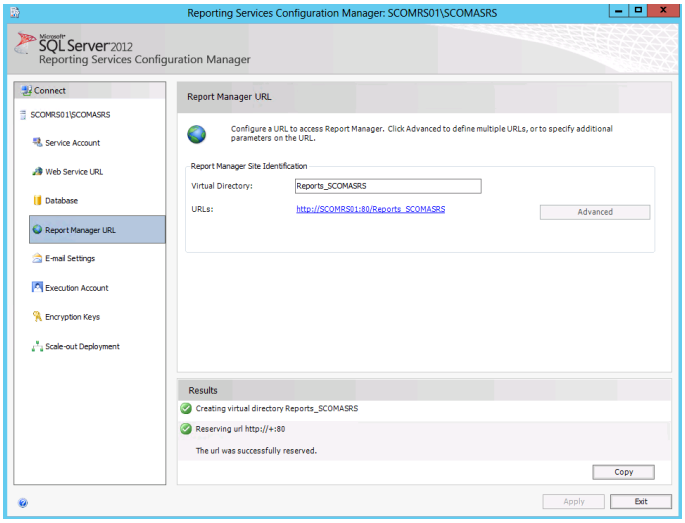
51. In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.



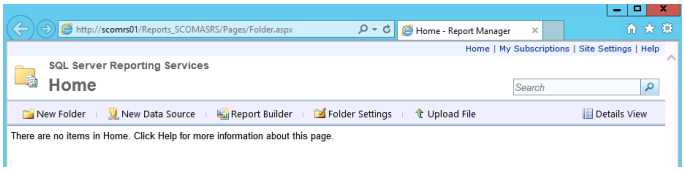
52. In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:
    a. In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer_SCOMASRS** in the provided text box.
53. In the **Report Server Web Service Site Identification** section, set the following values**:**
    a. **IP Address** – *set the **All Assigned** drop-down menu value.*
    b. **TCP Port** – *specify the desired TCP Port (default 80).*
    c. **SSL Certificate** – *select the available certificate or choose the default of (Not Selected).*
54. Click the **Apply** button to save the settings and create the Web Service URL.



55. In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:
    a. In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports_SCOMASRS** in the provided text box.
56. Click the **Apply** button to save the settings and create the Report Manager URL.

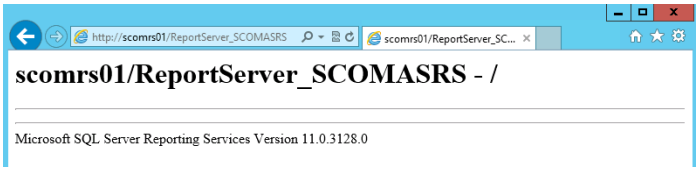


57. Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



58. 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.



59. Close the Reporting Server Configuration Manager.	

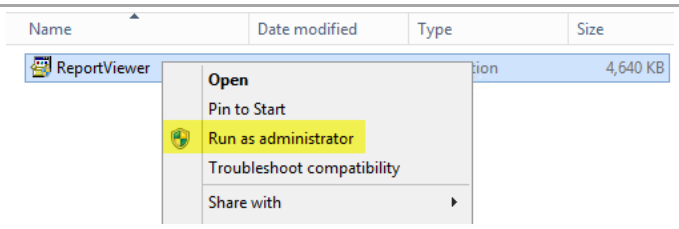
Install Microsoft Report Viewer 2010 SP1

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package to be installed prior to the installation of Operations Manager.[10] Follow the provided steps to install Microsoft Report Viewer 2010 SP1.

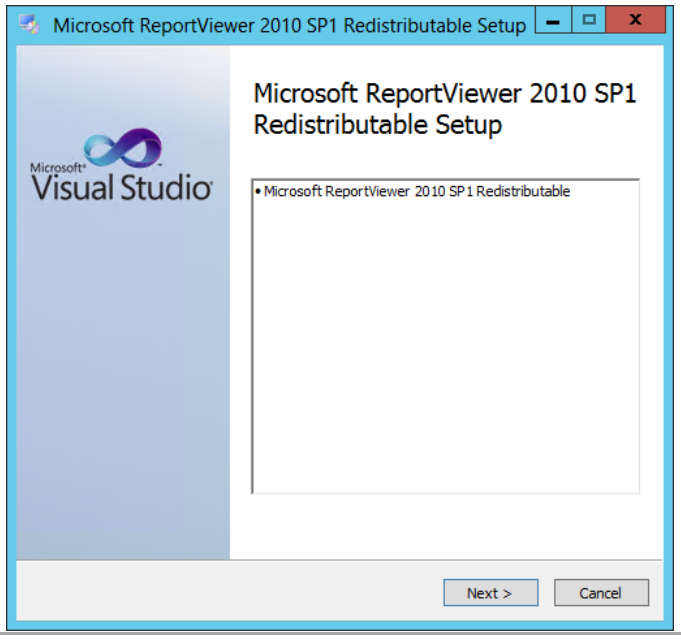
[10] Microsoft Report Viewer 2010 SP1 Redistributable Package - http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en.

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

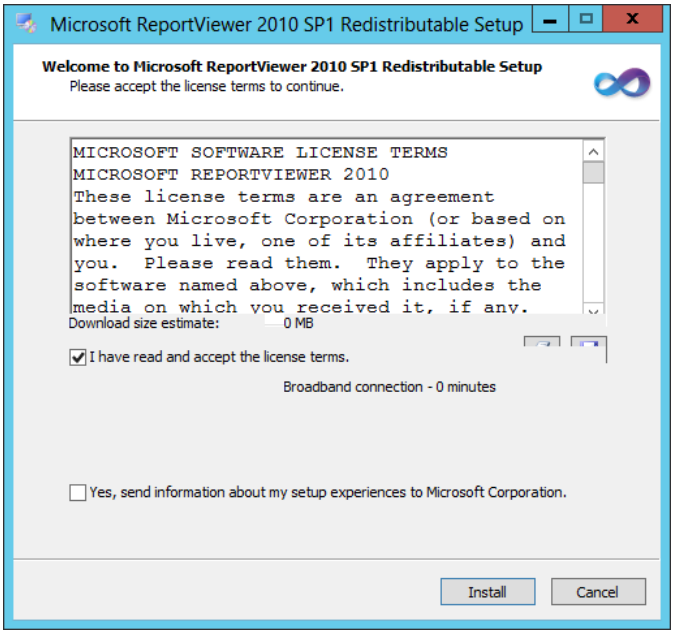
1. From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

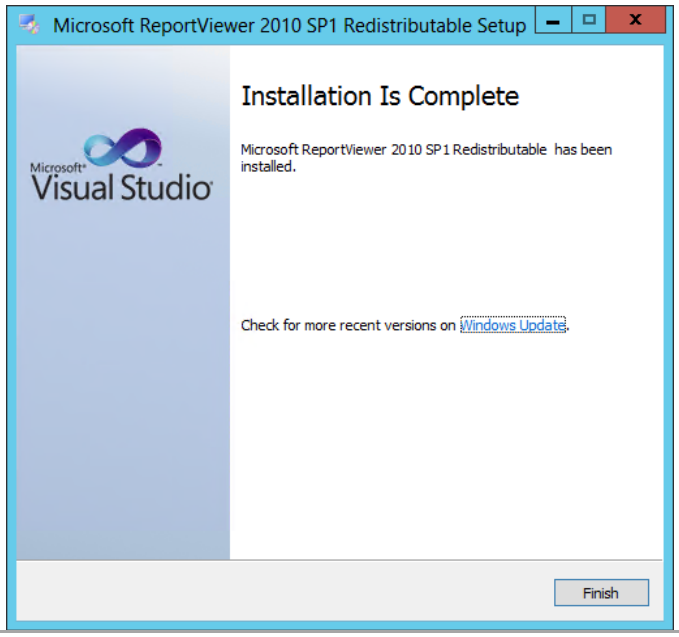


2. Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.



3. Select the **I have read and accept the license terms** check box and click **Install.**



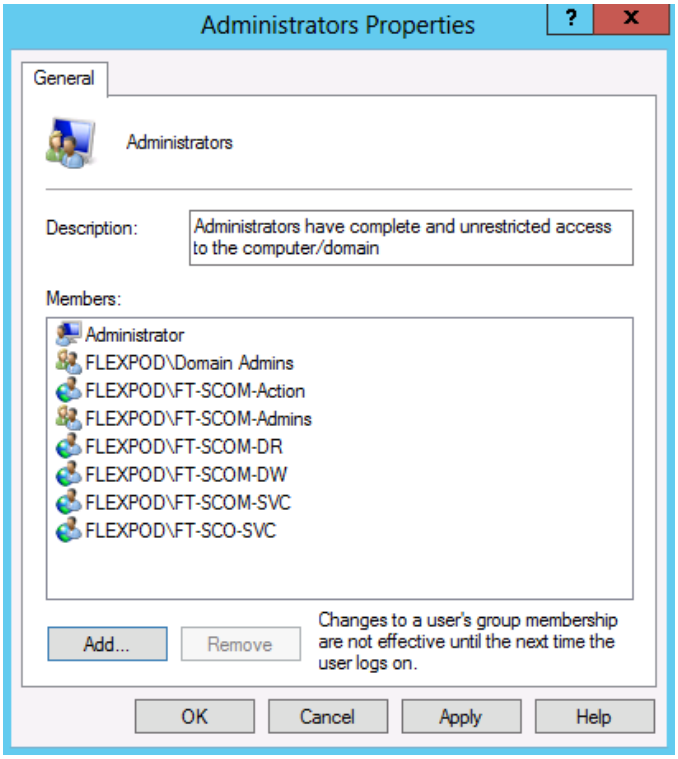
4. The installation progress will be displayed in the setup wizard. When completed, click **Finish** to exit the installation.	

Configuration of Operations Manager SQL Server Prerequisites

The following prerequisite steps must be completed prior to the installation of Operations Manager roles.[11]

▶ Perform the following steps on the **Operations Manager management server** virtual machines.

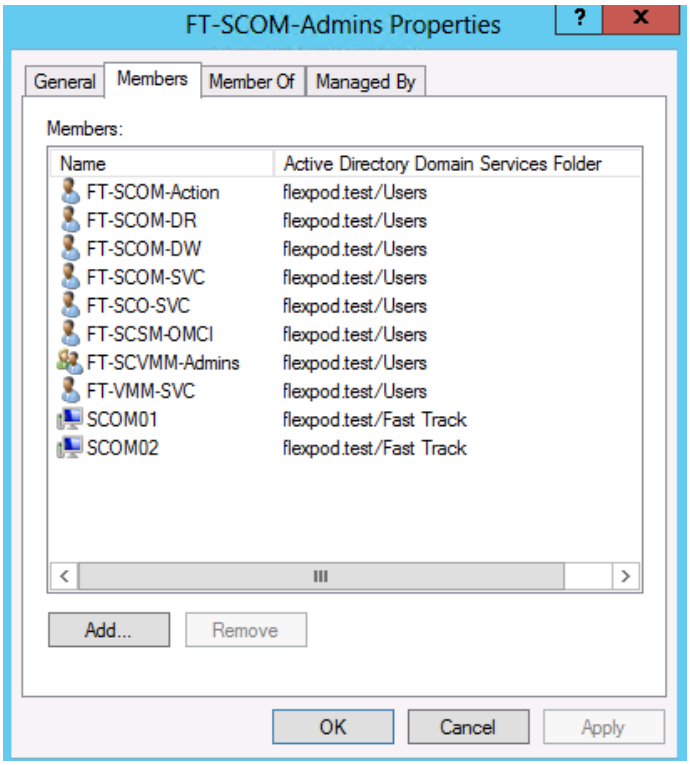
1. Log on to the Operations Manager virtual machine as a user with local admin rights.
2. Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager virtual machine:
   - Orchestrator service account.
   - Operations Manager action account.
   - 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.

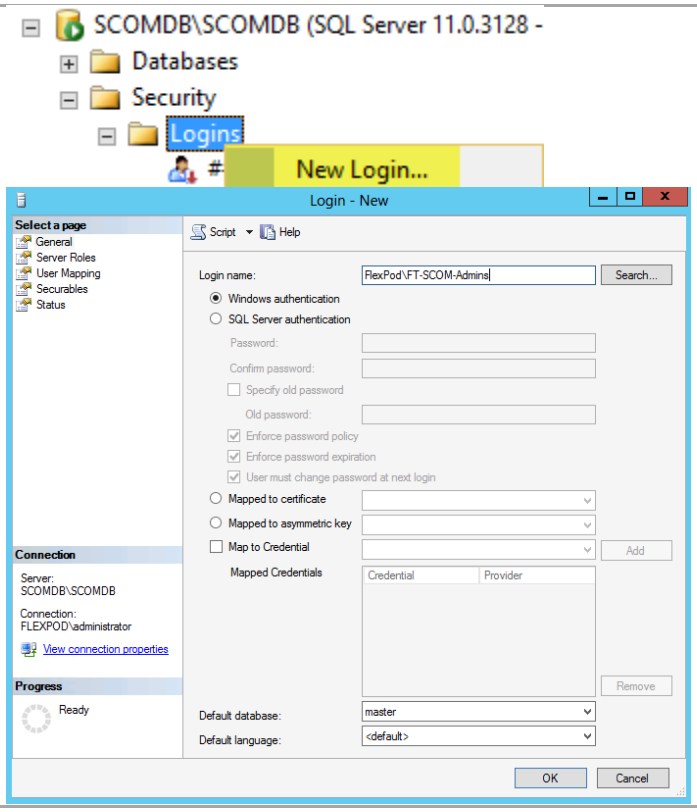
[11] Deploying System Center 2012 - Operations Manager - http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin.

1. 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.

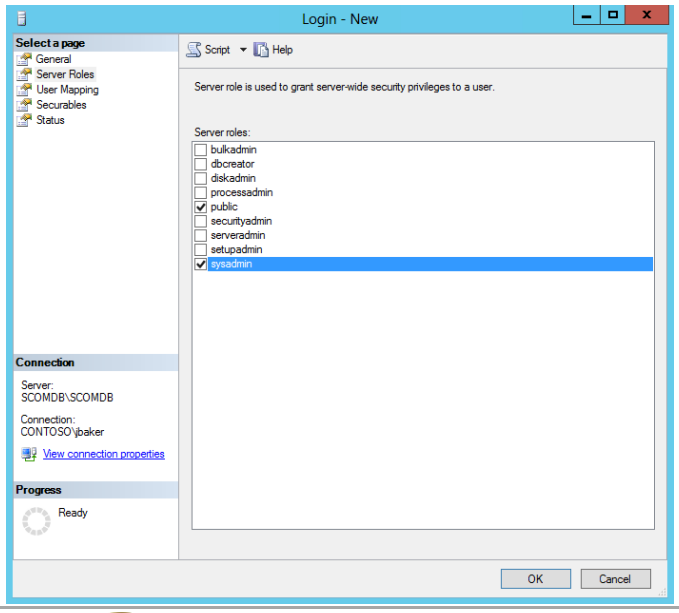


▶ Perform the following steps on the **primary SQL Server cluster node**.

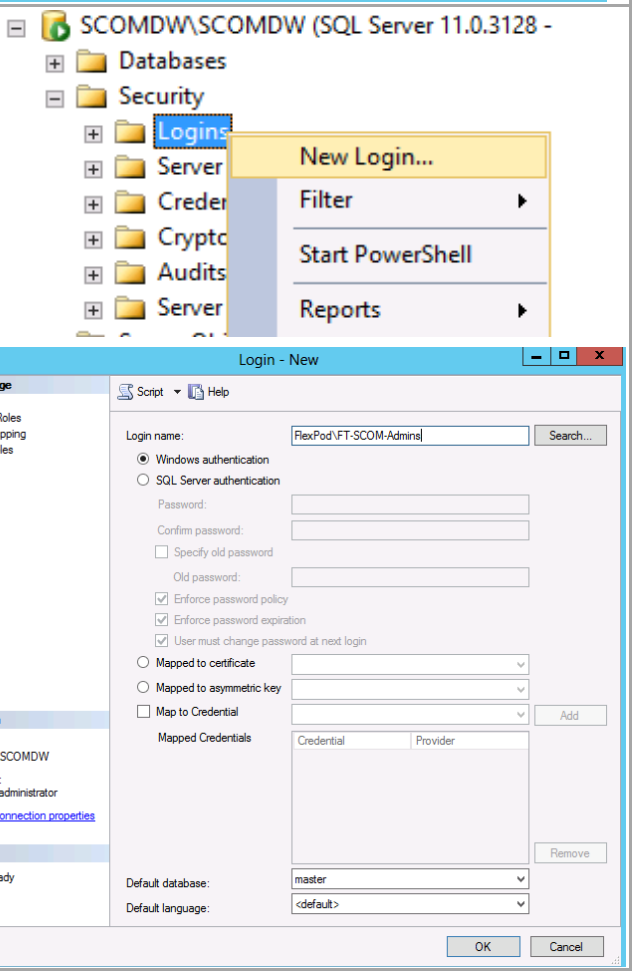
1. Using Administrative credentials, log on to the first SQL Server and open SSMS. Connect to the Operations Manager SQL Server instance using the values specified earlier. Create a new login by navigating to the **Logins** node under **Security** within SQL Management Studio. Right-click the **Logins** node and select **New Login...** from the context menu.
2. In the **Login – New** dialog, specify the Operations Manager Admins group created earlier as the new **Login name** and click **OK** to create the new login.



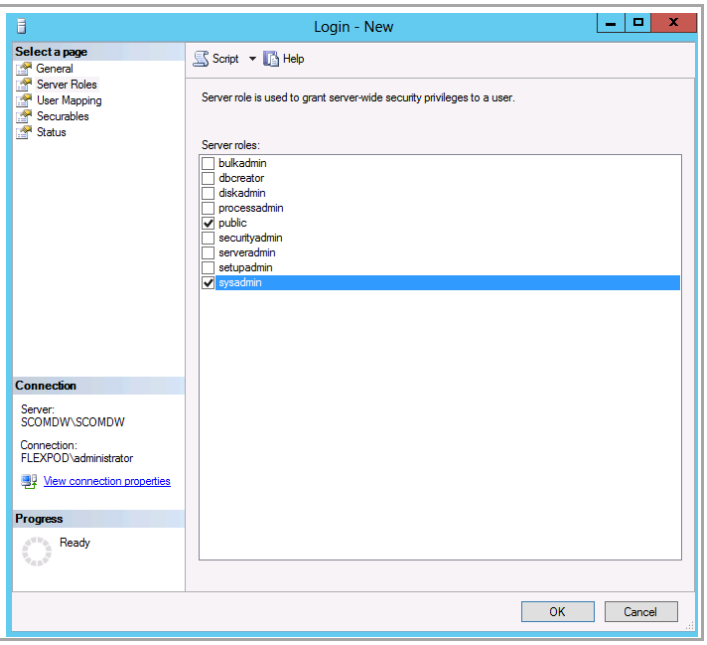
3. While still in the **Login – New** dialog, select the **Server Roles** page. Select the **sysadmin** role and click **OK** to add this login to the sysadmin role of the instance.



4. Repeat this procedure for the Operations Manager Data Warehous SQL Server instance.



5. 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.



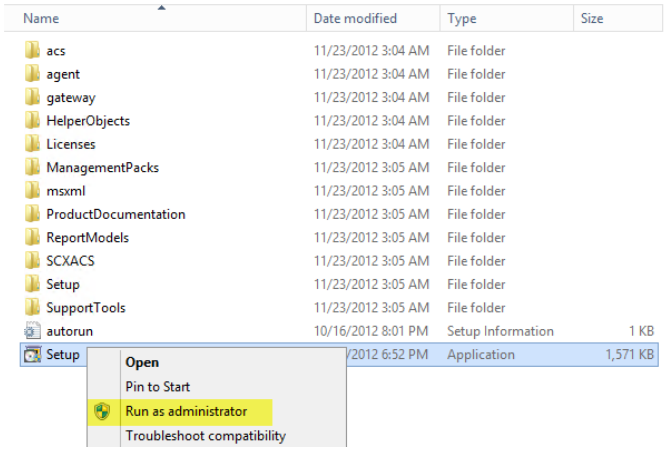
18.3 Installation

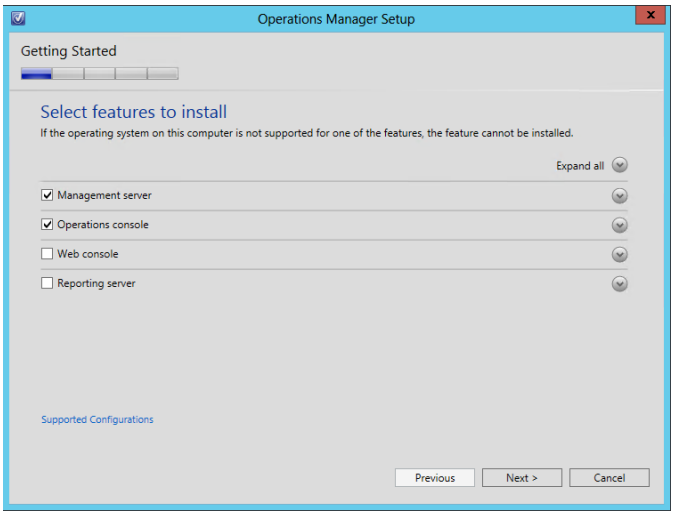
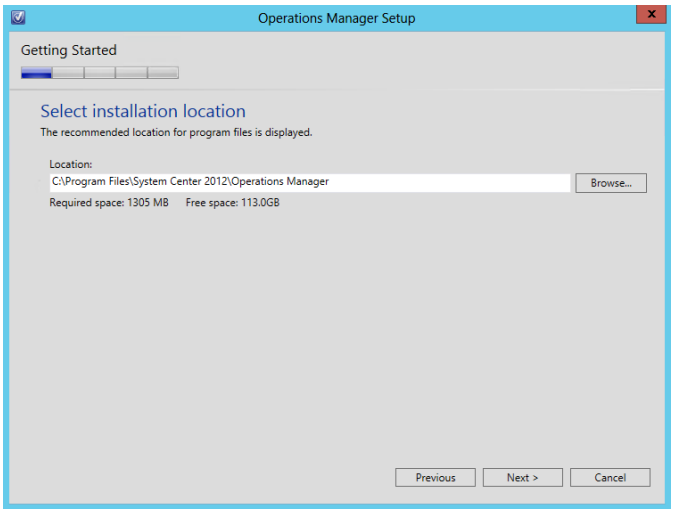
Install the Operations Manager Management Server

The following steps must be completed in order to install and configure the Operations Manager database and server roles.

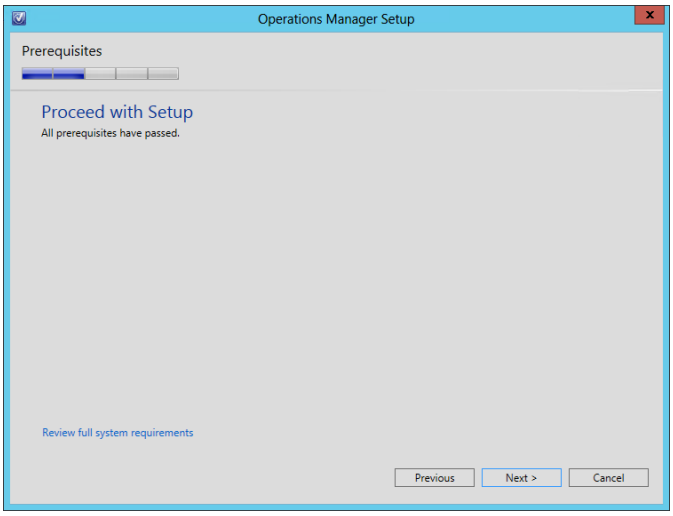
▶ Perform the following steps on the first **Operations Manager management server** virtual machine.

1. From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

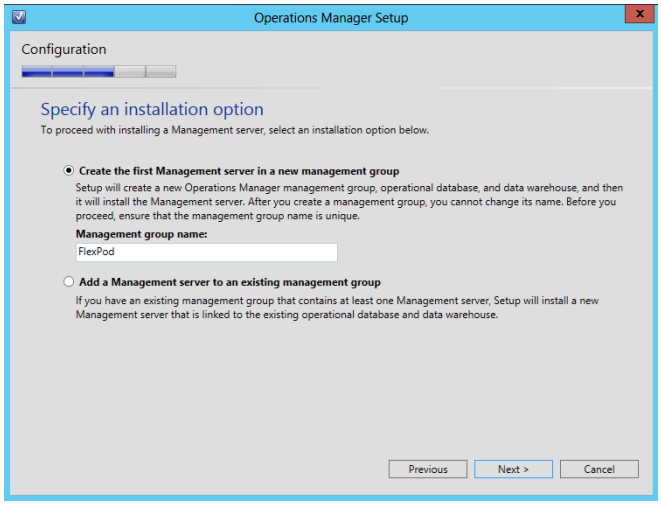


2. The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.	
3. In the **Select features to install** dialog, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.	
4. 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.	

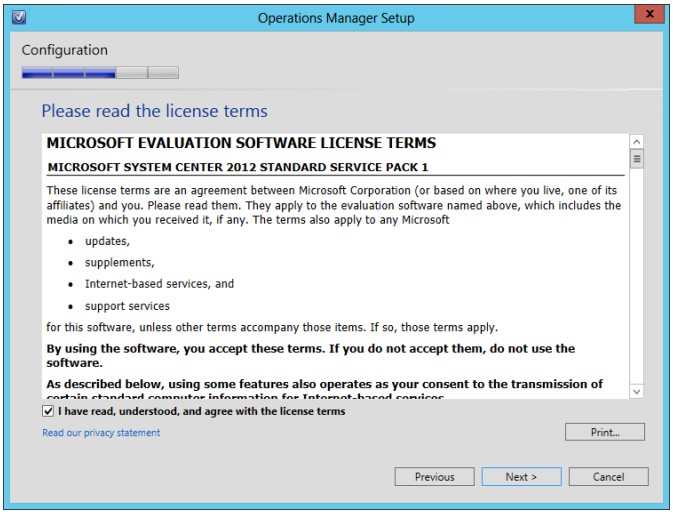
5. The setup will verify that all system pre-requisites are met in the **Proceed with Setup** dialog. If any pre-requisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



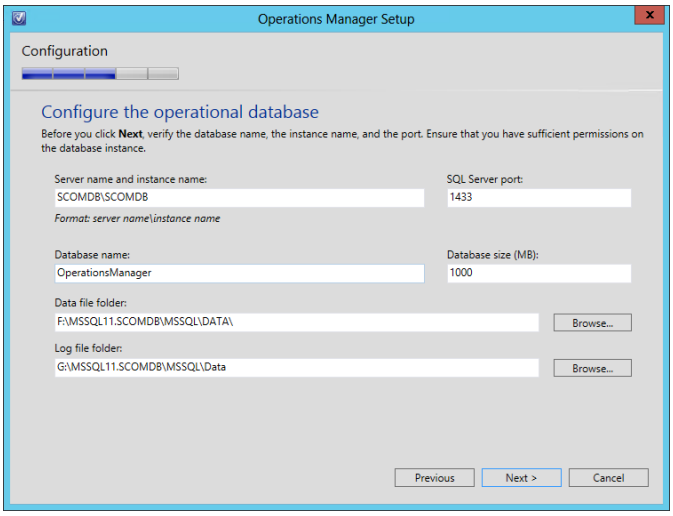
6. In the **Specify an installation option** dialog, two installation options are provided:
   a. **Create the first management server in a new management group**.
   b. **Add a Management server to an existing management group**.
7. Select the **Create the first Management server in a new management 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.
8. Click **Next** to continue.



9. 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.

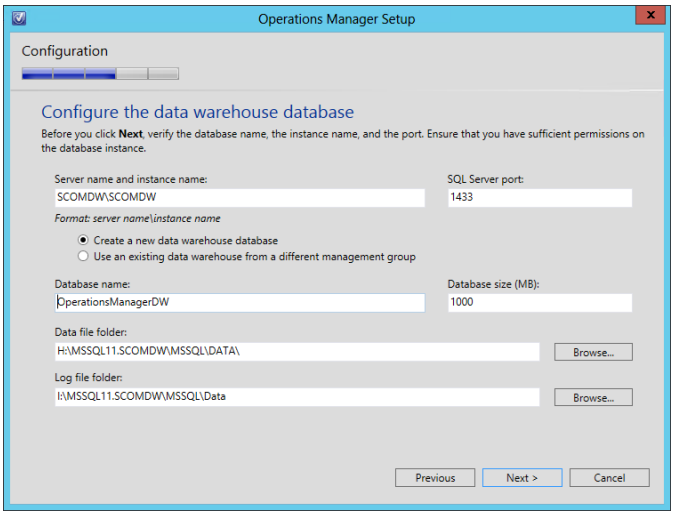


10. In the **Configure the operational database** dialog, Specify the following information in the provided text boxes:
    a. **Server name and instance name** – *specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.*
    b. **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).*
    c. **Database name** – *specify the name of the Operations Manager database. In most cases the default value of OperationsManager should be used.*
    d. **Database size (MB)** – *specify the initial database size.* [12] *The following values can be used as a general guideline:*
    e. Up to 500 agents: 12 GB.
    f. Up to 1000 agents: 24 GB.
    g. **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.*
    h. **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.*
11. Click **Next** to continue.



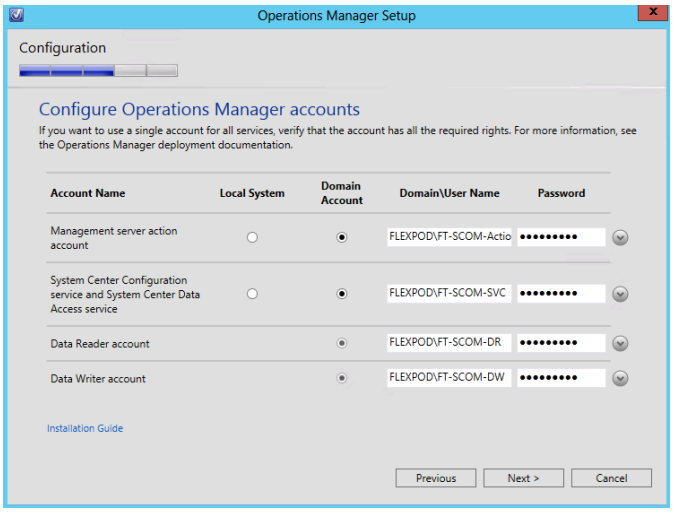
[12] System Center 2012 - Operations Manager Component Add – On - http://www.microsoft.com/en-us/download/details.aspx?id=29270 provides general guidance for database sizing.

12. In the **Configure the data warehouse database** dialog, specify the following information in the provided text boxes:
    a. **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.*
    b. **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).*
    c. **Database name** – *specify the name of the Operations Manager Data Warehouse database. In most cases the default value of OperationsManagerDW should be used.*
    d. **Database size (MB)** – *specify the initial database size.* [13] *The following values can be used as a general guideline:*
    e. Up to 500 agents: 356 GB.
    f. Up to 1000 agents: 720 GB.
    g. **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.*
    h. **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.*
13. Click **Next** to continue.

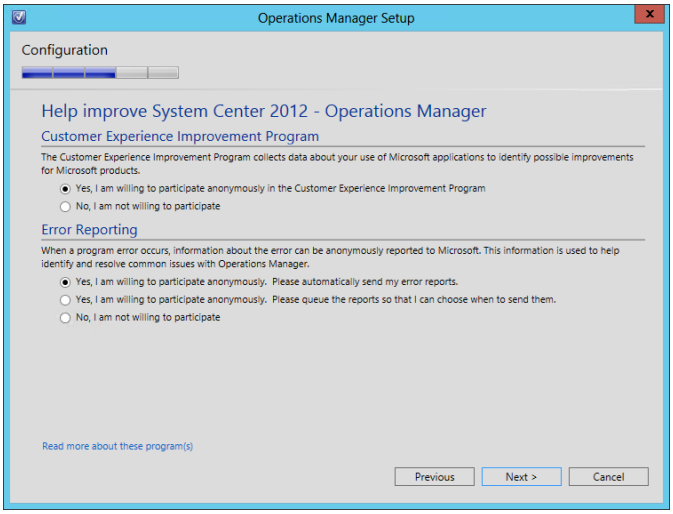


[13] System Center 2012 - Operations Manager Component Add – On - http://www.microsoft.com/en-us/download/details.aspx?id=29270 provides general guidance for database sizing.

14. 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:
    a. **Management server action account.**
    b. **System Center Configuration service and System Center Data Access service.**
    c. **Data Reader account.**
    d. **Data Writer account.**
15. If the use of a Domain Account is specified, enter the user account information as *<DOMAIN>\<USERNAME>* and enter the appropriate password.
16. When completed, click **Next** to continue.

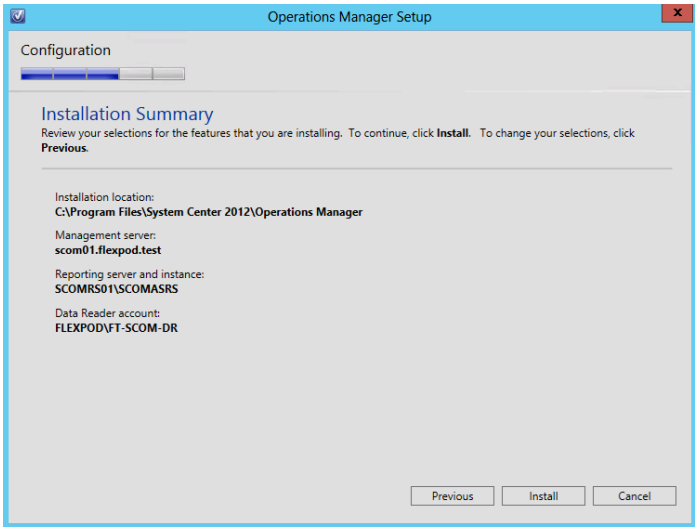


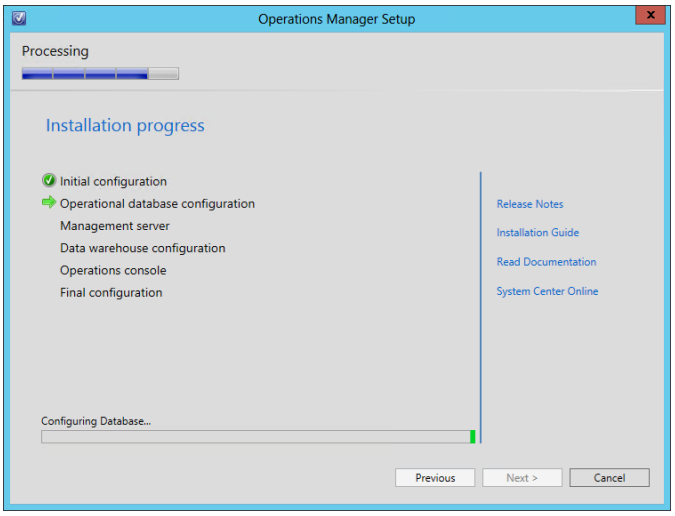
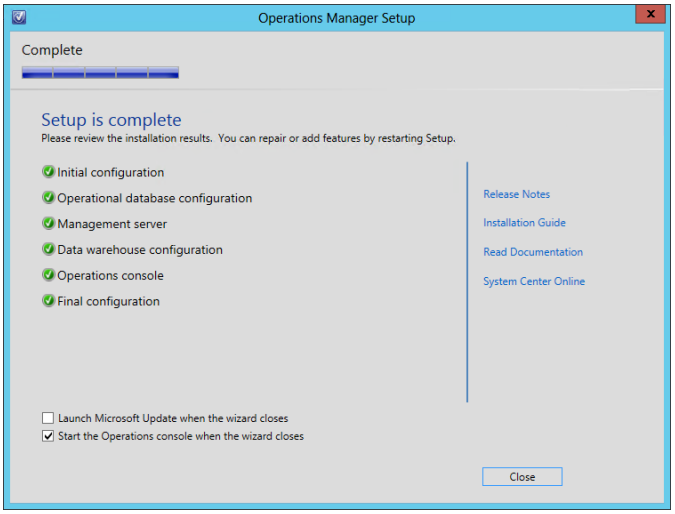
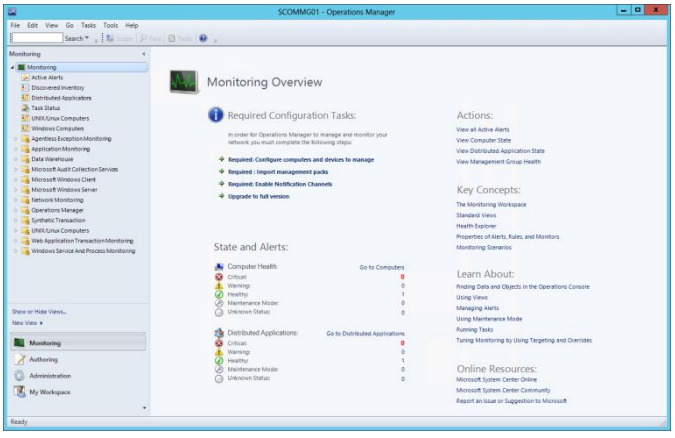
17. The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:
    a. **Customer Experience Improvement Program.**
    b. **Error Reporting.**
18. Select the appropriate option based on your organization's policies and click **Next** to continue.



19. 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: Make sure you set the database sizes appropriately for your particular deployment.



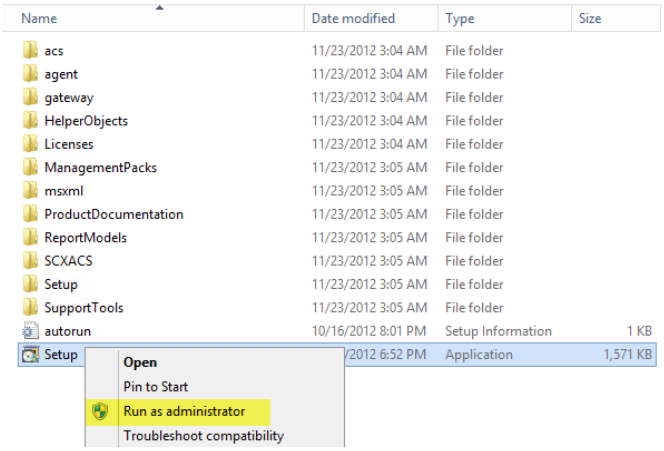
20. The wizard will display the progress while installing features.	
21. When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.	
22. 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 Operations Manager Reporting Server

The following steps must be completed in order to install and configure the Operations Manager reporting server role.

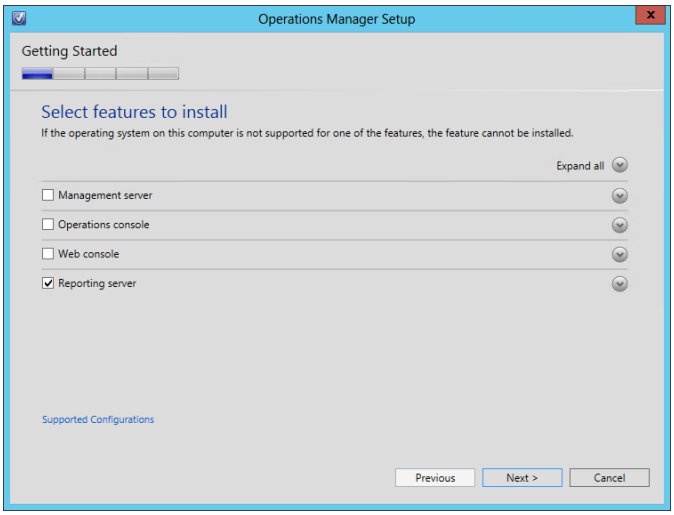
▶ Perform the following steps on the **Operations Manager reporting server** virtual machine.

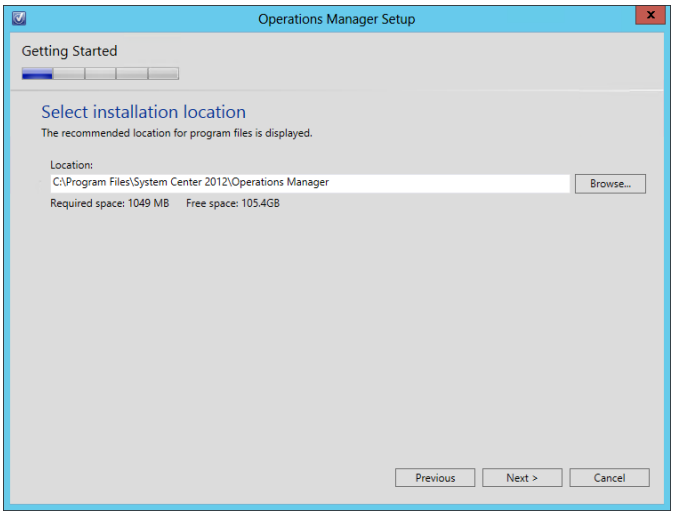
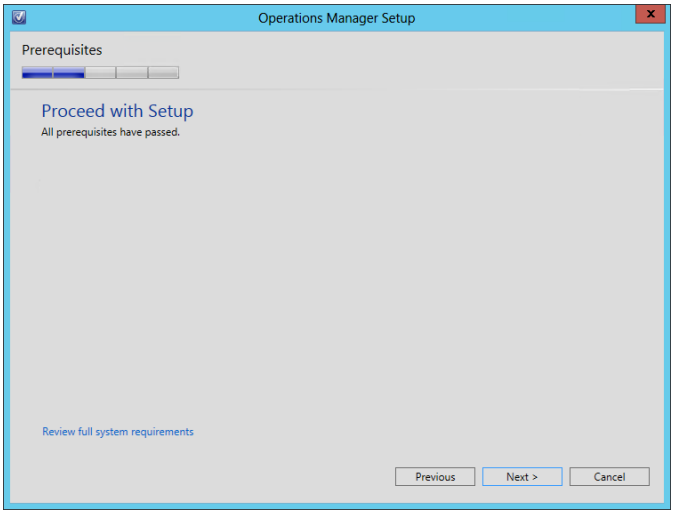
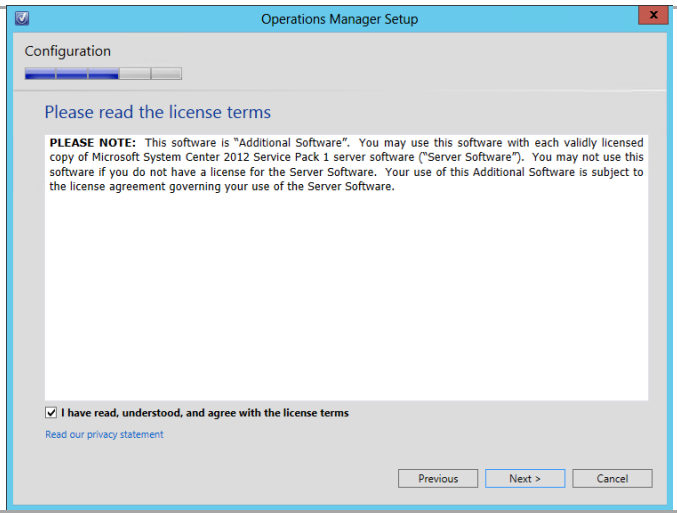
1. From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



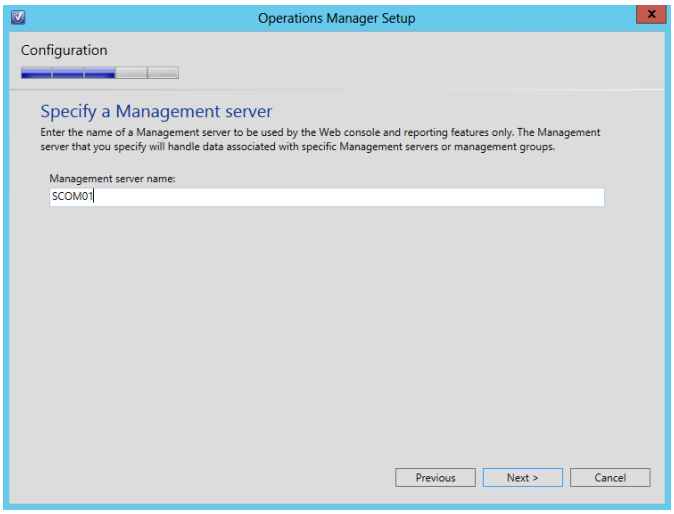
2. The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.

3. In the **Select features to install** dialog, verify that the **Reporting server** checkboxes are selected. Click **Next** to continue.

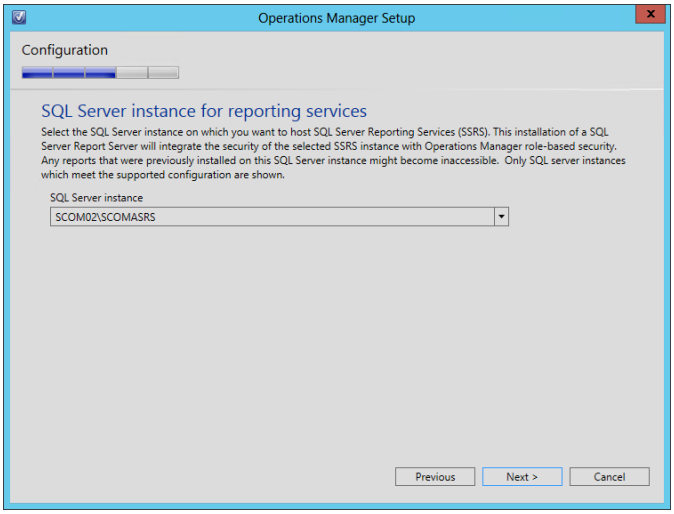


4. In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. 5. Click **Next** to continue.	
6. The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.	
7. 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.	

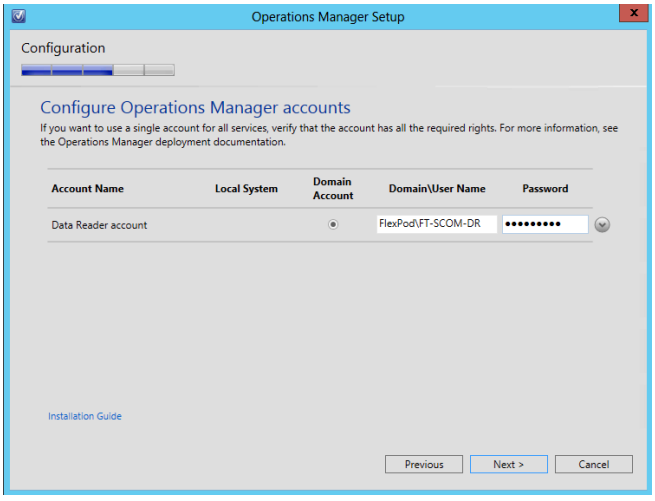
8. In the **Specify a Management server** dialog, type the name of the previously installed management server in the **Management server name** text box. Click **Next** to continue.



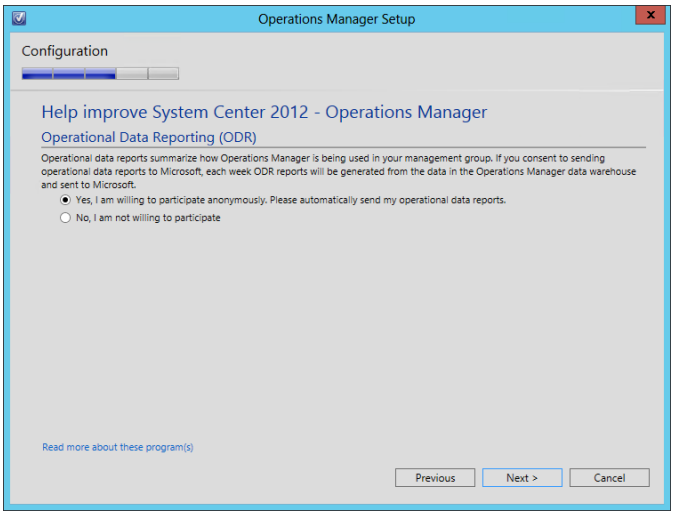
9. In the **SQL Server instance for reporting services** dialog, select the SQL Server instance hosting the local SQL Server Reporting Services and SQL Server Analysis Services from the drop-down menu created during earlier steps. Click **Next** to continue.



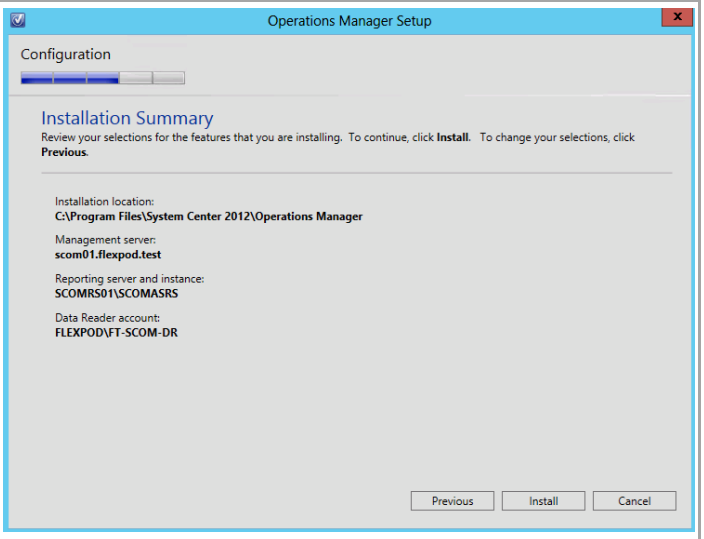
10. In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:
    a. **Data Reader account.**
    b. If the use of a Domain Account is specified, enter the user account information as *<DOMAIN>\<USERNAME>* and enter the appropriate password.
11. When completed, click **Next** to continue.



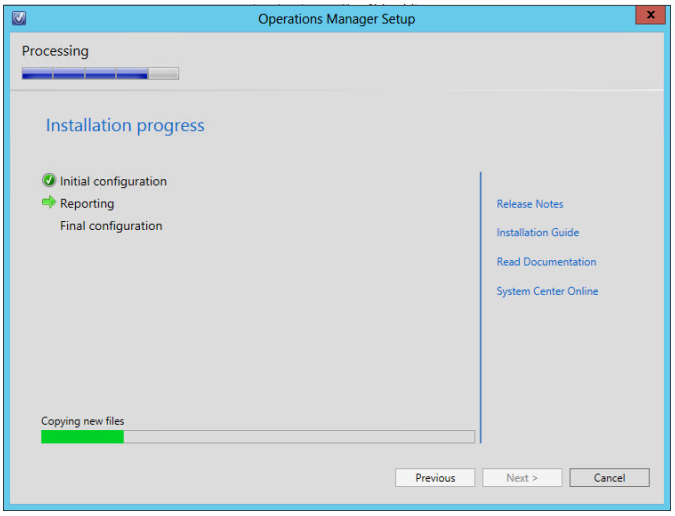
12. The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. This includes:
    a. **Operational Data Reporting (ODR).**
13. Select the appropriate option based on your organization's policies and click **Next** to continue.

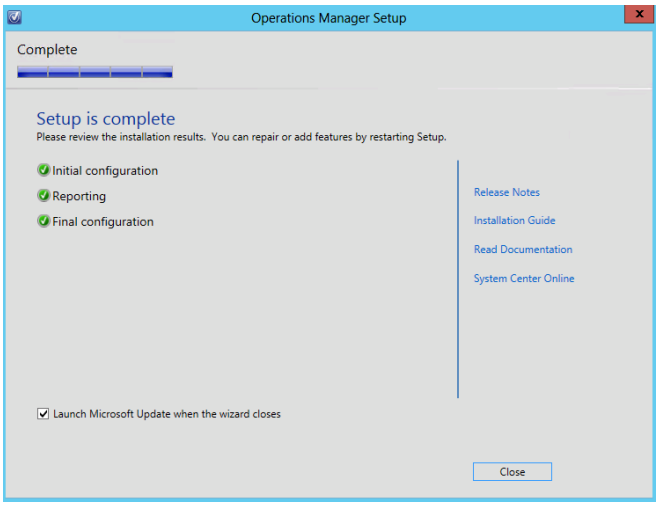
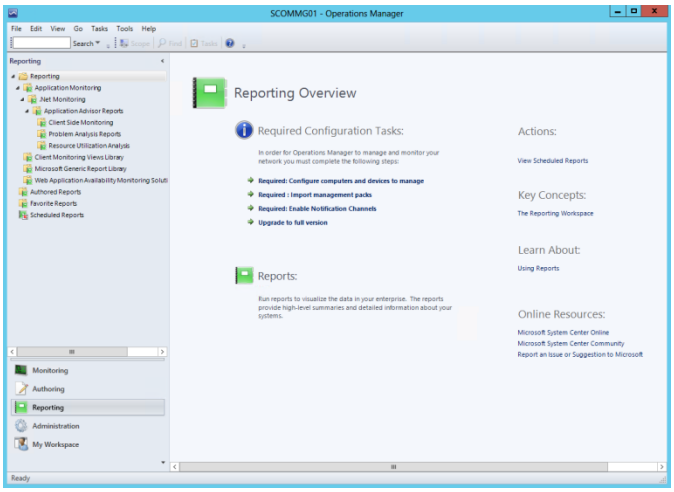


14. The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



15. The wizard will display the progress while installing features.



16. 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.	
17. 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.	

18.4 Post-Installation Tasks

When the installation is complete, the following tasks must be performed to complete Operations Manager and Virtual Machine Manager integration.

Register the Required Service Principal Names for the Operations Manager Management Servers

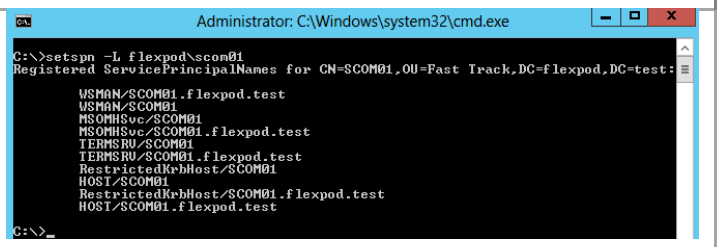
The following steps must be performed on a Domain Controller or one of the Operations Manager servers using a domain admin account or an account with permissions to create SPNs.

▶ Perform the following steps on a **Domain Controller** in the domain where Operations Manager is installed.

1. 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.



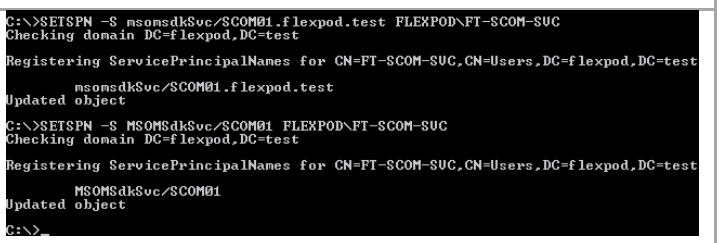
2. The Data Access Service account runs under a domain user account context and is not able to create the appropriate SPNs in Active Directory. The following command must be executed by a domain admin account or an account with delegated permissions to user objects.
3. To set the SPN run the following commands from an administrative command prompt:

SETSPN.exe –S MSOMSdkSvc/<ManagementServerFQDN> <domain>\<SDKServiceAccount>

SETSPN.exe –S MSOMSdkSvc/<ManagementServerNetBIOS> <domain>\<SDKServiceAccount>

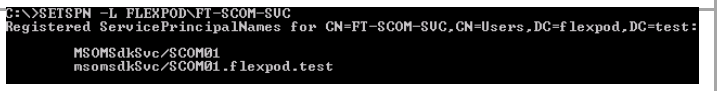
Where <ManagementServerFQDN> is the name of the Operations Manager management server and <SDKServiceAccount> is the name of the Operations Manager Service Account.

4. If there is more than one Management Server being deployed then these commands must be run for each Management Server.



5. When complete the SPNs can be confirmed with the following command:

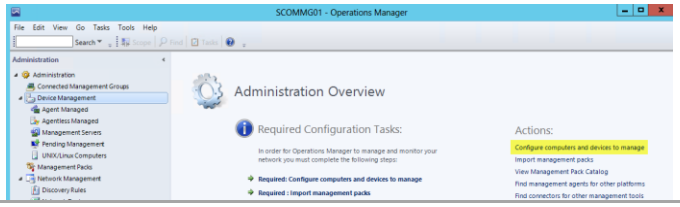
`SETSPN -L <DOMAIN>\<SDKServiceAccount>`



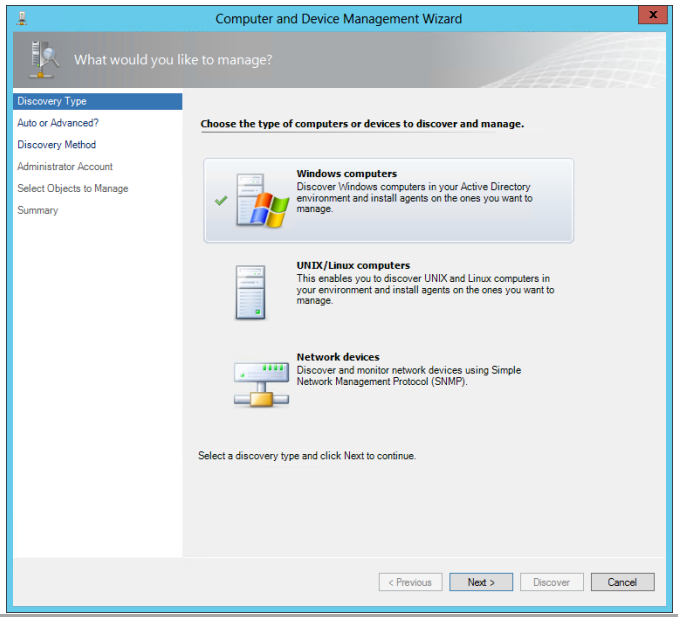
Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Server Nodes

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

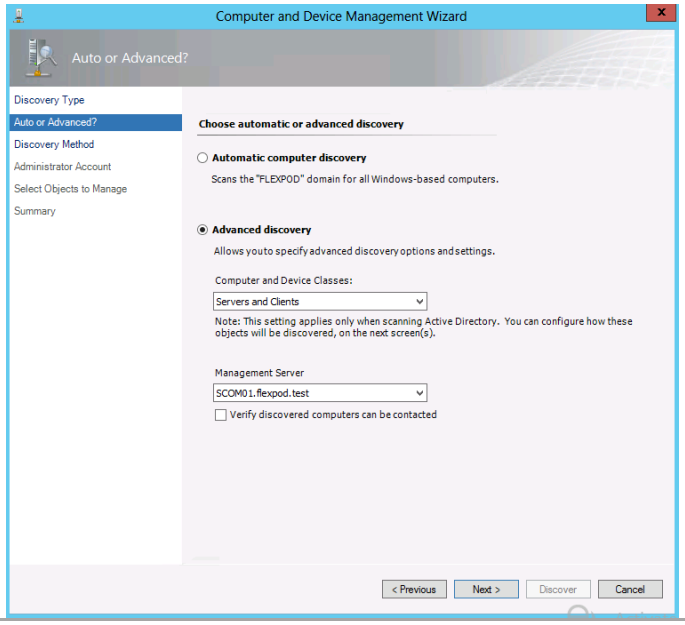
1. In Operations Manager console, navigate to the Administration workspace. Under Actions, select Configure computers and devices to manage.

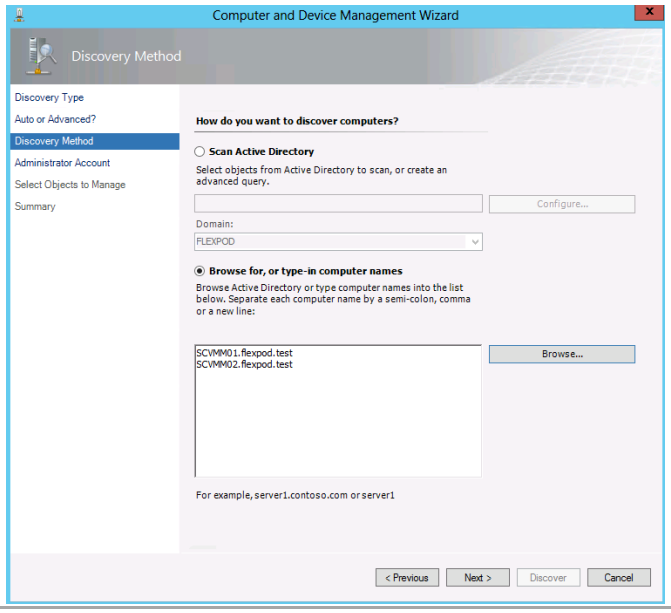
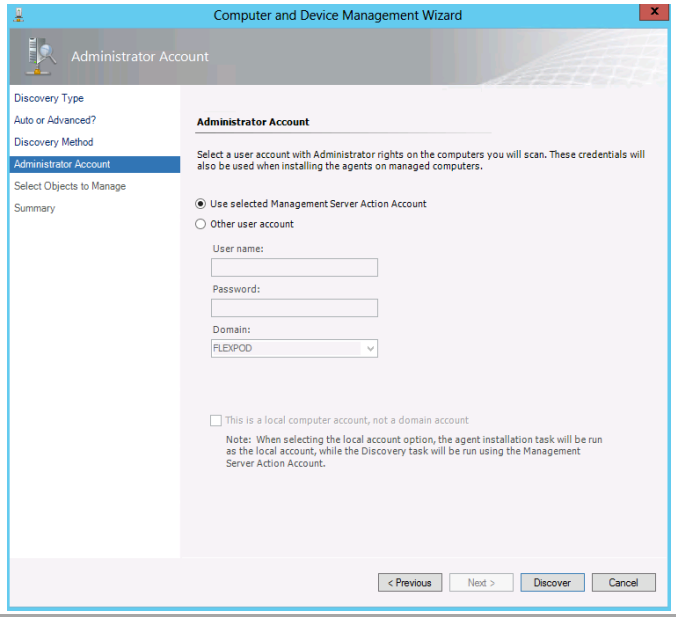


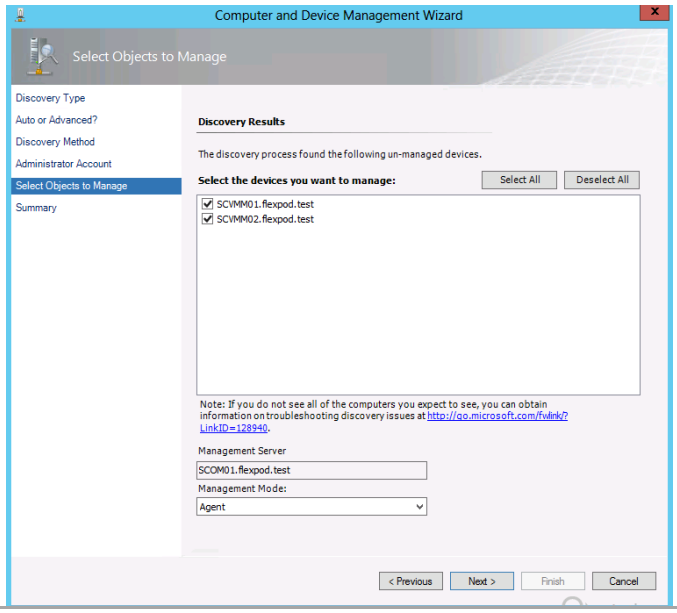
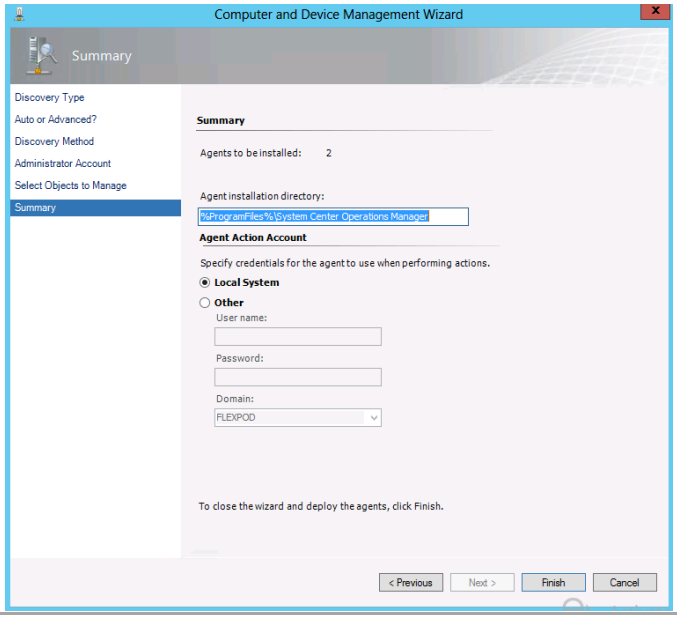
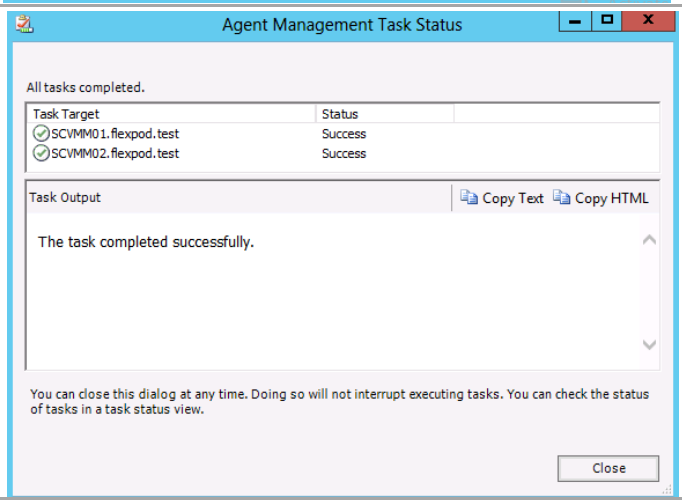
2. The Computer and Device Management Wizard will appear. In the Discovery Type dialog, select Windows computers from the available options and click Next to continue.

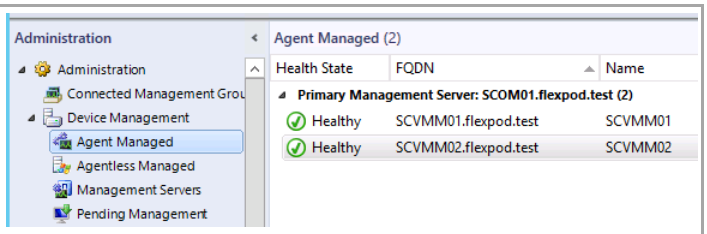
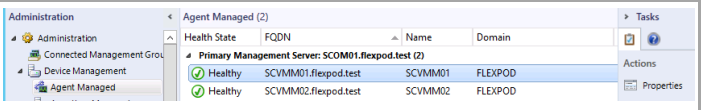
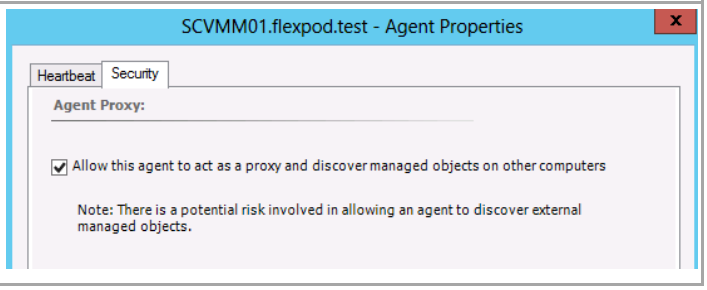


3. In the Auto or Advanced? Select the Automatic computer discovery option and click Next to continue.



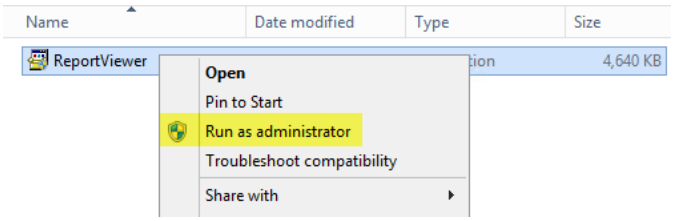
4. In the Discovery Method dialog box, under Browse for, or type-in computer names, input the names of both VMM servers. Click Next to continue.	
5. In the Administrator Account dialog, select the Other user account option and provide the credentials required to access Active Directory and perform discovery in your environment. Verify that this a local computer account, not a domain account check box is clear and click Next to continue.	

6. In the Select Objects to Manage dialog, review the Discovery Results and select the VMM server. From the Management Mode drop-down menu, select Agent and click Next to continue.	
7. 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. When complete, click Finish to perform the agent installation.	
8. In the Agent Management Task Status dialog, verify that the agent installation completes successfully. When successful, click Close to complete the operation.	

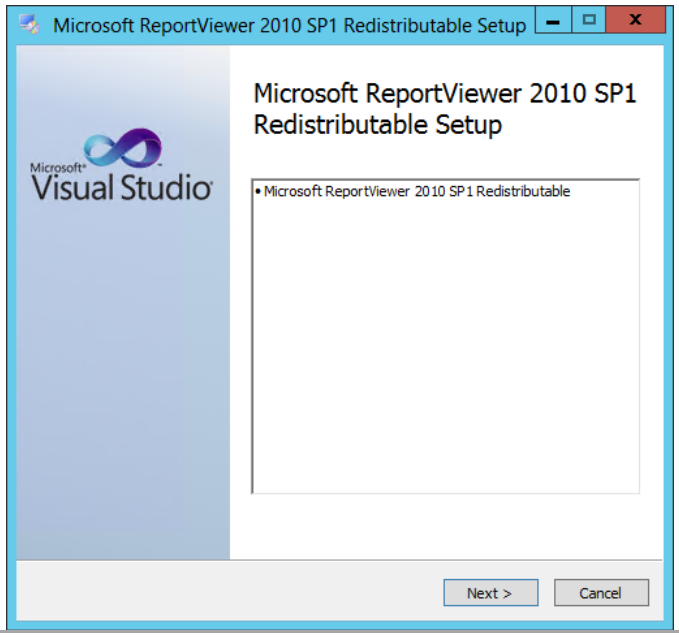
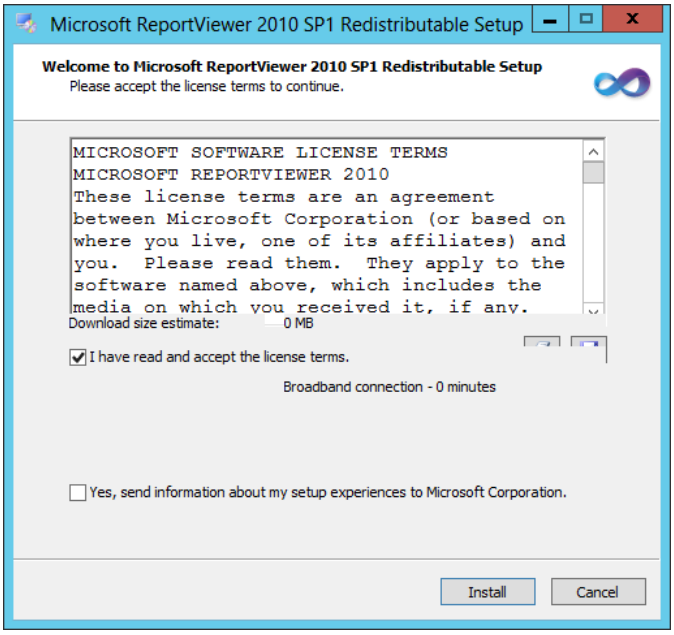
9. The next step is to enable the Operations Manager agent deployed to the Virtual Machine Manager management server to be a proxy agent. 10. In Operations Manager console, navigate to the Administration workspace, expand the Device Management node and select the Agent Managed view. **Note**: It can take a few minutes for the Health State to transition from Not Monitored to Healthy.	
11. In the Agent Managed pane, select the agent associated with the VMM Management Server and click Properties in the task pane.	
12. 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 then click OK to save the changes.	

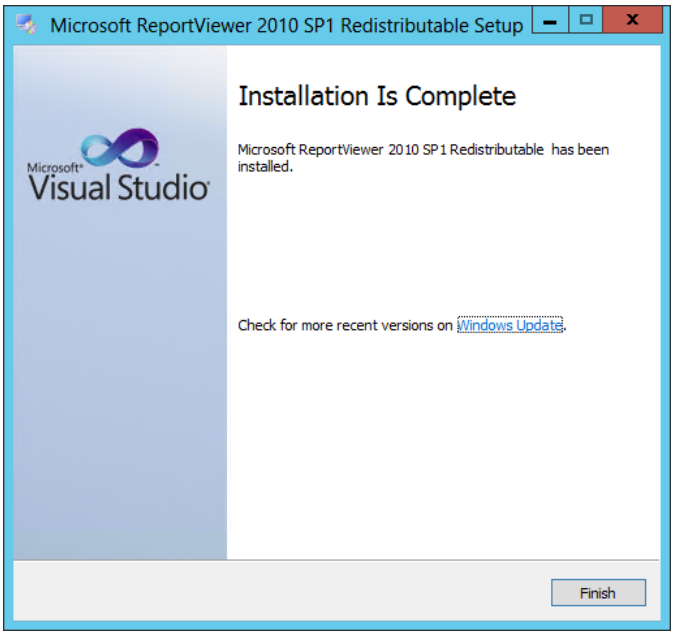
Install Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.[14] Follow the provided steps to install the Microsoft Report Viewer 2010 SP1 package.

▶ Perform the following steps on <u>each</u> **Virtual Machine Manager** virtual machine.	
1. From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.	

[14] Microsoft Report Viewer 2010 SP1 Redistributable Package - http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en.

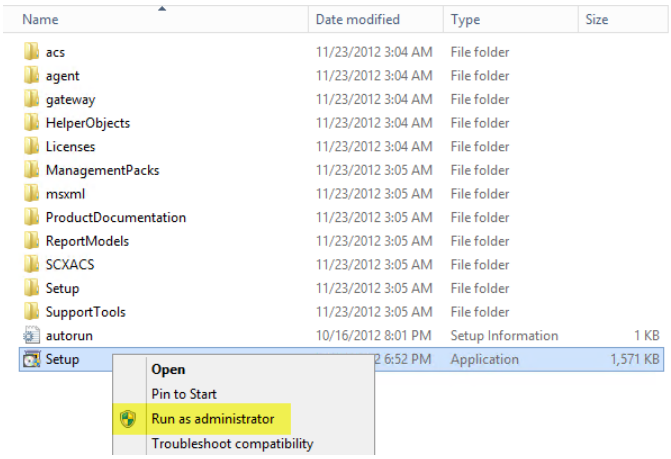
2. Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.	
3. Select the **I have read and accept the license terms** check box and click **Install.**	

4. The installation progress will be displayed in the setup wizard. When completed, click **Finish** to exit the installation.	

Install Operations Manager Console on the Virtual Machine Manager Management Server

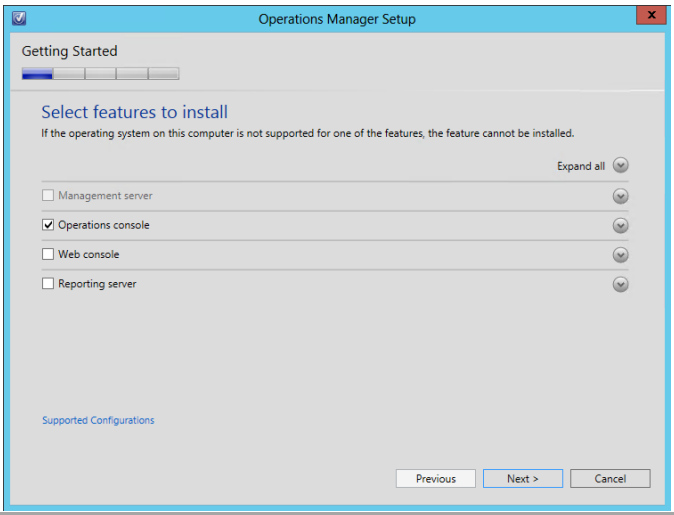
▶ Perform the following steps on each **Virtual Machine Manager** virtual machine.

1. From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

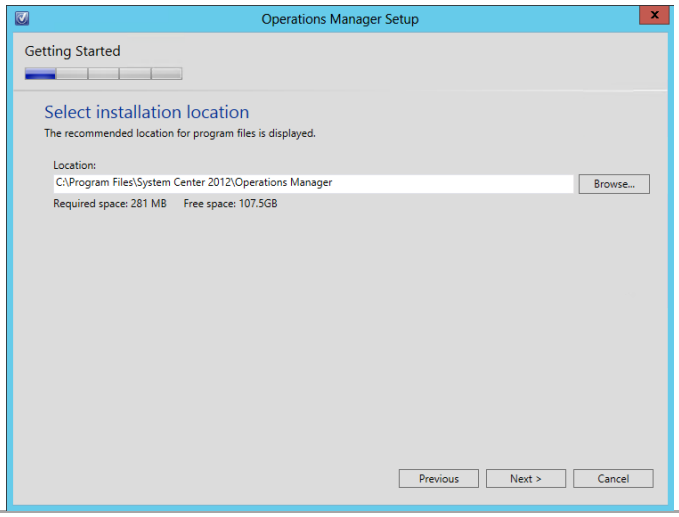


2. The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.

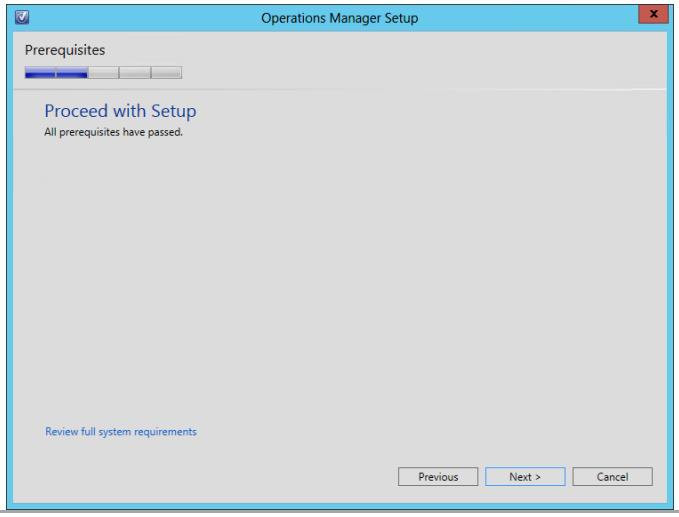
3. In the **Select features to install** dialog, verify that the **Operations console** checkbox is selected. Click **Next** to continue.



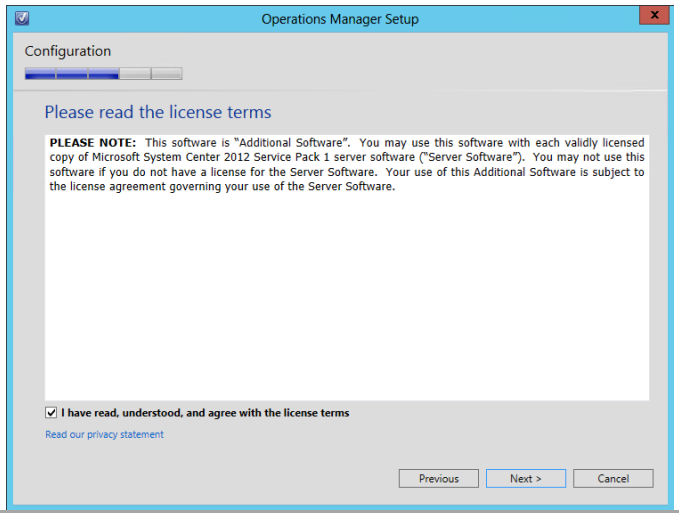
4. In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation.
5. Click **Next** to continue.



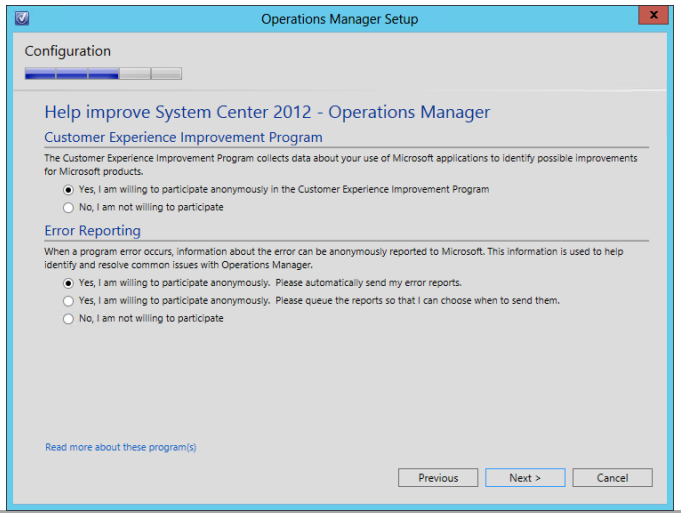
6. The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



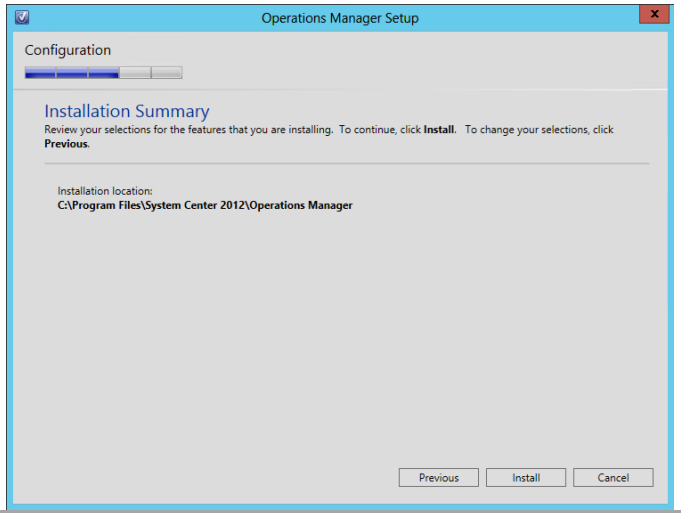
7. In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.



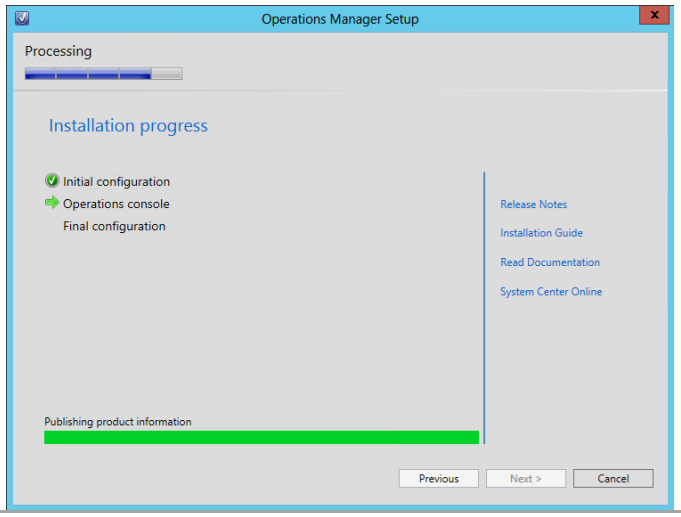
8. The **Help Improve System Center 2012 – Operations Manager** dialog provides options for participating in various product feedback mechanisms. These include:
    a. Customer Experience Improvement Program.
    b. Error Reporting.
9. Select the appropriate option based on your organization's policies and click **Next** to continue.



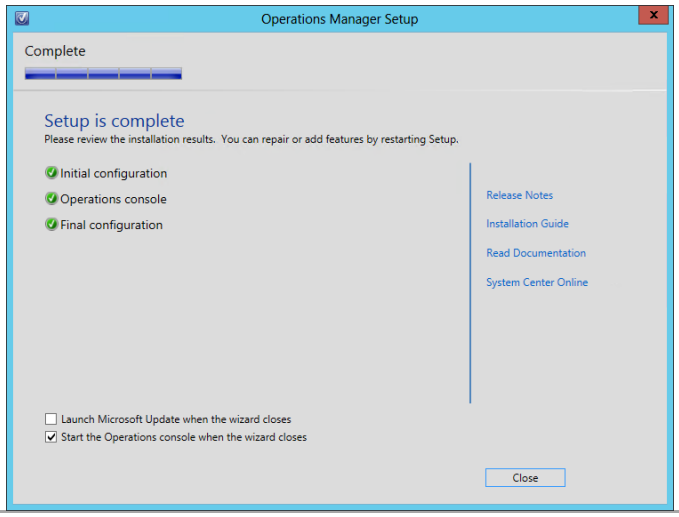
10. The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



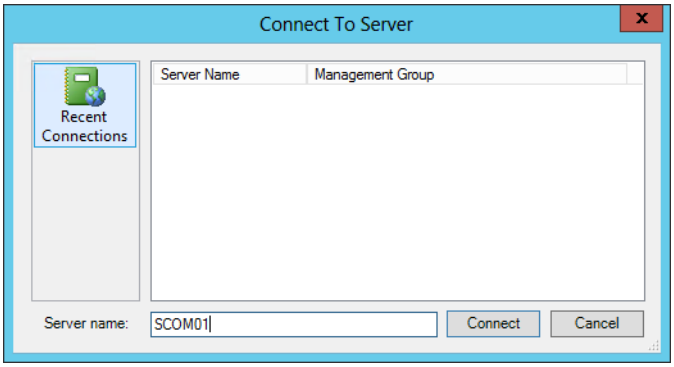
11. The wizard will display the progress while performing the installation.

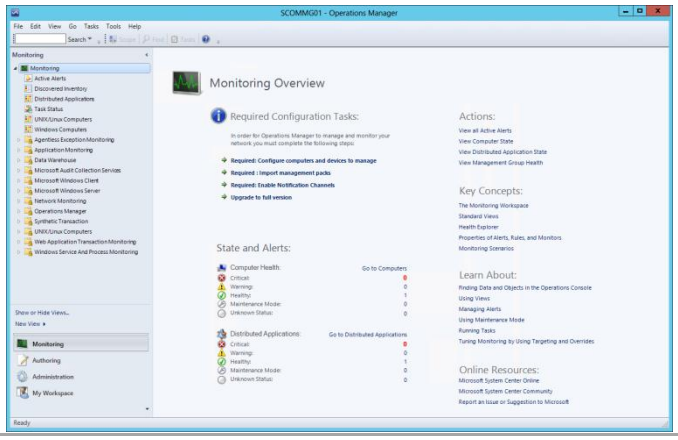


12. When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Management console when the wizard closes** checkbox is selected and click **Close** to complete the installation.



13. 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.

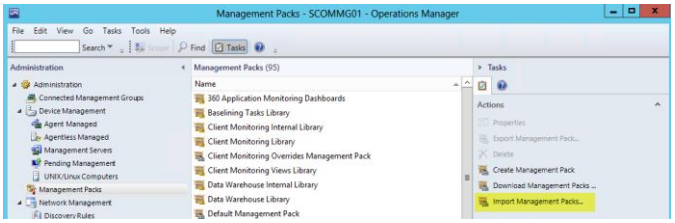




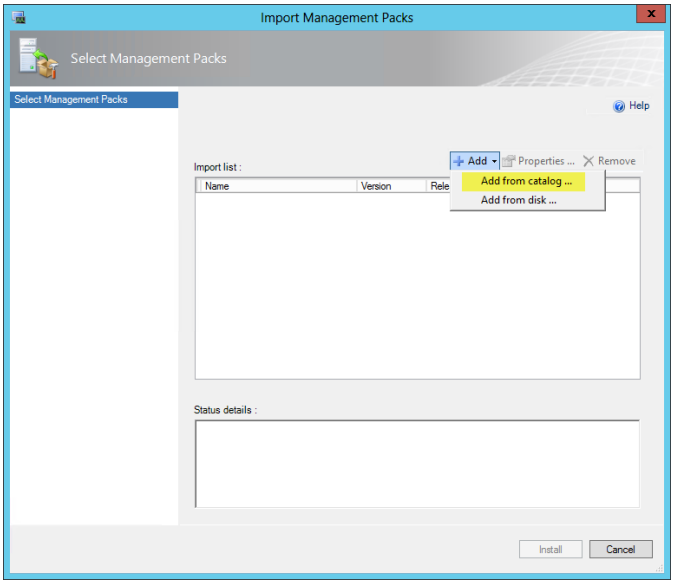
Download and Import the Required Prerequisite Management Packs in Operations Manager

▶ Perform the following steps on the **Operations Manager** virtual machine.

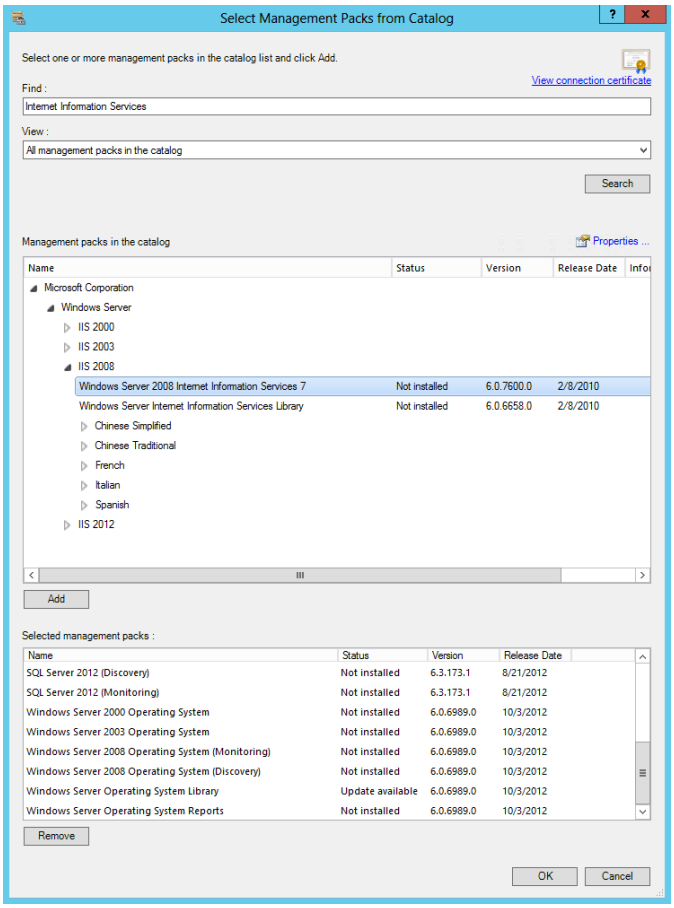
1. In the **Operations Manager** console, navigate to the **Administration** pane and select the **Management Packs** node. In the **Actions** pane, click **Import Management Packs...**

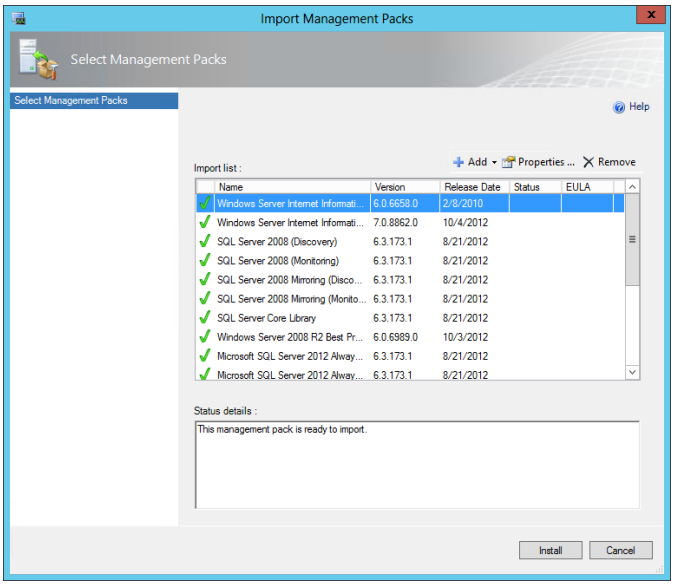
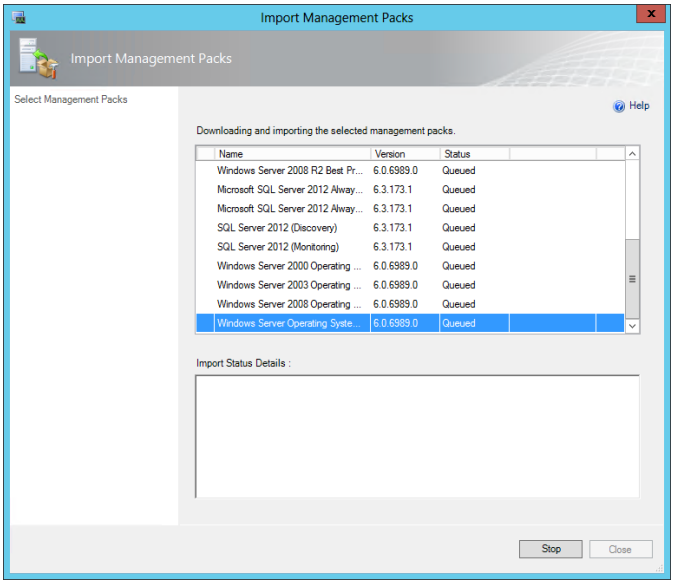
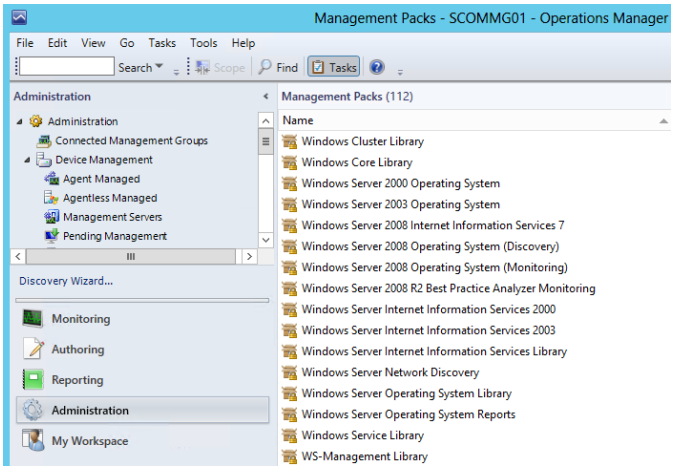


2. In the **Select Management Packs** dialog, click the **Add** button and select **Add from catalog...** in the drop-down menu.



3. In the **Select Management Packs from Catalog** dialog, find and add the following management packs:
    a. Windows Server Internet Information Services Library Version 6.0.6658.0
    b. Windows Server Internet Information Services Library Version 7.0.8862.0
    c. Windows Server Internet Information Services 2000 Version 6.0.6658.0
    d. Windows Server Internet Information Services 2003 Version 6.0.6658.0
    e. Windows Server 2008 Internet Information Services 7 Version 6.0.6658.0
    f. SQL Server 2008 (Discovery) version 6.3.173.1
    g. SQL Server 2008 (Monitoring) version 6.3.173.1
    h. SQL Server 2008 Mirroring (Discovery) version 6.3.173.1
    i. SQL Server 2008 Mirroring (Monitoring) version 6.3.173.1
    j. SQL Server Core Library version 6.3.173.1
    k. SQL Server 2012 (Discovery) version 6.3.173.1
    l. SQL Server 2012 (Monitoring) version 6.3.173.1
    m. Windows Server 2008 R2 Best Practice Analyzer Monitoring version 6.0.6989.0
    n. Windows Server 2000 Operating System version 6.0.6989.0
    o. Windows Server 2003 Operating System version 6.0.6989.0
    p. Windows Server 2008 Operating System (Discovery) version 6.0.6989.0
    q. Windows Server 2008 Operating System (Monitoring) version 6.0.6989.0
    r. Windows Server Operating System Library version 6.0.6989.0
    s. Windows Server Operating System Reports version 6.0.6989.0
    t. Windows Server 2012 Operating System (Discovery) version 6.0.6989.0
    u. Windows Server 2012 Operating System (Monitoring) version 6.0.6989.0
4. When added, click **OK** to continue.



5. At the **Select Management Packs** dialog, click **Install** to import the selected management packs.	
6. The management packs will download and import into Operations Manager. When complete, verify that the imports were successful and click **Close** to exit the Import Management Packs wizard.	
7. In the **Operations Manager** console, go to the Administration workspace and verify the previously selected management packs are now installed.	

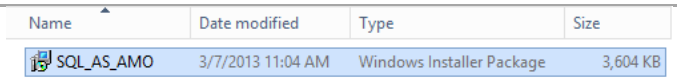
Install SQL Analysis Management Objects

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.

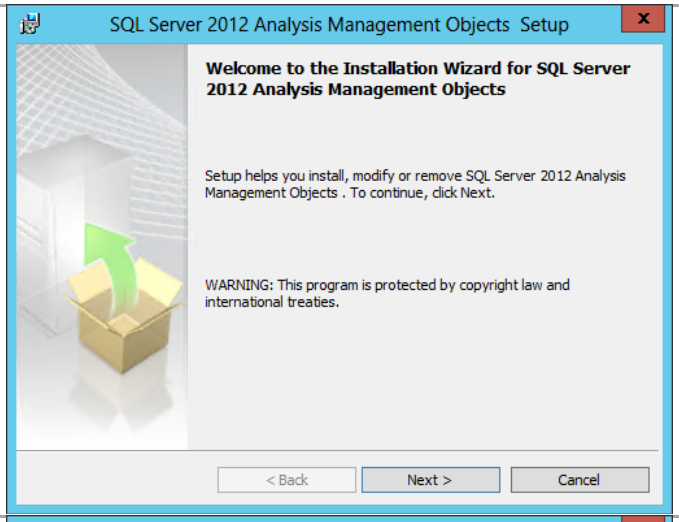
▶ Perform the following steps on both **Virtual Machine Manager** virtual machines.

1. From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.

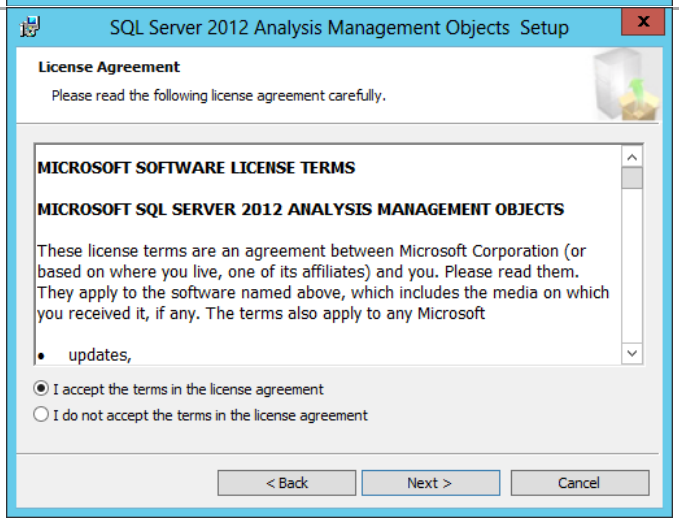
Note: The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580.

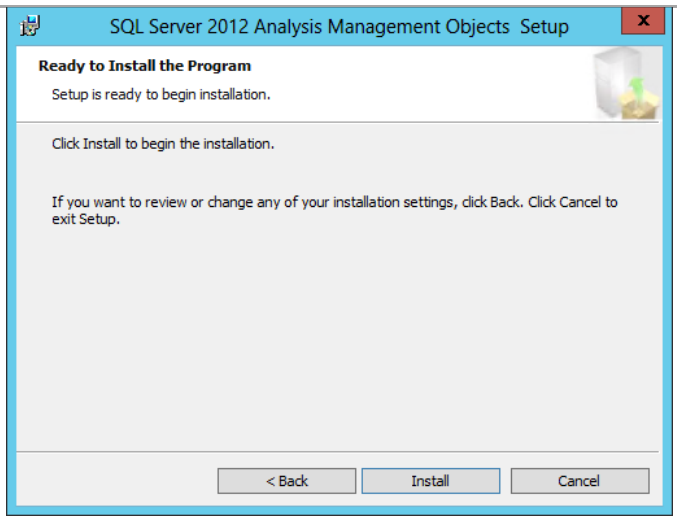
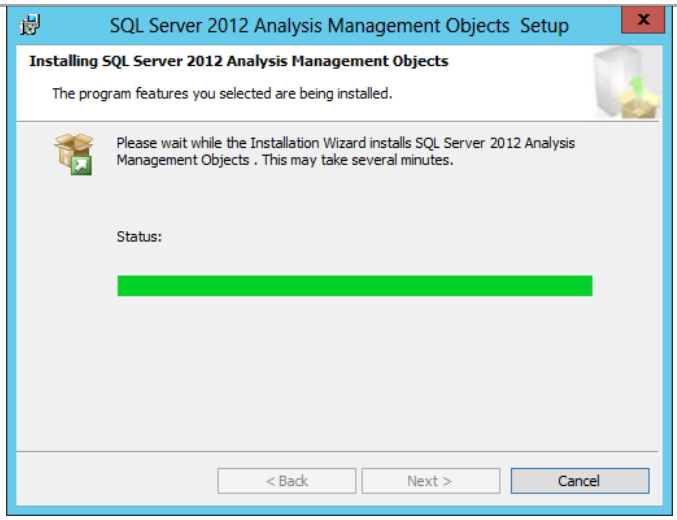
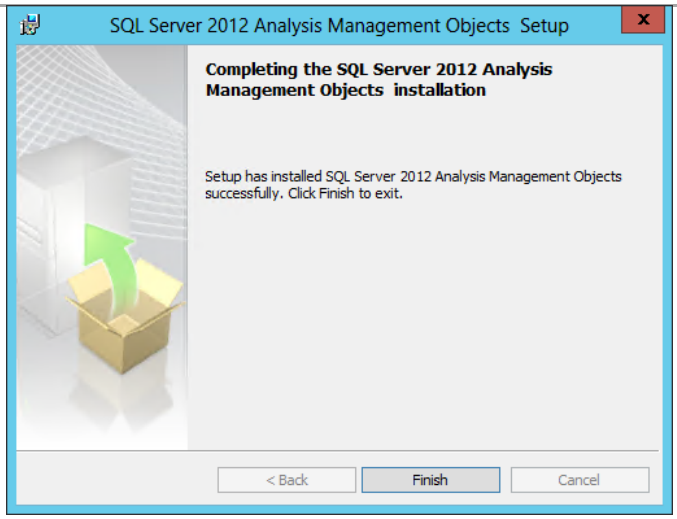


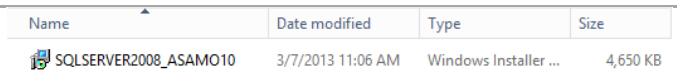
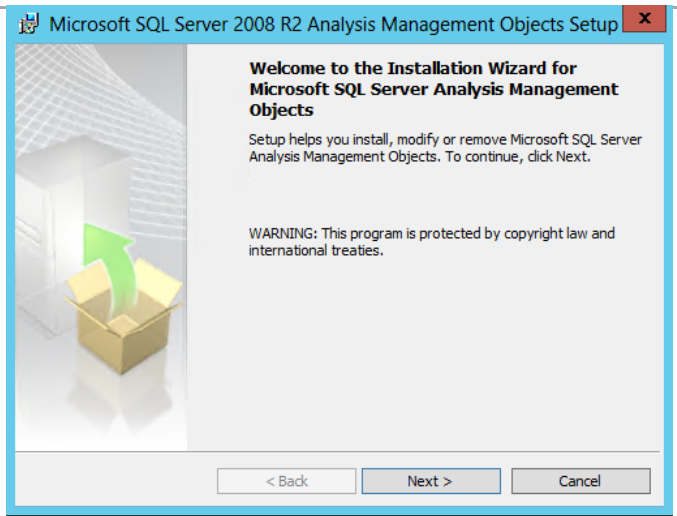
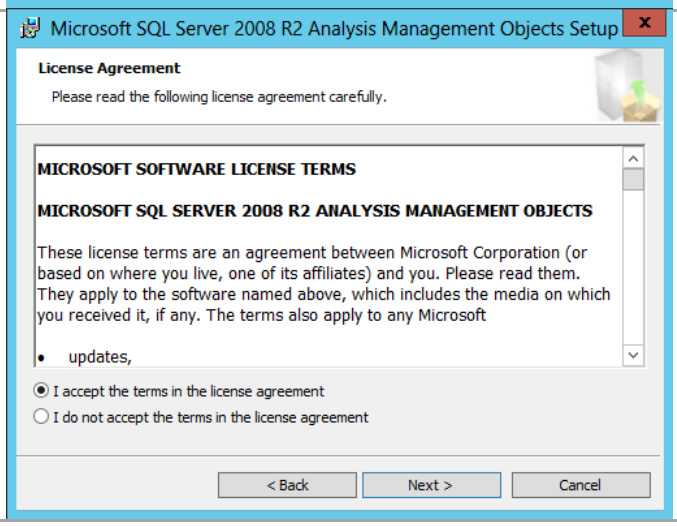
2. The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



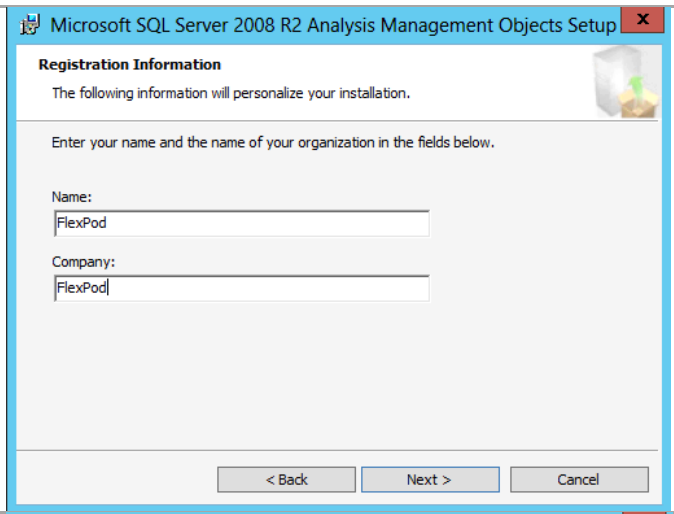
3. In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.



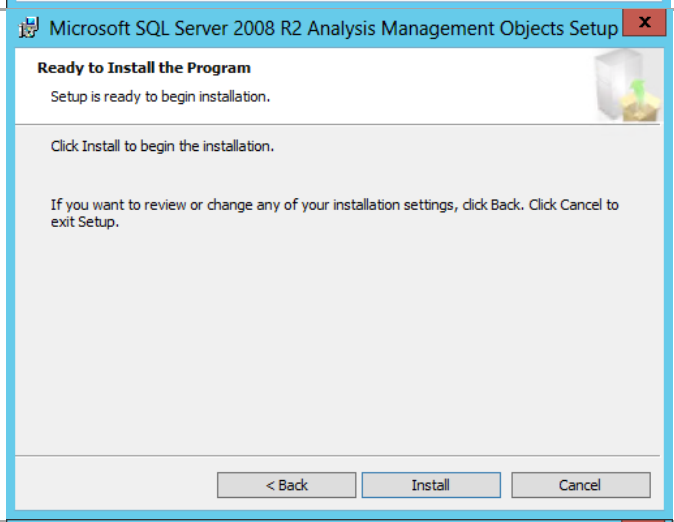
4. In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
5. The installation process may take several minutes to complete. The progress is displayed on the status dialog.	
6. In the **Completing the SQL Server 2012 Analysis Management Objects installation** dialog, click **Finish** to exit the installation.	

7. 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.	
8. The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.	
9. 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.	

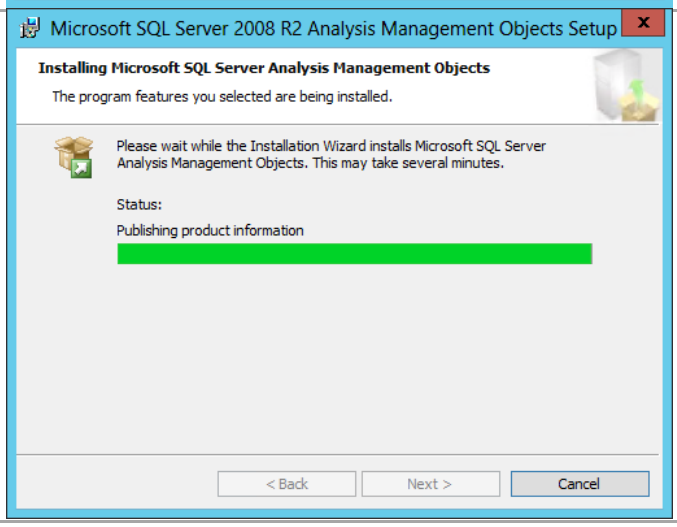
10. In the **Registration Information** dialog, provide values in the **Name** and **Company** textboxes and then click **Next** to continue.



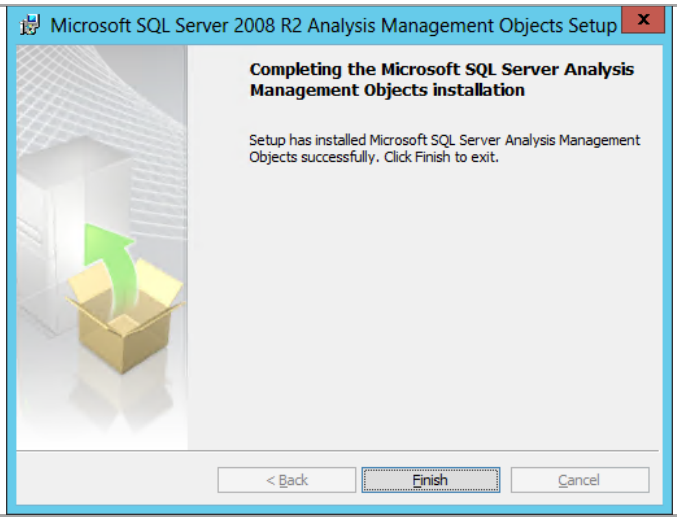
11. On the **Ready to Install the Program** screen, click **Install** to begin the installation.



12. The installation process may take several minutes to complete. The progress is displayed on the Status screen.



13. On the **Completing the SQL Server 2008 Analysis Management Objects** installation screen, click **Finish** to exit the installation.

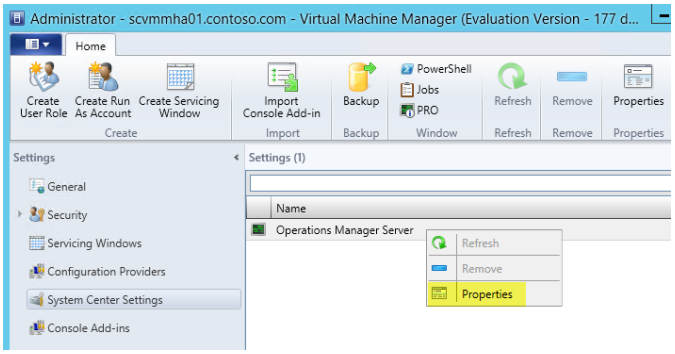


Perform Virtual Machine Manager and Operations Manager Integration

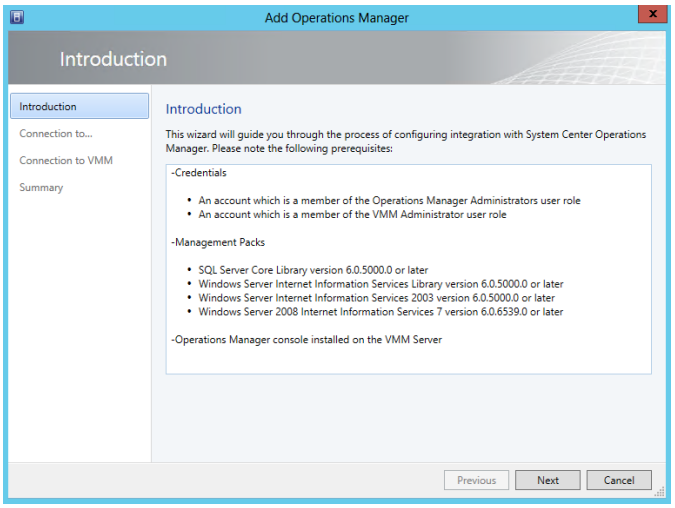
When all pre-requisite configurations and installations are performed, the integration of Virtual Machine Manager and Operations Manager can be completed.

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

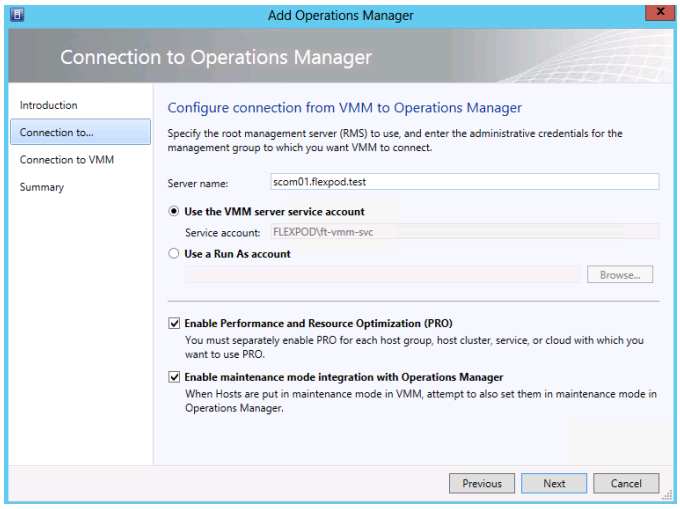
1. In the Virtual Machine Manager console, navigate to Settings pane and select System Center Settings, right-click Operations Manager Server and select Properties from the context menu.

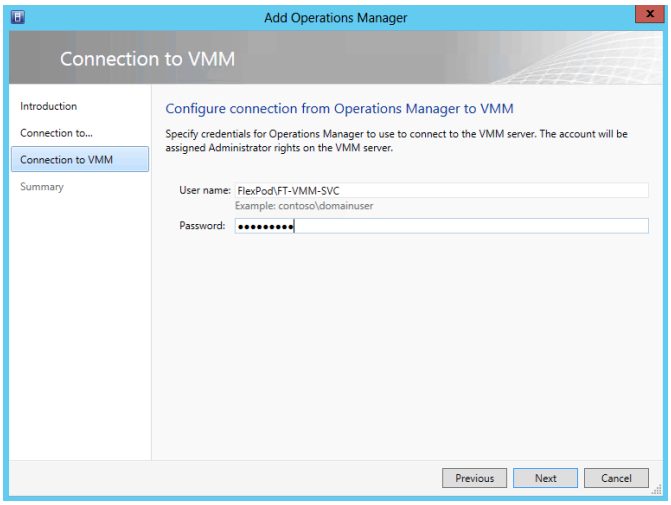
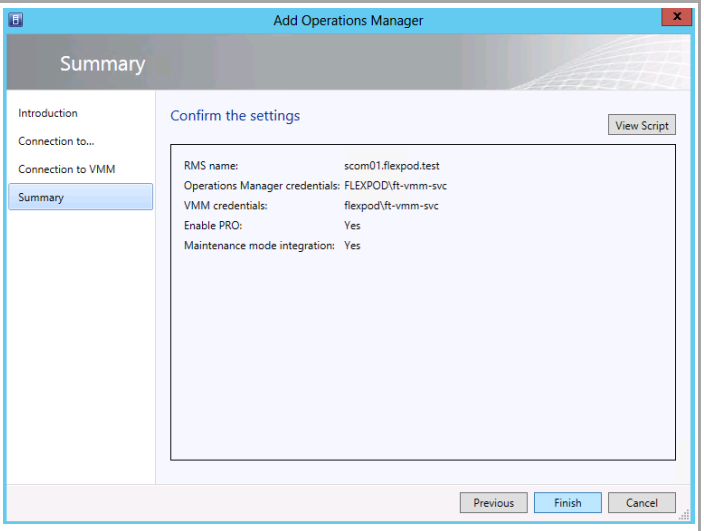
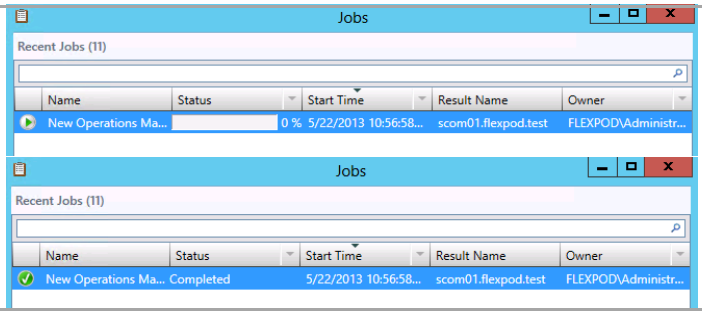


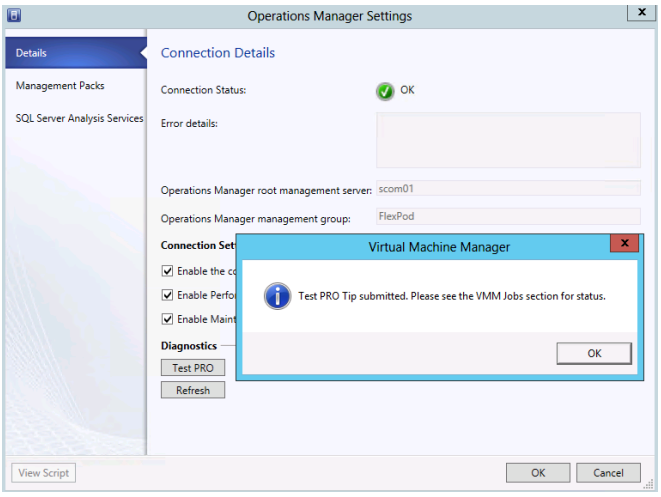
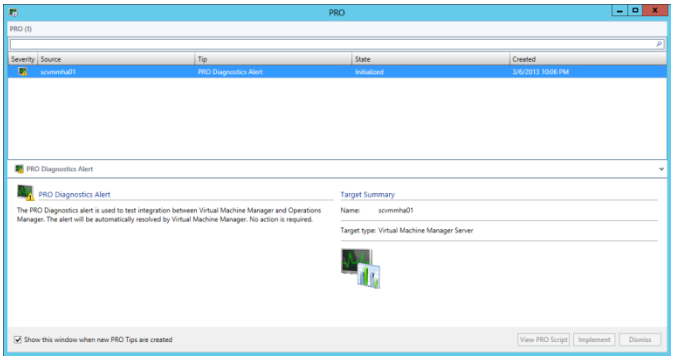
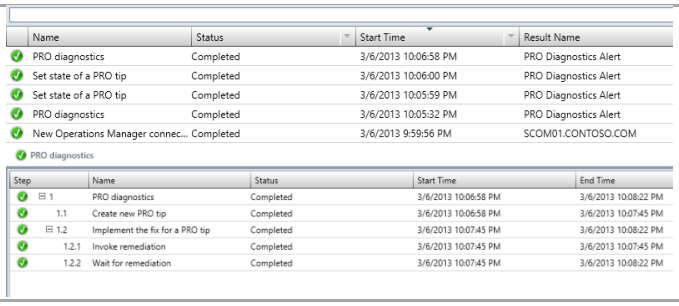
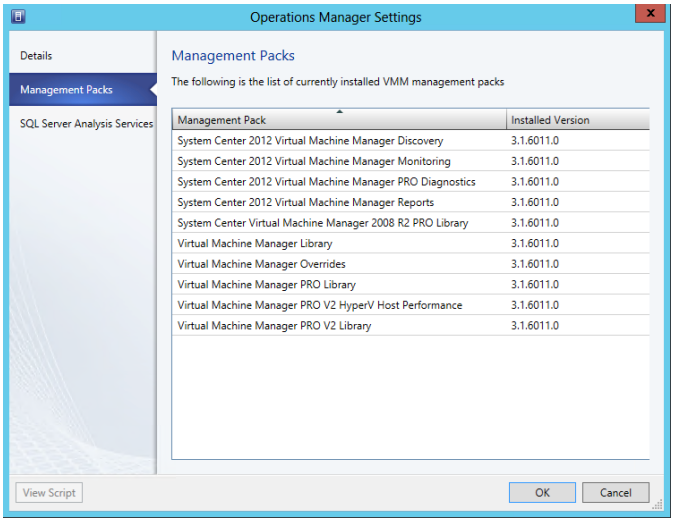
2. The Add Operations Manager dialog will appear. In the Introduction dialog, verify the prerequisites have been met and click Next to continue.



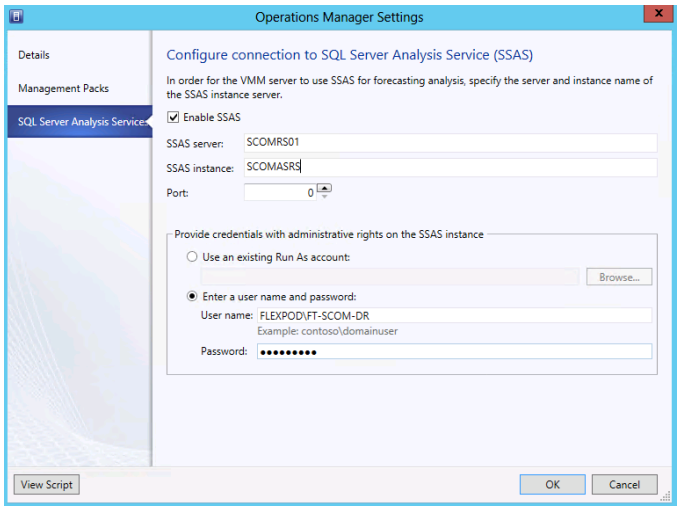
3. In the Connection to Operations Manager dialog, type the FQDN of the Operations Manager server in the Server name text box. Select the Use the VMM server service account option. Select the Enable Performance and Resource Optimization (PRO) and Enable maintenance mode integration with Operations Manager check boxes.
4. When complete, click Next to continue.



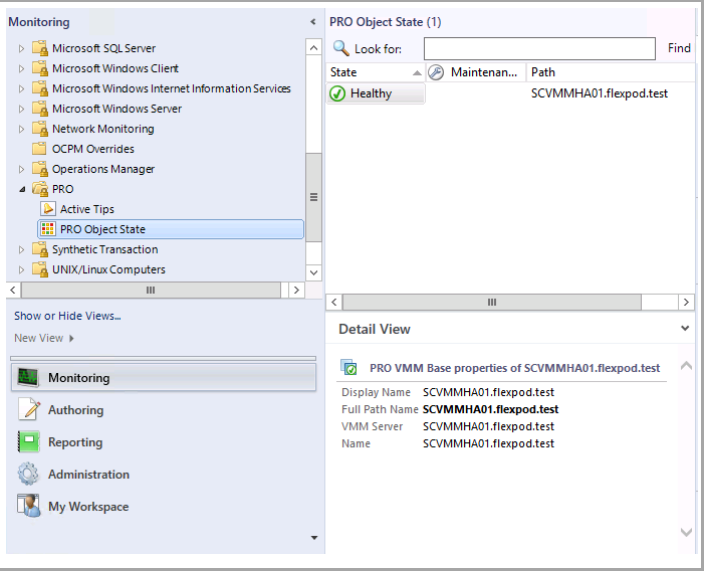
5. In the Connection to VMM dialog, specify the VMM service account credentials in the User name and Password text boxes and click Next to continue.	
6. In the Summary dialog, verify the options selected click Finish to begin the Operations Manager integration process.	
7. The Jobs pane will appear. Before moving forward, wait for the job to complete successfully.	

8. 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. 9. In the Details pane, click the Test PRO button.	
10. As part of the test, PRO will generate a diagnostics alert.	
11. After a few minutes, verify that the PRO test is successful. Navigate to the Jobs pane and verify the PRO jobs completed successfully.	
12. In the Management Packs dialog, verify all Virtual Machine Manager Management Packs were successfully installed.	

13. In the Configure connection to SQL Server Analysis Services (SSAS) dialog, provide the following information.
14. Select the Enable SSAS check box. Provide the following information on the text boxes provided:
    a. SSAS server – *Specify the Operations Manager database server instance.*
    b. SSAS Instance – *Specify the SSAS instance name created earlier.*
15. 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.



16. 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.*"

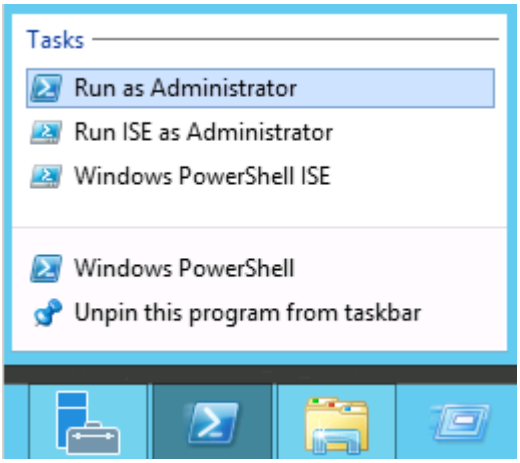
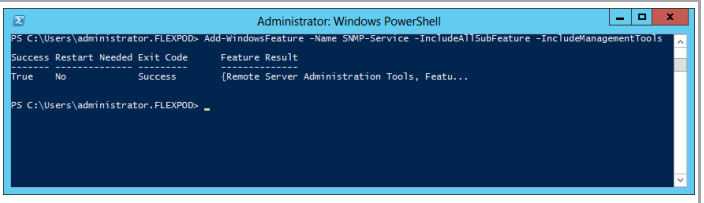
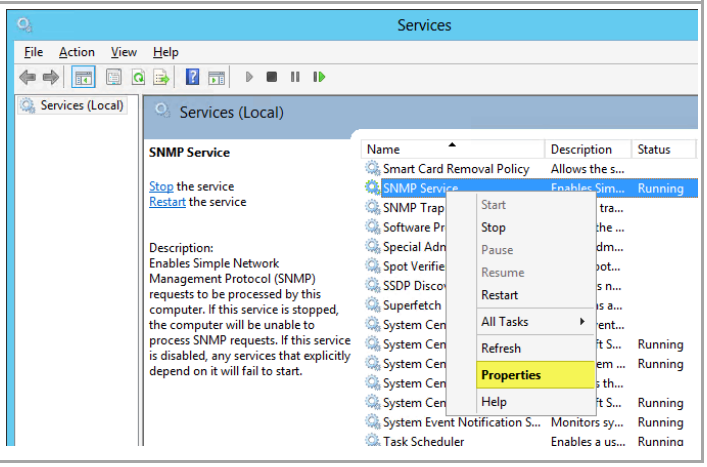


18.5 Install NetApp Management Pack

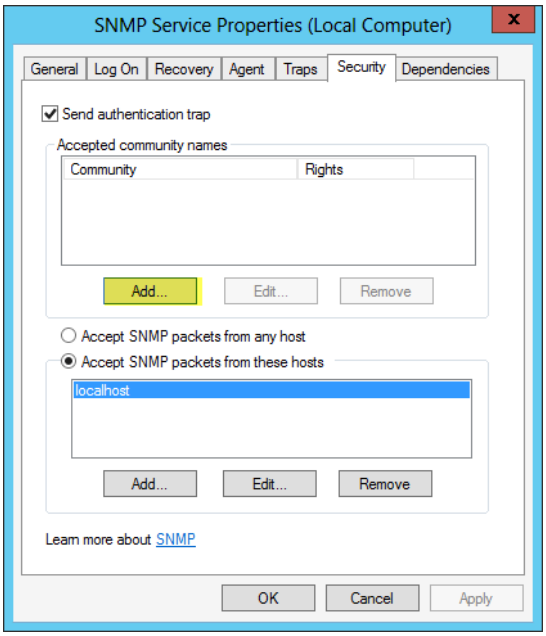
Complete the following steps to install and configure the NetApp OnCommand SCOM Management Pack.

Install and Configure SNMP

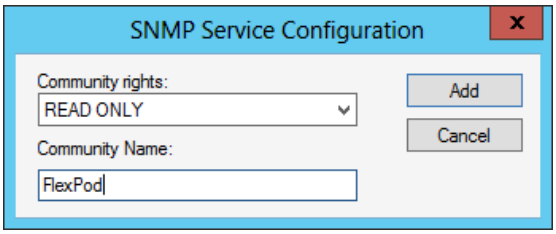
▶ Perform the following steps on the **Operations Manager management server** virtual machine.

1. Launch a PowerShell prompt with administrative permissions: Right-click the PowerShell icon and select **Run as Administrator.**	
2. Add the SNMP feature by entering the following command:	
3. Open the Services management console, right-click **SNMP Service**, and select **Properties.**	

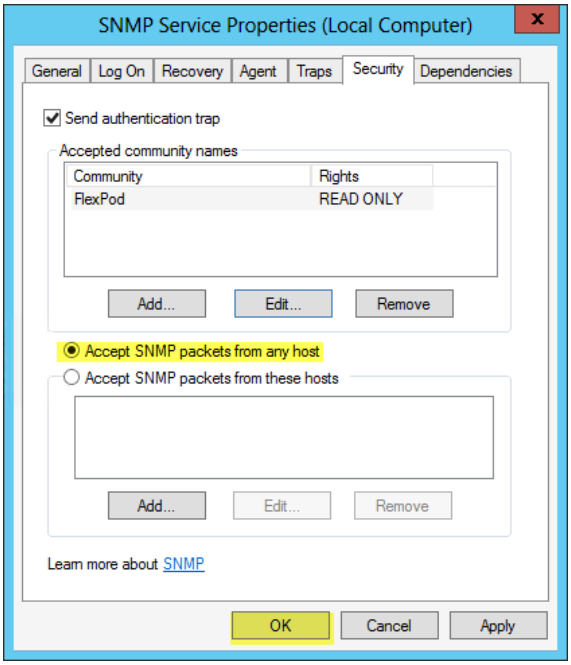
4. On the SNMP Service Properties page select the **Security tab**, and under Accepted Community Names click **Add**.



5. In the SNMP Service Configuration dialog box, set the following values and then click **Add.**

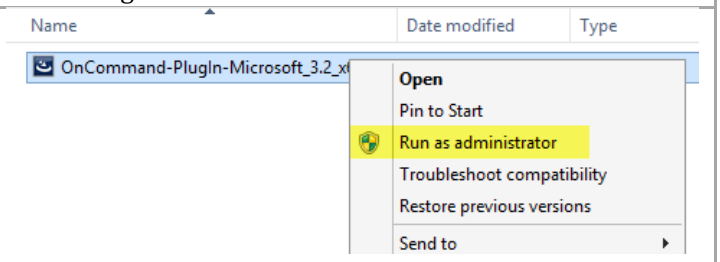
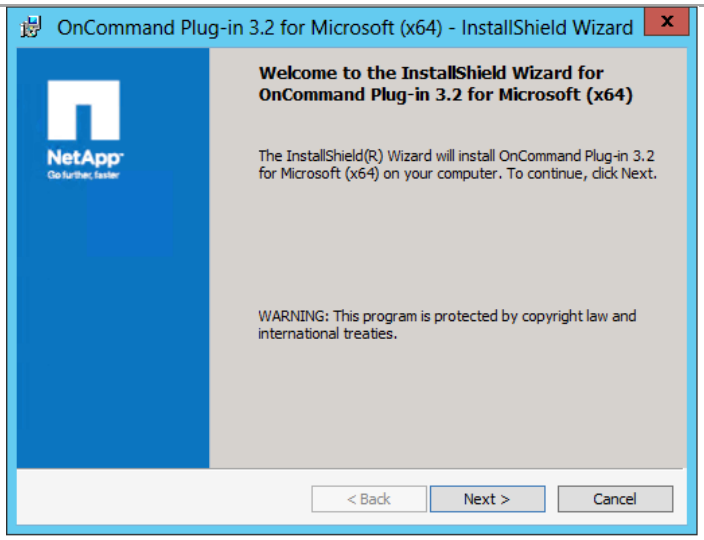
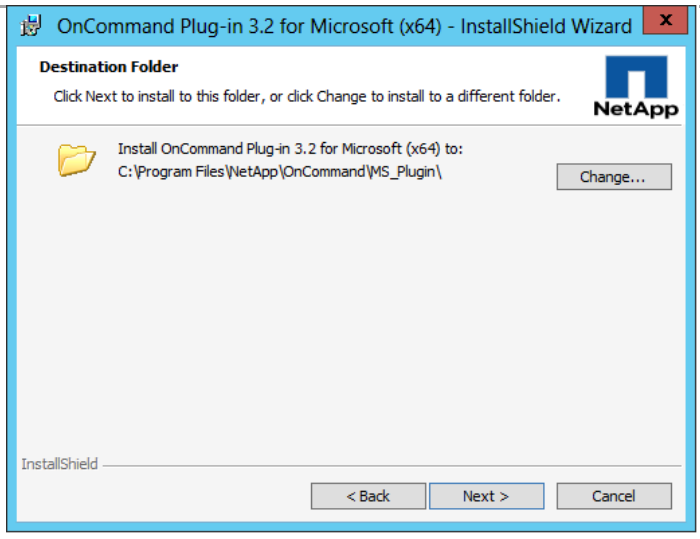


6. On the Security tab, select **Accept SNMP packets from any host.** Click **OK** to complete the configuration.

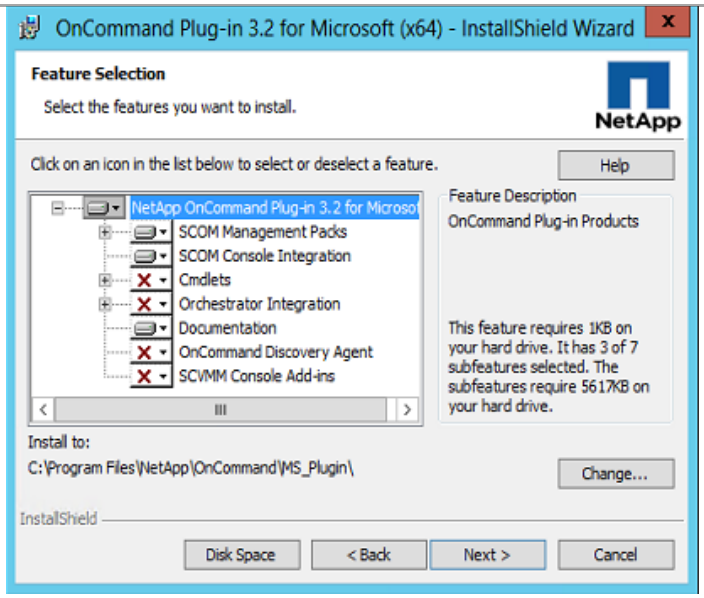


Install NetApp OnCommand Plug-In Management Pack

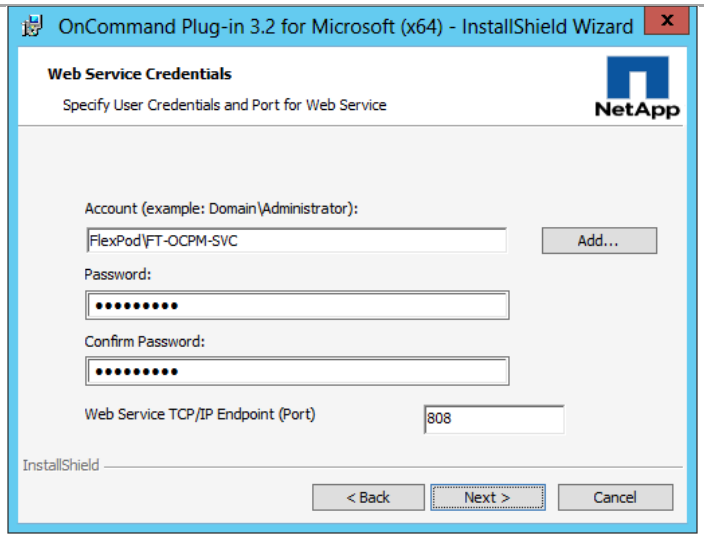
▶ Perform the following steps on the **Operations Manager management server** virtual machine.

<DOMAIN>\FT-OCPM-SVC	This account needs: • Full administrative permissions on all Hyper-V hosts to be managed. • Full administrative permissions on the Operation Management servers.
1. Log in to the SCO management server, right-click the **OCPM 3.2 installation package**, and select **Run as Administrator** to start the OCPM installation wizard.	
2. On the Welcome Page, click **Next**.	
3. On the Destination Folder page, click Next to keep the default installation folder.	

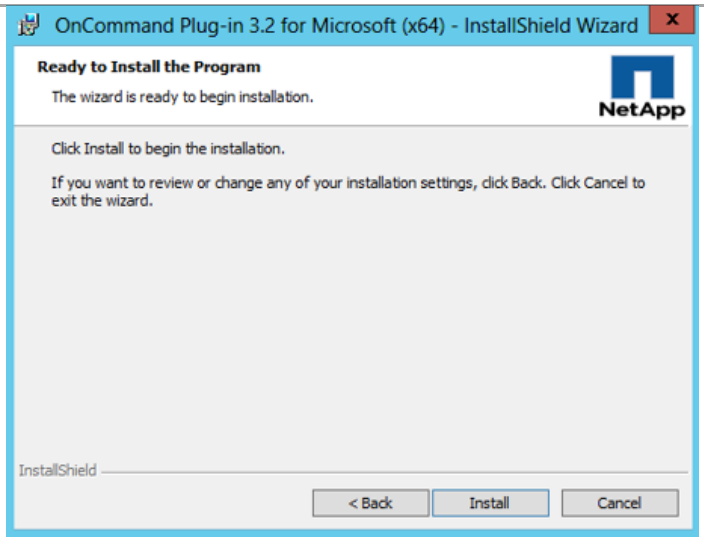
4. On the Feature Selection page, select the following features and click Next:
    a. SCOM Management Packs
    b. SCOM Console Integration
    c. Documentation



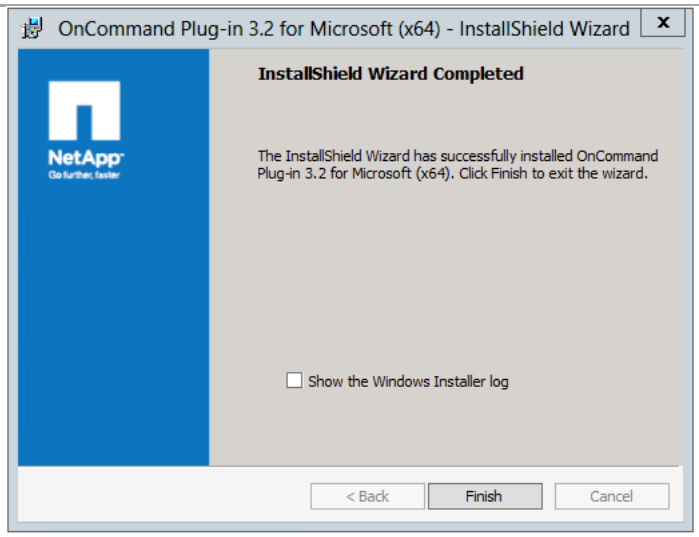
5. On the Web Service Credentials page, enter the following credentials and click Next:
    a. Account: Active Directory domain user account to be used for web service communication
    b. Password: Password of the domain user account
    c. Web Service TCP/IP Endpoint (Port): Leave the default value of 808 unless there is a port conflict or firewall configuration that requires a change in the port
6. All System Center servers running the OCPM web service must use the same port for communication.



7. Click Install to continue the installation.



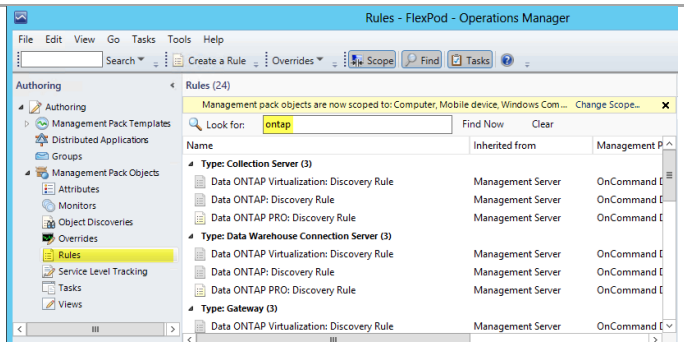
8. On the InstallShield Wizard Completed page, click Finish to complete the installation.
9. It may be necessary to reboot the server to completely register the management pack and its associated tasks.



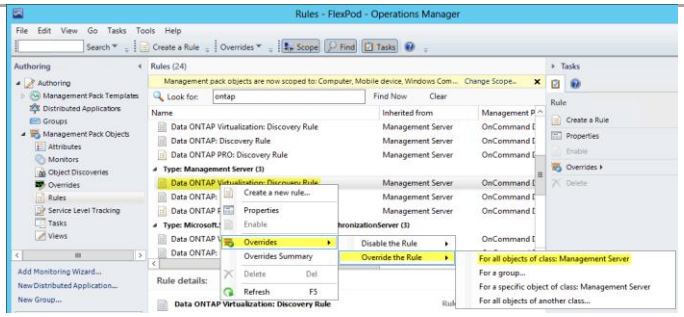
Enable NetApp OnCommand Plug-In Management Pack

▶ Perform the following steps on the **Operations Manager** virtual machine.

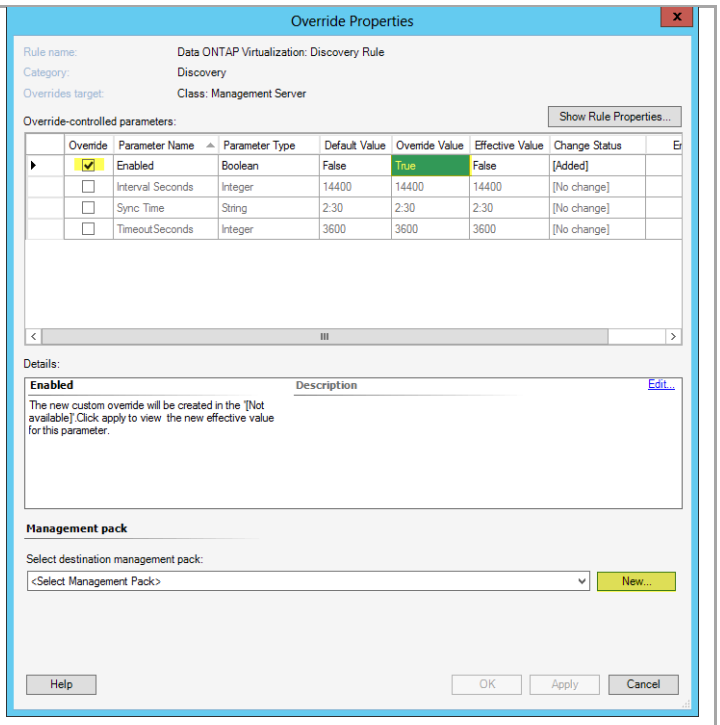
1. In the **Operations Manager** console, navigate to the **Authoring** pane and select the **Management Packs Objects** node and the **Rules** subnode.
2. Enter `ontap` in the Look For field and click **Find Now**.

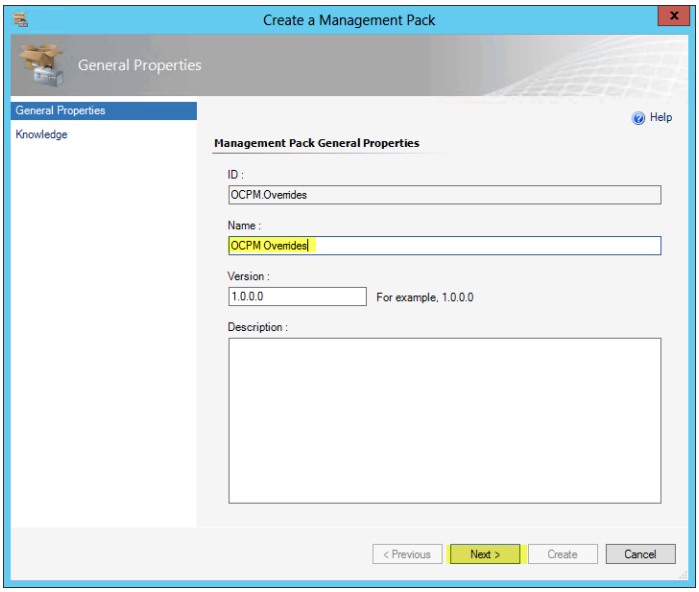


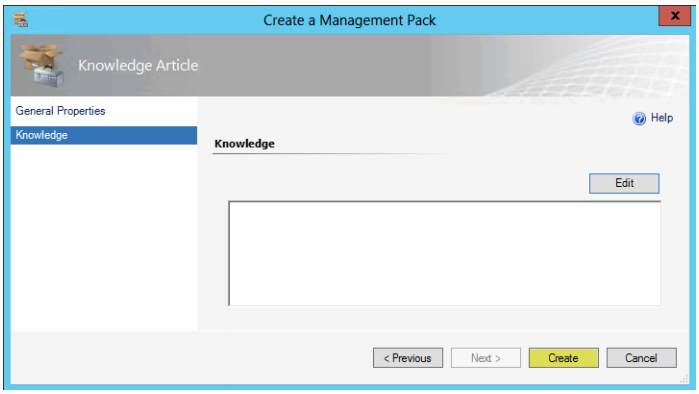
3. Scroll down to the **Type: Management Server** list.
4. Right-click Virtualization Discovery Rule and select Overrides > Override the Rule > For all Objects of Class: Management Server.



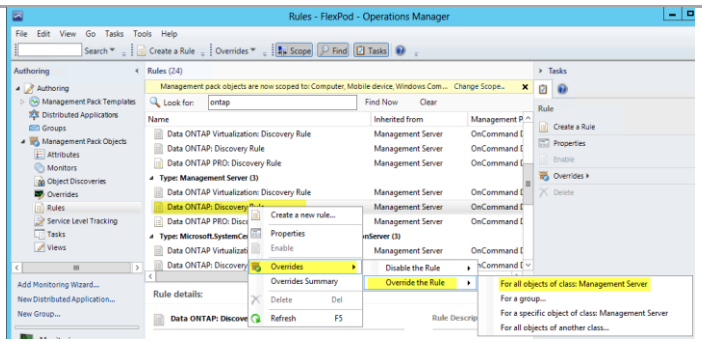
5. On the Override Properties page, set the following properties for the Enabled parameter:
    a. Override: **Select**
    b. Override Value: **True**
    c. Optional: Set additional override values as required
6. Under Select destination management pack, click **New** to launch the Create a Management Pack Wizard.
7. Enter a **name** for the new management pack and click **Next**.
8. Click **Create**.
9. Click **OK** to save the override settings to the new management pack.



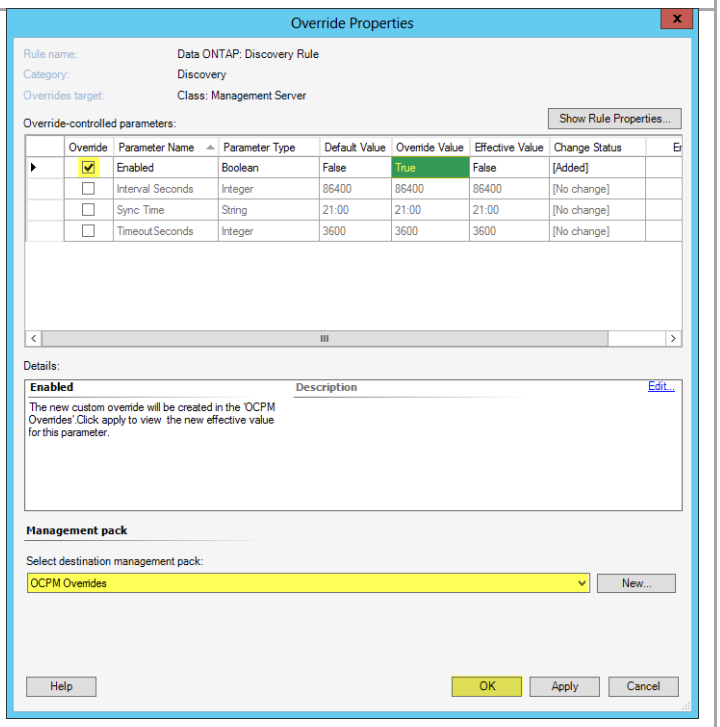




10. Scroll down to the **Type: Management Server** list.
11. Right-click Discovery Rule and select Overrides > Override the Rule > For all Objects of Class: Management Server.



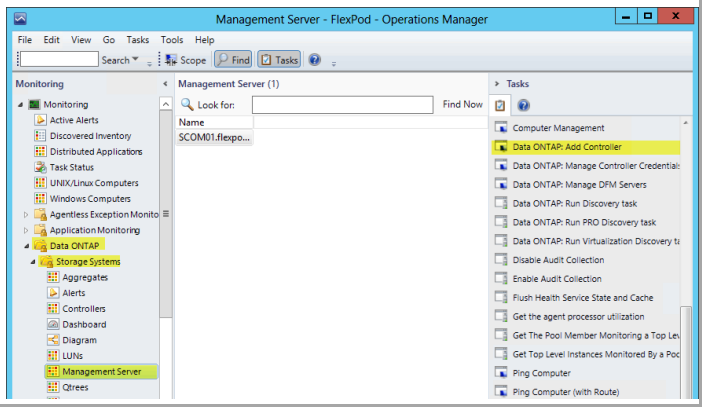
12. On the Override Properties page, set the following properties for the Enabled parameter:
    a. Override: **Select**
    b. Override Value: **True**
    c. Optional: Set additional override values as required
13. Under Select destination management pack, **select the management pack** created on the last override.
14. Click **OK** to save the override settings to the new management pack.



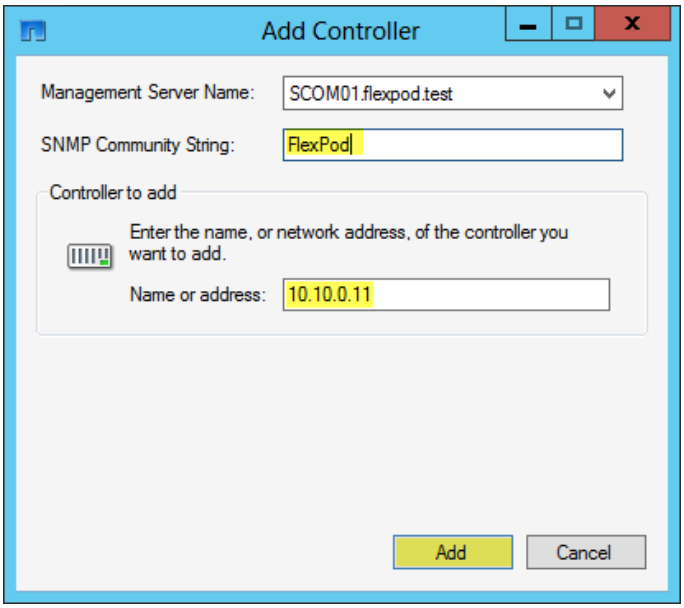
Configure NetApp OnCommand Plug-In Management Pack

▶ Perform the following steps on the **Operations Manager** virtual machine.

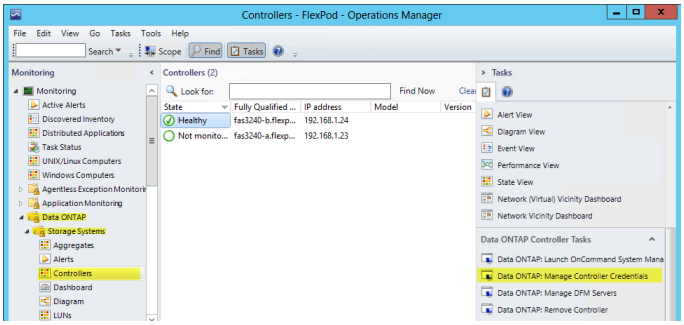
1. In the Operations Manager console, navigate to the Monitoring pane and select Data ONTAP -> Storage Systems -> Management Server.
2. In the Tasks pane, select Data ONTAP Add Controller.



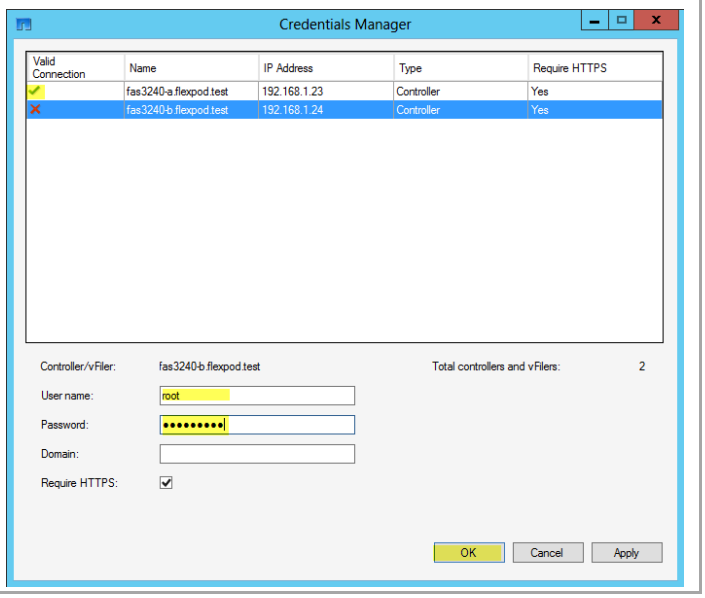
3. Change the SNMP community string to the one set during the controller setup.
4. Enter the controller name or IP address and click Add.
5. Repeat for each node in the environment.
6. It may be necessary to add the VMM host to the traphosts in Data ONTAP to enable discovery. To do so, enter the following command:
   `snmp traphost add <VMM IP>.`



7. In the Operations Manager console, navigate to the Monitoring pane and select Data ONTAP -> Storage Systems -> Controllers.
8. In the Tasks pane, select Data ONTAP Manage Controller Credentials.



9. Enter the credentials for each storage controller.
10. Click Apply to validate each credential.
11. A green check mark in the Valid Connection column indicates a successful connection.
12. Click OK to save the credential changes.
13. It can take 15 minutes to an hour to complete discovery after the credentials are saved.



18.6 Install the Cisco UCS Management Pack

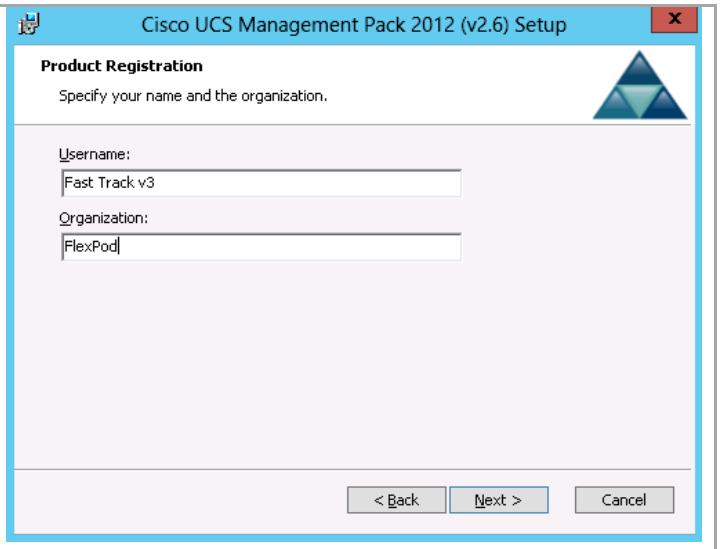
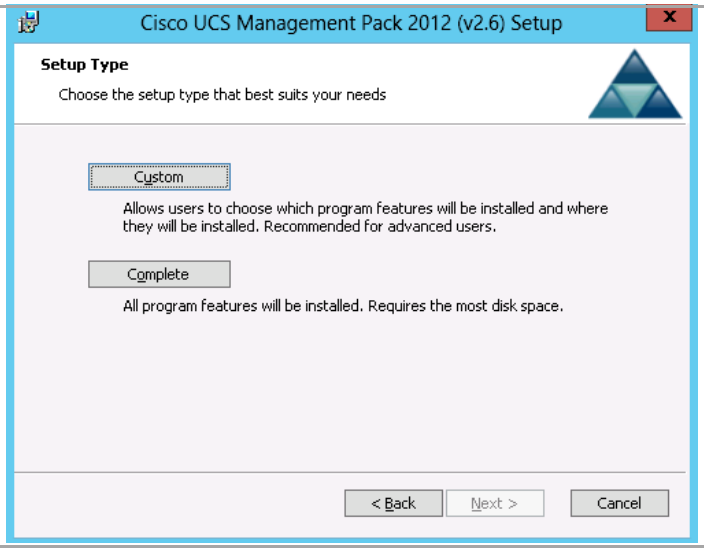
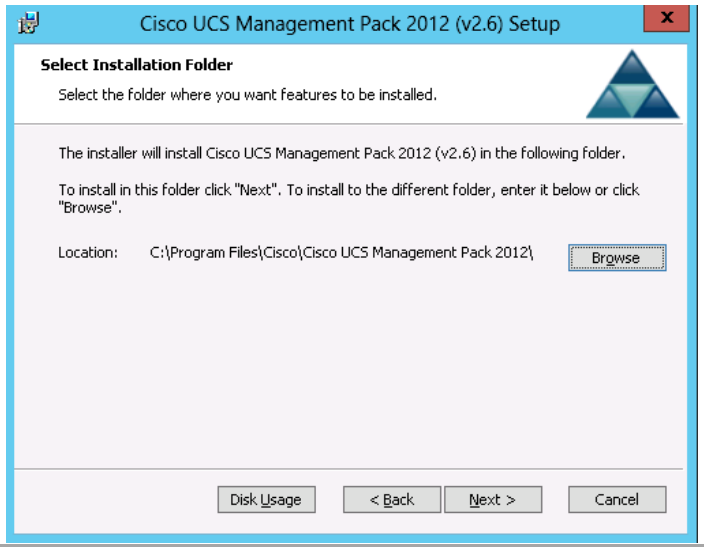
Verify the following Components are installed in the virtual machine where management pack will be installed

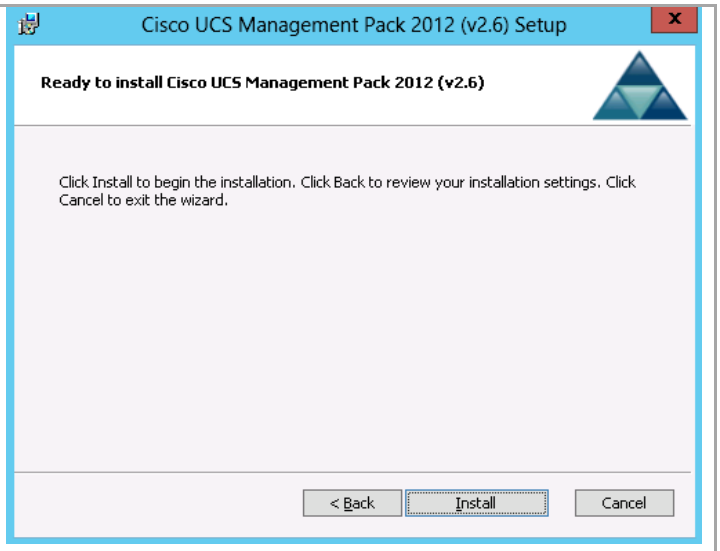
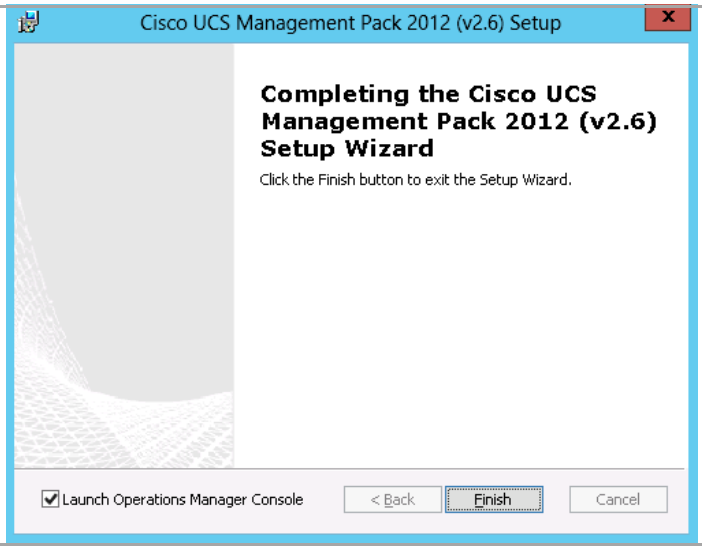
- Windows PowerShell 2.0
- .NET Framework 4
- Microsoft XM Core Services 6.0 (with latest Service Pack)
- System Center 2012 Operations Manager

▶ Perform the following steps on all the Operations Manager virtual machine.

1. Launch the Management Pack Installer. The **Setup Wizard** screen appears.

2. Click the **Next** button. The **License Agreement** screen appears. Select **I agree** radio button and click the **Next** button.

3. Enter Username and Organization.	
4. Select the Complete installation option.	
5. The **Select Installation Folder** Screen appears. Specify the folder location to install the Management Pack, in the **Location** field and click the **Next** button.	

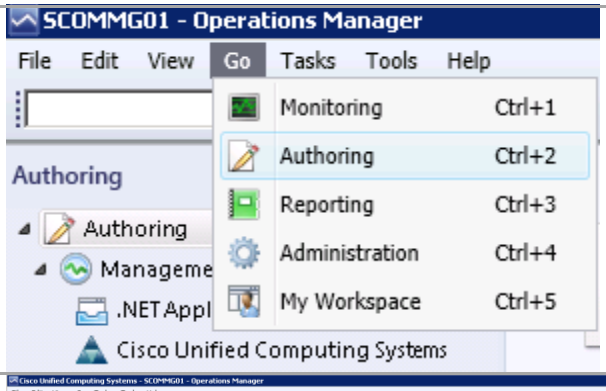
6. Click the **Install** button to start the installation.	
7. After successful installation of Cisco UCS Management Pack the **Installation Complete** screen appears. Click the **Finish** button to exit and launch the Operations Manager Console.	

Configuring SCOM to Monitor Cisco Unified Computing System

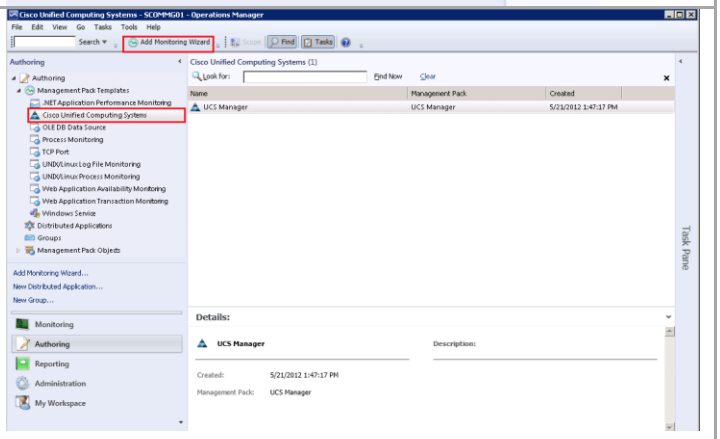
After the Cisco UCS Management Pack is successfully installed on the Operation Manager virtual machine it must be configured for accessing configuration and event data on the Cisco Unified Compute System. The following procedures provide guidance for this process.

▶ Perform the following steps on all the Operations Manager virtual Machine.

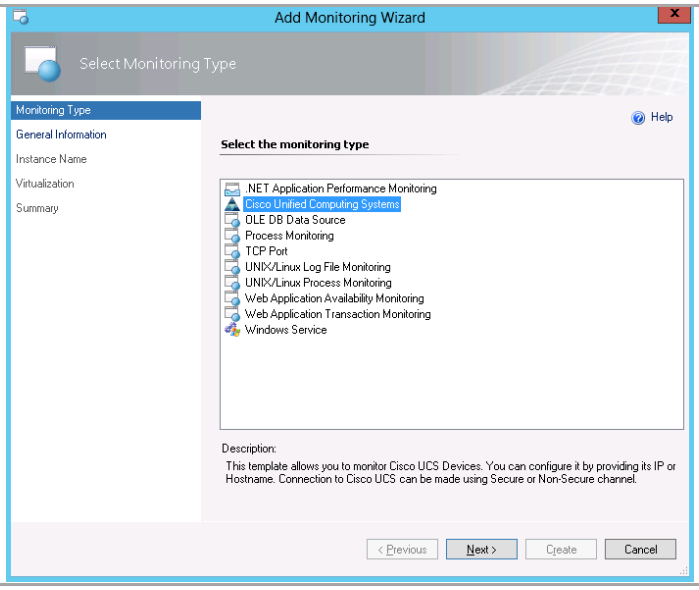
1. In the **Operations Manager** console, click the **Go** tab in the menu bar.
2. Select **Authoring** from the drop-down menu. The **Authoring** column options appear.

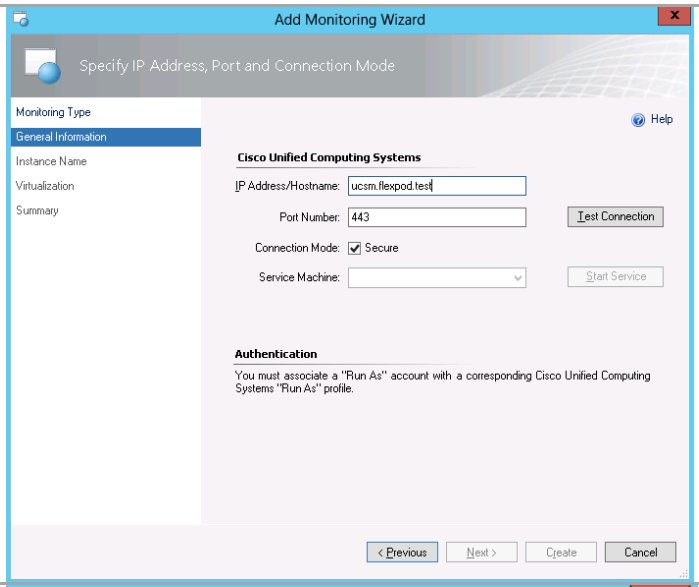


3. In the **Authoring** column, expand **Management Pack Templates** and select **Cisco Unified Computing Systems**. In the **Tasks** panel, click the **Add Monitoring Wizard**.

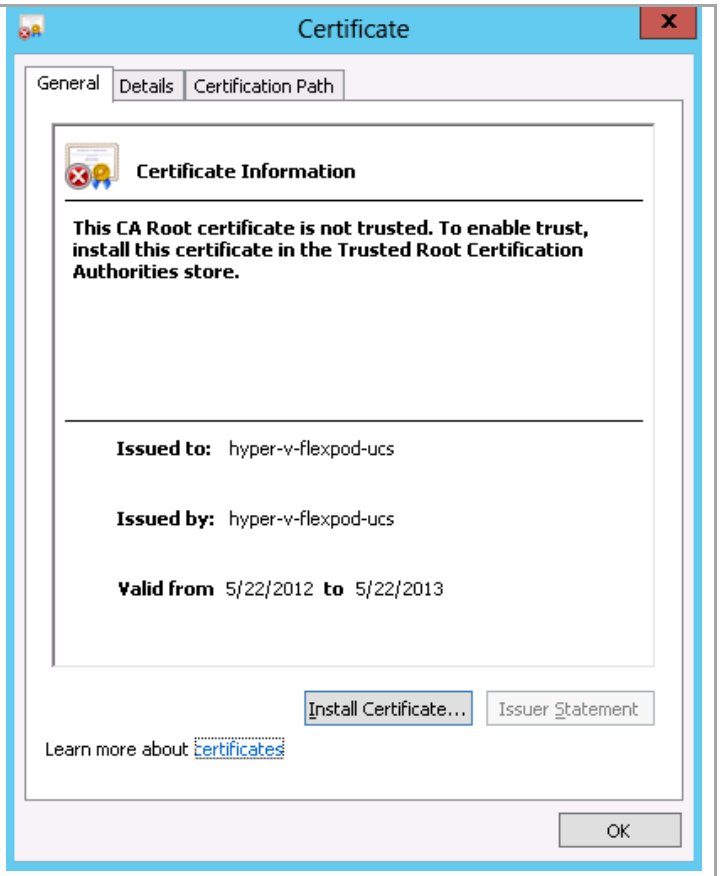


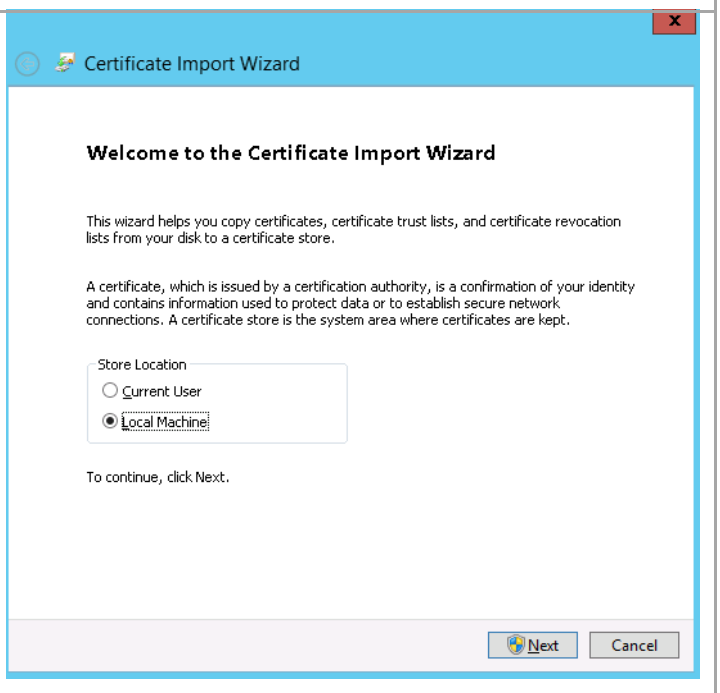
4. The **Select Monitoring Type** screen appears. Select **Cisco Unified Computing Systems** as the monitoring type and click the **Next** button.

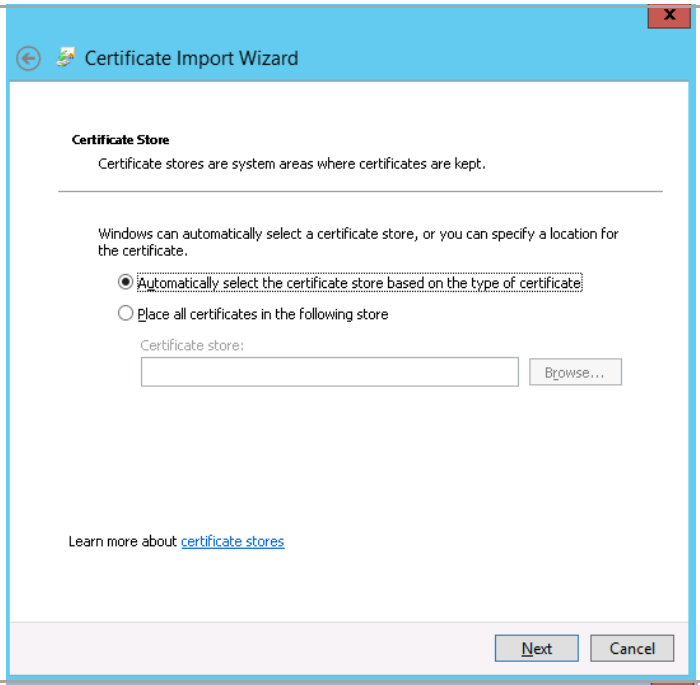
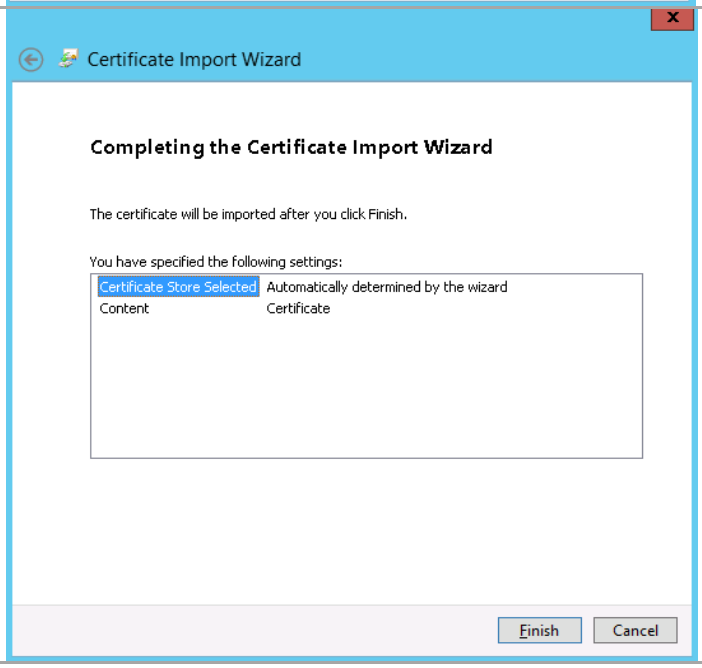


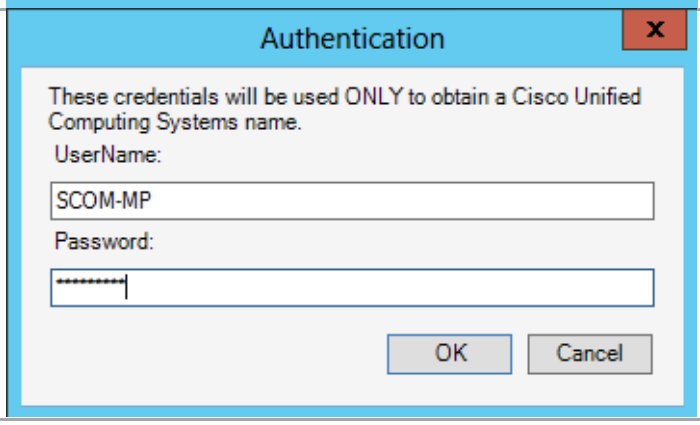
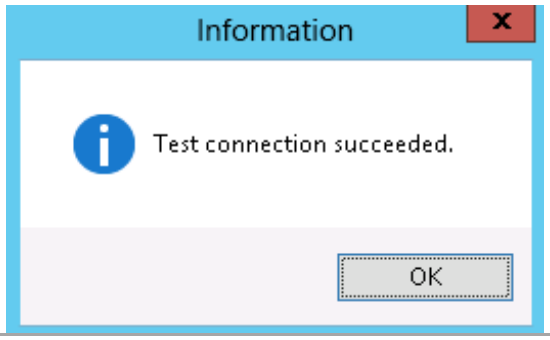
5. The **General Information** screen appears. Specify **IP Address/Hostname, Port Number** and **Connection Mode**. Click the **Test connection** button.	
6. Click **View Certificate**.	

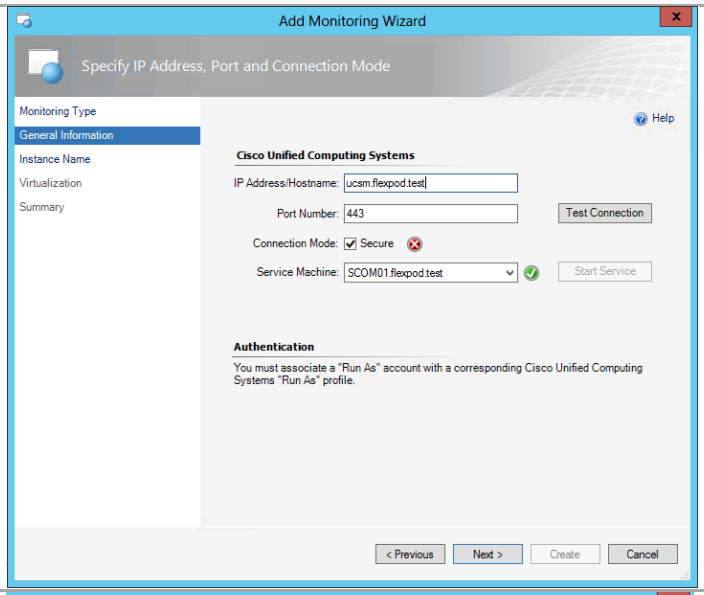
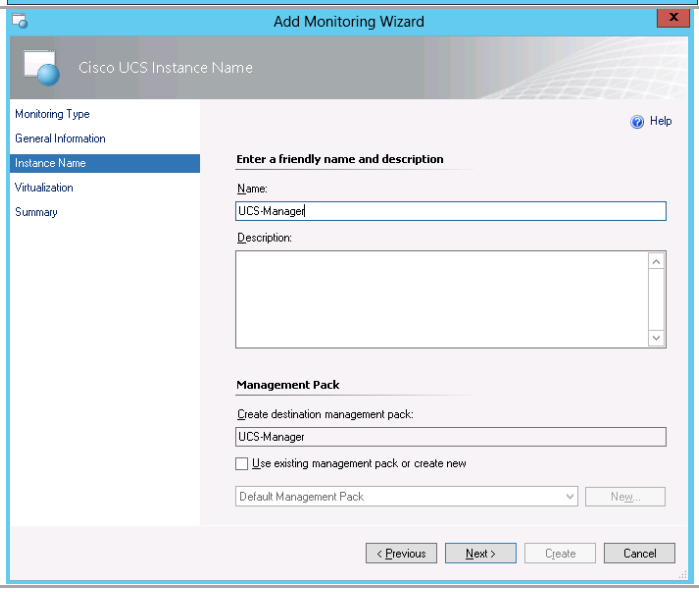
7. Click **Install Certificate**.



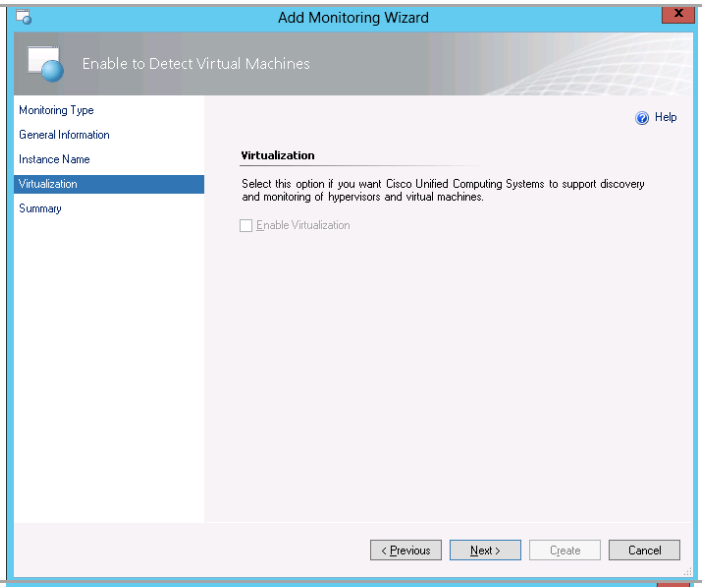


8. Select the option **Automatically select the certificate store based on the type of certificate** and click **Next**.	
9. Select the default location and click **Finish**.	

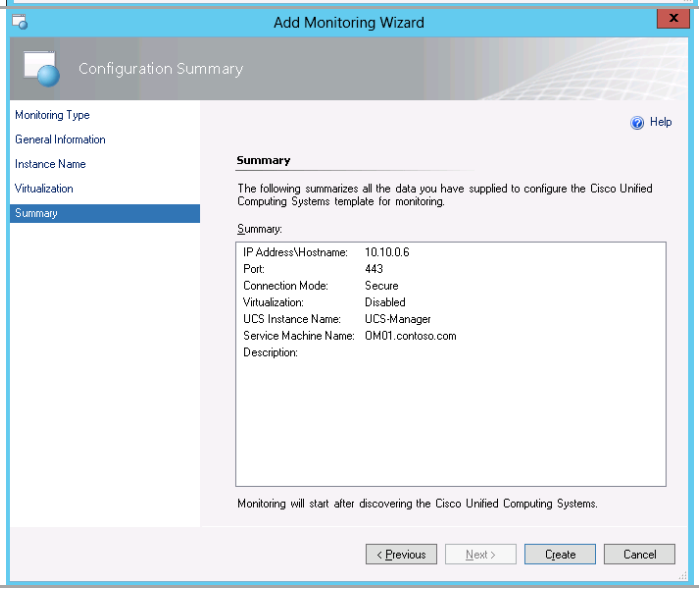
10. Click **Yes** to proceed.	
11. Enter the **Cisco UCS Manager SCOM Management Pack account** created earlier. Enter the account **password** and click **Next**.	
12. Click **OK** to close the information window.	

13. Click **Next** to proceed.	
14. Enter the **Cisco UCS Manager instance name** and click **Next**.	

15. In the Enable to Detect Virtual Machines window the Enable Virtualization selection is disabled. Click **Next** to proceed.



16. Review the configuration summary and click the **Create** button to complete the wizard.

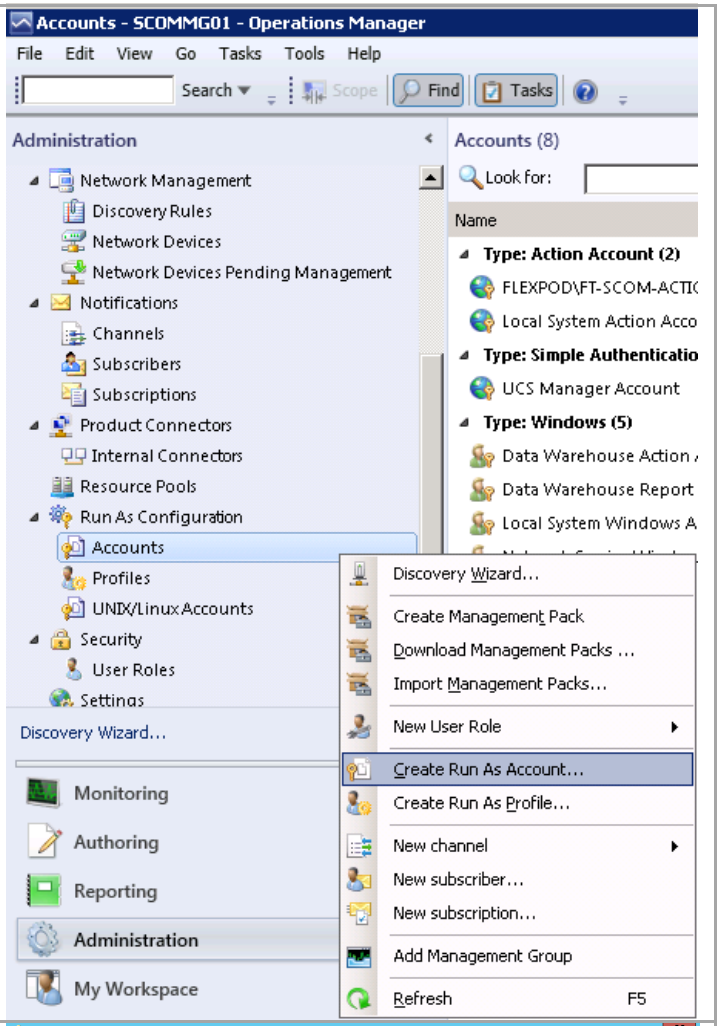


Creating an Administration Account

▶ Perform the following steps on all the Operations Manager virtual machine

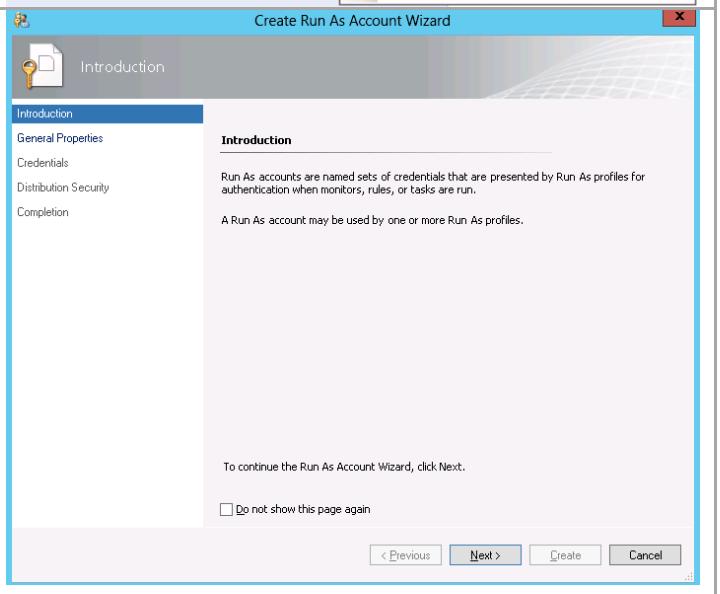
1. In the Operations Manager console, click the **Go** tab in the menu bar.
2. Select **Administration** from the drop-down menu.

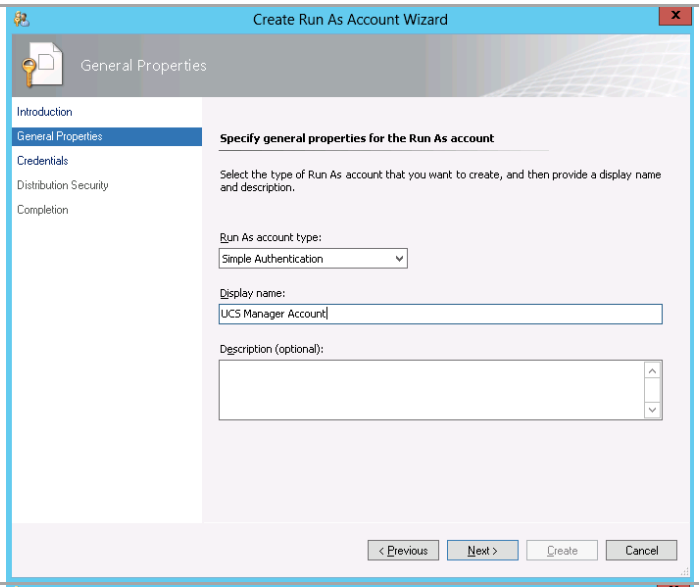
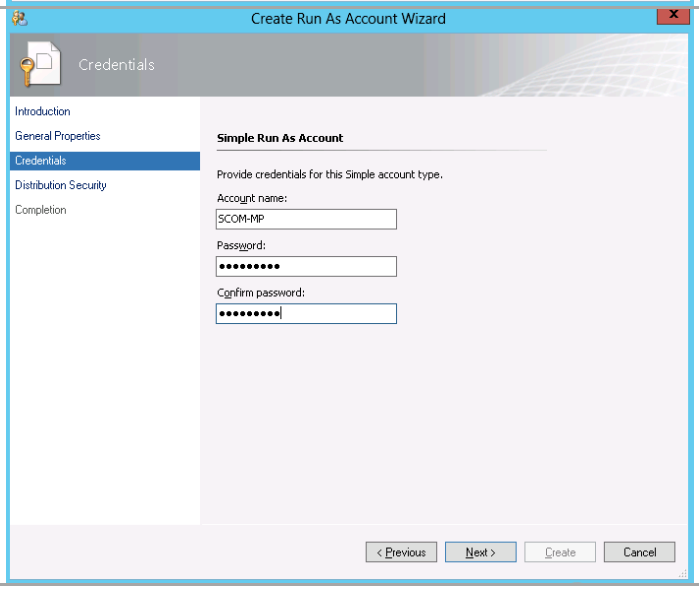
3. In the Administration column, right click on **Accounts**. Select **Create Run as Accounts** from the drop-down menu.



4. The **Create Run as Accounts Wizard** screen appears. Click the **Next** button.

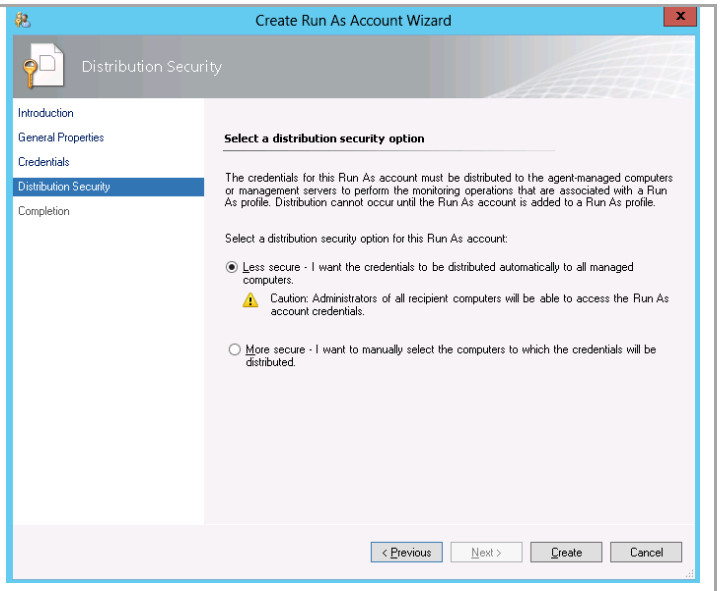
Note: Operations Manager uses Run as Accounts to establish connection to Cisco UCS.



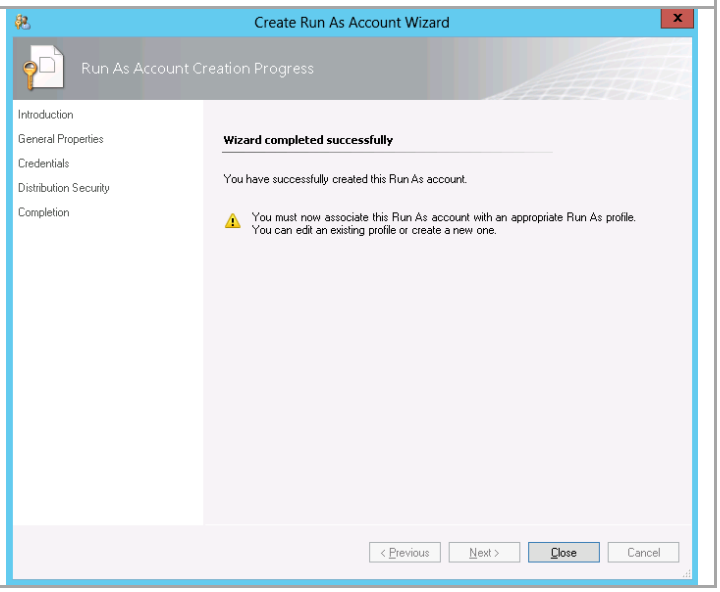
5. The **General Properties** screen appears. Select **Run as Account Type** as **Simple Authentication** from the drop down menu. Specify **Display name** and **Description.** Click the **Next** button.	
6. The **Credentials** screen appears. Specify **Account name**, **Password** and **Confirm Password**. Click the **Next** button. **Note:** These credentials are used for all communication with Cisco Unified Computing System.	

7. The **Distribution Security** screen appears. Select a distribution security option as **Less Secure.** Click the **Create** button.

Note: More Secure feature is provided to management packs for managing computers or devices running the Windows operating system. Cisco UCS does not run Windows. Cisco recommends using the **Less Secure** option.



8. **The Create Run as Account Wizard - Completion** screen appears. Click the **Close** button.
9. The Administrator Account is created. Proceed to associating a Run As Profile with this account.



Associating a Run As Account with a Run As Profile

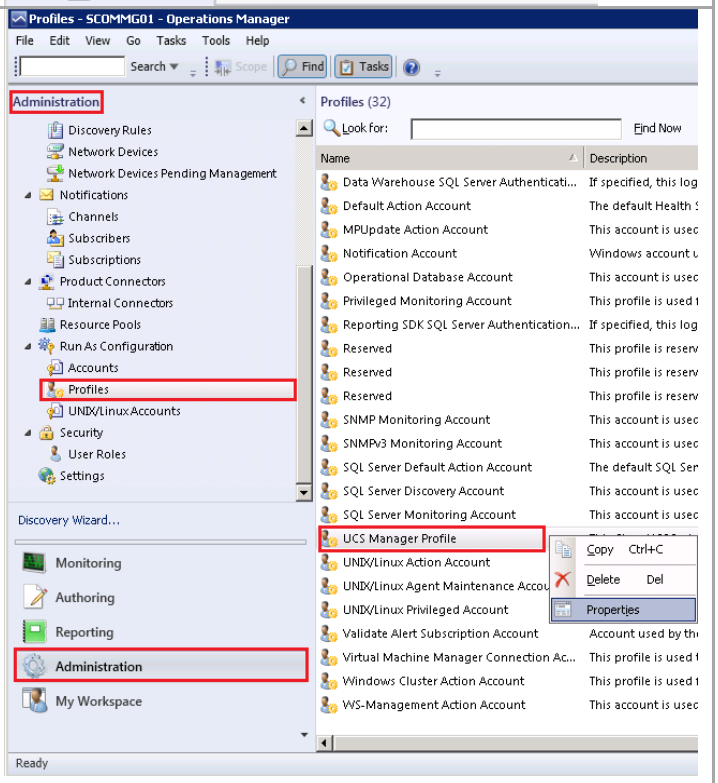
The Run As account that was created in the previous step must not be associated with a Runs As profile.

▶ Perform the following steps on the Operations Manager virtual machine.

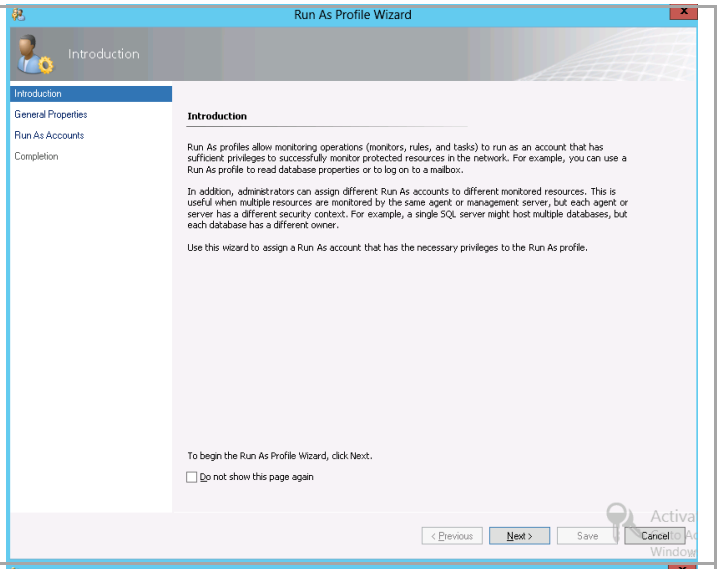
1. In the Operations Manager console, click the **Go** tab in the menu bar.
2. Select **Administration** from the drop-down menu.

3. In the Administration column, click on **Profiles**. A list of profiles is displayed on the window. Choose a profile and select **Properties** from its right click menu.

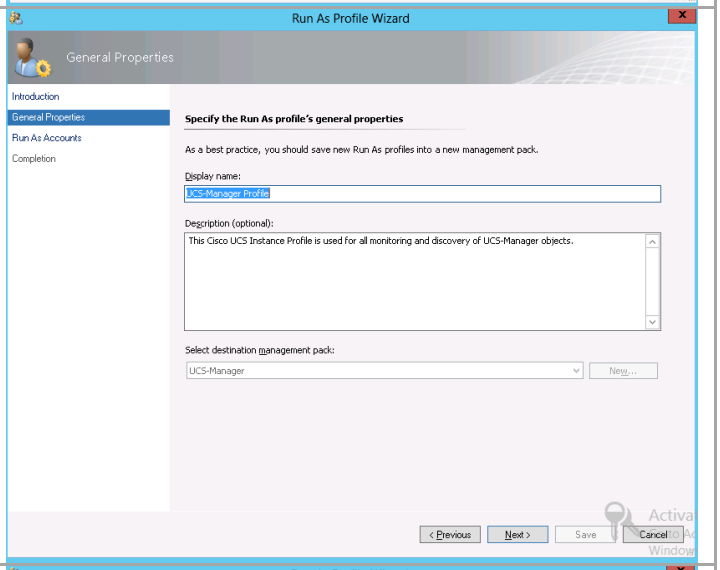
Note: The Cisco UCS Manager Profile is used in this example.



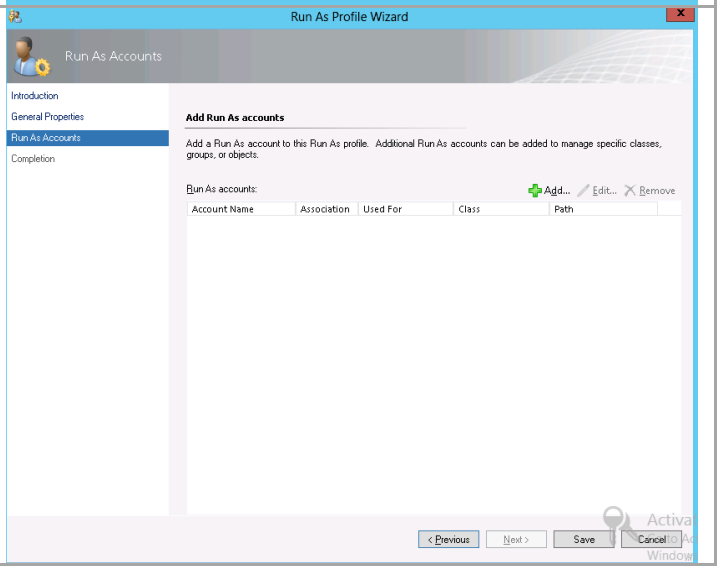
4. The **Run as Profile Wizard** opens. Click **Next** to continue on to the next screen.



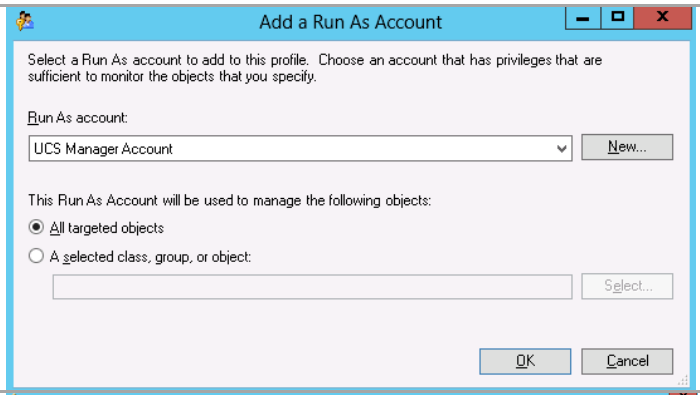
5. Click **Next** again to continue on to the next screen.



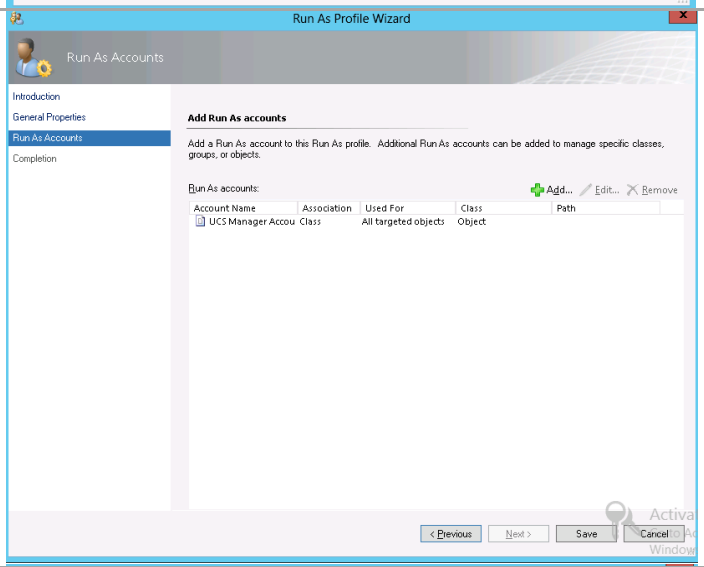
6. Click **Add** to add the Run As account.



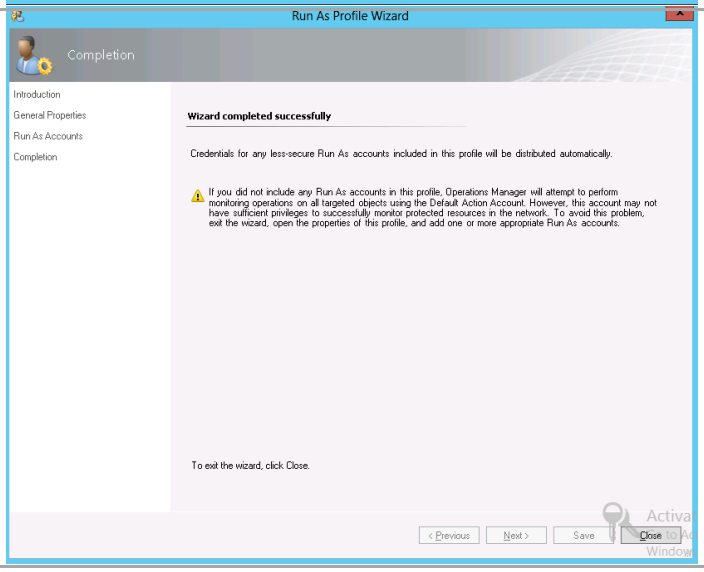
7. Select the **Cisco UCS Manager Account** from the **Run As Account** drop-down menu. This is the account created in the previous section.
8. Select the **All targeted objects** options and click **OK**.



9. Click the **Save** button to save the account configuration.



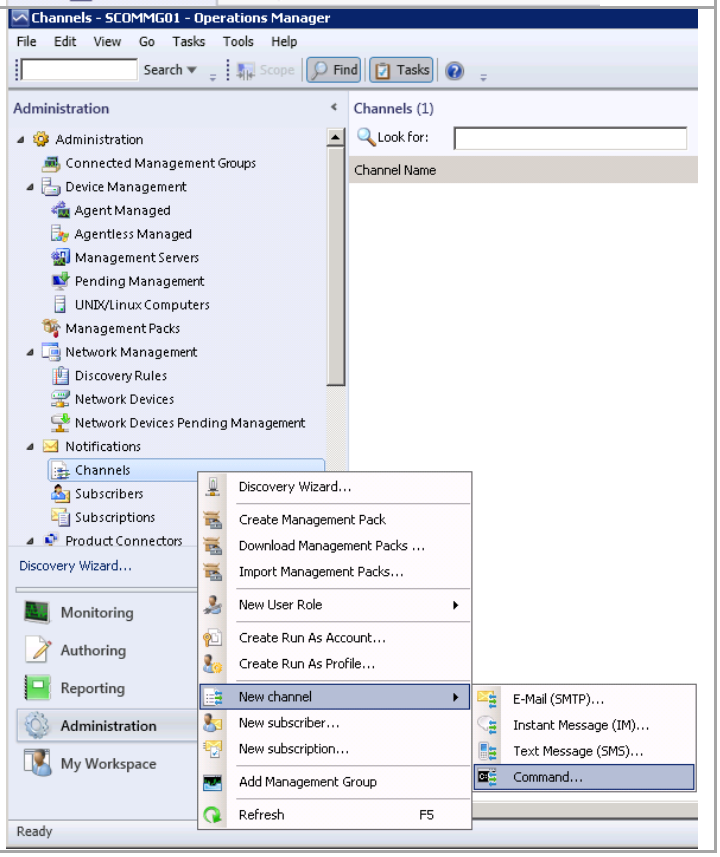
10. The **Completion** screen appears. Click the **Close** button to close the wizard.



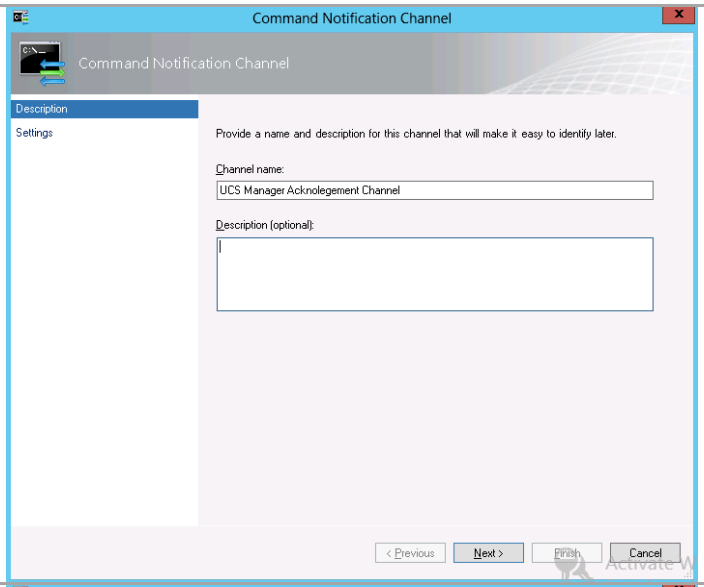
Configuring Bidirectional Communication

The following procedure describes the required configuration to communicate with Cisco UCS for acknowledging alerts from the Operations Manager Console.

Note: The Bidirectional feature is currently limited to Management Servers on which SCOM 2012 Console and Cisco UCS MP are both installed.

1. In the Operations Manager console, click the **Go** tab in the menu bar. Select **Administration** from the drop-down menu.	
2. In the Administration column, right-click on **Channels.** Select **New Channel** from the menu and select the **Command** option.	

3. The **Command Notification Channel** opens. Specify **Channel Name** and **Description**. Click the **Next** button.



4. The **Settings** page of the Command Notification Channel opens.
5. Specify **Full path of the command file** as

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

6. Specify **Command Line parameters** as

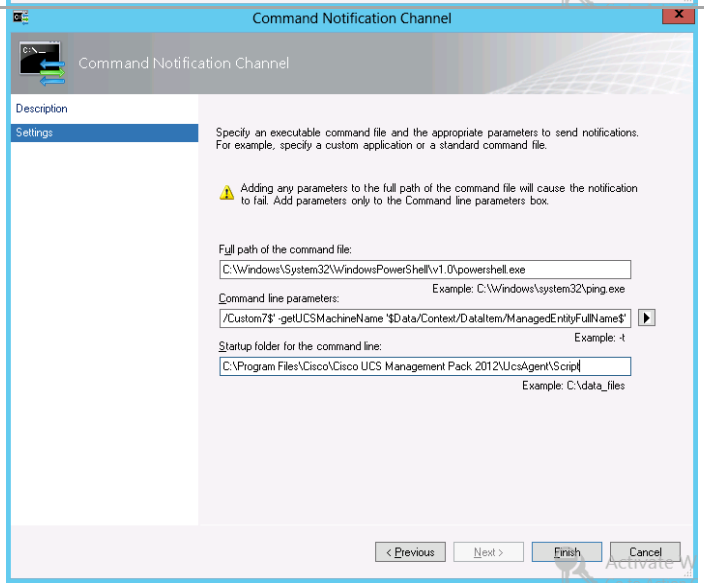
-Command "& '"C:\Program Files\Cisco\Cisco UCS Management Pack 2012\UcsAgent\Script\Bidirectional.ps1'" -getFaultID '$Data/Context/DataItem/Custom7$' -getUCSMachineName '$Data/Context/DataItem/ManagedEntityFullName$'

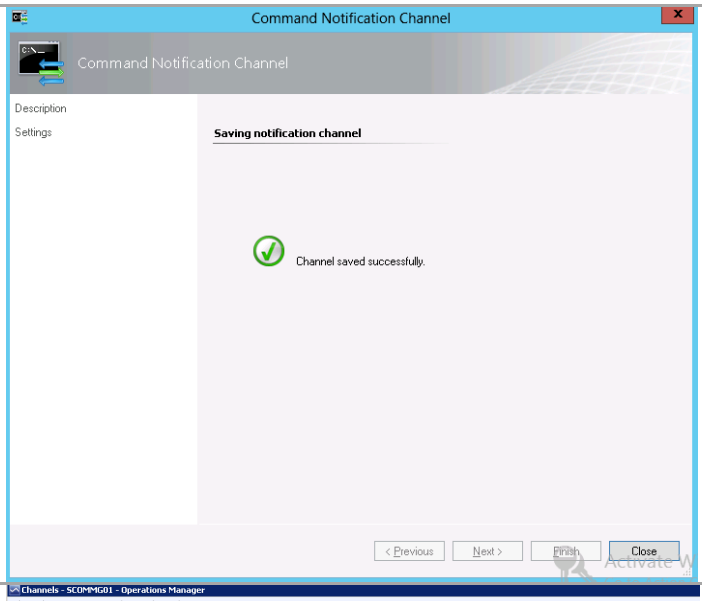
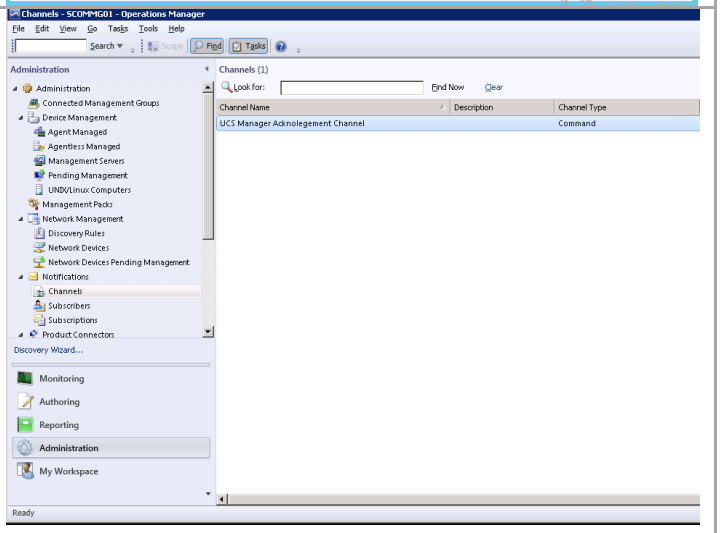
7. Specify **Start up folder for the command line** as

C:\Program Files\Cisco\Cisco UCS Management Pack 2012\UcsAgent\Script

Note: Verify the path for script is valid.

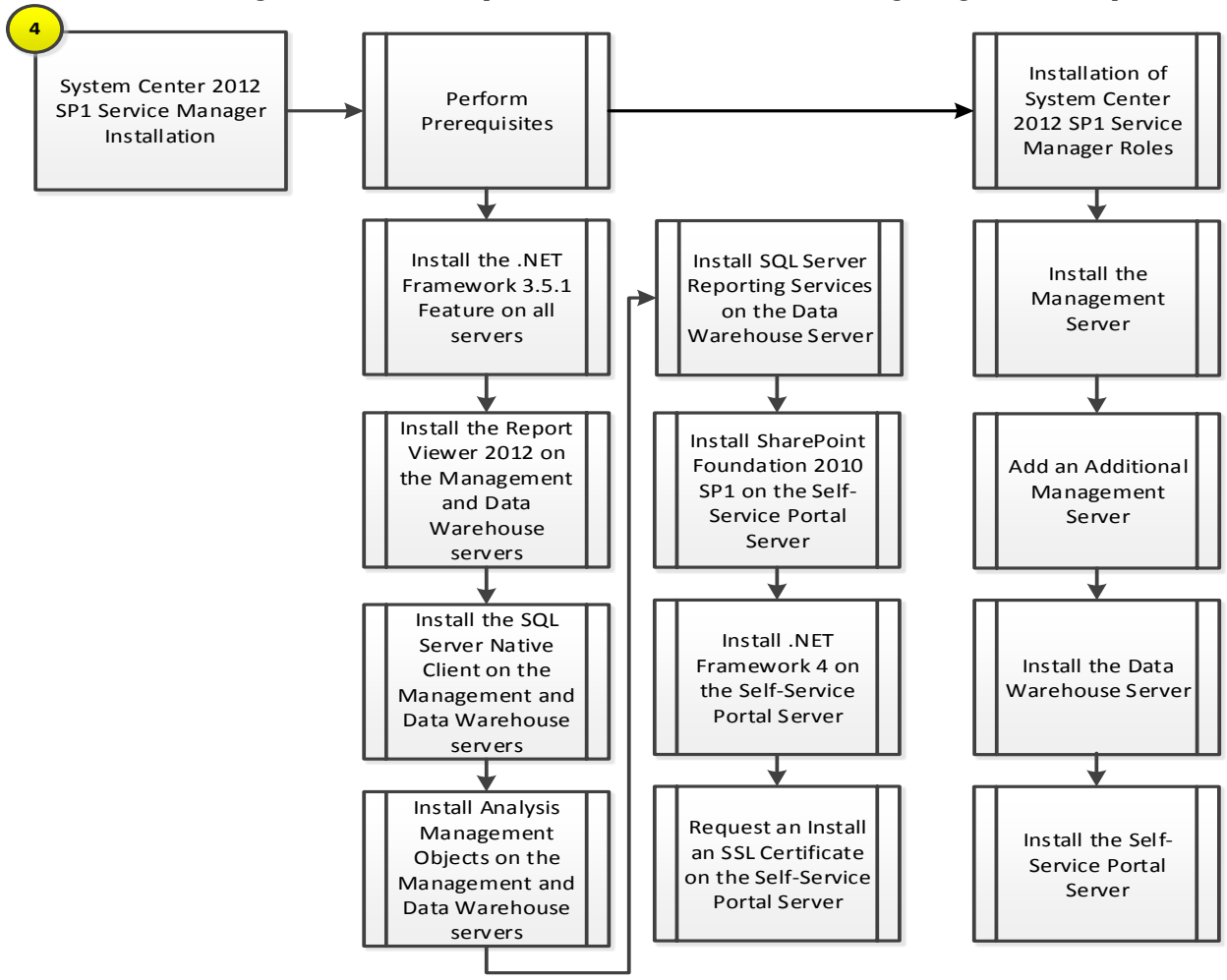
8. Click the **Finish** button.



9. The new Channel is saved successfully. Click **Close** to close the wizard.	
10. The new channel appears in the **Channel** view.	

19 Service Manager

The Service Manager installation process includes the following high-level steps



19.1 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 dedicated instance that has been established in previous steps for Service Manager.
    - SCSPFarm – 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.

19.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

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 Server nodes.

User name	Purpose	Permissions
<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 Server nodes.
<DOMAIN>\ FT-SCSM-SSRS	SCSM reporting account	Must be a local admin on all SQL Server 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.
<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-SCSM-OLAP	Service Manager Analysis Services account	Must be a local admin on all SQL Server nodes.

Groups

Verify that the following security groups have been created:

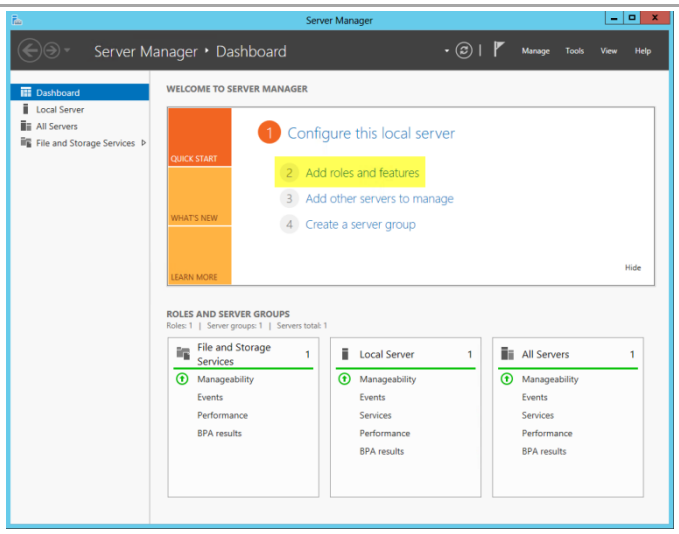
Security group name	Group scope	Members	Member of
<DOMAIN>\FT-SCSM-ADMINS	Global	DOMAIN\FT-SCSM-SVC	Must be added to the Service Manager Administrators user role and added to the Operations Manager Administrators role in Operations Manager and a member of the Administrators group on each SQL Server.

Add the .NET Framework 3.5 Feature on all Server Manager Servers

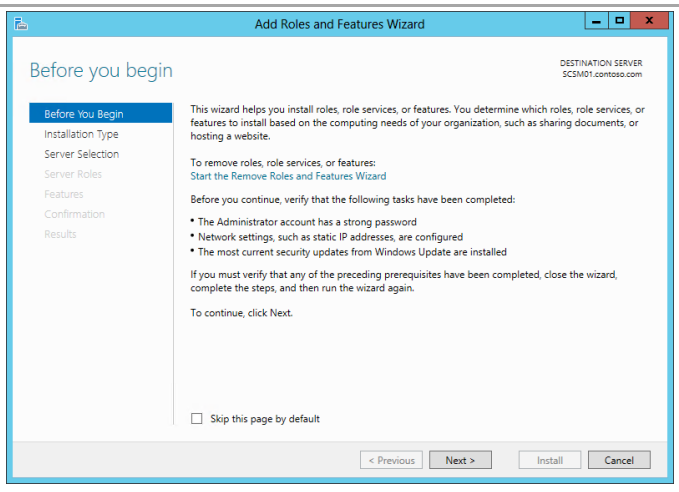
The Service Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on the **Service Manager management server and data warehouse** virtual machines.

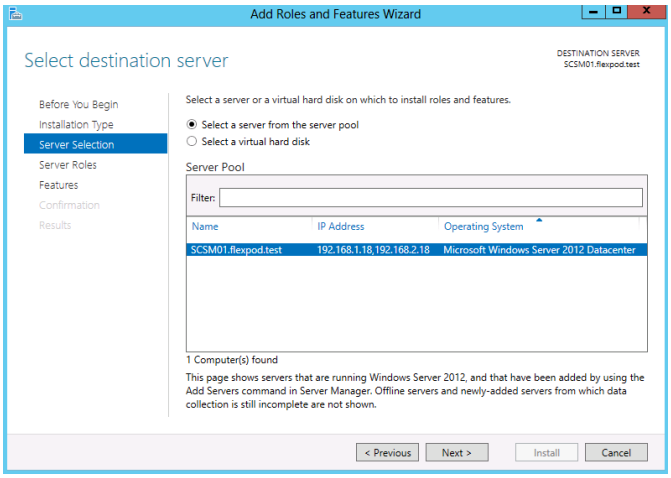
1. Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



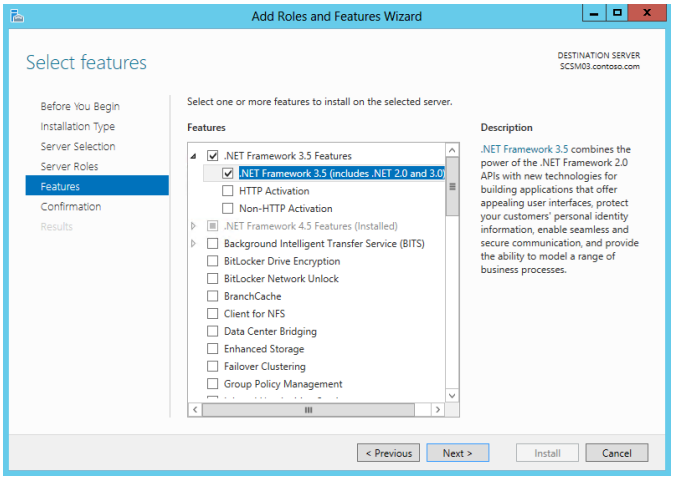
2. The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



3. 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.



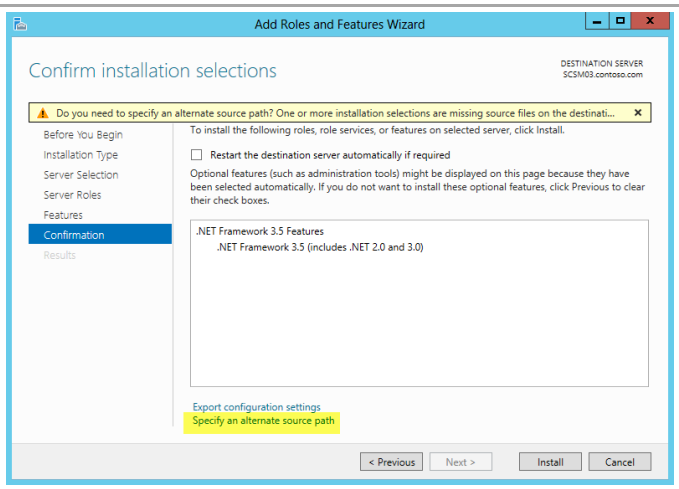
4. To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



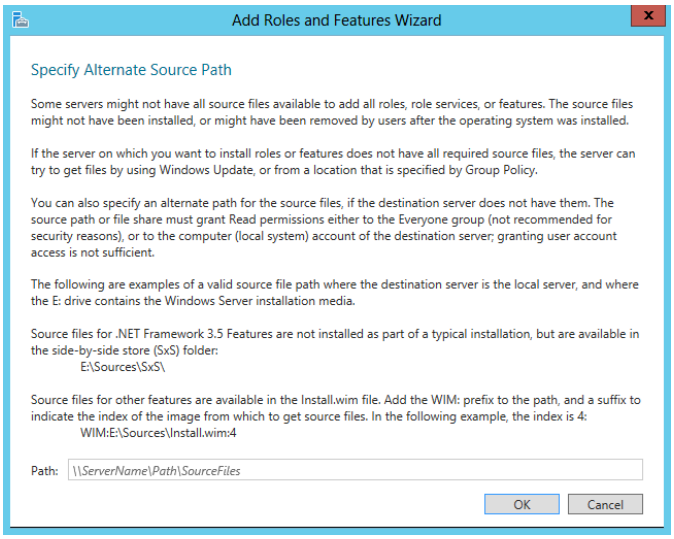
5. In the **Confirm installation selections** dialog verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

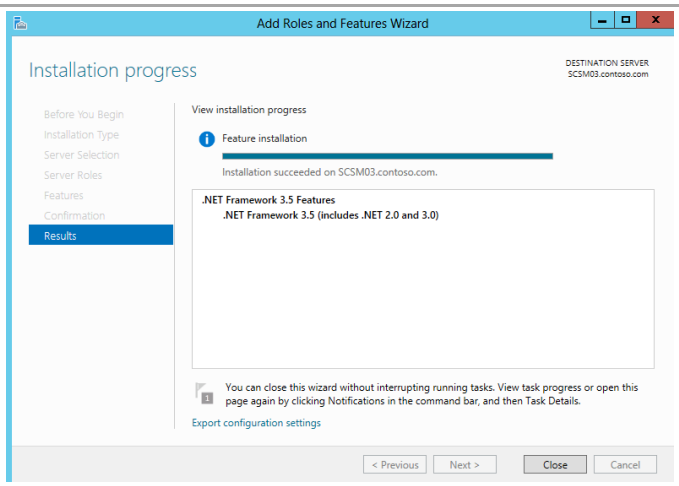
Also, If the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.



6. 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.

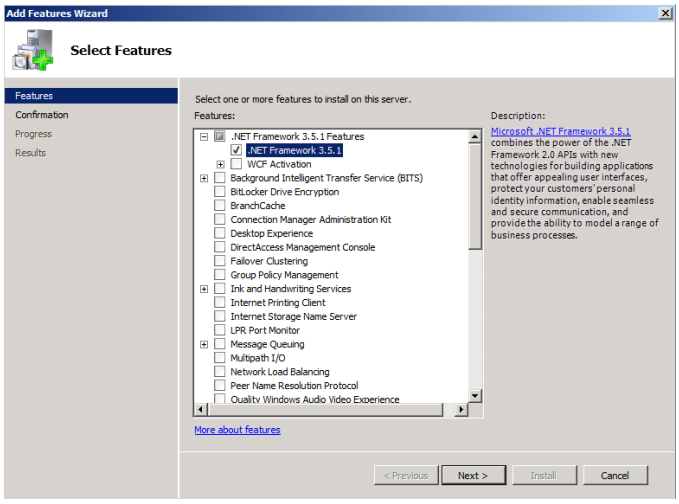


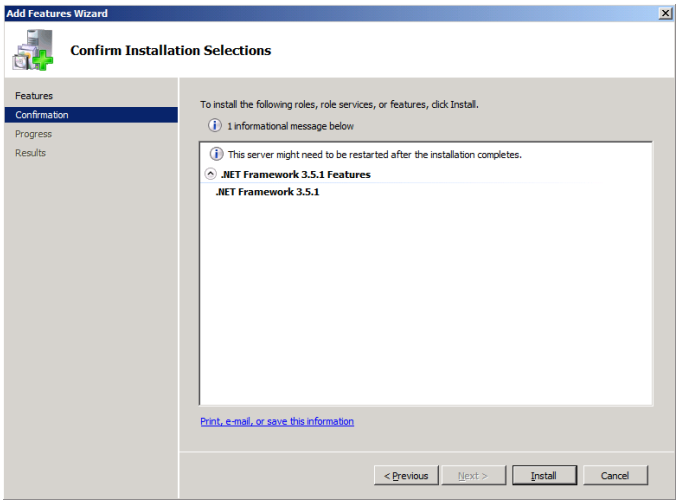
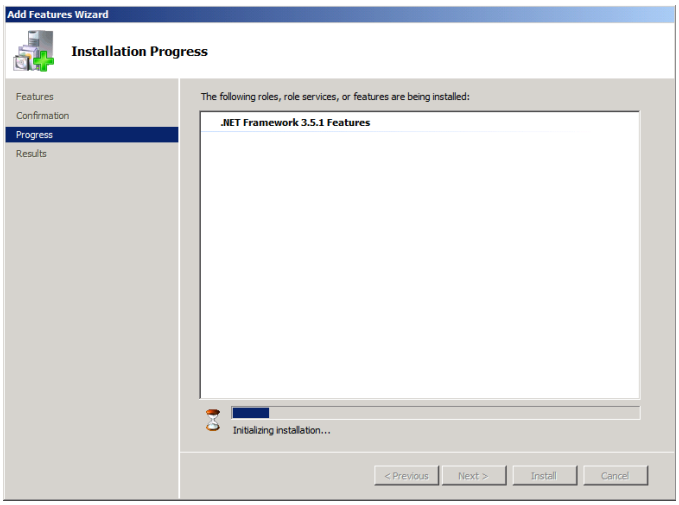
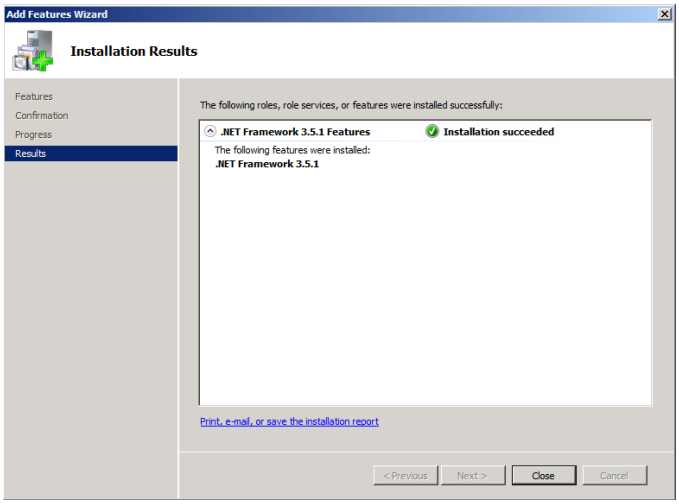
7. The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



▶ Perform the following steps on the **Service Manager Self-Service Portal** virtual machine running Windows Server 2008 R2.

1. 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** checkbox only. Leave **WCF Activation** check box clear.



2. In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.	
3. The **Installation Progress** dialog will show the progress of the feature install.	
4. When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.	

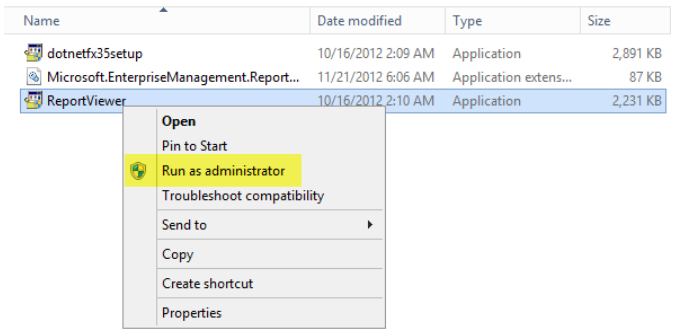
Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers

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.

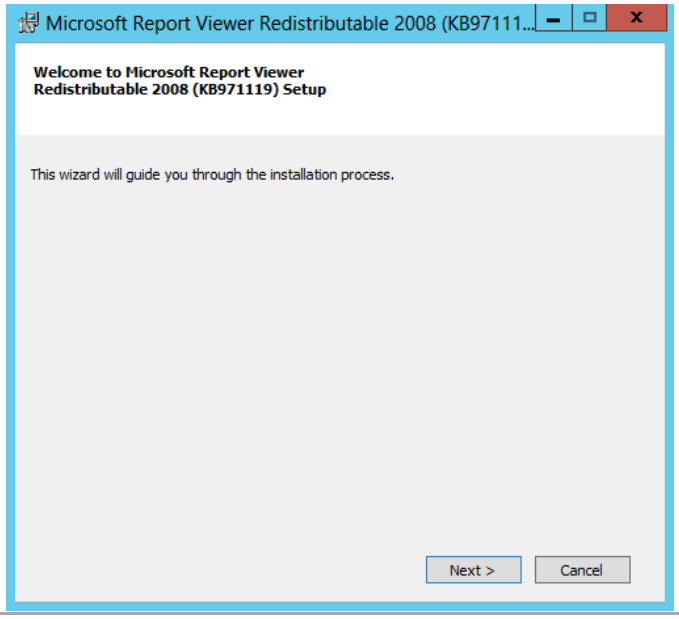
▶ Perform the following steps on the **Server Manager management** (SCSM01) **and Data Warehouse server** (SCSM02) virtual machines.

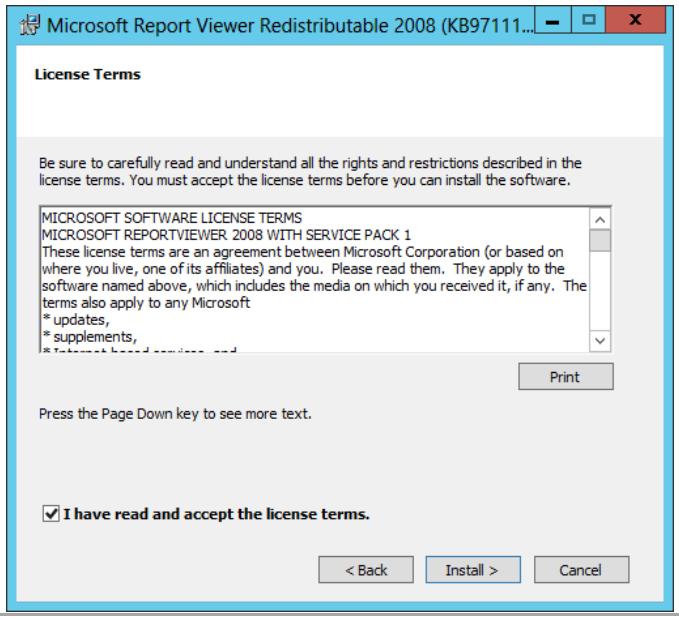
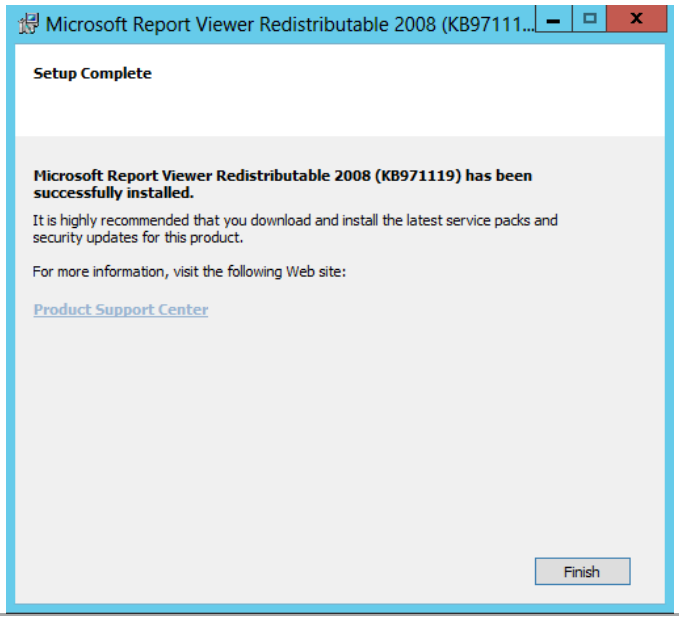
From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

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*](http://www.microsoft.com/en-us/download/details.aspx?id=3203)



The setup wizard will appear. Click **Next** to continue.



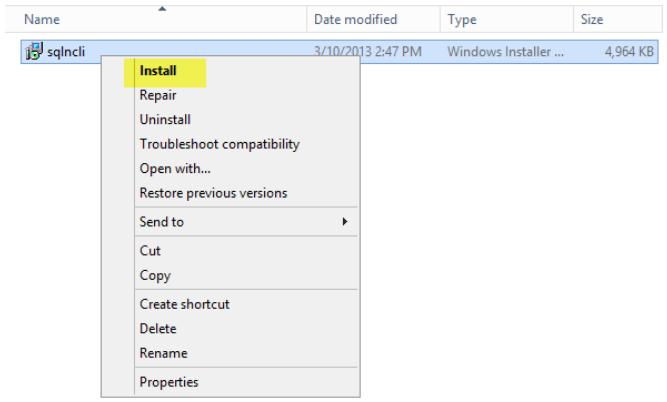
Within the **License Terms** dialog, select the **I have read and accept the license terms** check box. Click **Install** to begin the installation.	
When completed, click **Finish** to exit the installation.	

Install SQL Server 2012 Native Client on the on the Management and Data Warehouse Servers

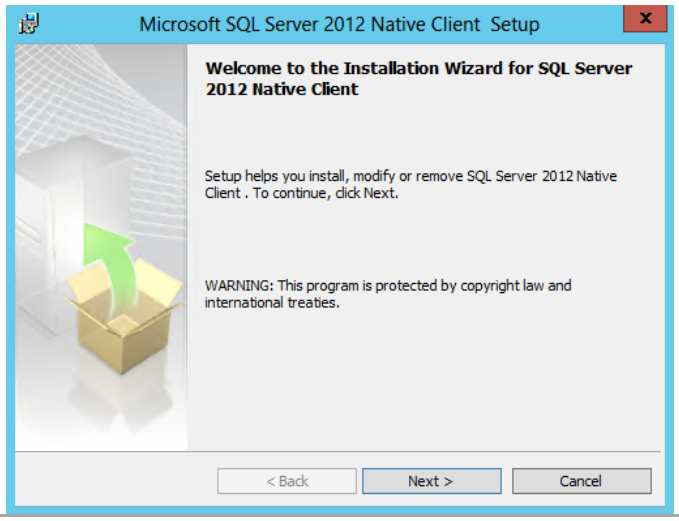
The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 Native Client be installed prior to installation. Follow the provided steps to install the SQL Server 2012 Native Client.

▶ Perform the following steps on the **Server Manager management** (SCSM01) **and Data Warehouse server** (SCSM02) virtual machines.

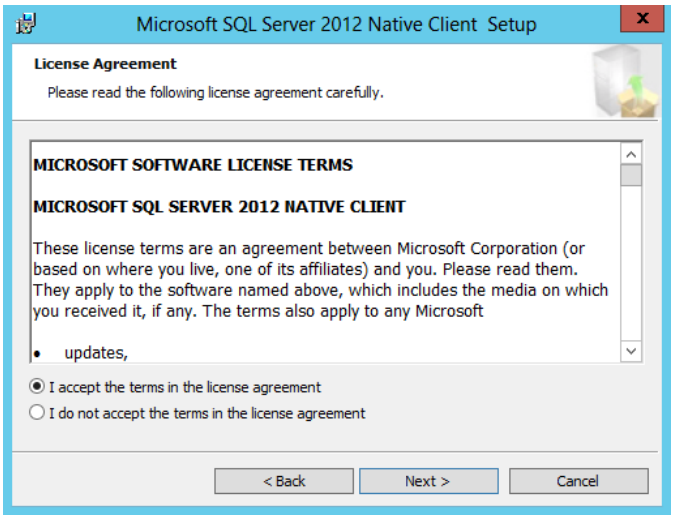
1. From the installation media source, right-click **SQLNCLI.MSI** and select **Install** from the context menu to begin setup.
2. **Note:** the SQL Server 2012 SP1 Native Client installer, **1033\x64\sqlncli.msi,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580

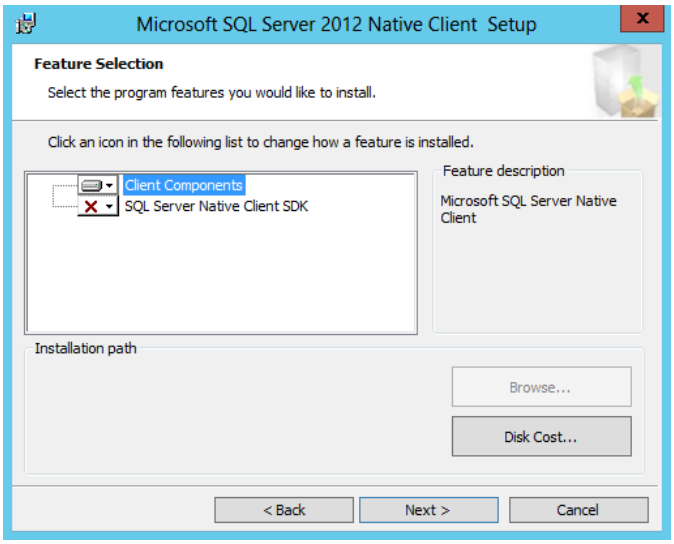
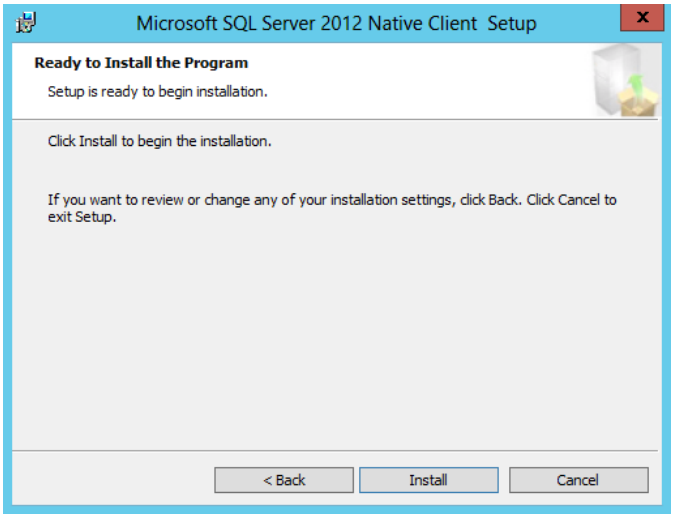
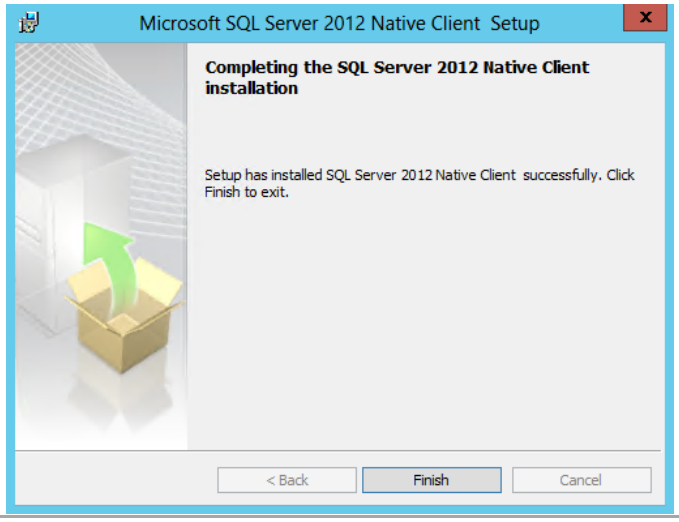


3. The setup wizard will appear. Click **Next** to continue.



4. Within the **License Terms** dialog, select the **I accept the terms in the license agreement** check box. Click **Next** to continue.



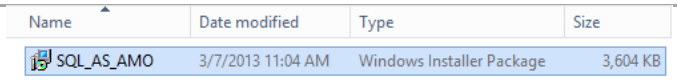
5. In the **Feature Selection** dialog, verify that the **Client Components** feature is selected for installation. Click **Next** to continue.	
6. In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
7. When completed, click **Finish** to exit the installation.	

Install SQL Server 2012 SP1 Analysis Management Objects

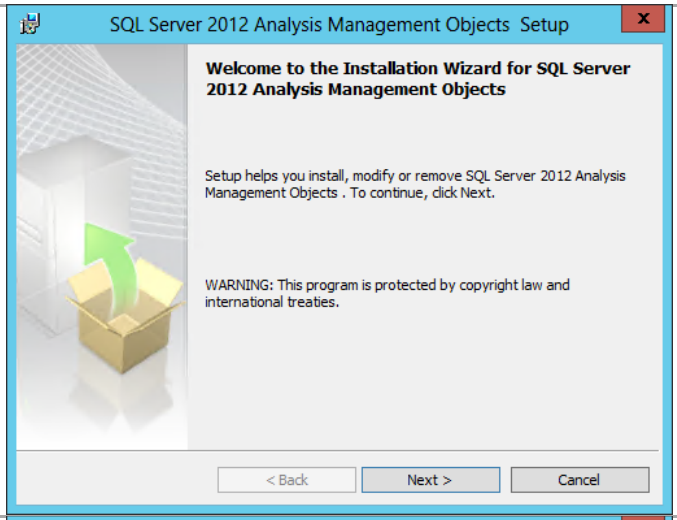
The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 SP1 Analysis Management Object be installed prior to installation. Follow the provided steps to install the SQL Server 2012 SP1 Analysis Management Objects.

▶ Perform the following steps on the **Server Manager management** (SCSM01) **and Data Warehouse server** (SCSM02) virtual machines.

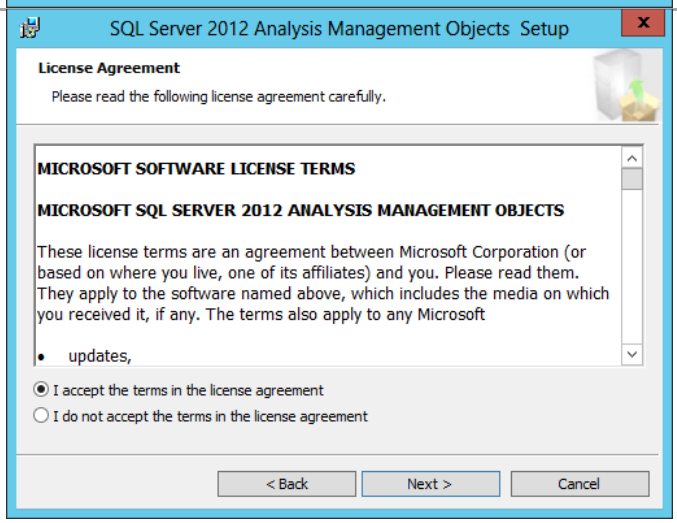
1. From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.
2. **Note:** The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI,** can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=35580.

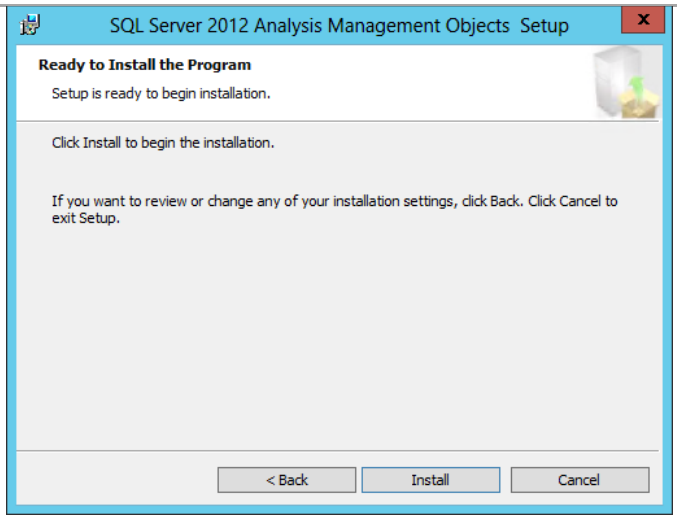
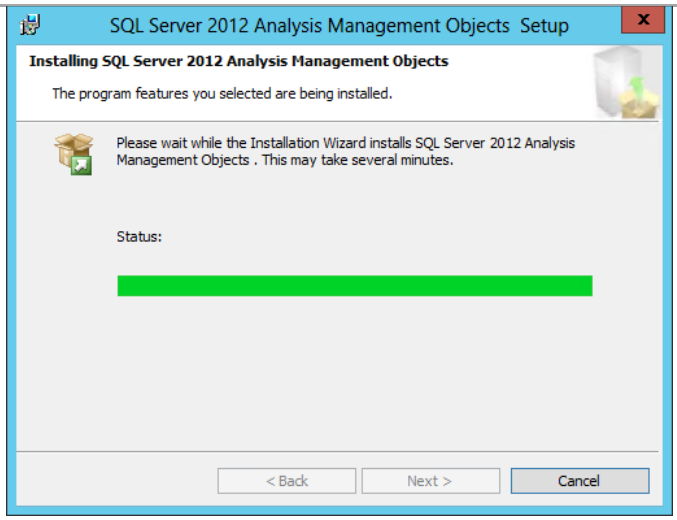
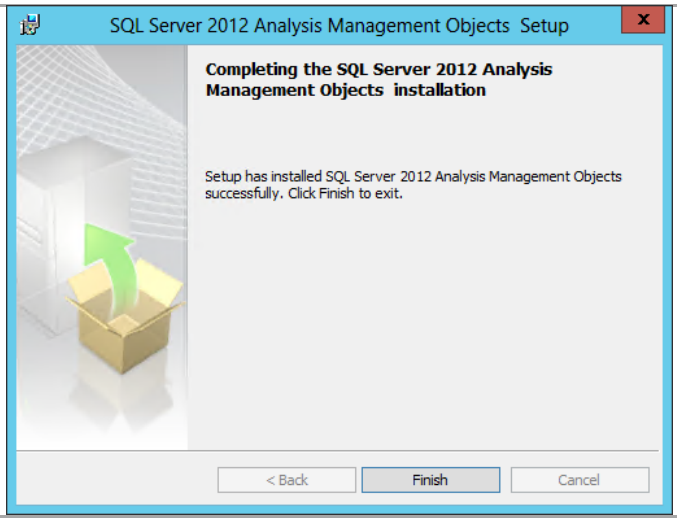


3. The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



4. 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.



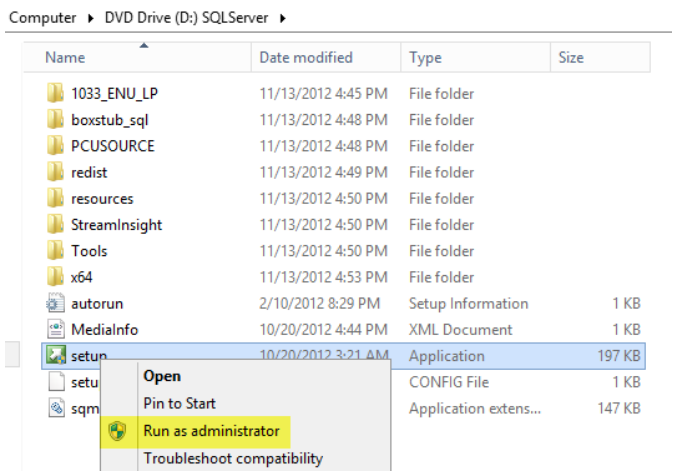
5. In the **Ready to Install the Program** dialog, click **Install** to begin the installation.	
6. The installation process may take several minutes to complete. The progress is displayed on the status dialog.	
7. In the **Completing the SQL Server 2012 Analysis Management Objects installation** dialog, click **Finish** to exit the installation.	

Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

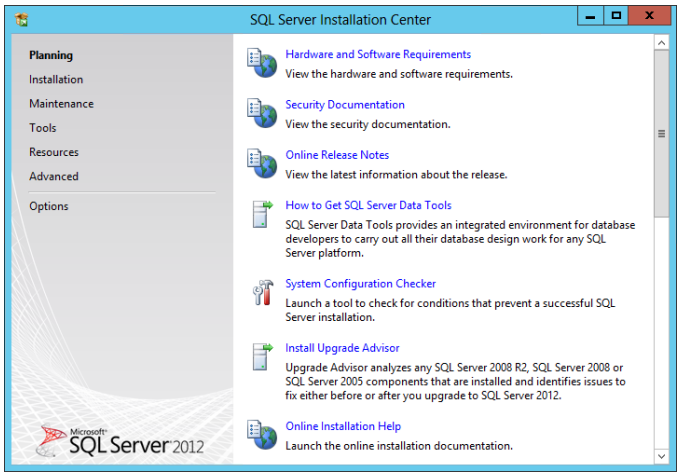
The Service Manager Data Warehouse installation requires SQL Server Reporting Services to be installed to support the Service Manager reporting features. Follow the provided steps to install SQL Server Reporting Services.

▶ Perform the following steps on the **Service Manager Data Warehouse** (SCSM02) virtual machine.

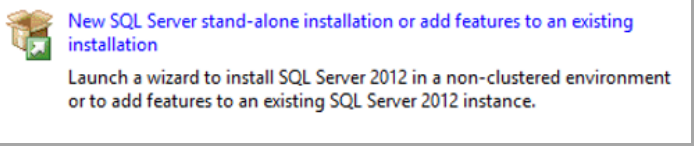
1. From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



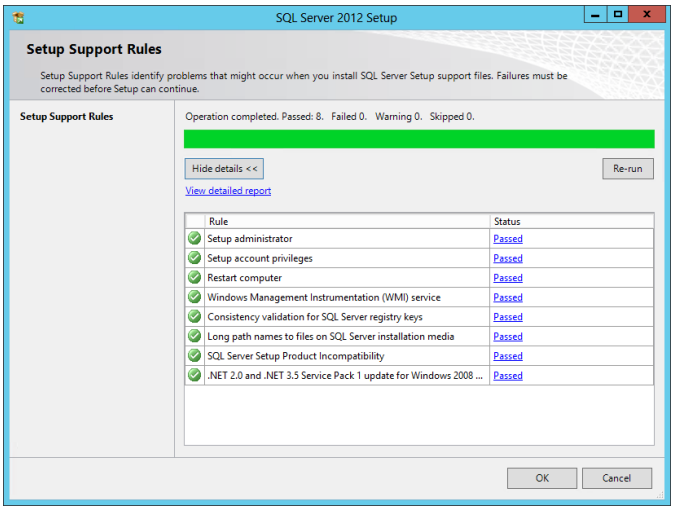
2. The **SQL Server Installation Center** will appear. Select the **Installation** menu option.



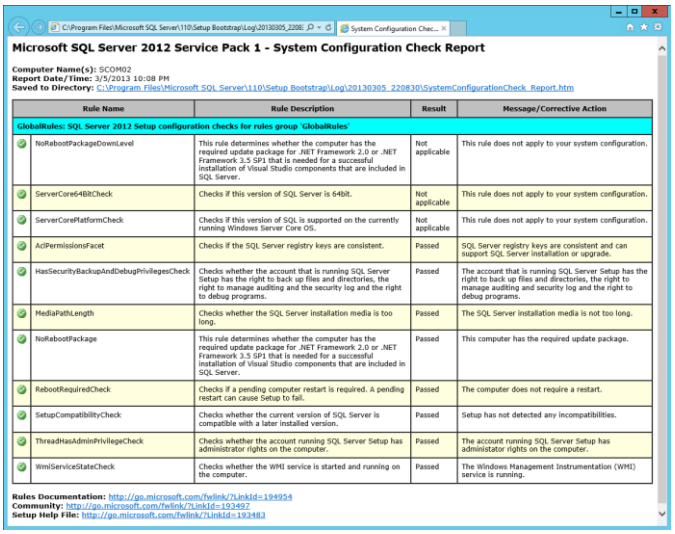
3. From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.



4. 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.

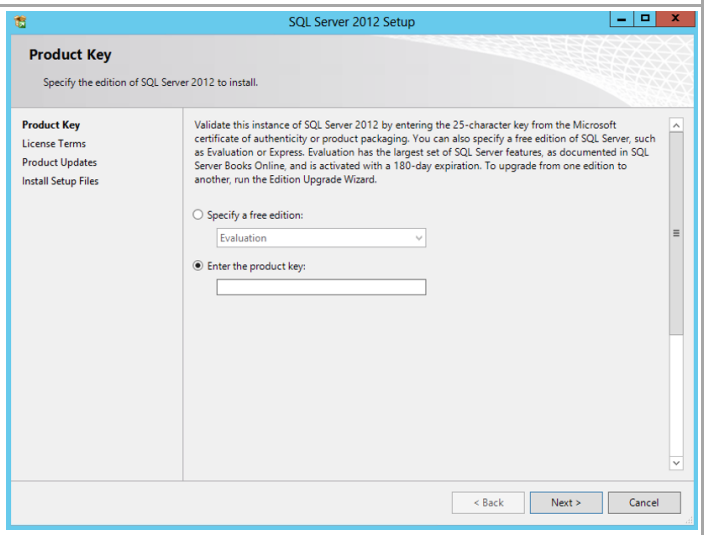


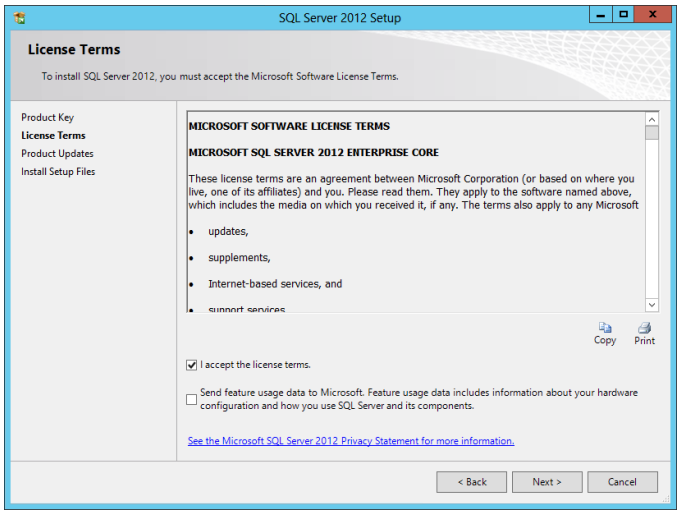
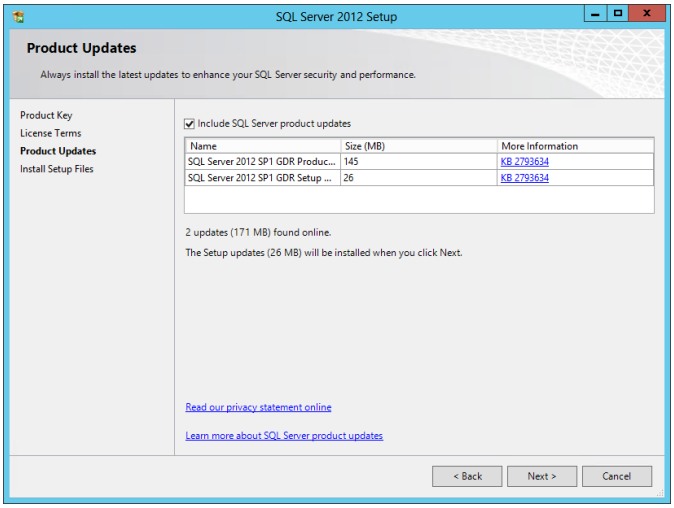
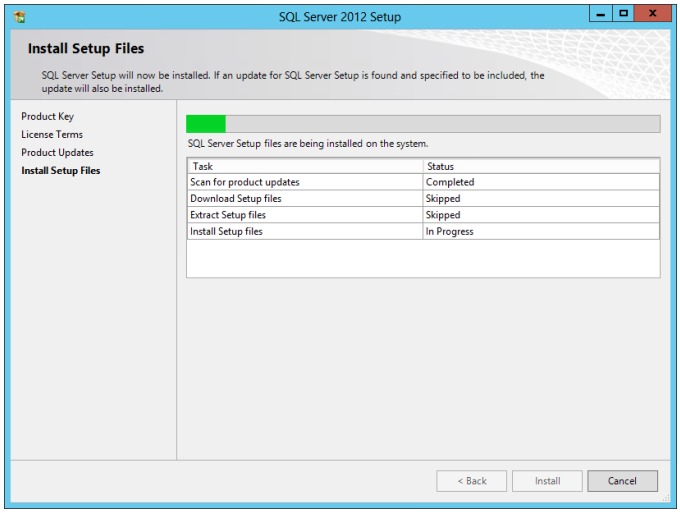
5. If the **View detailed report** link is selected, the following report is available.

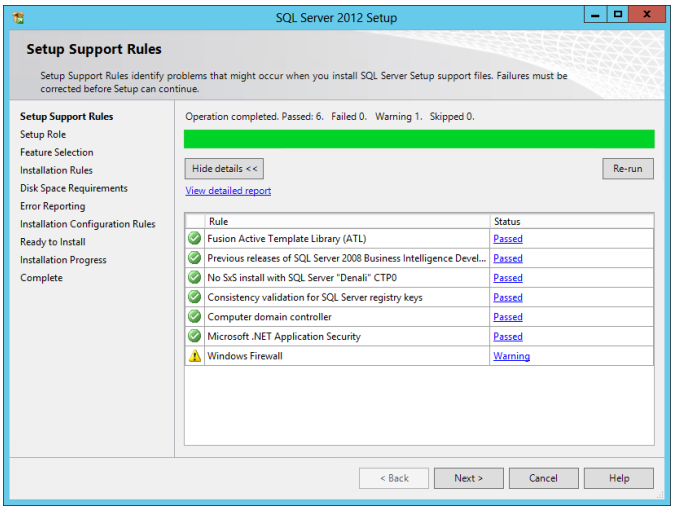
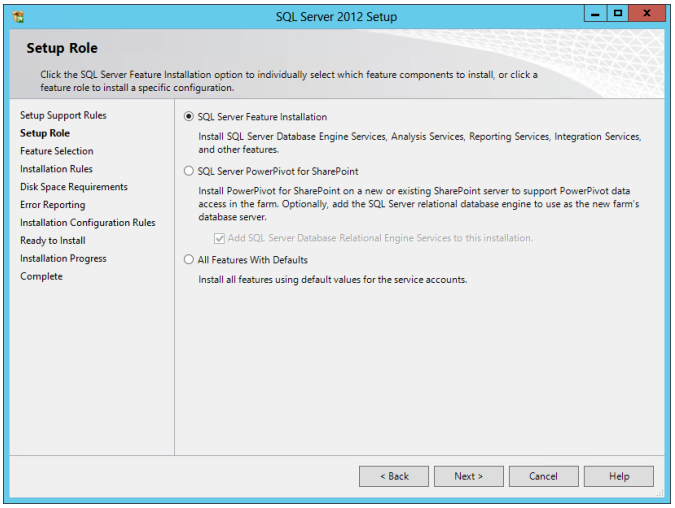


6. In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

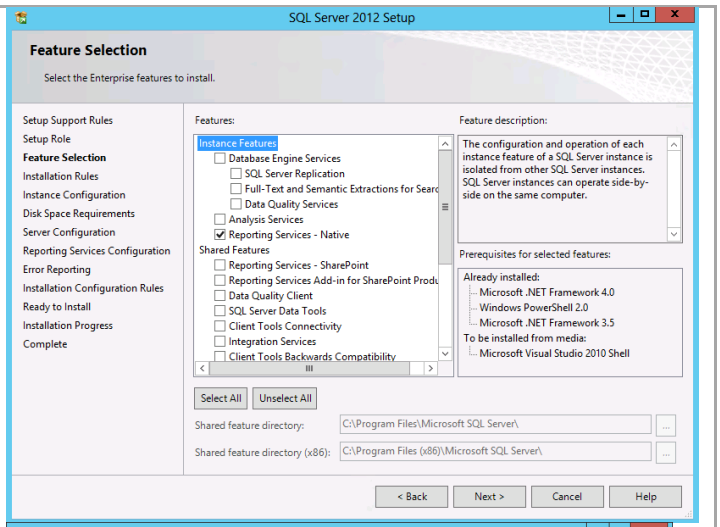
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.

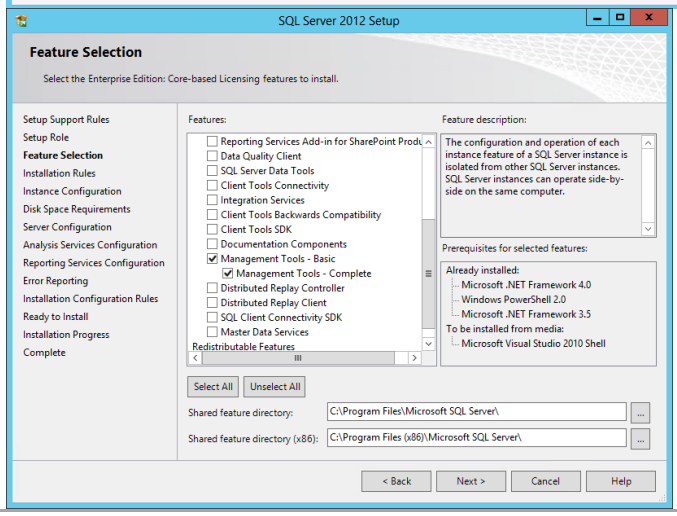


7. In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.	
8. In the **Product Updates** dialog, select the **Include SQL Server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

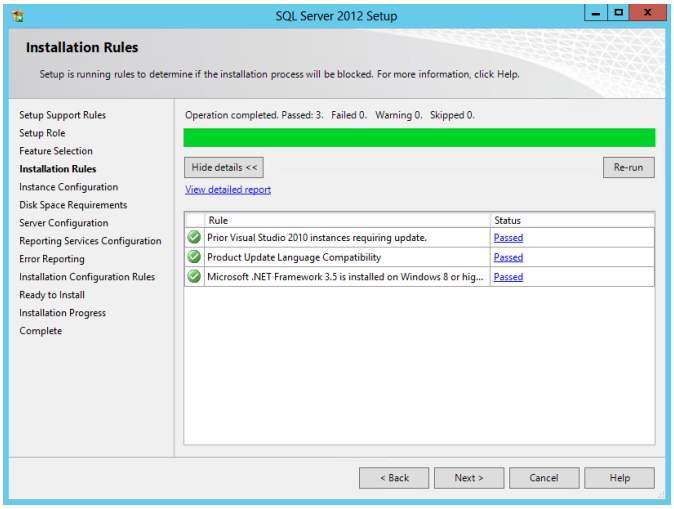
10. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the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

12. In the **Feature Selection** dialog, select the **Reporting Services - Native**, **Management Tools – Basic,** and **Management Tools – Complete, SQL Client Connectivity SDK** check boxes. When all selections are made, click **Next** to continue.



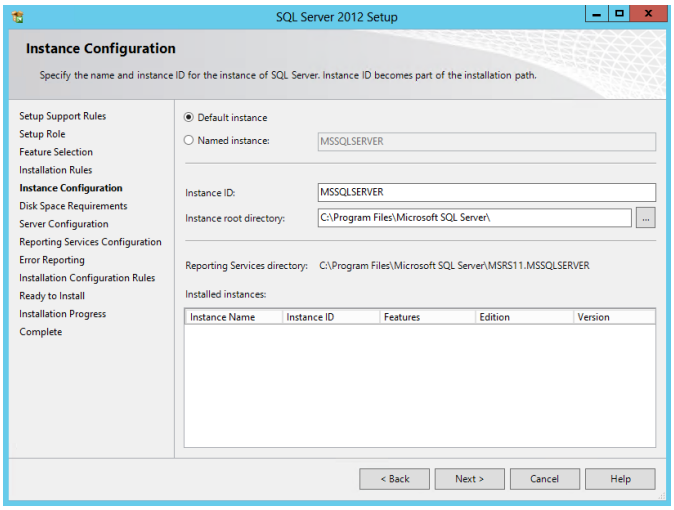


13. In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

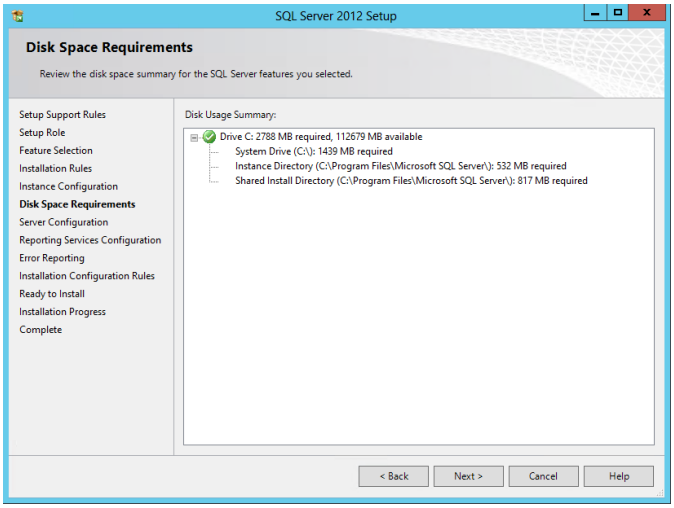


14. In the **Instance Configuration** dialog, select the **Default instance** option and accept the default options for **Instance ID** and **Instance root directory** values. Click **Next** to continue.

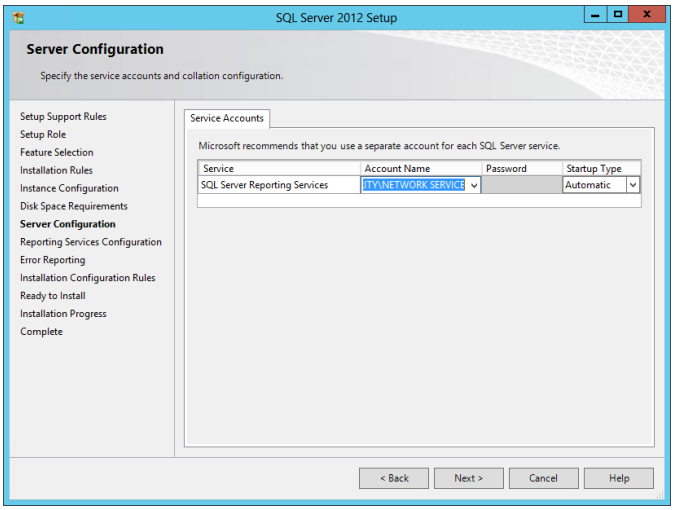
Note: A post-installation configuration process will occur to configure the reporting server database within the Service Manager Data Warehouse SQL Server instance.



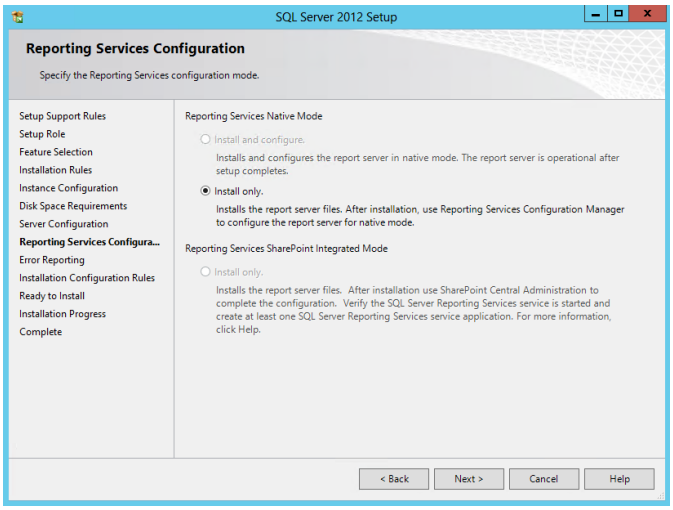
15. In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.



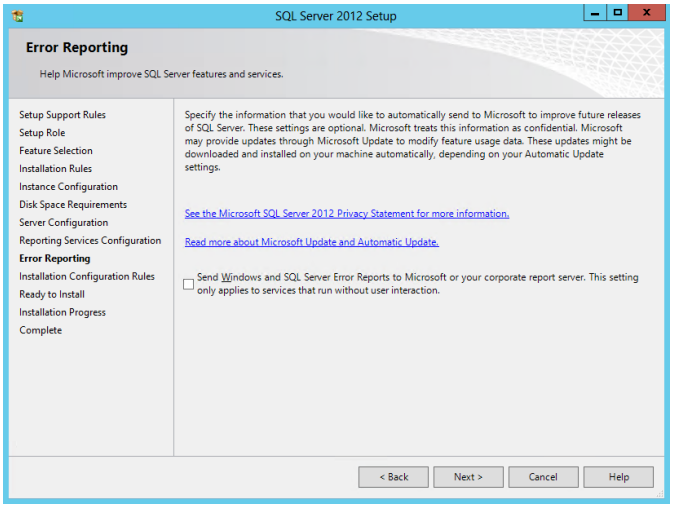
16. In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NETWORK SERVICE** account for the SQL Server Reporting Services service. Click **Next** to continue.



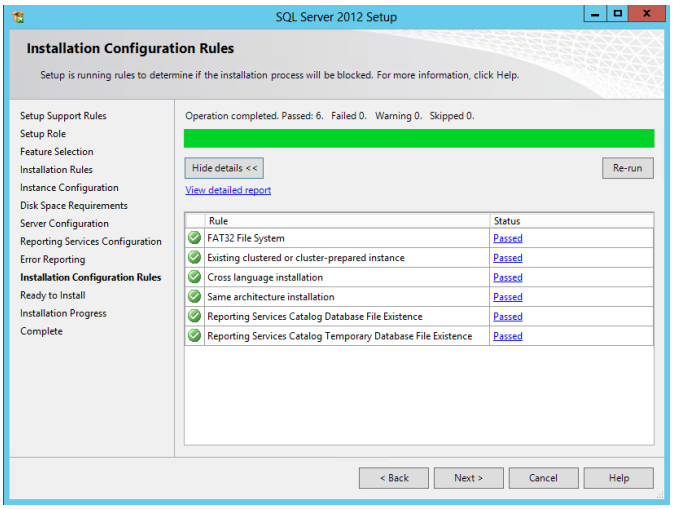
17. In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.



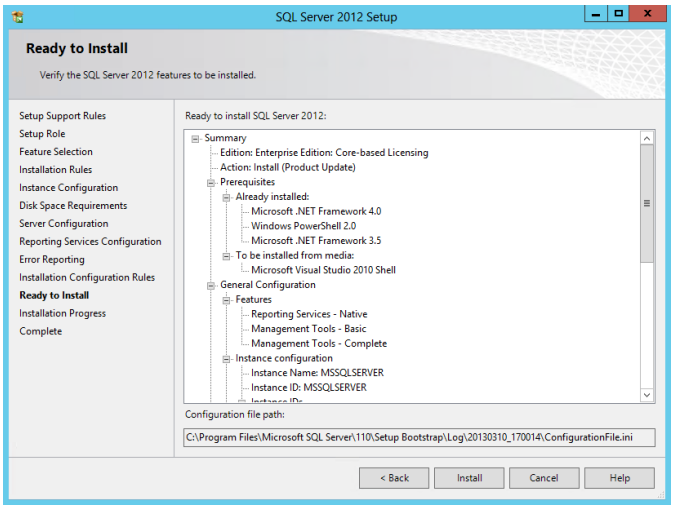
18. In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



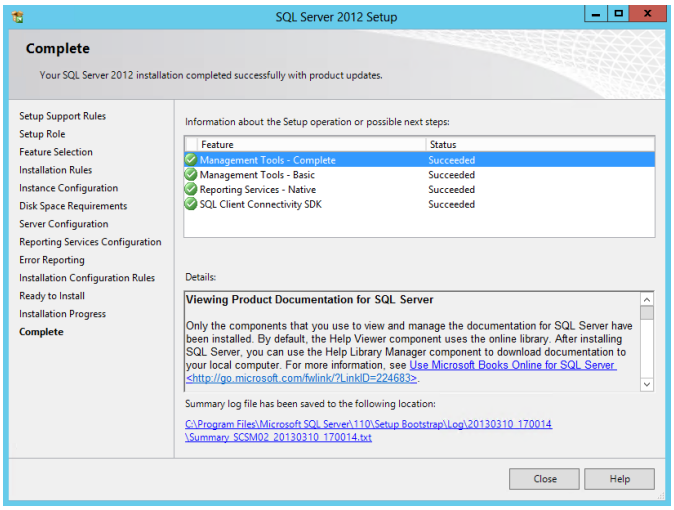
19. In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



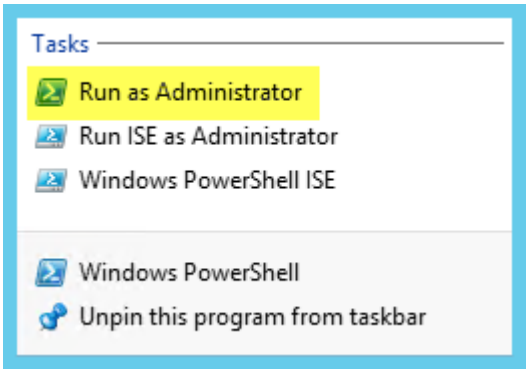
20. In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



21. When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



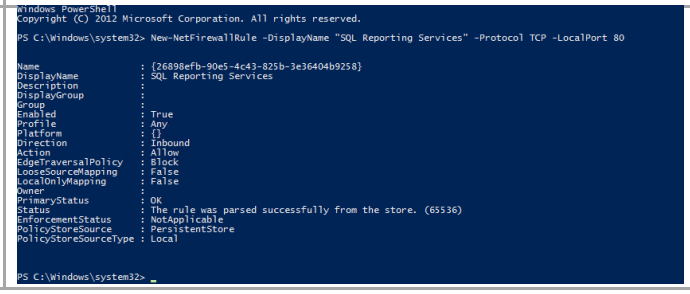
22. By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled.
23. Open an administrative session of PowerShell.



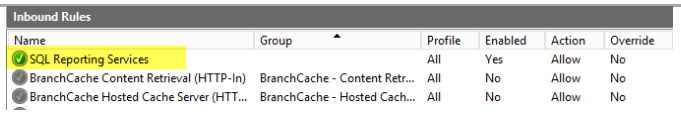
24. Execute the following commands to create the needed Firewall Rules:

```
New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80
```

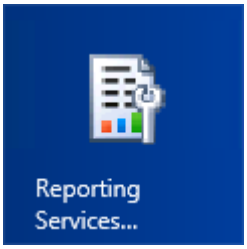
25. Adjust the display names and ports based on organizational requirements.



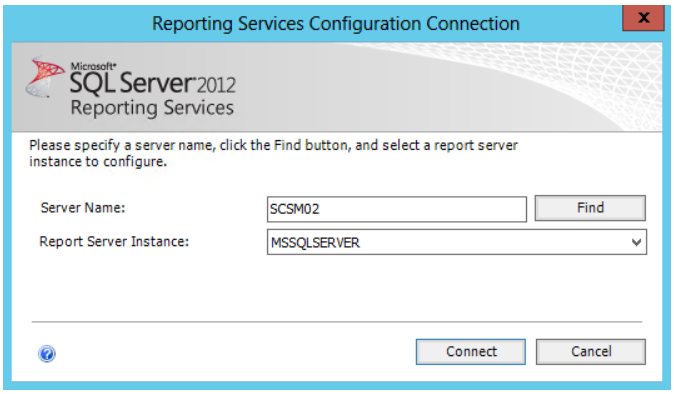
26. Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.



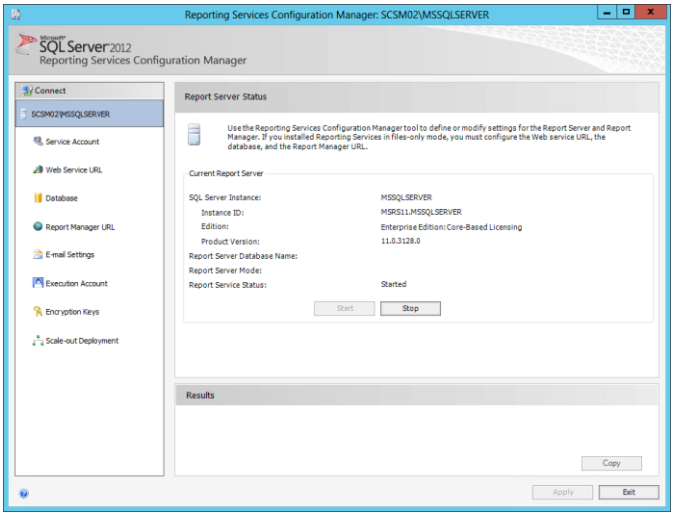
27. When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start** screen, navigate and select the **Reporting Services Configuration Manager** tile.



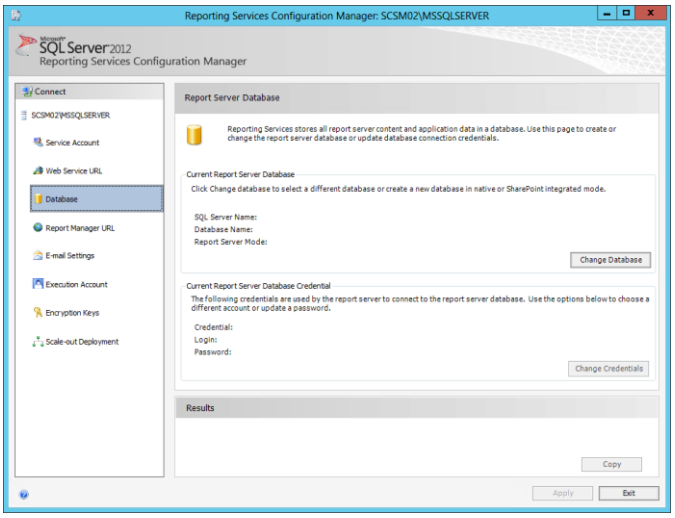
28. The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Service Manager server. In the **Report Server Instance** text box, use the default **MSSQLSERVER** drop-down menu value. Click **Connect**.



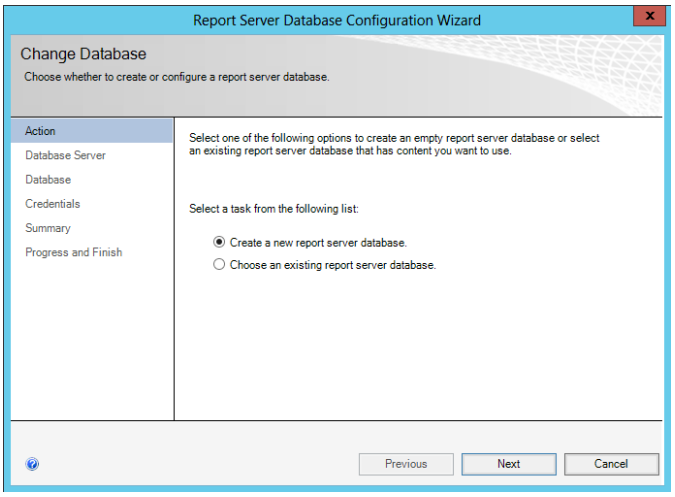
29. The **Reporting Services Configuration Manager** tool will appear.



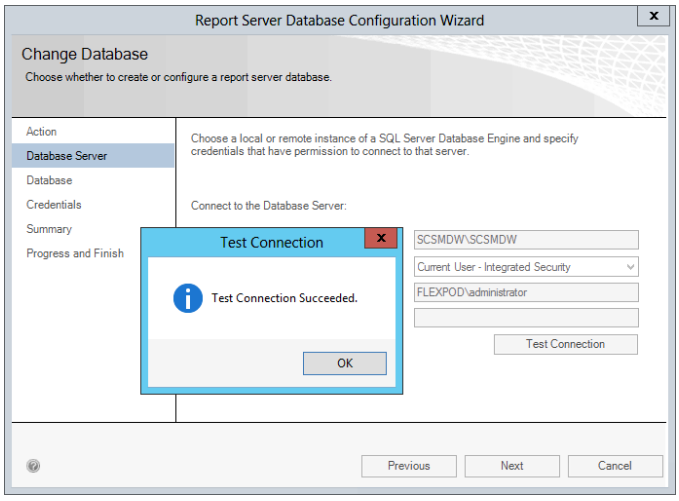
30. In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.



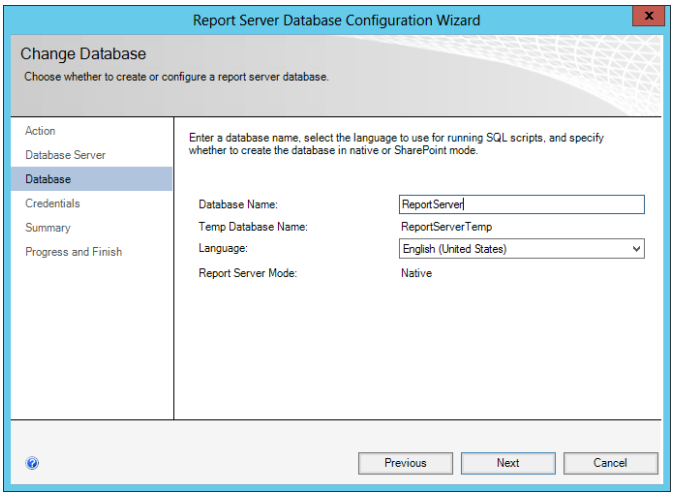
31. The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



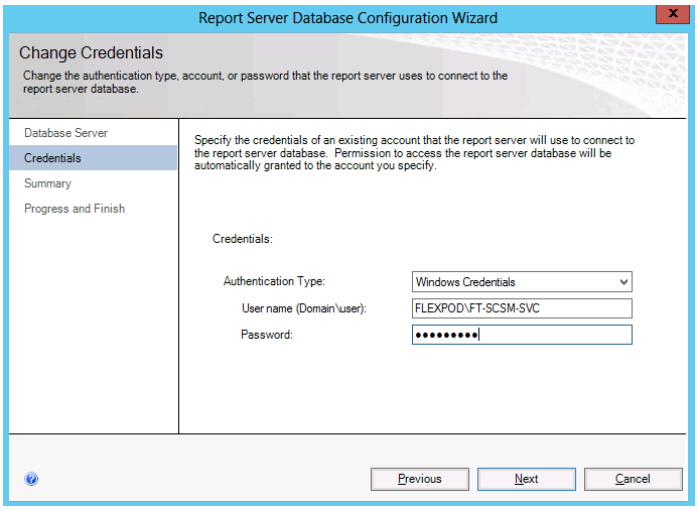
32. In the **Database Server** section, specify the following values:
    a. **Server Name** – *specify the name of the SQL Server Cluster SCSMDW Instance CNO and the database instance created for the Service Manager Data Warehouse installation.*
    b. **Authentication Type** – *specify **Current User – Integrated Security** from the drop-down menu.*
33. Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



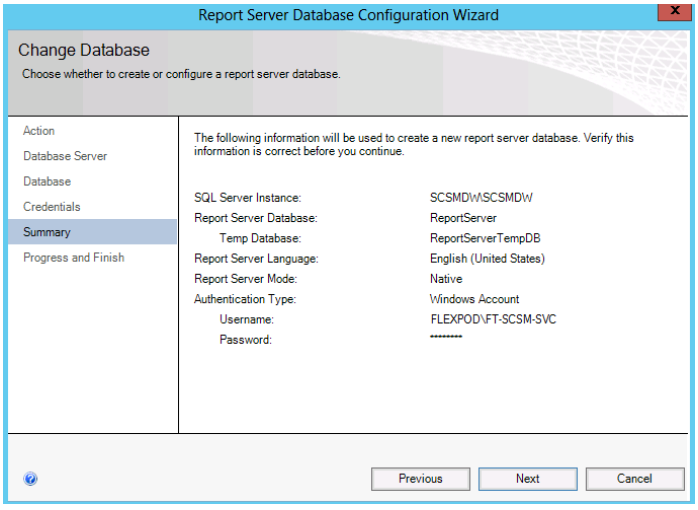
34. In the **Database** section, specify the following values:
    a. **Database Name** – *accept the default value of ReportServer.*
    b. **Language** – *specify the desired language option from the drop-down menu.*
    c. **Report Server Mode** – *select the **Native Mode** option.*
35. Click **Next** to continue.



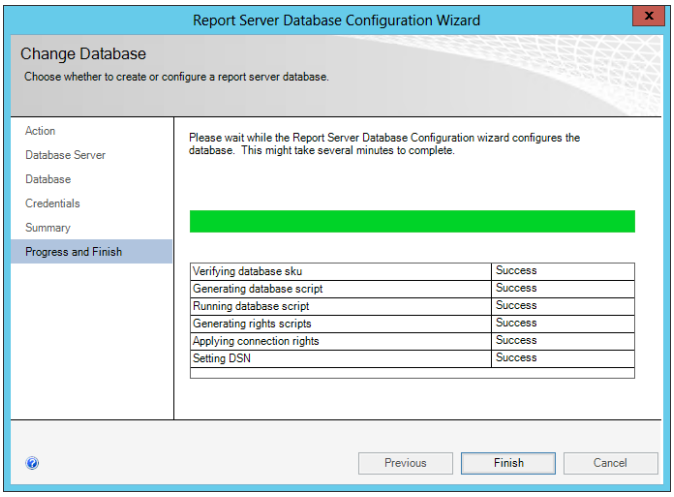
36. In the **Credentials** section, specify the **Authentication Type** as **Windows Credentials** from the drop-down menu. Enterh the **System Center Service Manager Service account** and **password**. Click **Next** to continue.



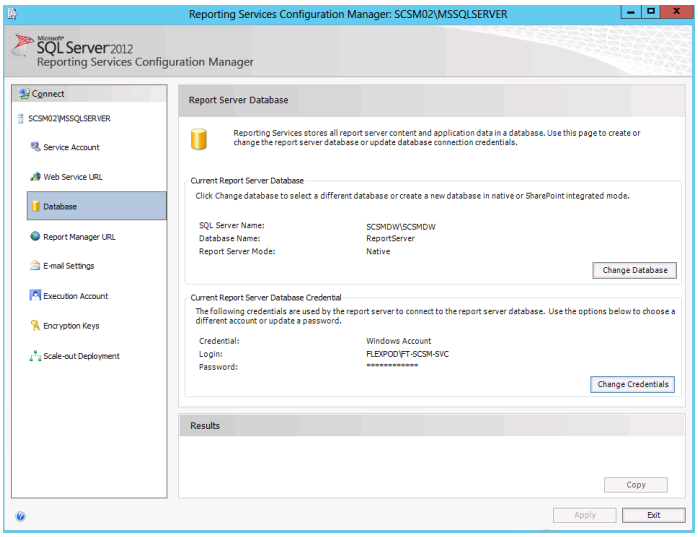
37. In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.



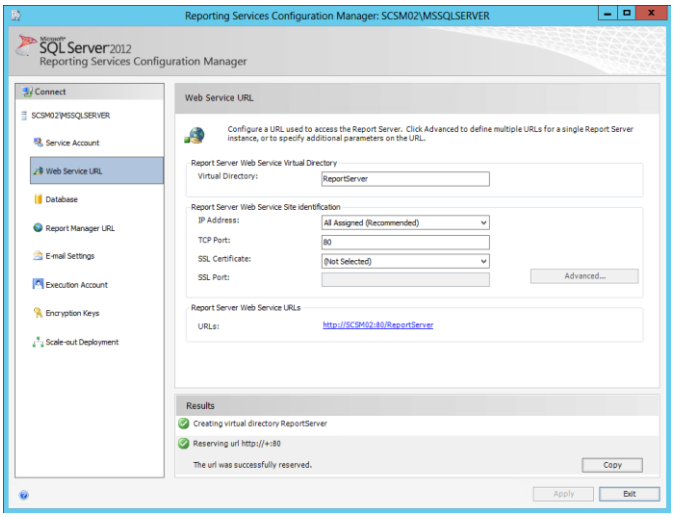
38. The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.



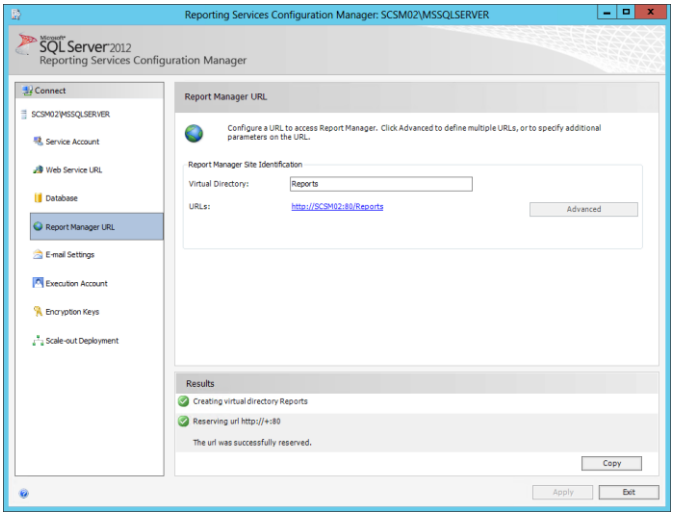
39. In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.



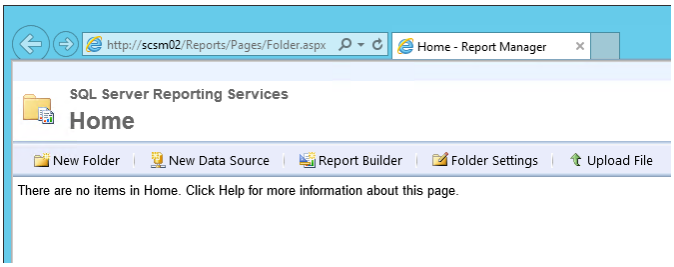
40. In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:
    a. In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer** in the provided text box.
    b. In the **Report Server Web Service Site Identification** section, set the following values**:**
    c. **IP Address** – *set the **All Assigned** drop-down menu value.*
    d. **TCP Port** – *specify the desired TCP Port (default 80).*
    e. **SSL Certificate** – *select the available certificate or choose the default of (Not Selected).*
41. Click the **Apply** button to save the settings and create the Web Service URL.

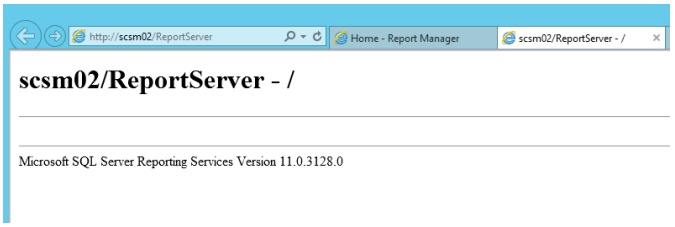


42. In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:
    a. In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports** (default) in the provided text box.
43. Click the **Apply** button to save the settings and create the Report Manager URL.



44. Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.

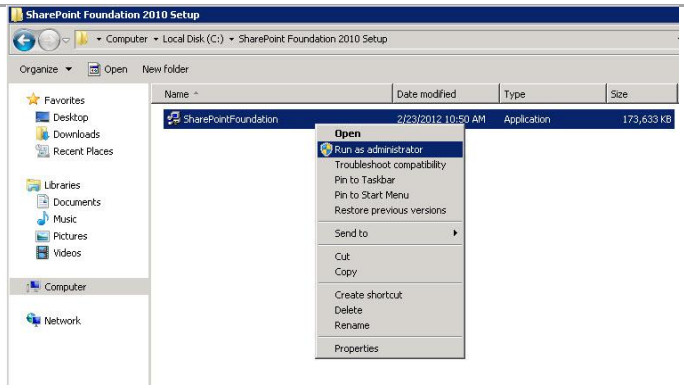


45. Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly. **Note**: In order to test the URL directory from the Service Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.	
46. Close the Reporting Server Configuration Manager.	

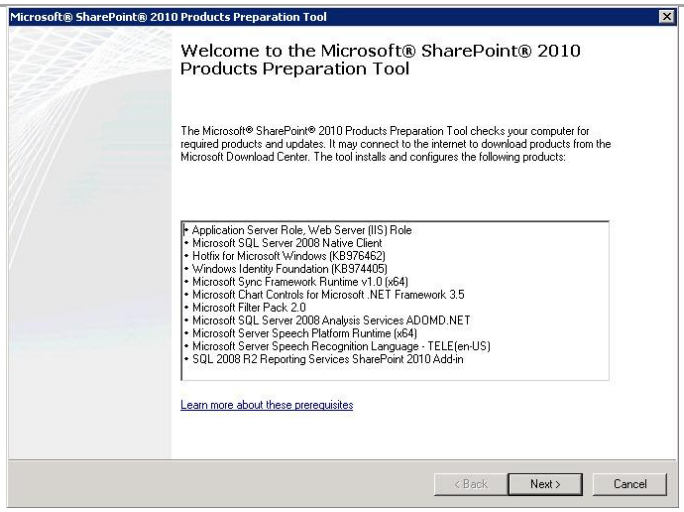
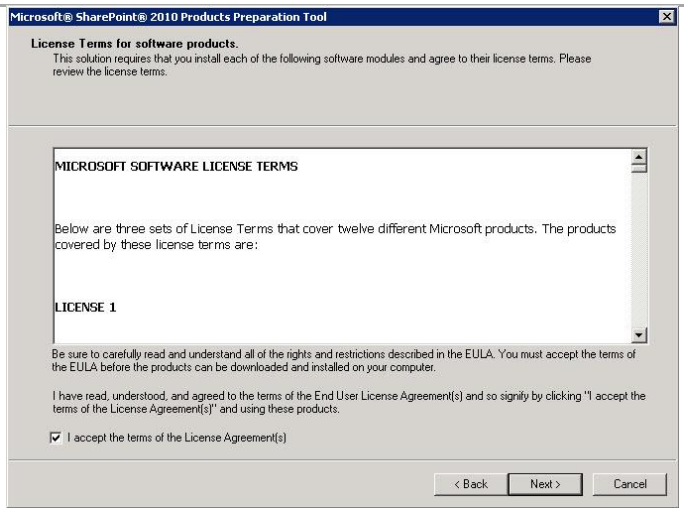
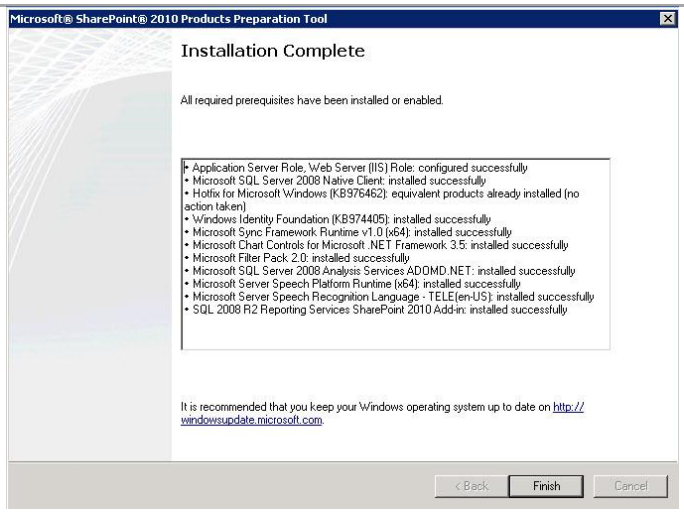
Install SharePoint Foundation 2010 Service Pack 1 on the Self-Service Portal Server

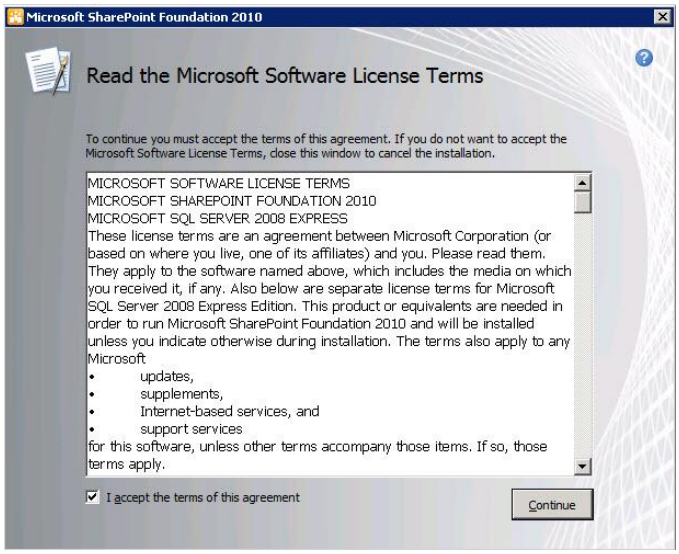
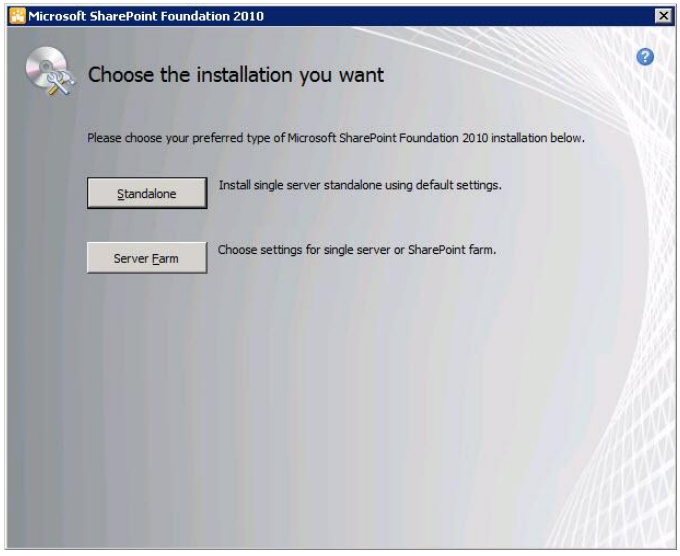
SharePoint Foundation 2010 SP1 must be installed to allow for configuration of SharePoint with the SQL Server 2012 installation. The following steps must to be completed in order to install SharePoint Foundation 2010 SP1 on the Service Manager self-service portal server only.

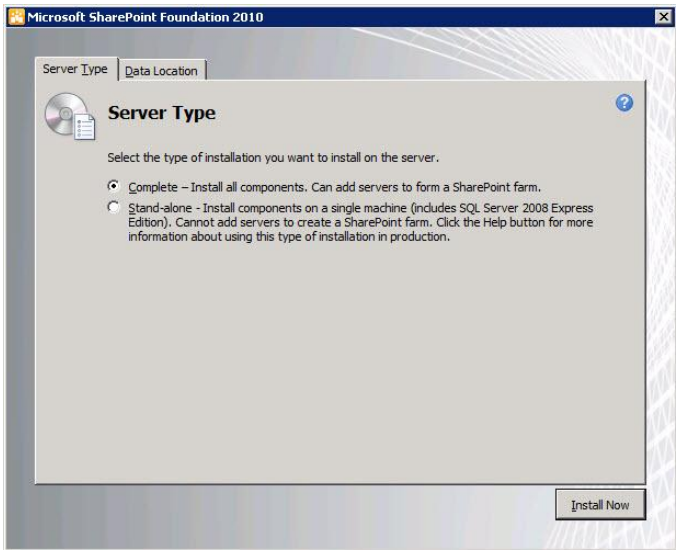
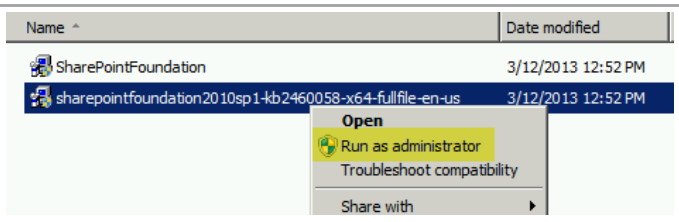
▶ Perform the following steps on the **Service Manager self-service portal** (SCSM03) virtual machine.

1. 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]	
2. The **SharePoint Foundation 2010** setup dialog will appear. In the **Install** section, select **Install software prerequisites**.	

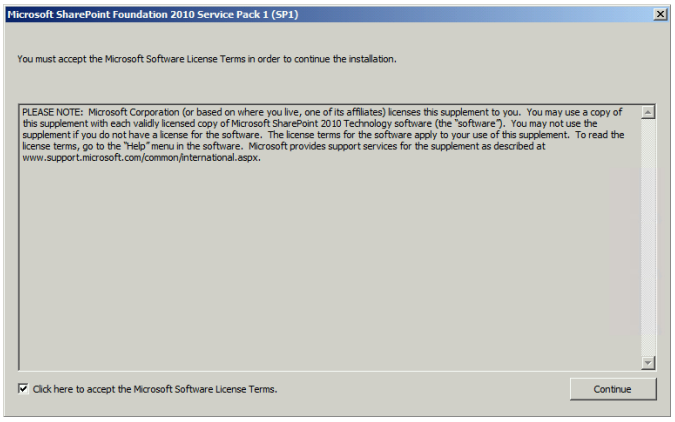
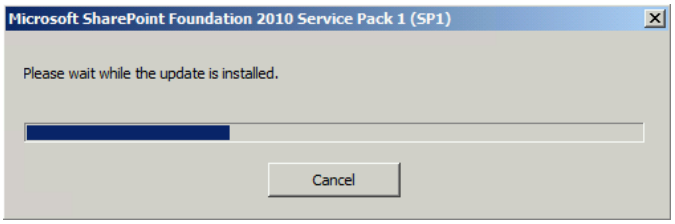
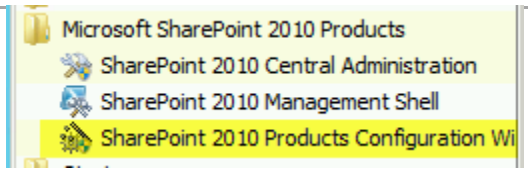
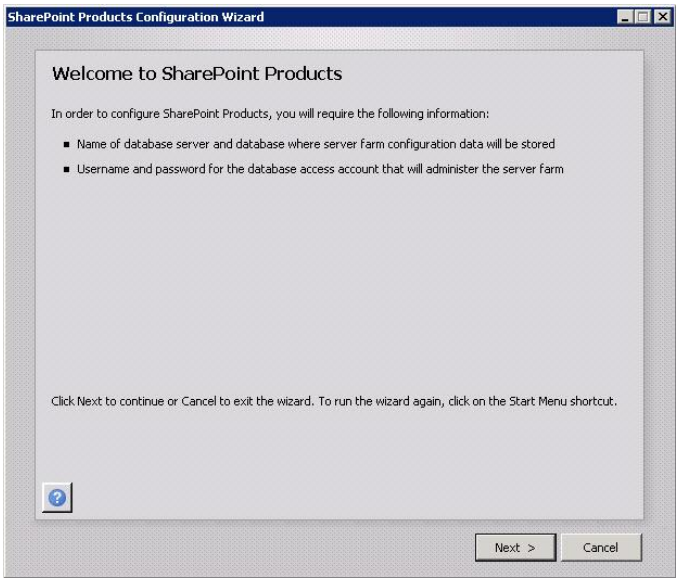
[15] Microsoft SharePoint Foundation 2010 - http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5970.

3. The **Microsoft SharePoint 2010 Products Preparation Tool** will open. Click **Next** to continue.	
4. 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.	
5. After the prerequisites install, the **Installation Complete** dialog will appear. Click **Finish** to complete the installation then **<u>restart</u>** the system.	

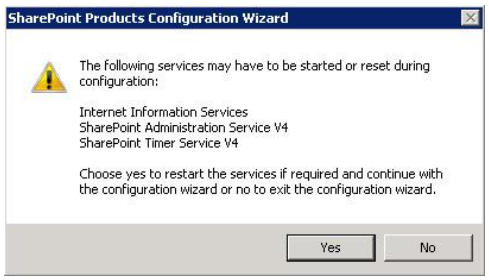
6. After the system restart, log back on with an account with administrative privileges. Re-launch the SharePoint Foundation 2010 installation. In the **SharePoint Foundation 2010** setup dialog, navigate to the **Install** section and select **Install SharePoint Foundation**.	
7. In the **Read the Microsoft Software License Terms** dialog, verify that the **I accept the terms of this Agreement** installation option check box is selected and click **Continue**.	
8. In the **Choose the installation you want** dialog, click the **Server Farm** button.	

9. In the **Server Type** dialog, select the **Complete** option and click **Install Now**.	
10. After installation, the **Run Configuration Wizard** dialog will appear. Verify that the **Run the SharePoint Products Configuration Wizard now** check box is not selected and click **Close**. **Important**: SharePoint Foundation Server 2010 Service Pack 1 must be installed prior to the configuration wizard being run.	
11. Service Pack 1 must be applied to SharePoint Foundation server after this installation.[16] 12. 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.	

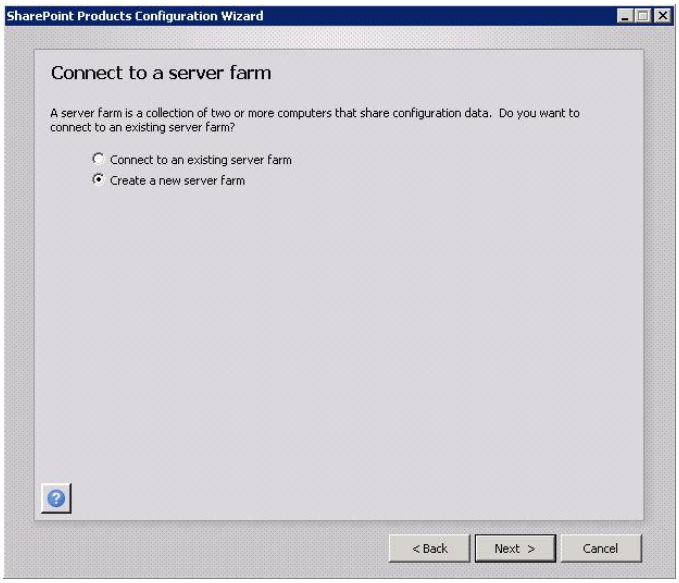
[16] Microsoft SharePoint Foundation 2010 SP1 - http://www.microsoft.com/download/en/details.aspx?id=26640.

13. 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.**	
14. 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.	
15. From the **Start** menu, expand the **Microsoft SharePoint 2010 Products** program folder and **select SharePoint 2010 Products Configuration Wizard**.	
16. The **SharePoint Products Configuration Wizard** will appear. Click **Next** to continue with the wizard.	

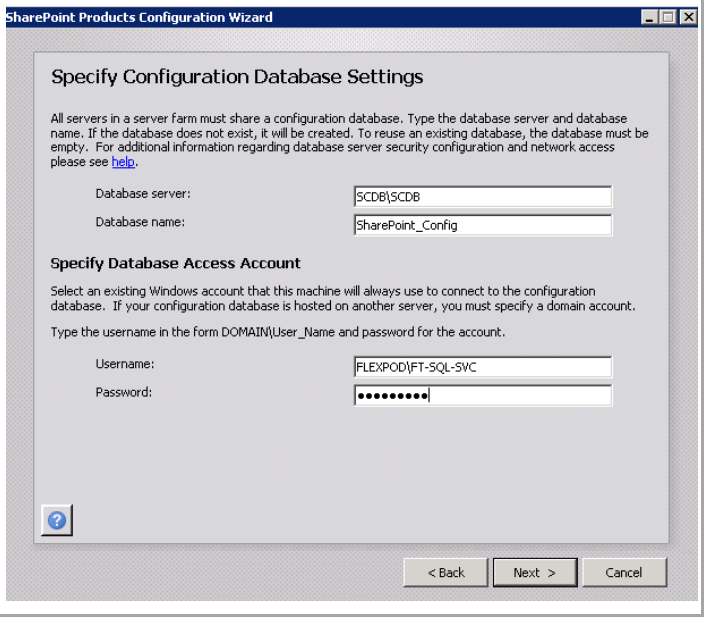
17. A dialog will appear that states that some services require restart as part of the installation. Click **Yes** to perform the services restart.



18. The **Connect to a server farm** dialog will appear. Select the **Create a new server farm** option and click **Next** to continue.

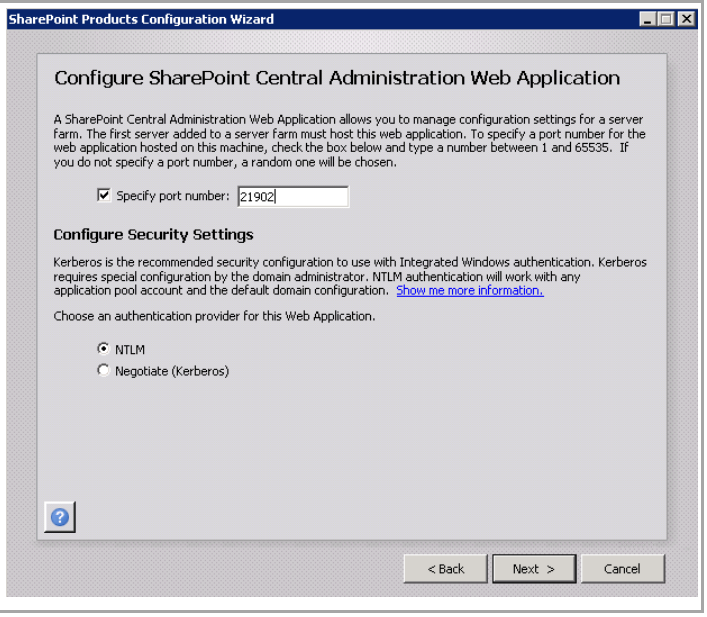


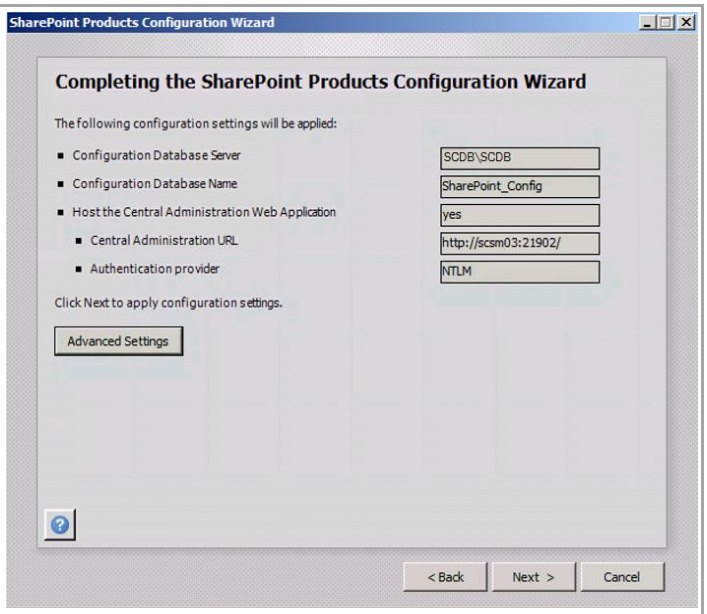
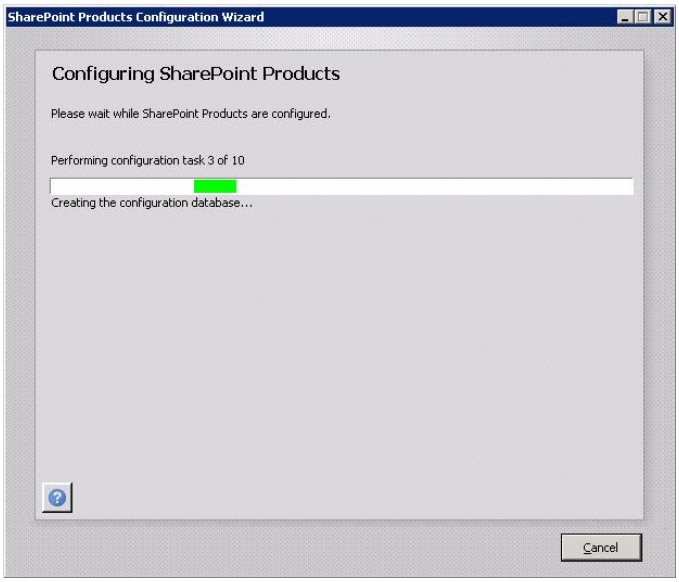
19. In the **Specify Configuration Database Settings** dialog, specify the following information in the provided text boxes:
    a. **Database server** – *specify the name of the SQL Server CNO and the database instance created for the Service Manager installation.*
    b. **Database name** – *specify the name of the SharePoint database. In most cases the default value of SharePoint_Config should be used.*
    c. In the **Specify Database Access Account** section, specify the Username (<DOMAIN>\<USERNAME>) and associated password for the Service Manager service account. When complete, click **Next** to continue.



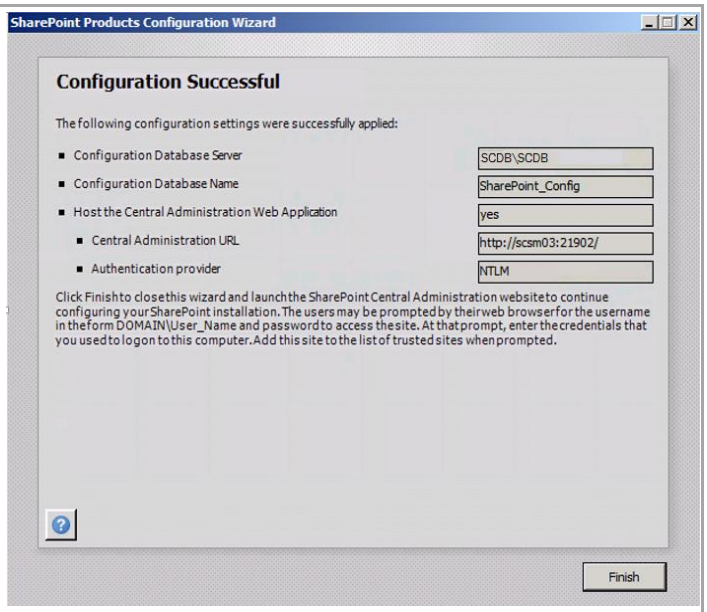
20. In the **Specify Farm Security Settings** dialog, enter a unique passphrase in the **Passphrase** text box. Re-type the passphrase in the **Confirm passphrase** text box and click **Next** to continue.

21. 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.
22. In the **Configure Security Settings** section, select the **NTLM** option.
23. When completed, click **Next** to continue.

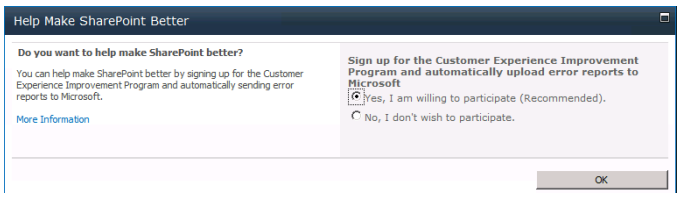


24. The **Completing the SharePoint Products Configuration Wizard** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Next** to continue.	
25. The wizard will display the progress while performing the SharePoint configuration.	

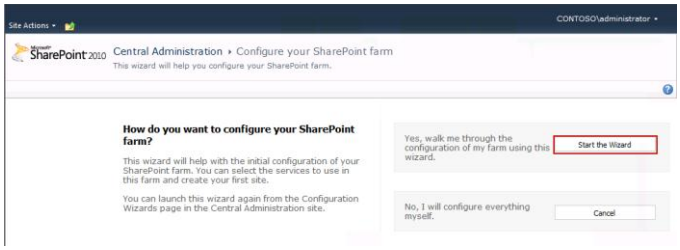
26. When successful, the **Configuration Successful** dialog will appear. Click **Finish** to complete the configuration of SharePoint Foundation 2010 Service Pack 1.



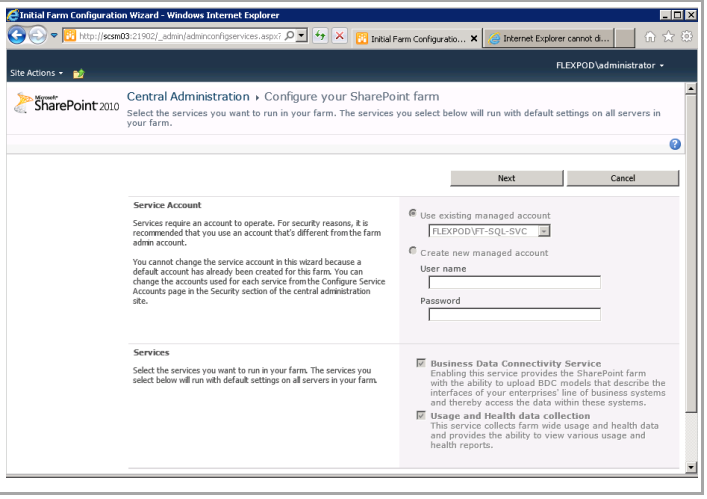
27. When prompted in the **Help Make SharePoint Better** page, select the appropriate option based on your organization's policies and click **OK** to save this setting.

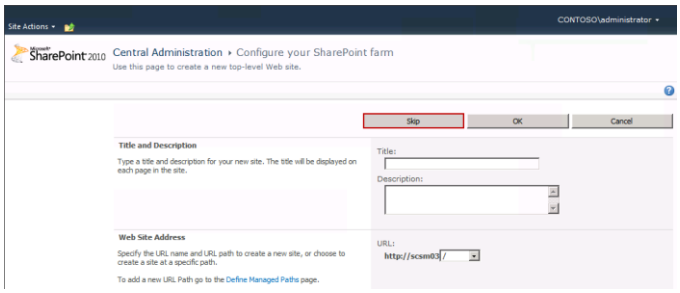
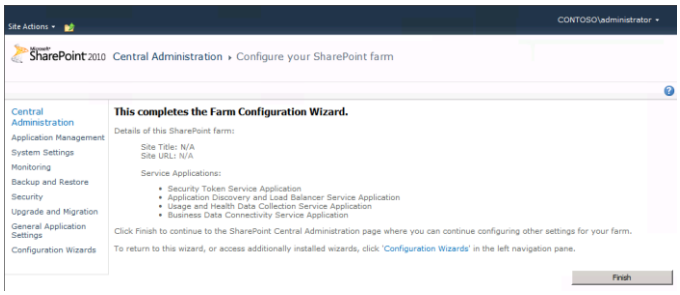
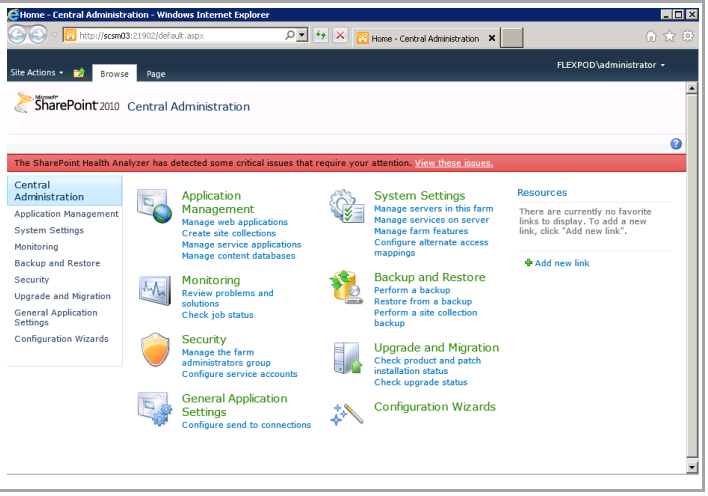


28. In the **Central Administration - Configure your SharePoint farm** page, click the **Start the Wizard** button to begin the SharePoint configuration.



29. In the **Service Account** section, select the **Use existing managed account** and select the Service Manager Service Account from the drop-down menu.
30. In the **Services** section, select the **Business Data Connectivity Services** and **Usage and Health data collection** check boxes.
31. Click **Next** to continue.



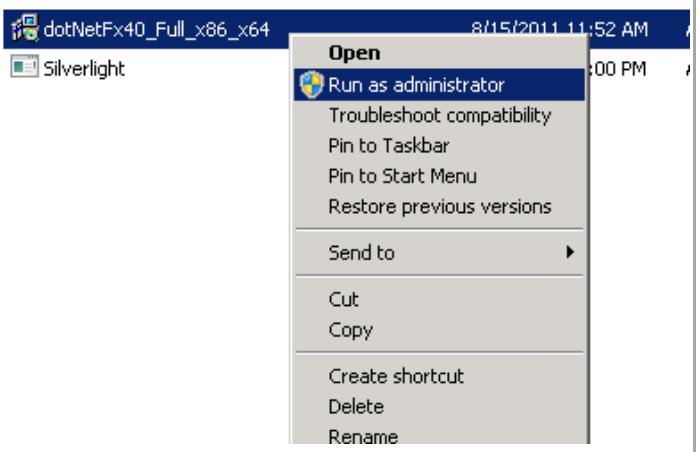
32. In the Web Site configuration page, click the **Skip** button to continue without configuring these settings.	
33. The SharePoint farm configuration is now complete. Click the **Finish** button to exit.	
34. The **SharePoint Central Administration** portal will open. Verify that SharePoint is operating 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

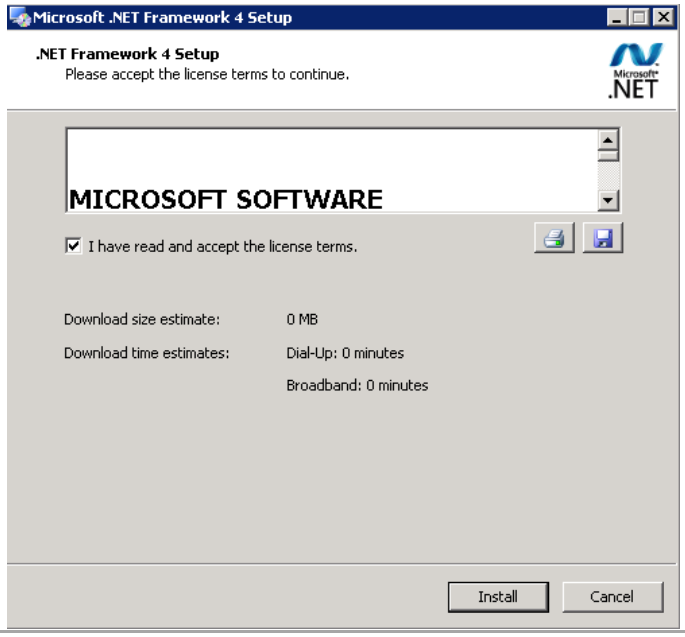
Additionally, the Service Manager self-service portal installation also requires the .NET Framework 4 package to be installed prior to installation. Follow the provided steps to install the .NET Framework 4 on the self-service portal.

▶ Perform the following steps on the **Service Manager self-service portal** (SCSM03) virtual machine.

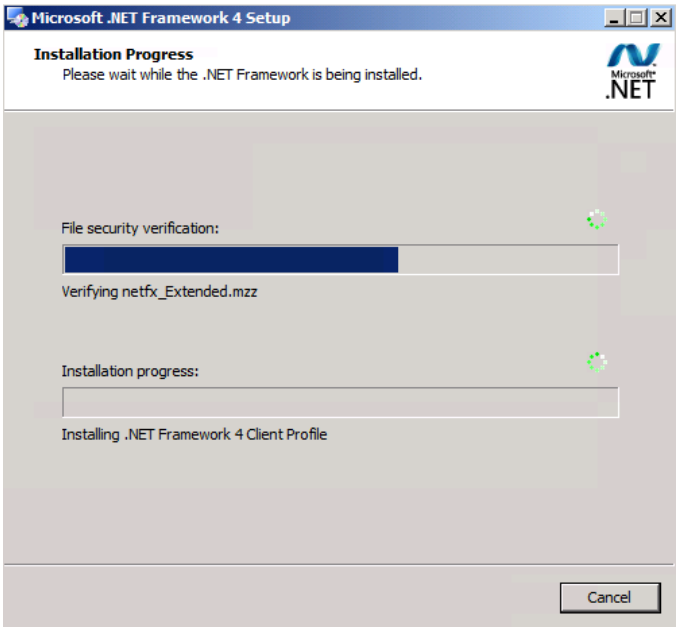
1. From the installation media source, right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** from the context menu to begin setup.



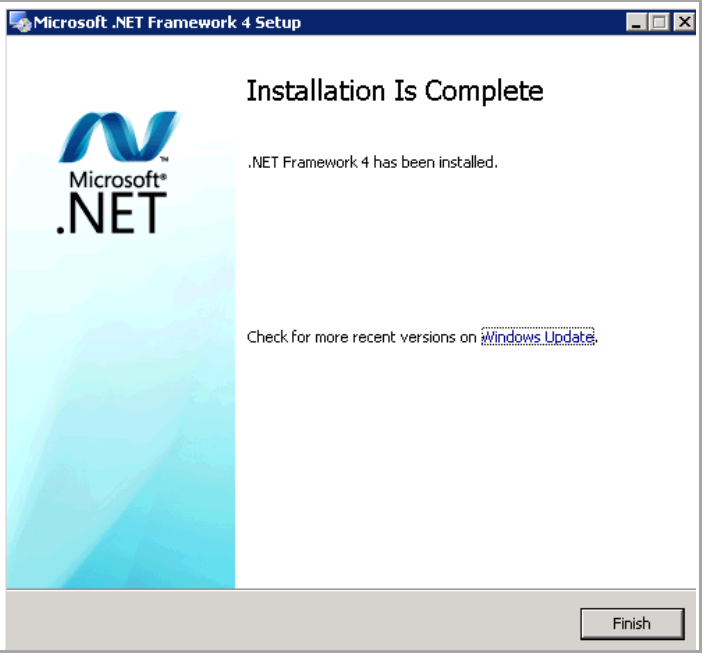
2. Within the **Microsoft .NET Framework 4 Setup** dialog, select the **I have read and accept the license terms** check box and click **Install** to begin the installation.



3. The installation progress will be displayed in the setup wizard.



4. When completed, click **Finish** to exit the installation.

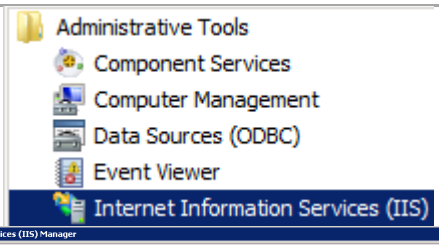
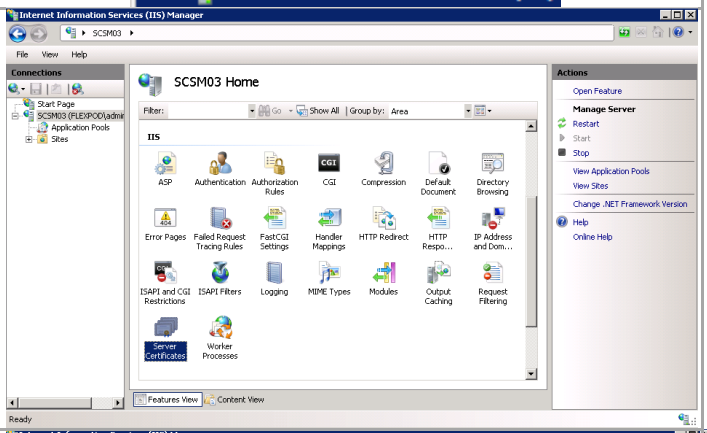
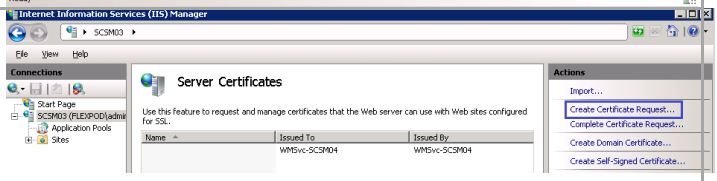


Request and Install an SSL Certificate on the Self-Service Portal Server

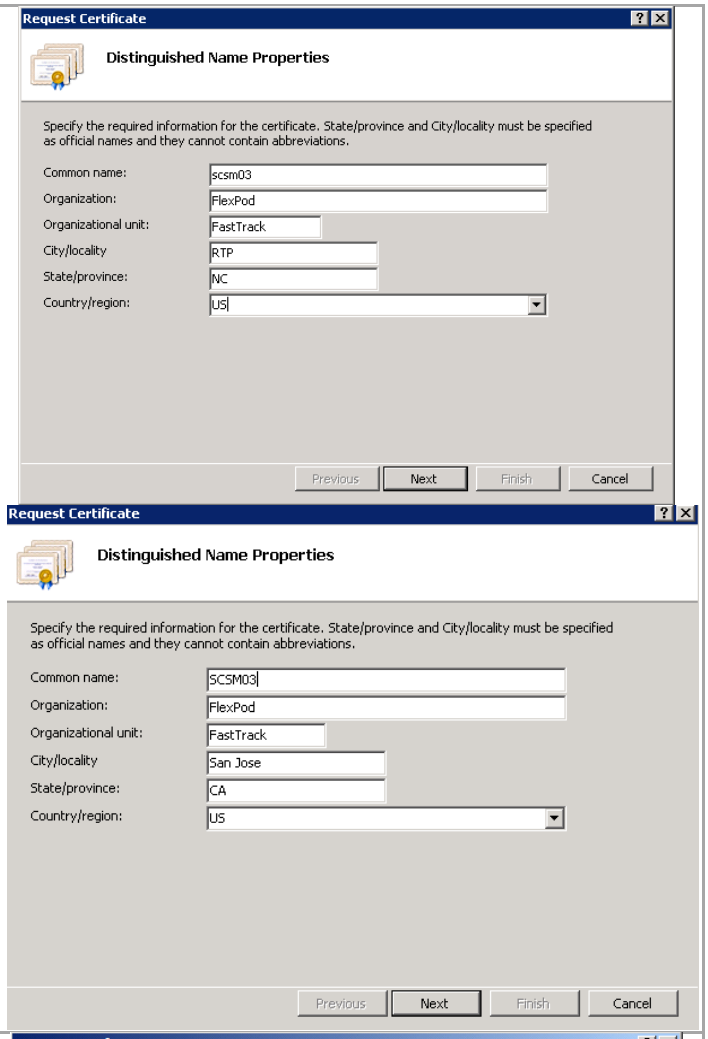
Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website.[17] If the self-service portal is to be installed without SSL this section can be skipped. There are several ways to request an SSL Certificate. One method, through the IIS Manager console, is outlined below.

▶ Perform the following steps on the **Service Manager self-service portal** (SCSM03) virtual machine.

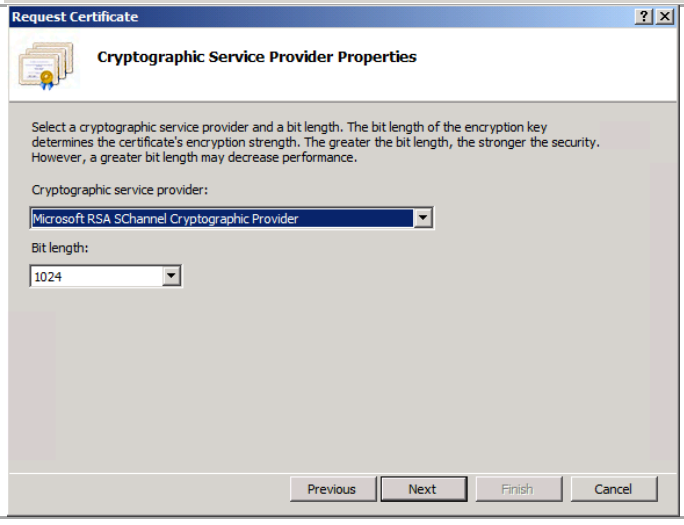
[17] SSL Certificates for the self-service portal - http://technet.microsoft.com/en-us/library/hh667343.aspx.

1. 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.**	
2. In the **Internet Information Services (IIS) Manager** console, select the server node and in the IIS section, double-click **Server Certificates**.	
3. The **Server Certificates** pane will expand. Under actions, click **Create Certificate Request...**	

4. 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.

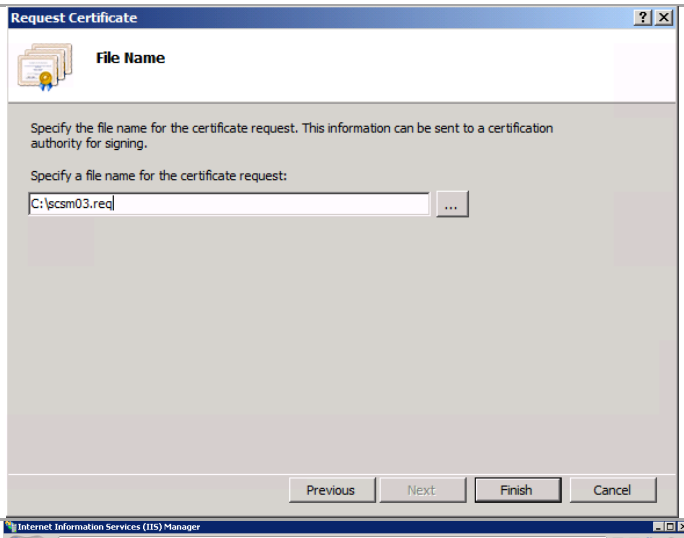


5. In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing certification authority (CA). In most cases, selecting the default CSP and default bit length is satisfactory. Click **Next** to continue.

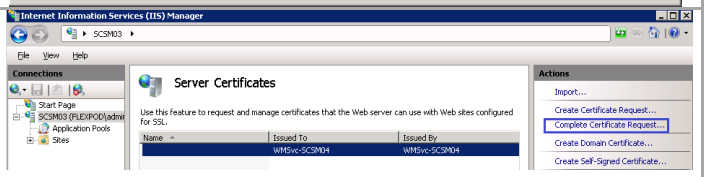


6. In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

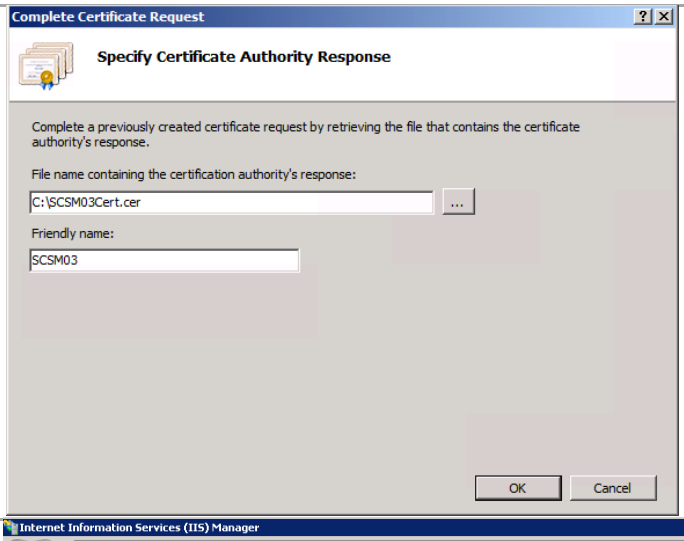
   When completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.



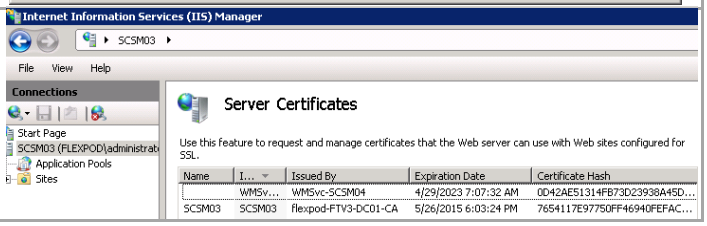
7. After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** once again. From the **Actions** pane, select **Complete Certificate Request...**



8. 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.



9. In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.

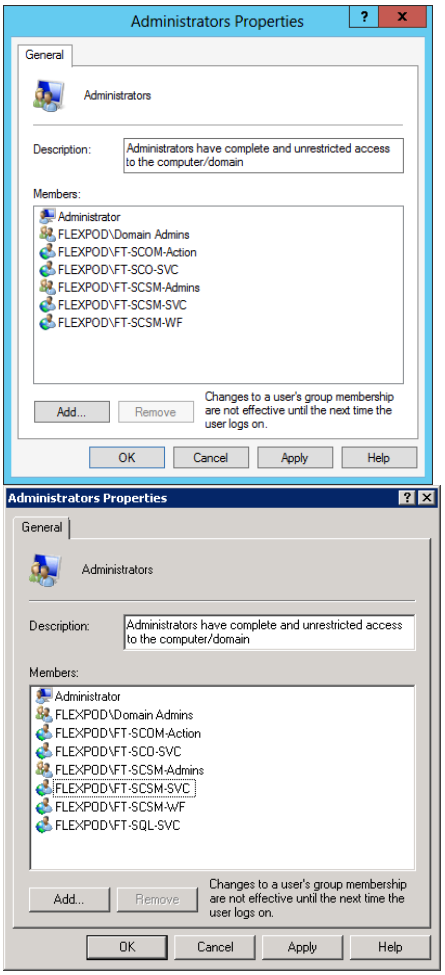


Configuration of Service Manager Environmental Prerequisites

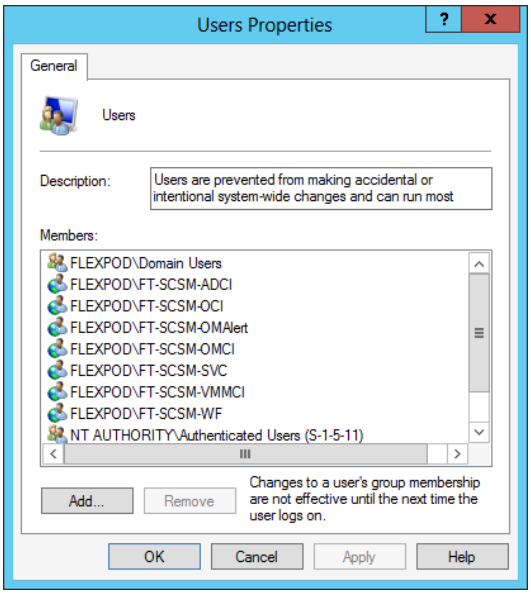
The following steps must to be completed in order to install the Service Manager roles correctly.

▶ Perform the following steps on **all Service Manager Servers** virtual machines.

1. Log on to each Service Manager virtual machine with a user with local admin rights.
2. 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.
3. On the self-service portal server, also add the following accounts:
   - SQL service account

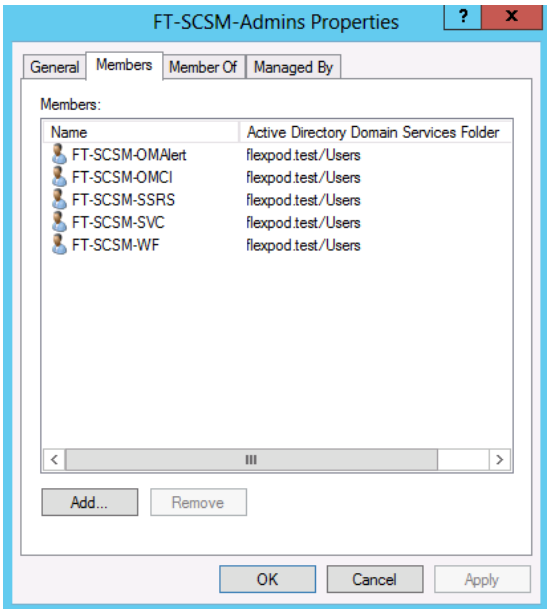


4. Verify that the following accounts and/or groups are members of the Local Users group on each Service Manager virtual machine:
   - Service Manager Active Directory CI connection account.
   - Service Manager Orchestrator CI connection account.
   - Service Manager Operations Manager alert connection 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.

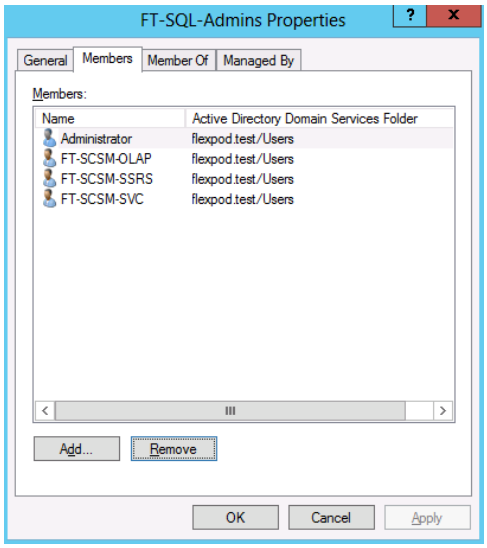


▶ Perform the following step on an **Active Directory Domain Controller** in the target environment.

1. 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.

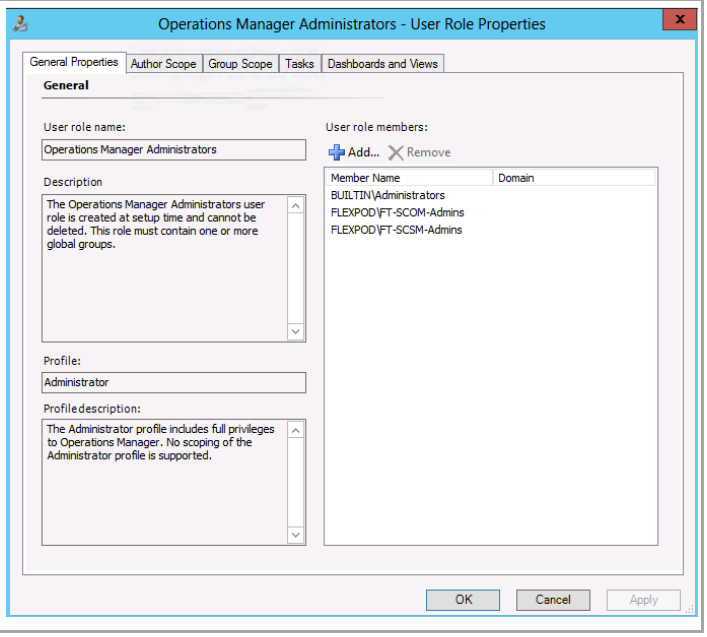


2. In the domain where Service Manager will be installed, verify that the SM OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group created earlier.

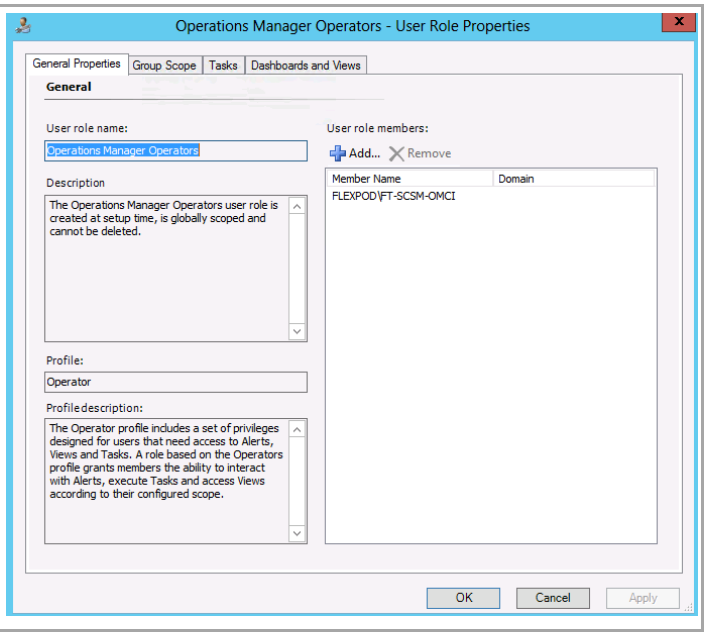


▶ Perform the following steps on the **Operations Manager** virtual machine.

1. 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.



2. 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.



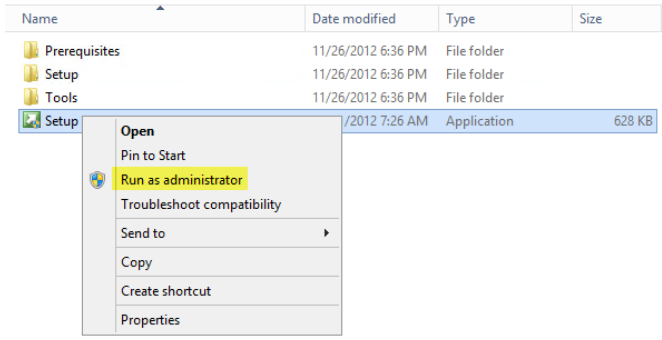
19.3 Installation

Install the Service Manager Management Server

The following steps must to be completed in order to install the Service Manager management server role.

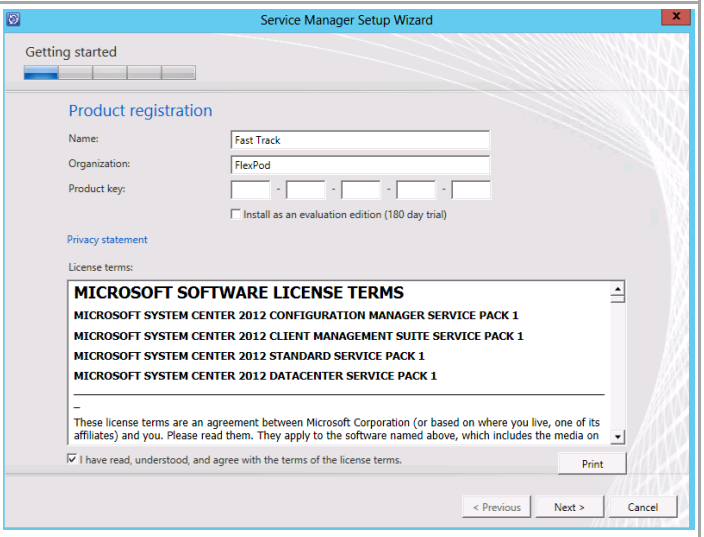
▶ Perform the following steps on the **first Service Manager management server** (SCSM01) virtual machine.

1. Log on to Service Manager management server (**NOT** the Service Manager Data Warehouse server or the self-service portal server).
2. From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

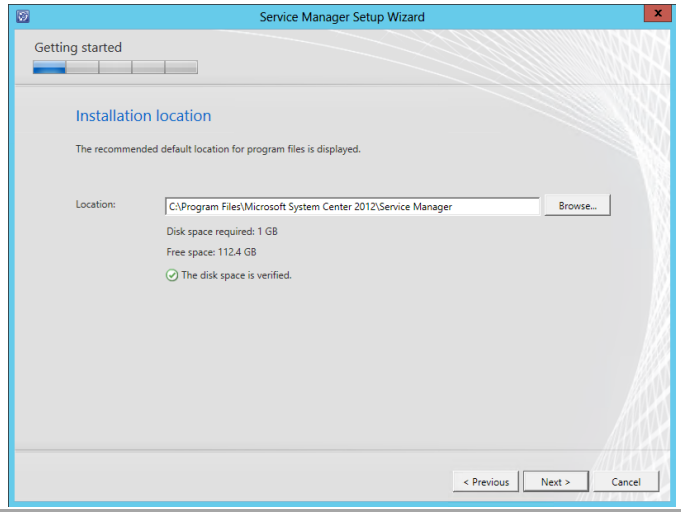


3. The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager management server** to begin the Service Manager server installation.

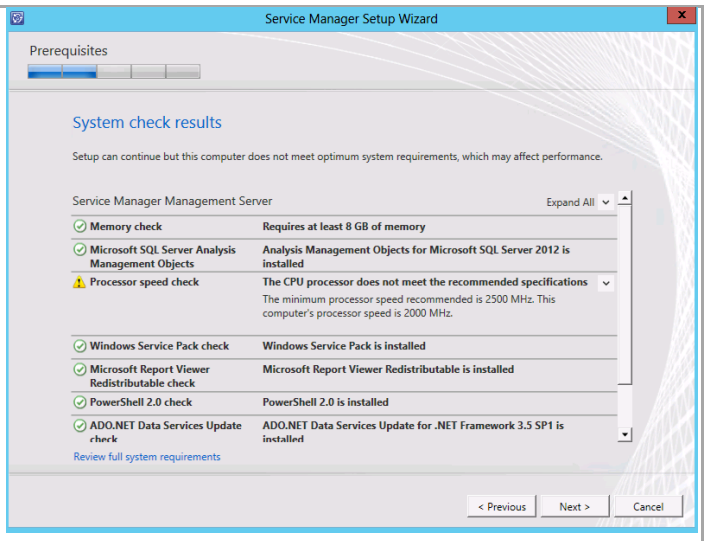
4. In the **Product registration** dialog, provide the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** – *specify the name of the licensed organization.*
    c. **Product 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.*
5. In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.



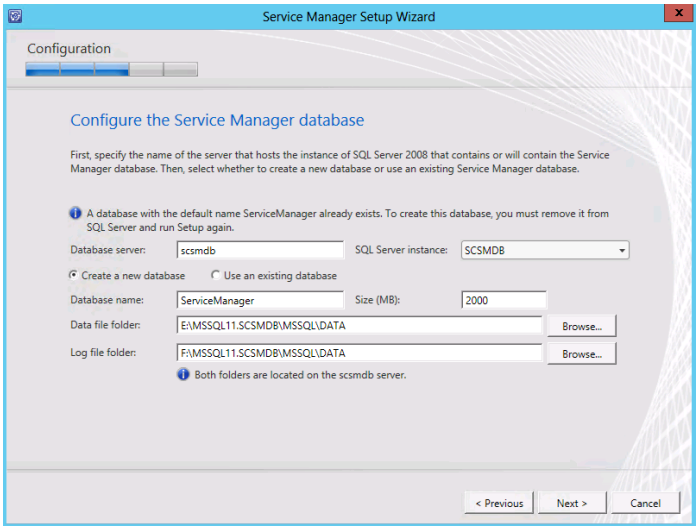
6. In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.



7. 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.
8. The processor speed check warning can be ignored. The Cisco UCS B200 M3 meets the processor requirements for Service Manager 2012 SP1.

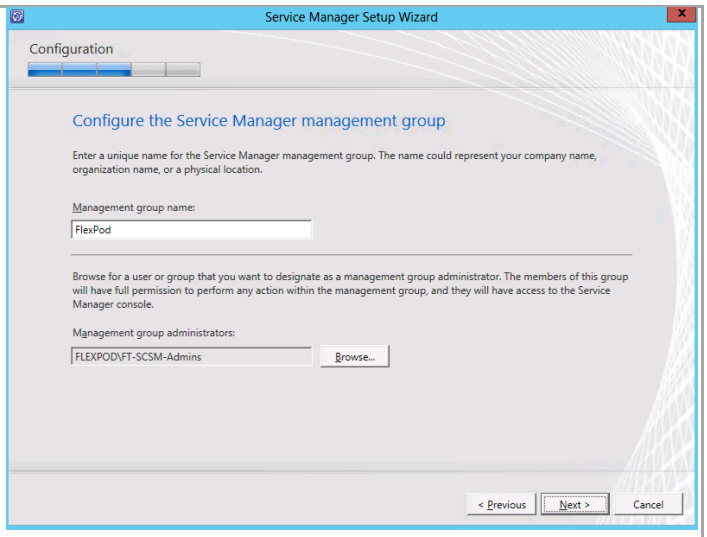


9. In the **Configure the Service Manager database** dialog, specify the following information in the provided text boxes:
    a. **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation.*
    b. **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation.*
    c. Select the **Create a new database** option and specify the following information in the provided text boxes:
    d. **Database name** – *specify the name of the Service Manager database. In most cases the default value of ServiceManager should be used.*
    e. **Size (MB)** – *specify the initial database size*[18]*. The default value can be used for Fast Track validation.*
    f. **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.*
    g. **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.*
10. Click **Next** to continue.

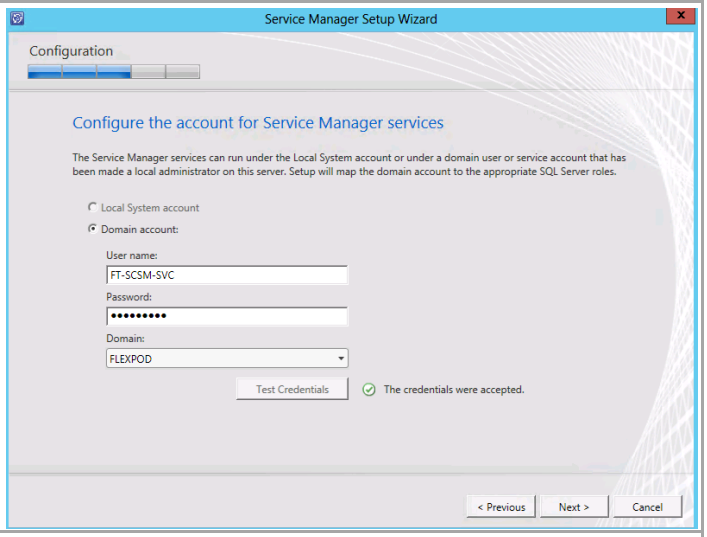


[18] Planning for Performance and Scalability in System Center 2012 - Service Manager - http://technet.microsoft.com/en-us/library/hh495684.aspx contains a link to the Service Manager job aids and provides general guidance for database sizing

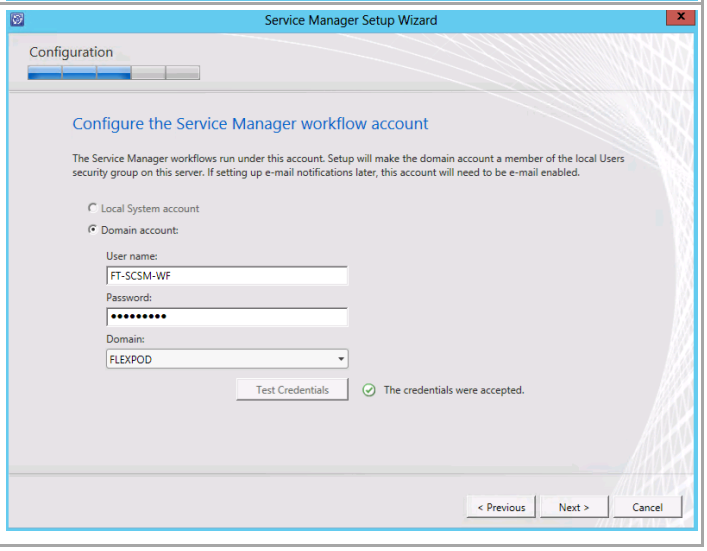
11. In the **Configure the Service Manager management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager Data Warehouse and Operations Manager installations.
12. Specify the Service Manager Administrators group in the **Management group administrators** object picker section.
13. Click **Next** to continue.

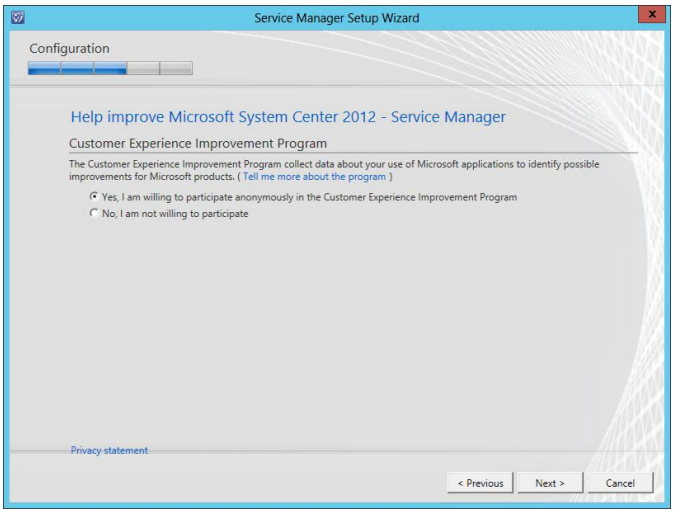
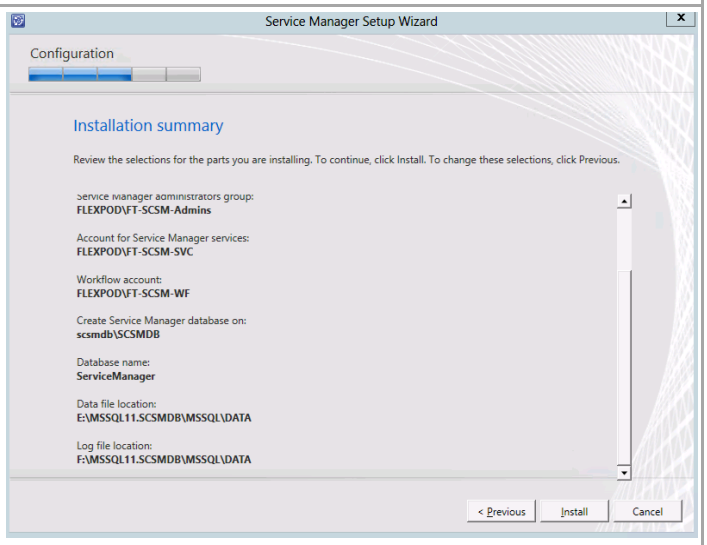


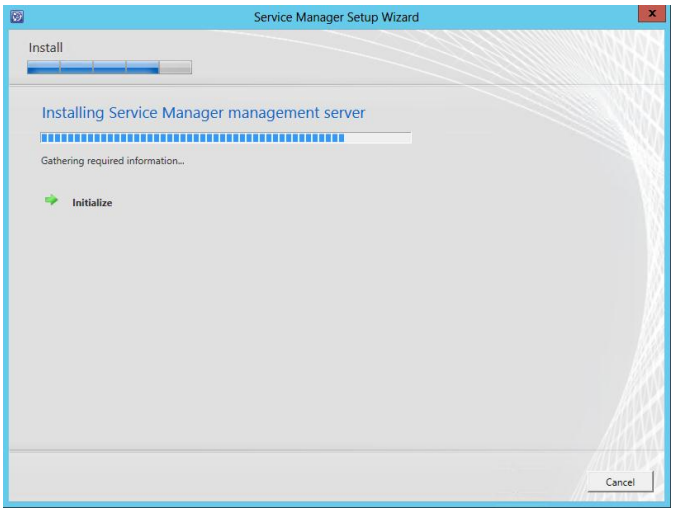
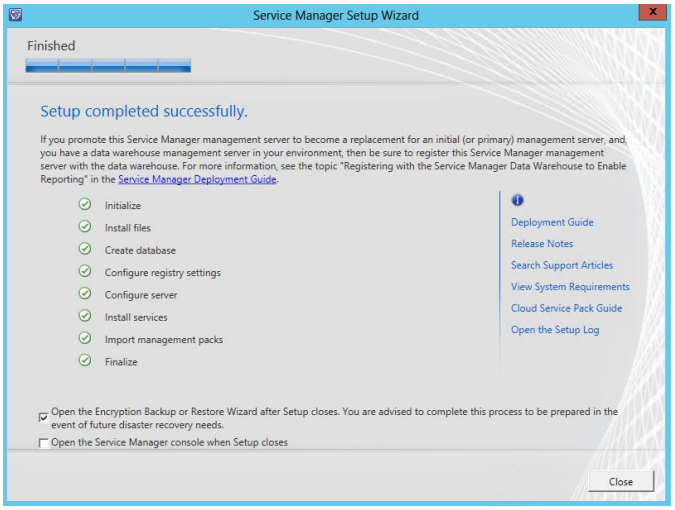
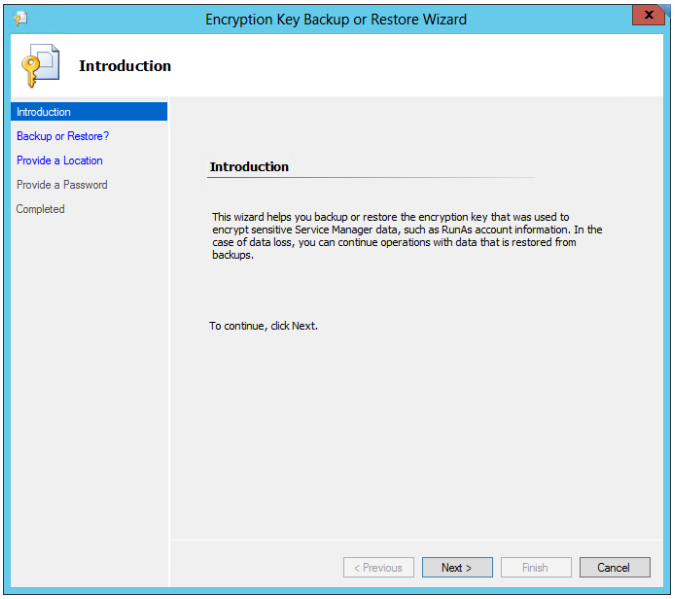
14. In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
15. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
16. When successful, click **Next** to continue.

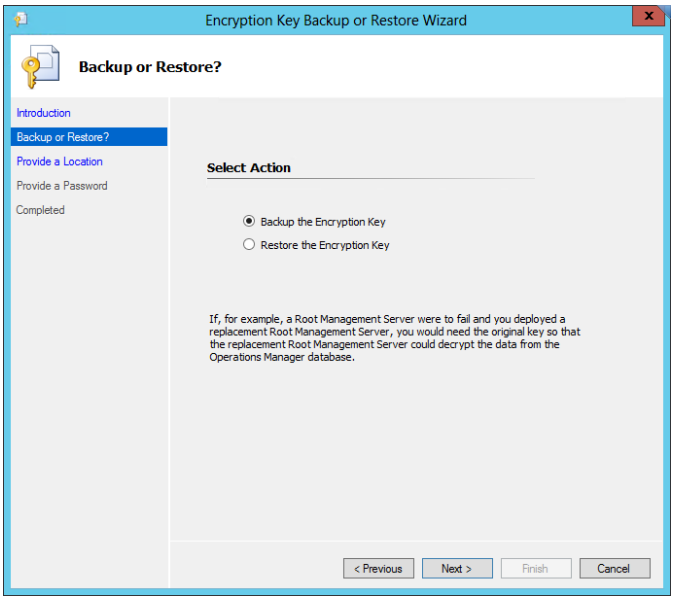
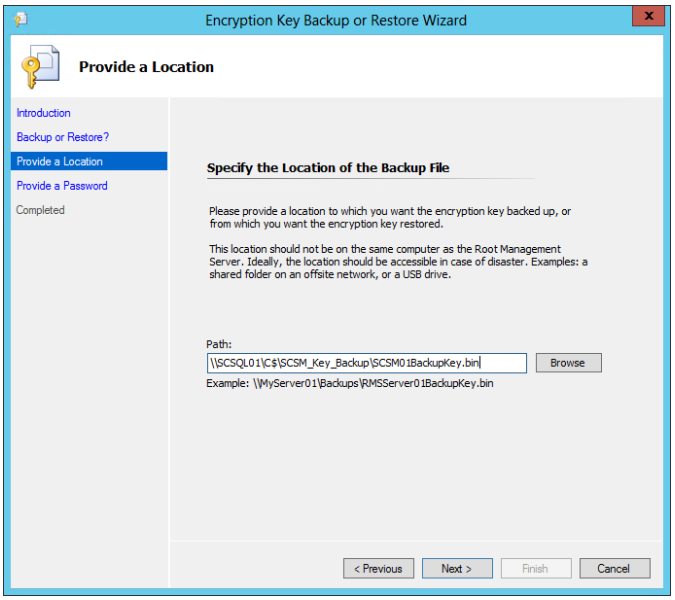


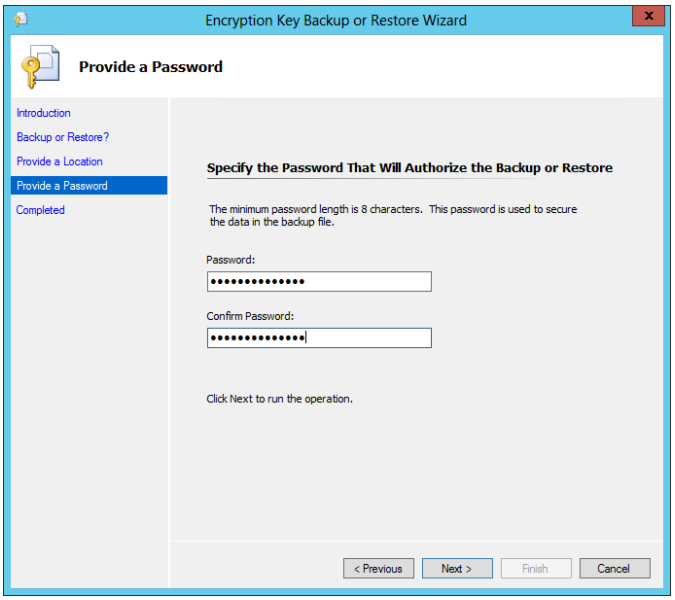
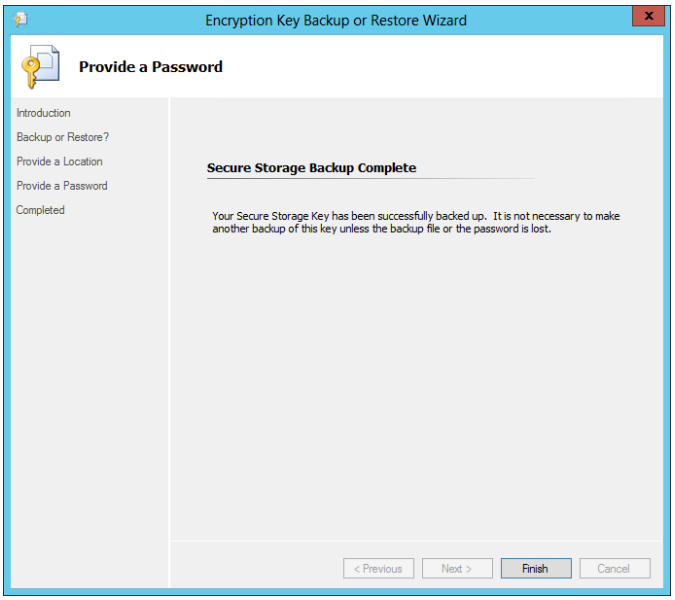
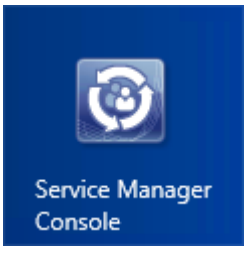
17. In the **Configure the account for Service Manager workflow account** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
18. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
19. When successful, click **Next** to continue.

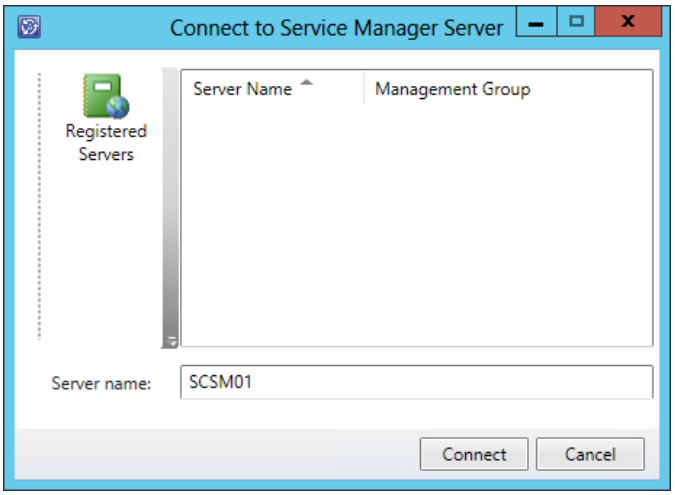
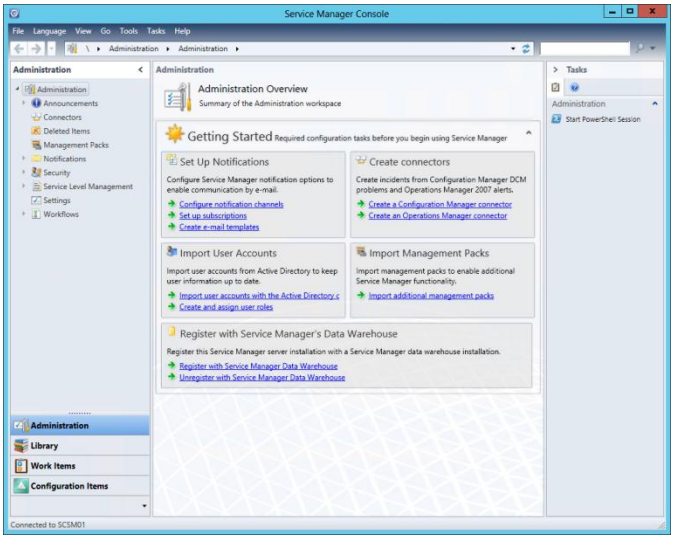


20. In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.	
21. Depending on your system's configuration, the **Use Microsoft Update to help 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.	
22. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

23. The wizard will display the progress while installing features.	
24. When the installation completes, the wizard will display the **Setup completed successfully** dialog. 25. When 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. 26. Click **Close** to complete the installation.	
27. When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.	

28. In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.	
29. 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.	

30. 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.	
31. When complete, click **Finish** to exit the wizard.	
32. 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.	

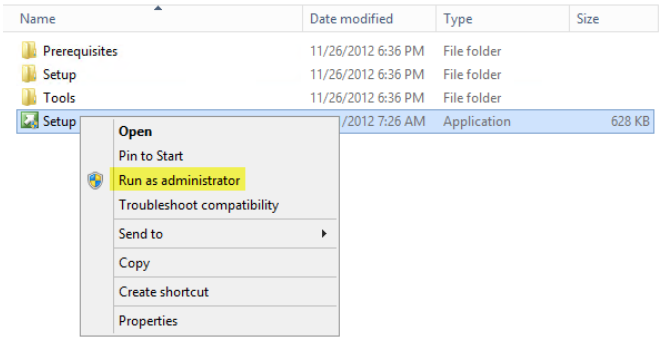
33. In the **Connect to Service Manager Server** dialog, specify the Service Manager management server name in the **Server name** text box and click **Connect** to start the console.	
34. The Service Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.	

Install the Service Manager Data Warehouse Server

The following steps must to be completed in order to install the Service Manager Data Warehouse server role.

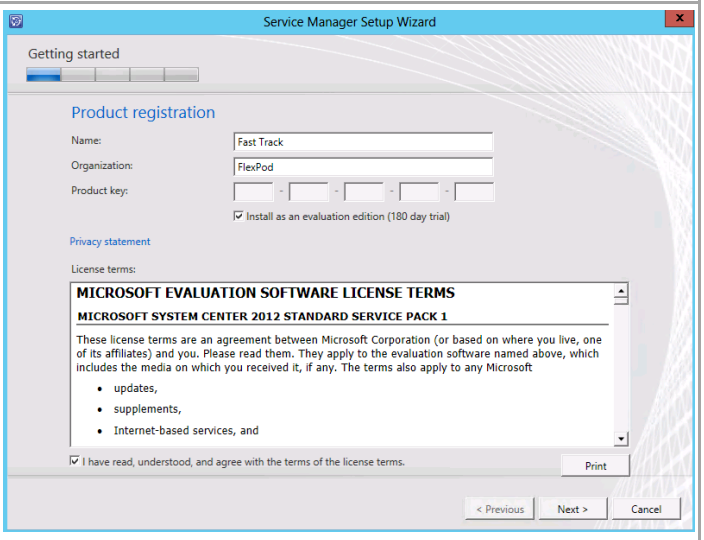
▶ Perform the following steps on the **Service Manager Data Warehouse server** (SCSM02) virtual machine.

1. Log on to Service Manager Data Warehouse server (**NOT** the Service Manager management server or the self-service portal server).
2. From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

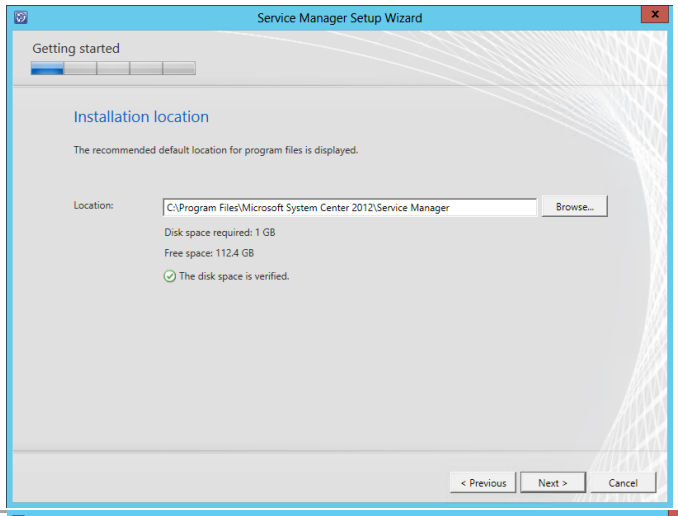


3. The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager data warehouse management server** to begin the Service Manager server installation.

4. In the **Product registration** dialog, provide the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** - *specify the name of the licensed organization.*
    c. **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.*
5. In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** checkbox. When all selections are confirmed, click **Next** to continue.

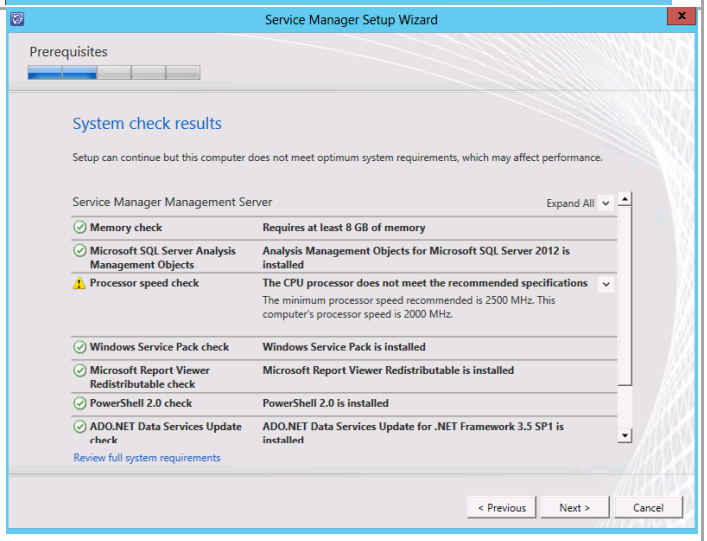


6. In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.

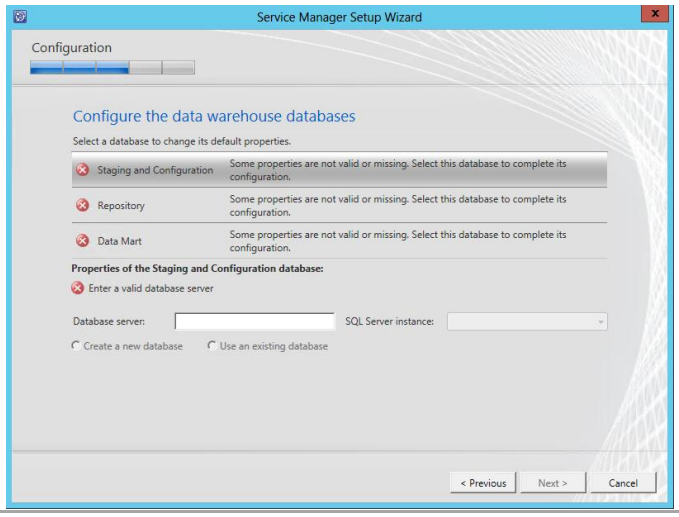


7. The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.

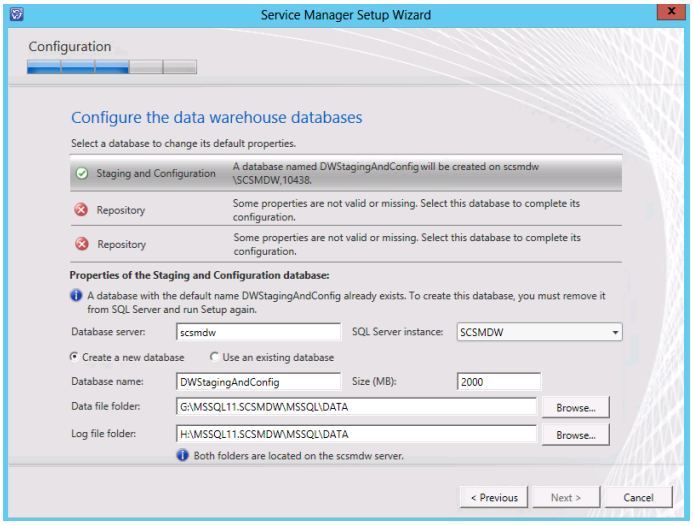
8. The processor speed check warning can be ignored. The Cisco UCS B200 M3 meets the processor requirements for Service Manager 2012 SP1.



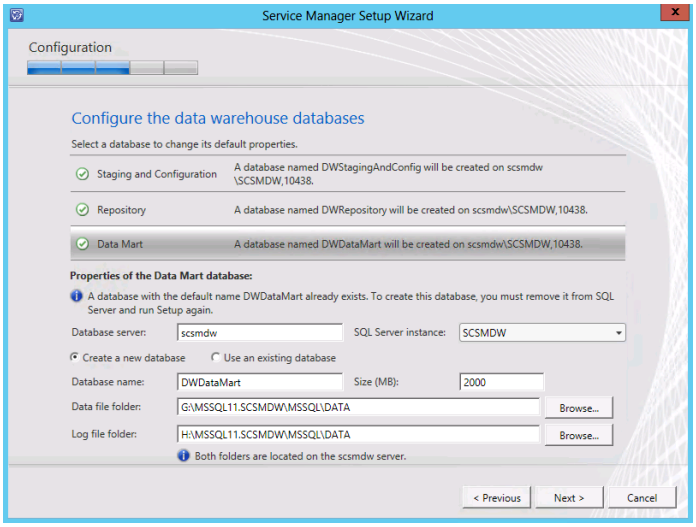
9. When the **Configure the data warehouse databases** dialog launches each subcategory will appear with an error message until each of the following sections are configured:
    a. Staging and Configuration.
    b. Repository.
    c. Data Mart.



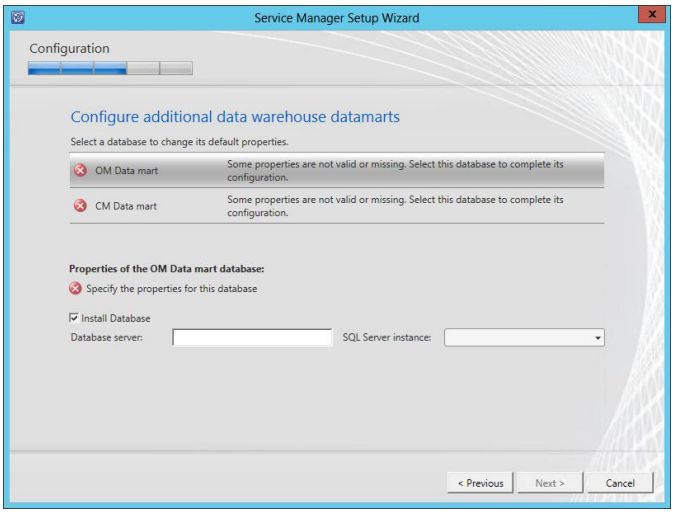
10. In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:
    a. **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.*
    b. **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse.*
    c. Select the **Create a new database** option and specify the following information in the provided text boxes:
    d. **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.*
    e. **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*
    f. **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.*
    g. **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*
11. Click **Data Mart** to continue.



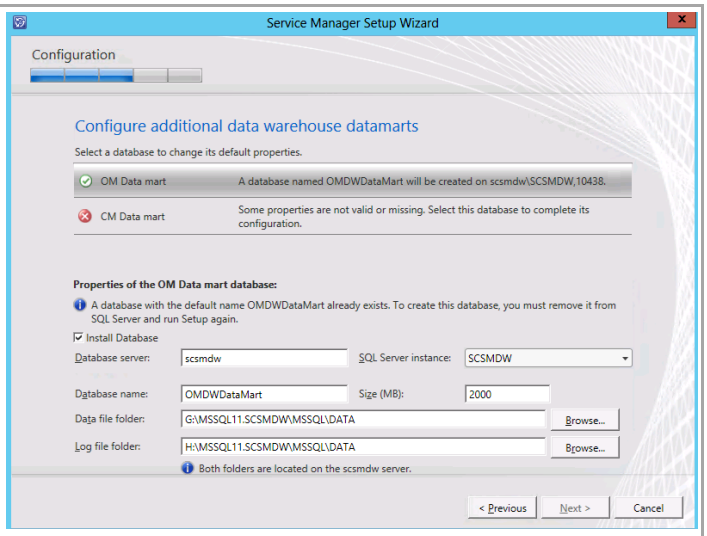
12. In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:
    a. **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).*
    b. **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).*
    c. Select the **Create a new database** option and specify the following information in the provided text boxes:
    d. **Database name** – *specify the name of the Service Manager Data Warehouse database. In most cases the default value of DWDataMart should be used.*
    e. **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*
    f. **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)*
    g. **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)*
13. Click **Next** to continue.



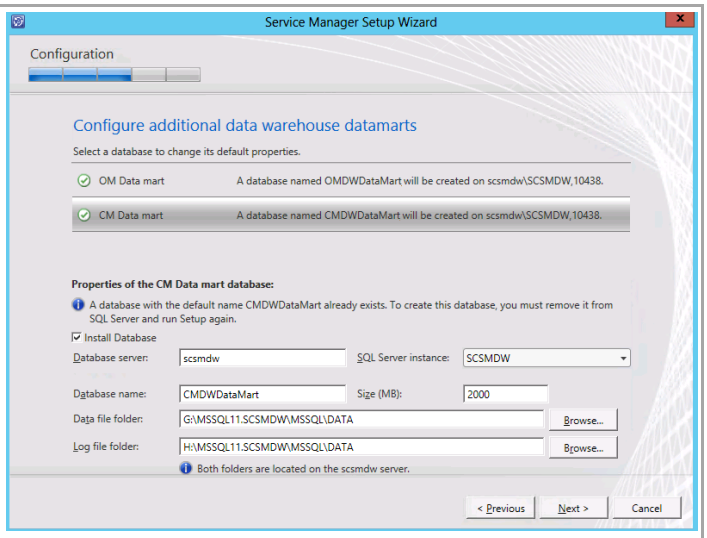
14. When the **Configure additional data warehouse datamarts** dialog launches, each subcategory will appear with an error message until each of the following sections are configured:
    a. OM Data mart.
    b. CM Data mart.



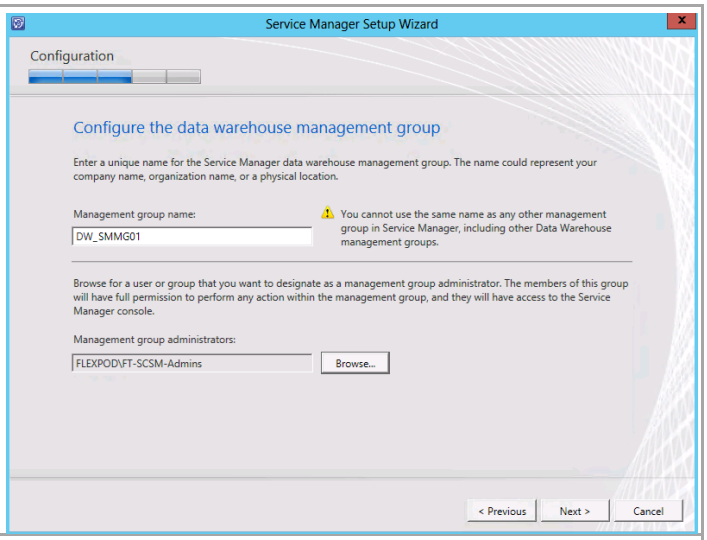
15. In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **OM Data Mart** section:
    a. **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*
    b. **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)*
    c. Select the **Create a new database** option and specify the following information in the provided text boxes:
    d. **Database name** – *specify the name of the Service Manager OM Data mart database. In most cases the default value of OMDWDataMart should be used.*
    e. **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*
    f. **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)*
    g. **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)*
16. Click **Next** to continue.



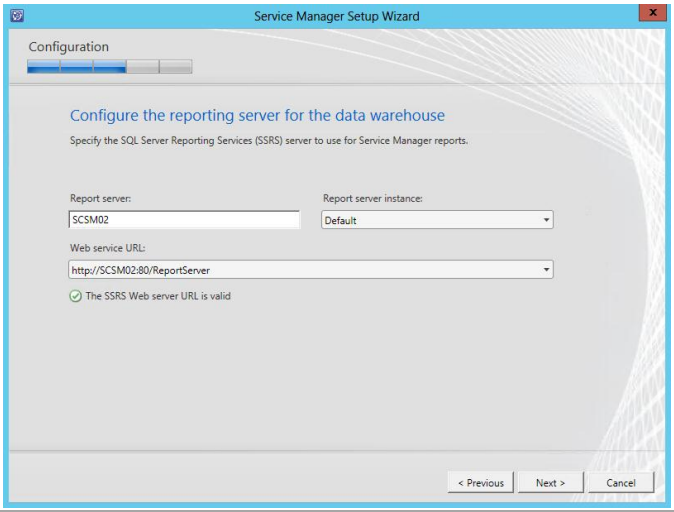
17. Optionally, a CM Data mart can be created for Configuration manager integration. To complete this, in the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **CM Data Mart** section:
    a. **Database server** – *specify 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)*
    b. **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)*
    c. Select the **Create a new database** option and specify the following information in the provided text boxes:
    d. **Database name** – *specify the name of the Service Manager CM Data mart database. In most cases the default value of CMDWDataMart should be used.*
    e. **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*
    f. **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)*
    g. **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)*
18. Click **Next** to continue.



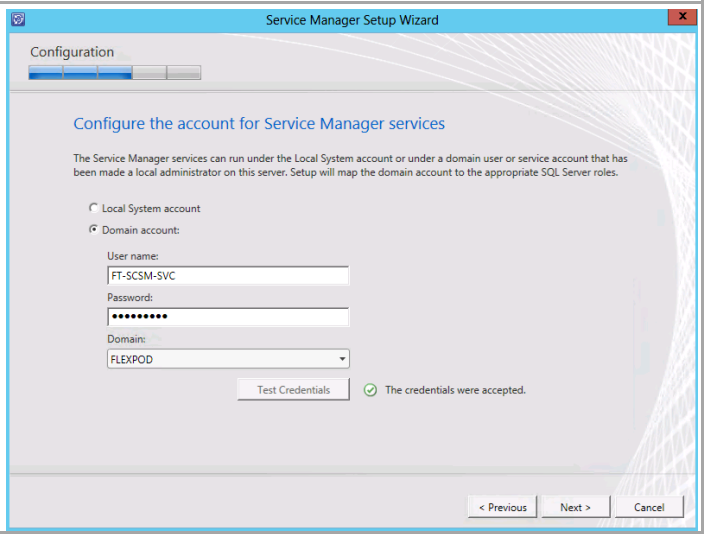
19. In the **Configure the data warehouse management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager management server and Service Manager Operations Manager installations.
20. Specify the SM Administrators group in the **Management group administrators** object picker section.
21. Click **Next** to continue.



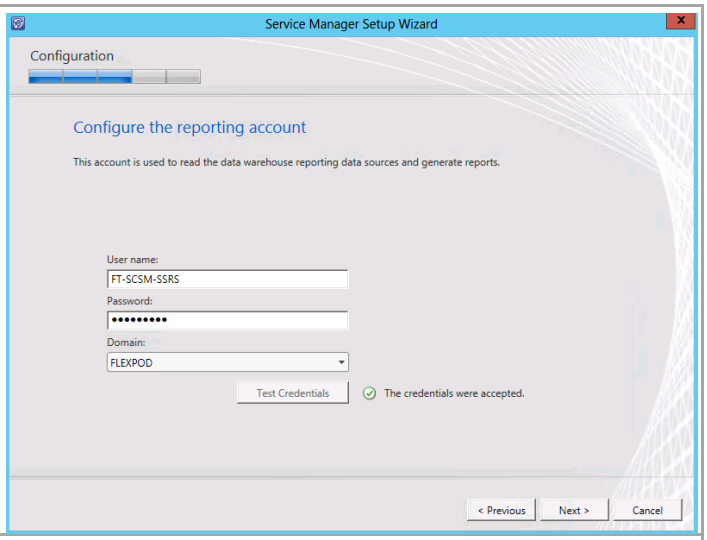
22. In the **Configure the reporting server for the data warehouse** dialog, specify the Data Warehouse server in the **Report server** text box.
23. In the **Report server instance** drop-down menu, select **Default**.
24. In the **Web service URL** drop-down menu, select the default reporting server URL.
25. Click **Next** to continue.



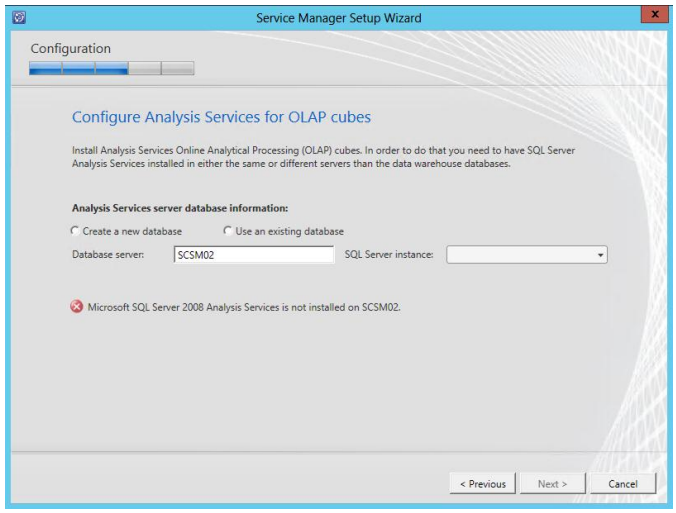
26. In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
27. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
28. When successful, click **Next** to continue.

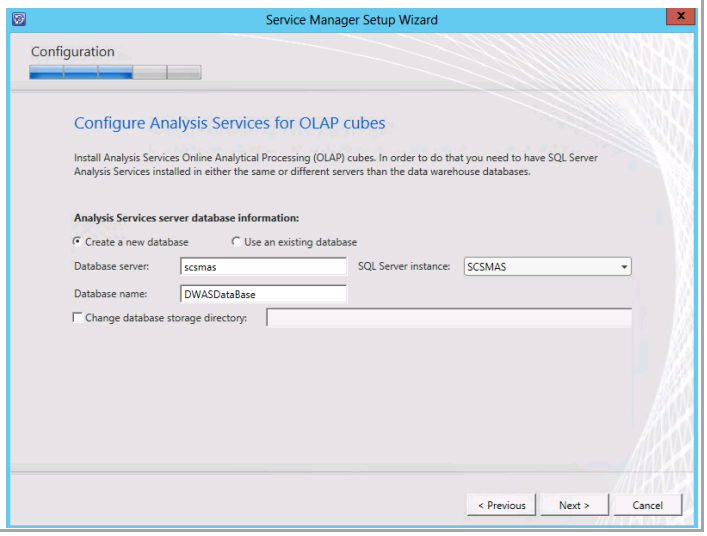


29. In the **Configure the reporting account** dialog, specify the SCSM SQL Server Reporting Services Account in the **User name** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
30. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
31. When successful, click **Next** to continue.

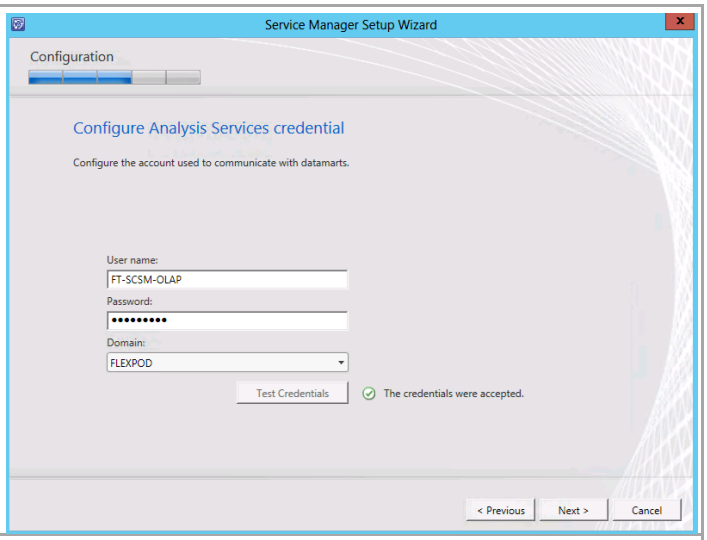


32. In the **Configure Analysis Services for OLAP cubes** dialog, select the **Create a new database** option and specify the following information in the provided text boxes:
    a. **Database server** – *specify the name of the SQL Server cluster CNO created for the Service Manager installation SQL Server Analysis Services.*
    b. **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation SQL Server Analysis Services.*
    c. **Database name** – *specify the name of the SQL Server Analysis Services database. In most cases the default value of DWASDataBase should be used.*
33. Confirm that the **Change database storage directory** check box is clear and click **Next** to continue.

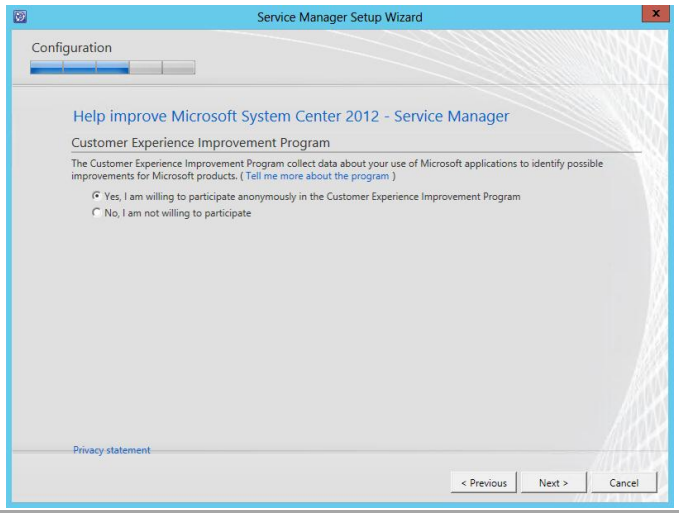




34. In the **Configure Analysis Services Credential** dialog, specify the SM OLAP Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
35. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
36. When successful, click **Next** to continue.

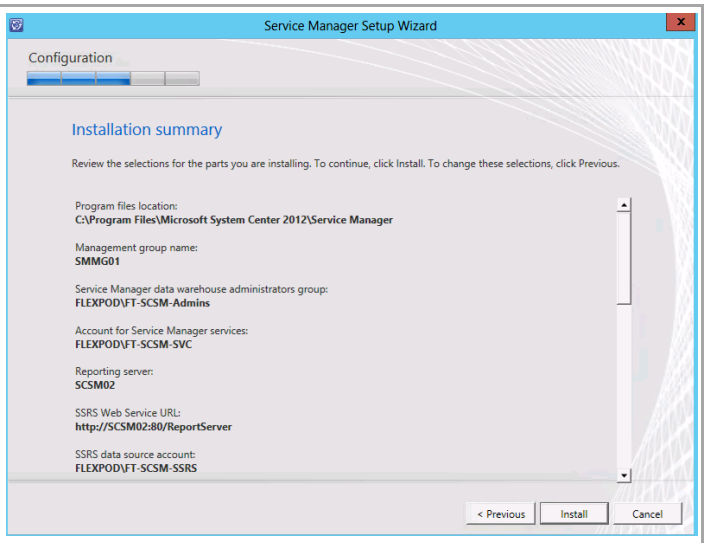


37. In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.

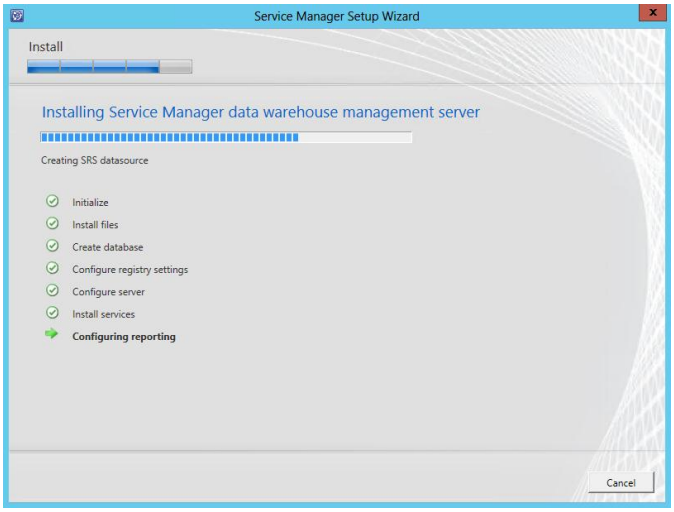


38. Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.

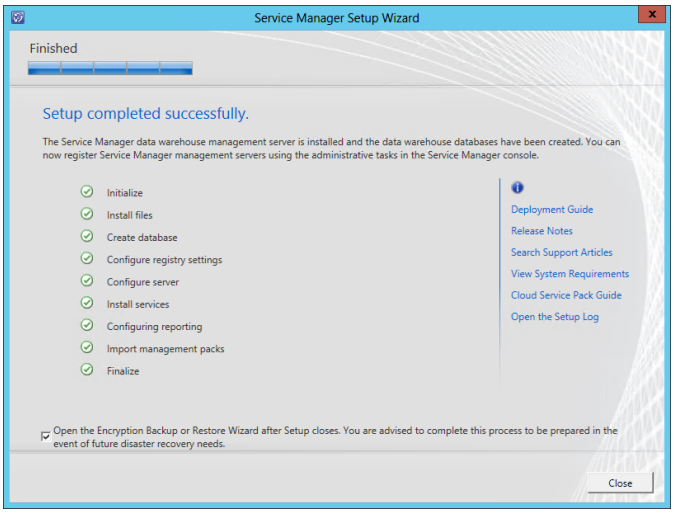
39. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

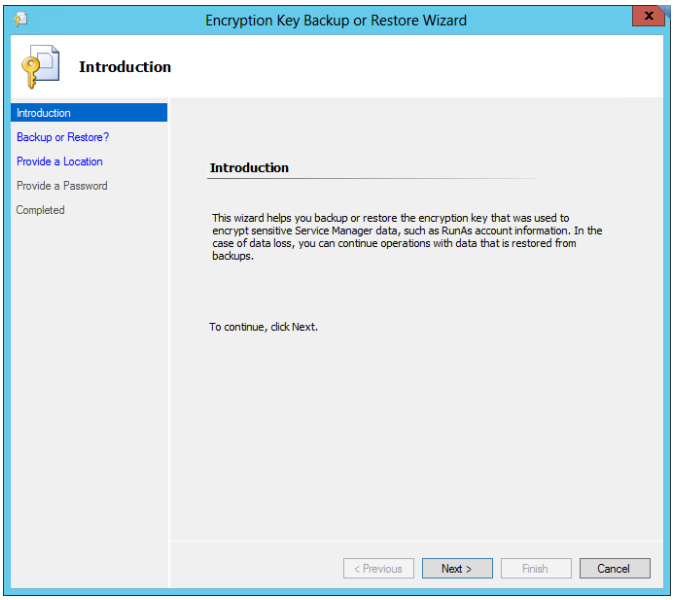
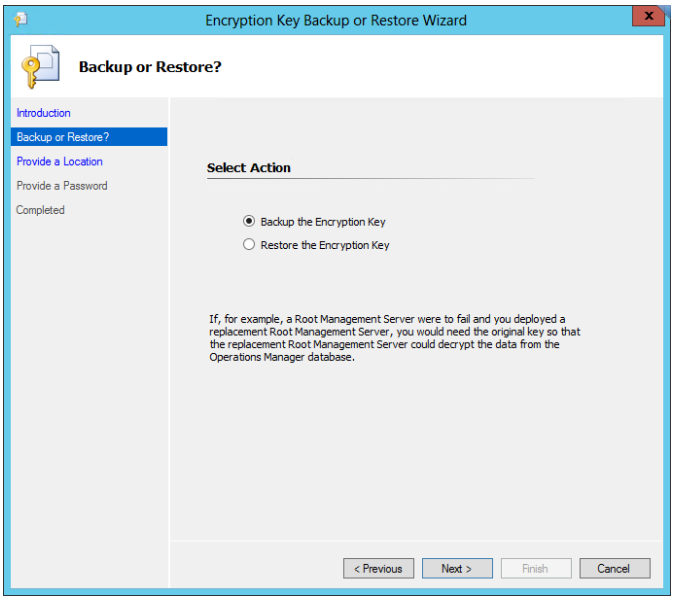


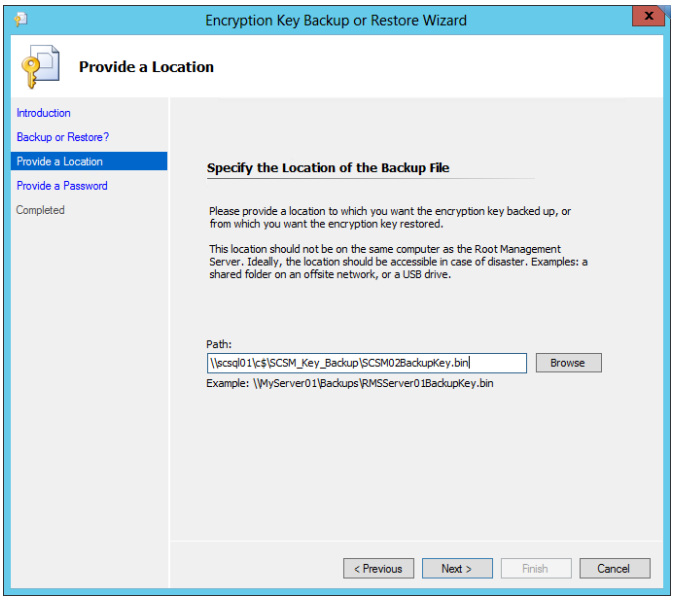
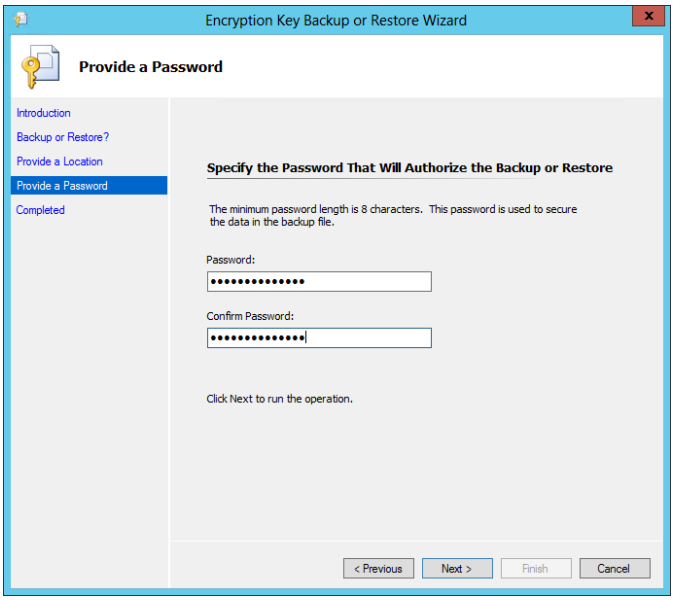
40. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.
41. The wizard will display the progress while installing features.



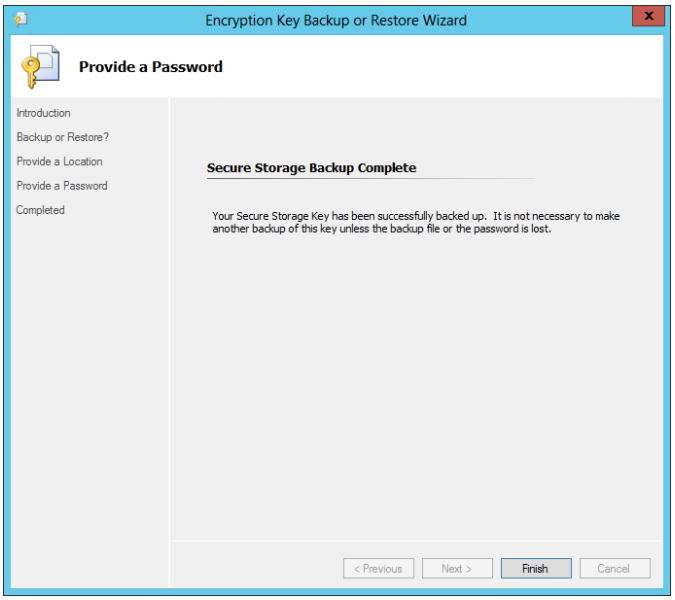
42. When the installation completes, the wizard will display the **Setup completed successfully** dialog.
43. Make sure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to launch the wizard after setup.
44. Click **Close** to complete the installation.



45. When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.	
46. In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.	

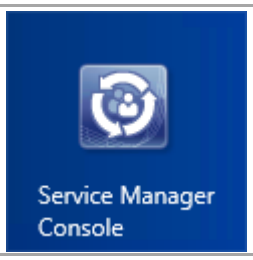
47. In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** text box and object picker. Click **Next** to continue.	
48. In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.	

49. When complete, click **Finish** to exit the wizard.



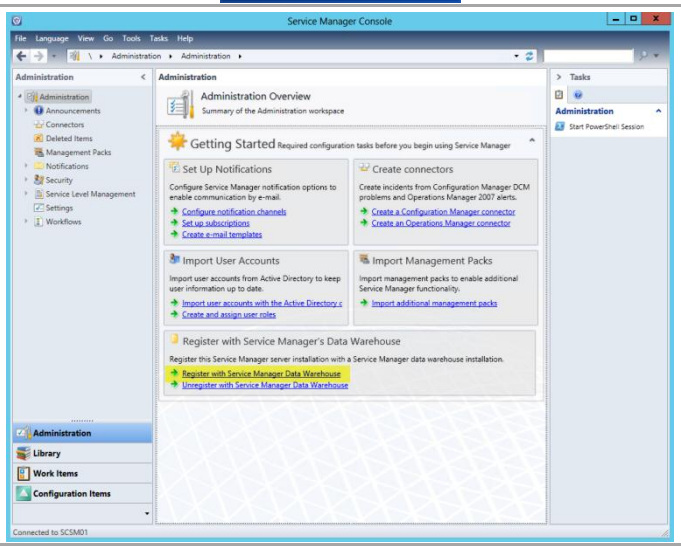
▶ Perform the following steps on the **Service Manager management server** (SCSM01) virtual machine to register the Service Manager Data Warehouse and enable reporting in the Service Manager instance.

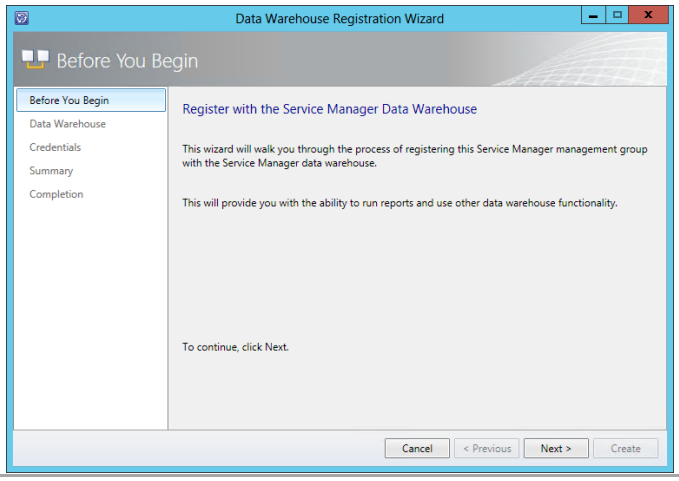
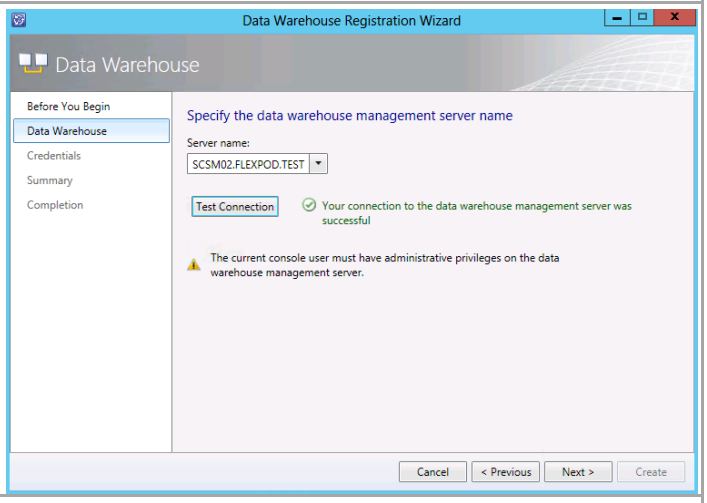
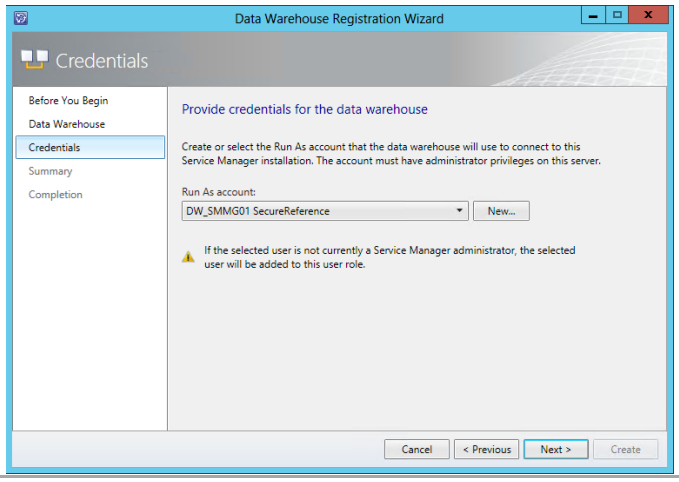
1. Logon to the Service Manager management server using an account with administrator permissions. From the Windows **Start** screen, select the **Service Manager Console** tile.

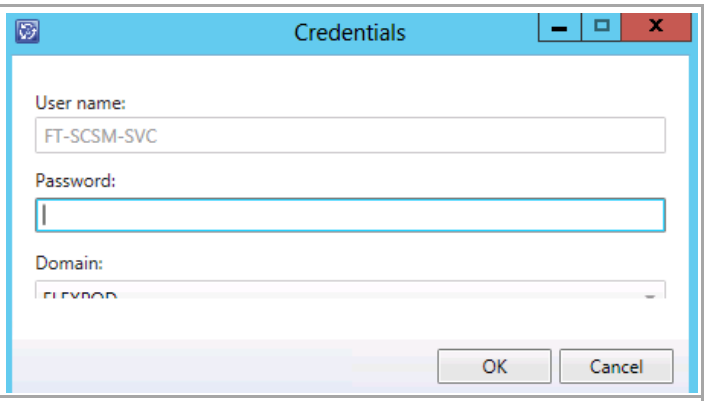
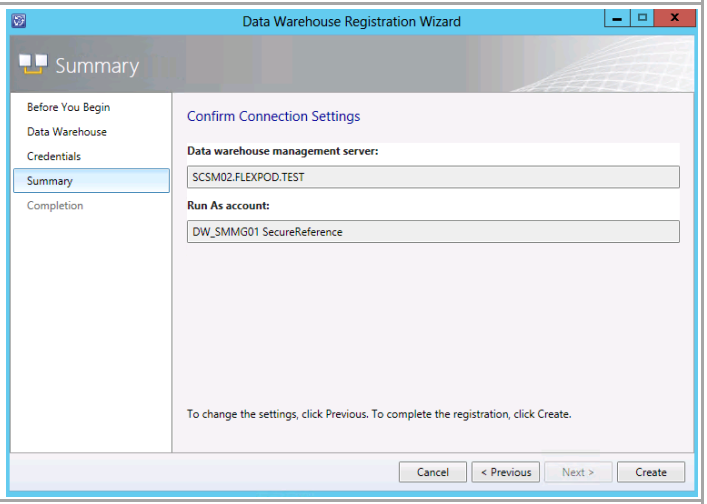
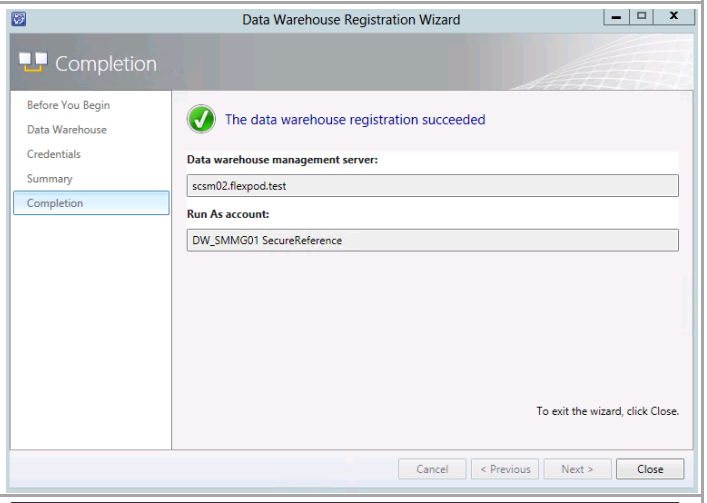
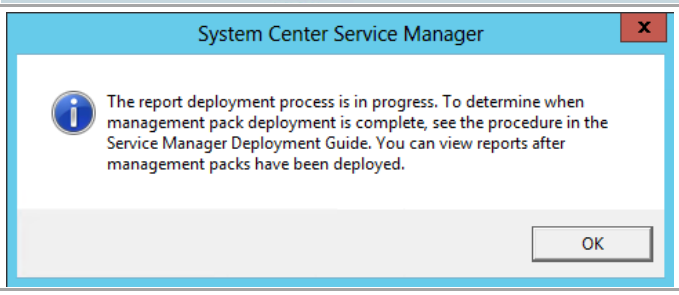


2. Within the **Service Manager Console**, select the **Administration** node and navigate to the **Register with Service Manager's Data Warehouse** section. Click the **Register with Service manager Data Warehouse** link to enable reporting.

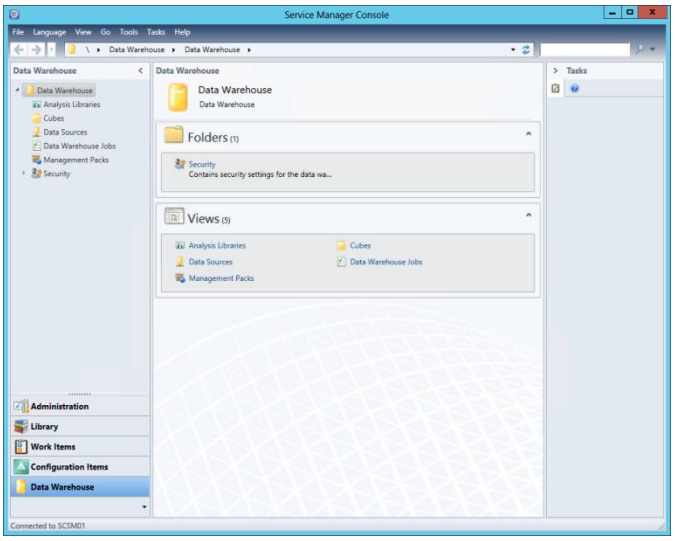
Note: if the console was open from the previous installation, close it and re-open the console.



3. The **Data Warehouse Registration Wizard** will launch. Click **Next** to begin registration.	
4. 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.1fLEXpOD1	
5. 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.	

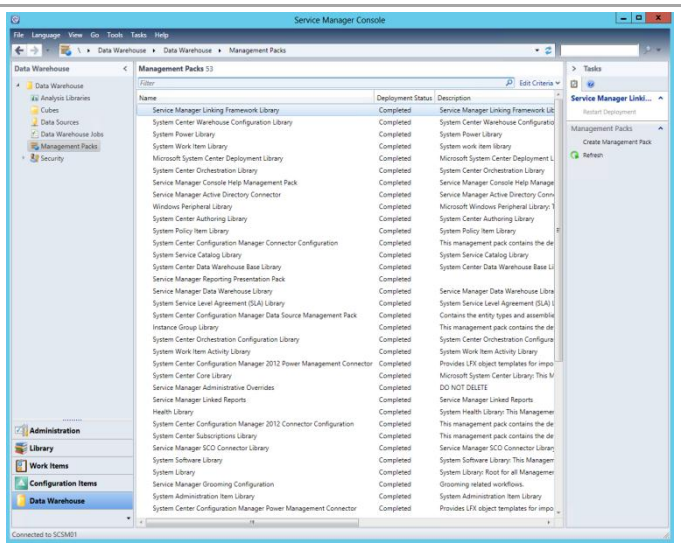
6. A **Credentials** dialog will appear and prompt you for the password for the SM service account. When provided, click **OK** to continue.	
7. The **Summary** dialog will appear. Review the information that was provided earlier and click **Create** to begin the registration process.	
8. The **Completion** 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.	

9. After a few minutes the **Data Warehouse** button will be added to the **Service Manager Console**.



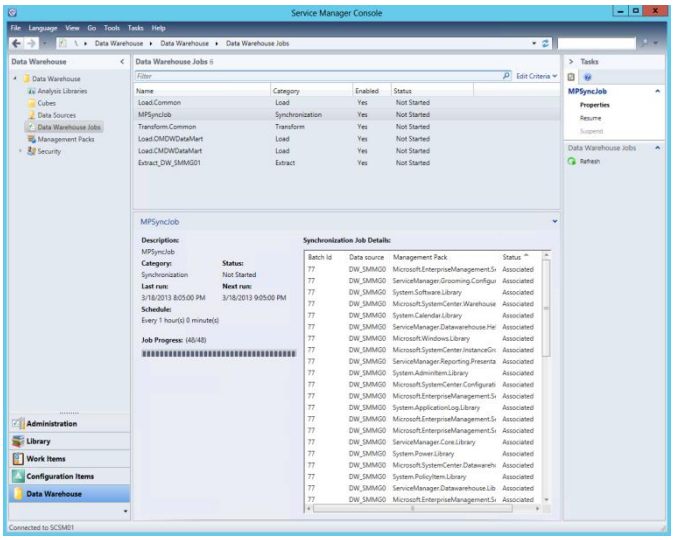
Note: this deployment and association process can take up to two hours to complete.

10. The status of the management pack imports can be checked by selecting **Management Packs** in the **Data Warehouse** pane.
11. 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.

12. In the **Data Warehouse** pane, select **Data Warehouse Jobs**.
13. In the **Data Warehouse Jobs** pane, click **MPSyncJob**.
14. 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.
15. 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.

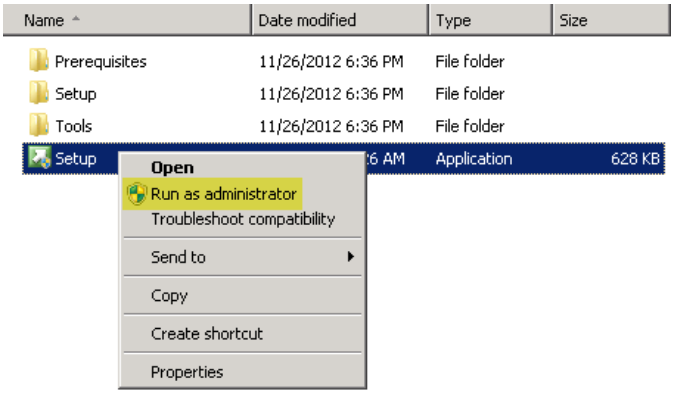


Install the Service Manager Self-Service Portal Server

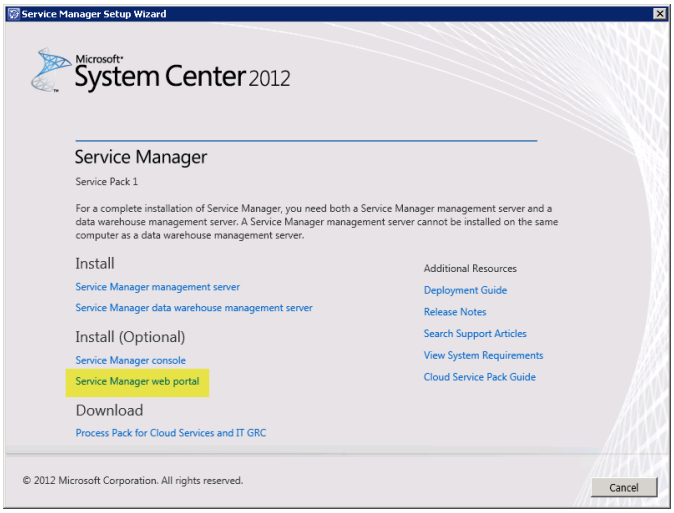
The following steps must to be completed in order to install the Service Manager self-service portal server role.

▶ Perform the following steps on the **System Center Service Manager self-service portal** (SCSM03) virtual machine.

1. Log on to Service Manager self-service portal server (**NOT** the Service Manager management server or the Data Warehouse server).
2. From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

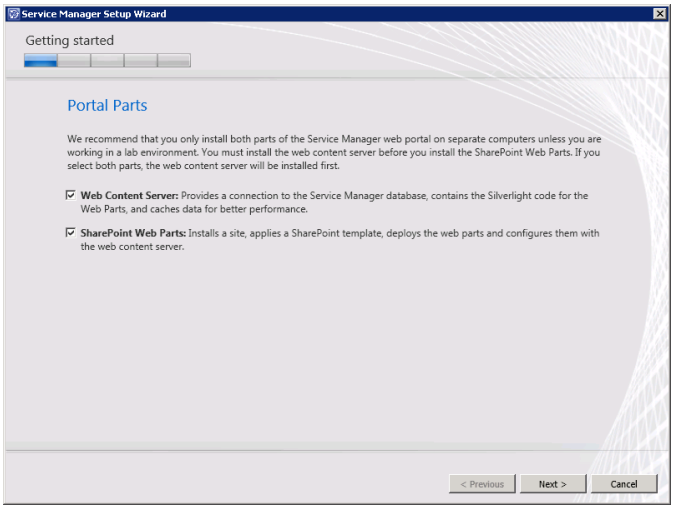


3. The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager web portal** to begin the Service Manager self-service portal server installation.

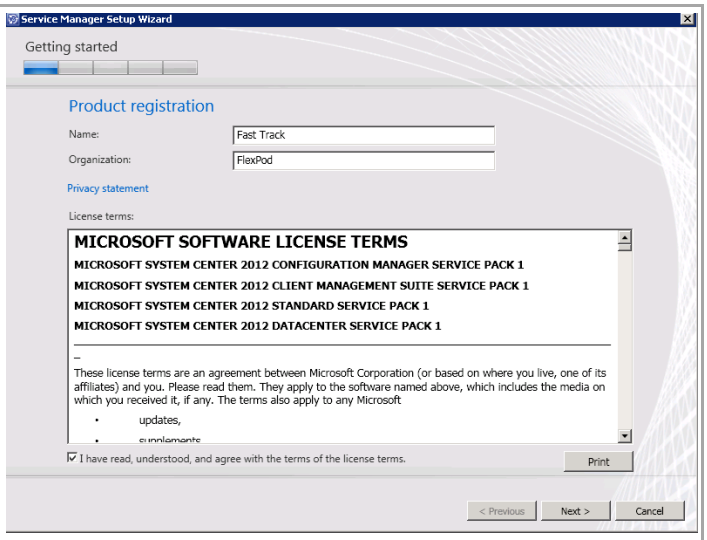


4. The **Service Manager Setup Wizard** will open. In the **Portal Parts** dialog, select the **Web Content Server** and **SharePoint Web Parts** check boxes and click **Next** to continue.

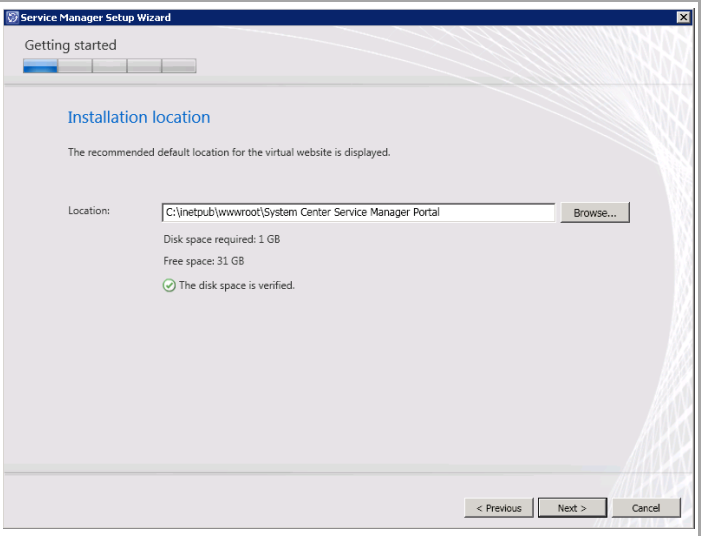
Note: The warning about installing both Portal Parts on a single server can be safely ignored. The setup wizard assumes that the SharePoint Farm is using a local SQL Server installation whereas the Fast Track design uses a dedicated SQL Server instance for the SharePoint farm drastically reducing the load on the SharePoint Web Parts installation.



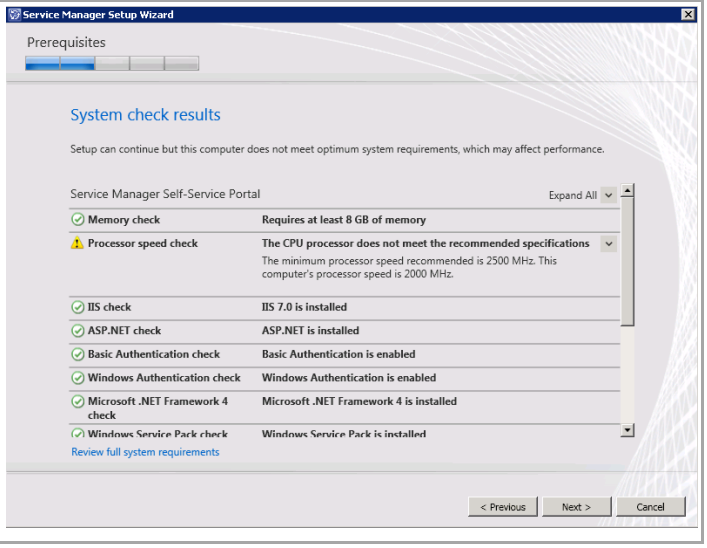
5. In the **Product registration** dialog, provide the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** – *specify the name of the licensed organization.*
6. In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** checkbox. When all selections are confirmed, click **Next** to continue.



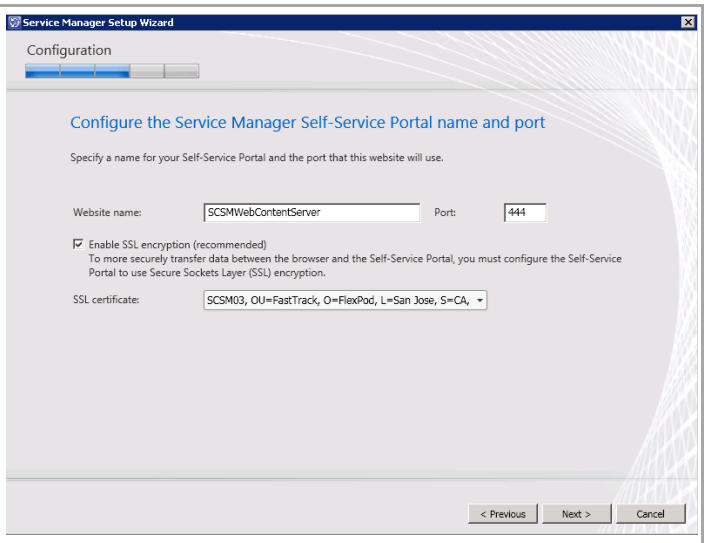
7. In the **Installation location** dialog, specify a location or accept the default location of *C:\inetpub\wwwroot\System Center Service Manager Portal* for the installation. Click **Next** to continue.



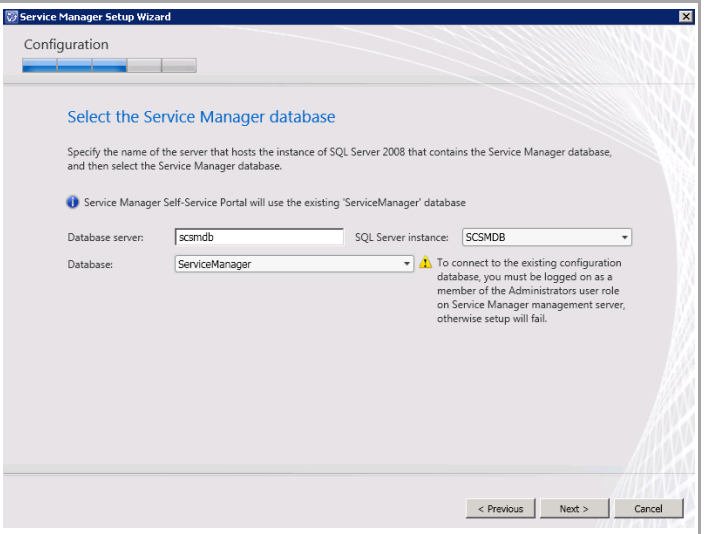
8. The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



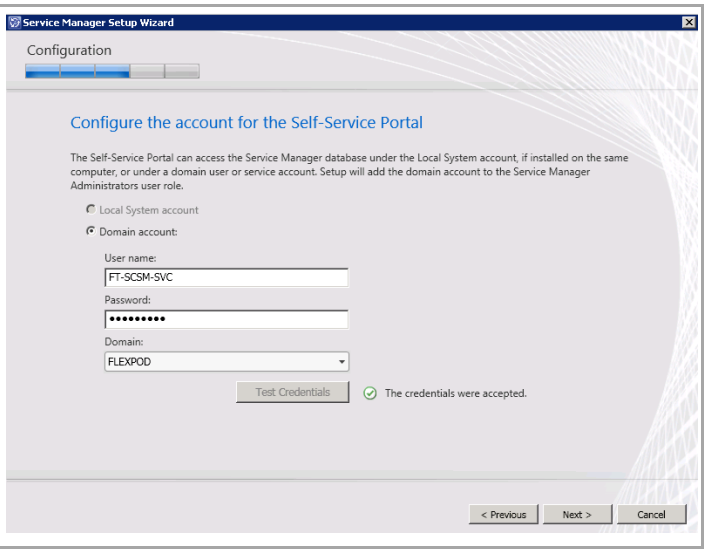
9. In the **Configure the Service Manager Self-Service Portal name and port** dialog, specify the following information in the provided text boxes:
    a. **Website name** – *specify the name of the website used for the self-service portal. In most cases, the default name of SCSMWebContentServer should be used.*
    b. **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**.*
10. 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.
11. Click **Next** to continue.



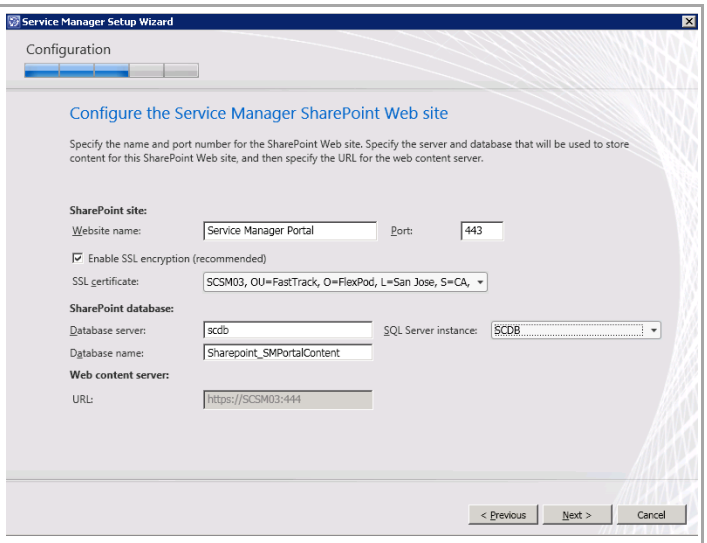
12. In the **Select the Service Manager database** dialog, specify the following information in the provided text boxes:
    a. **Database server** – *specify the name of the SQL Server cluster CNO created for the Service Manager management server.*
    b. **SQL Server instance** – *specify the SQL Server database instance created for the Service Manager management server (SCSMDB).*
    c. **Database** – *specify the name of the Service Manager database configured earlier. In most cases the default value of ServiceManager should be used.*
13. Click **Next** to continue.

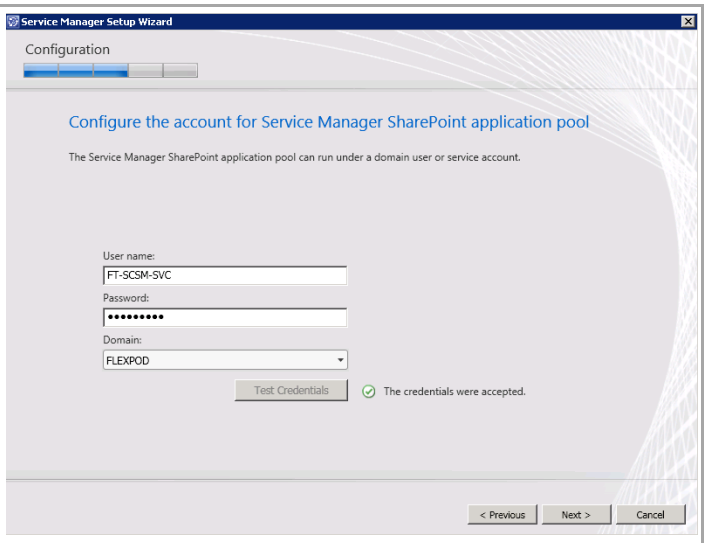
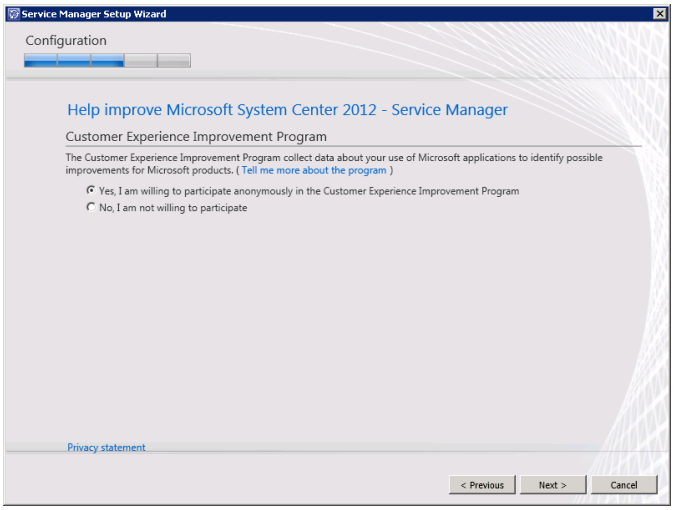


14. In the **Configure the account for the Self-Service Portal** dialog, verify that the **Domain account** option is selected and specify the SM Service Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
15. Before proceeding, click the **Test Credentials** button to verify the credentials provided.
16. When successful, click **Next** to continue.

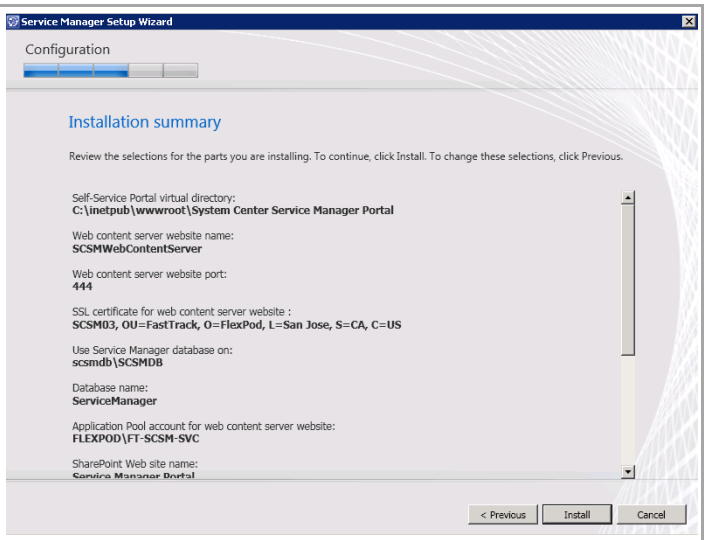


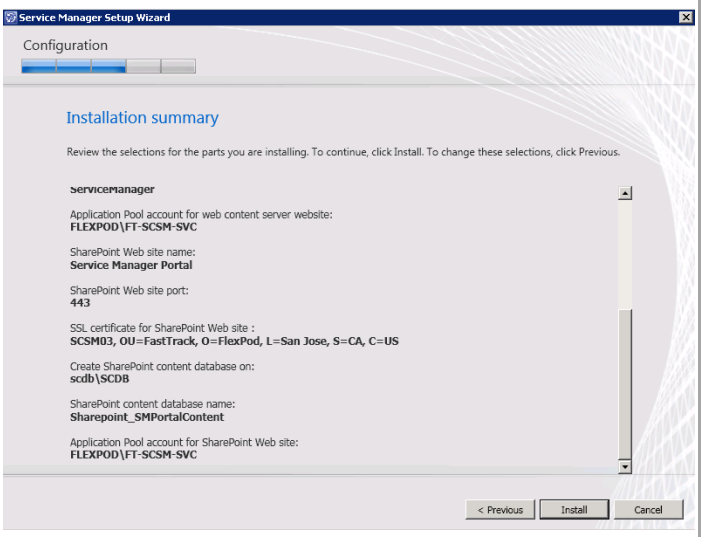
17. In the **Configure the Service Manager SharePoint Web site** dialog, provide the following information:
18. In the **SharePoint site** section, specify the following information in the provided text boxes:
    a. **Website name** – *specify the name of the website used for the self-service portal. In most cases, the default name of Service Manager Portal should be used.*
    b. **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.*
19. 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.
20. In the SharePoint database section, specify the following information in the provided text boxes:
    a. **Database server** – *specify the name of the SQL Server cluster network name created for the Service Manager installation SharePoint Farm (SCDB).*
    b. **SQL Server instance** – *specify the SQL Server database instance created for the Service Manager installation SharePoint Farm (SCDB).*
    c. **Database server** – *specify the database name for the portal. In most cases, the default value of SharePoint_SMPortalContent will be used.*
21. Click **Next** to continue.



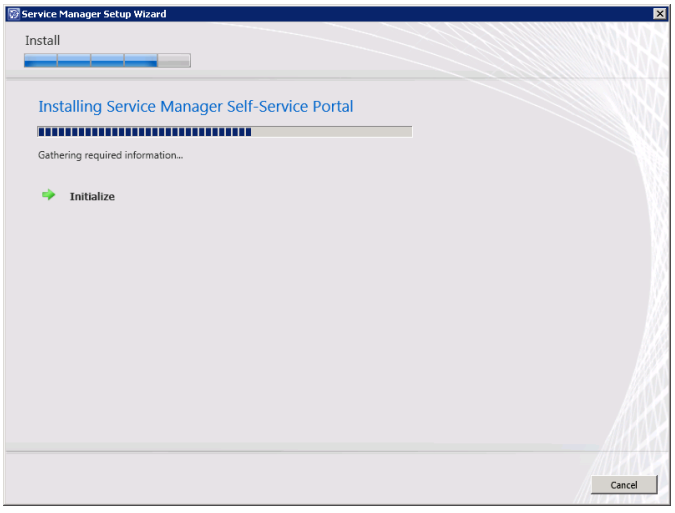
22. In the **Configure the account for Service Manager SharePoint application pool** dialog, specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. 23. Before proceeding, click the **Test Credentials** button to verify the credentials provided. 24. When successful, click **Next** to continue.	
25. 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.	
26. 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.	

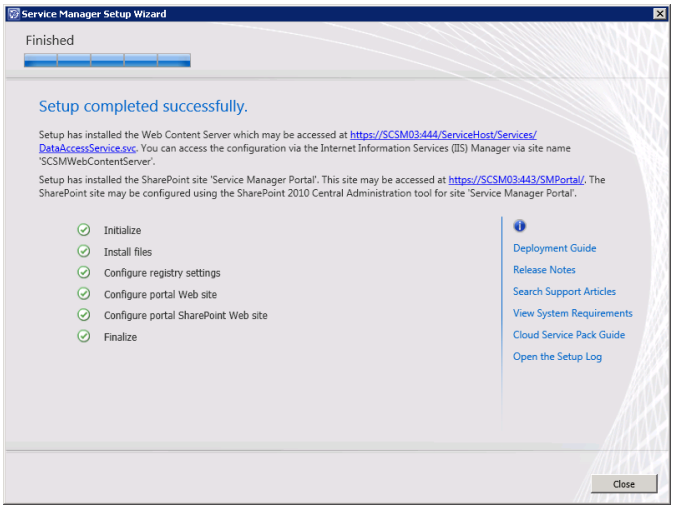
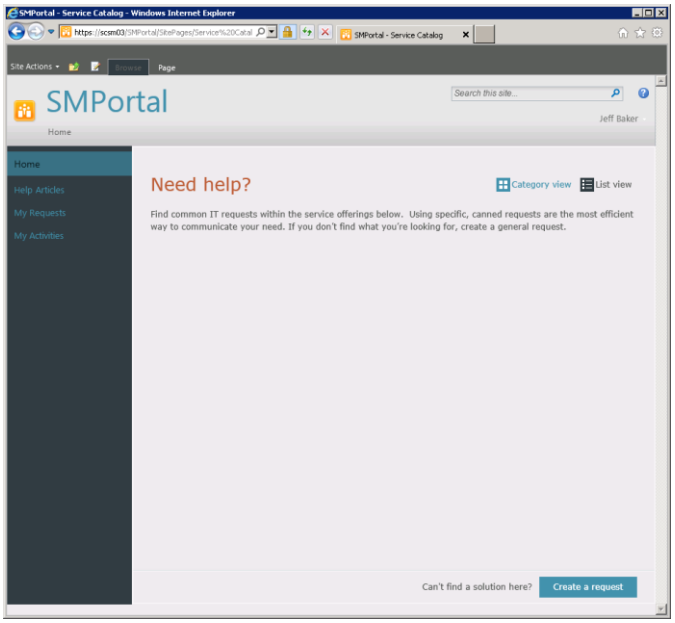
27. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.





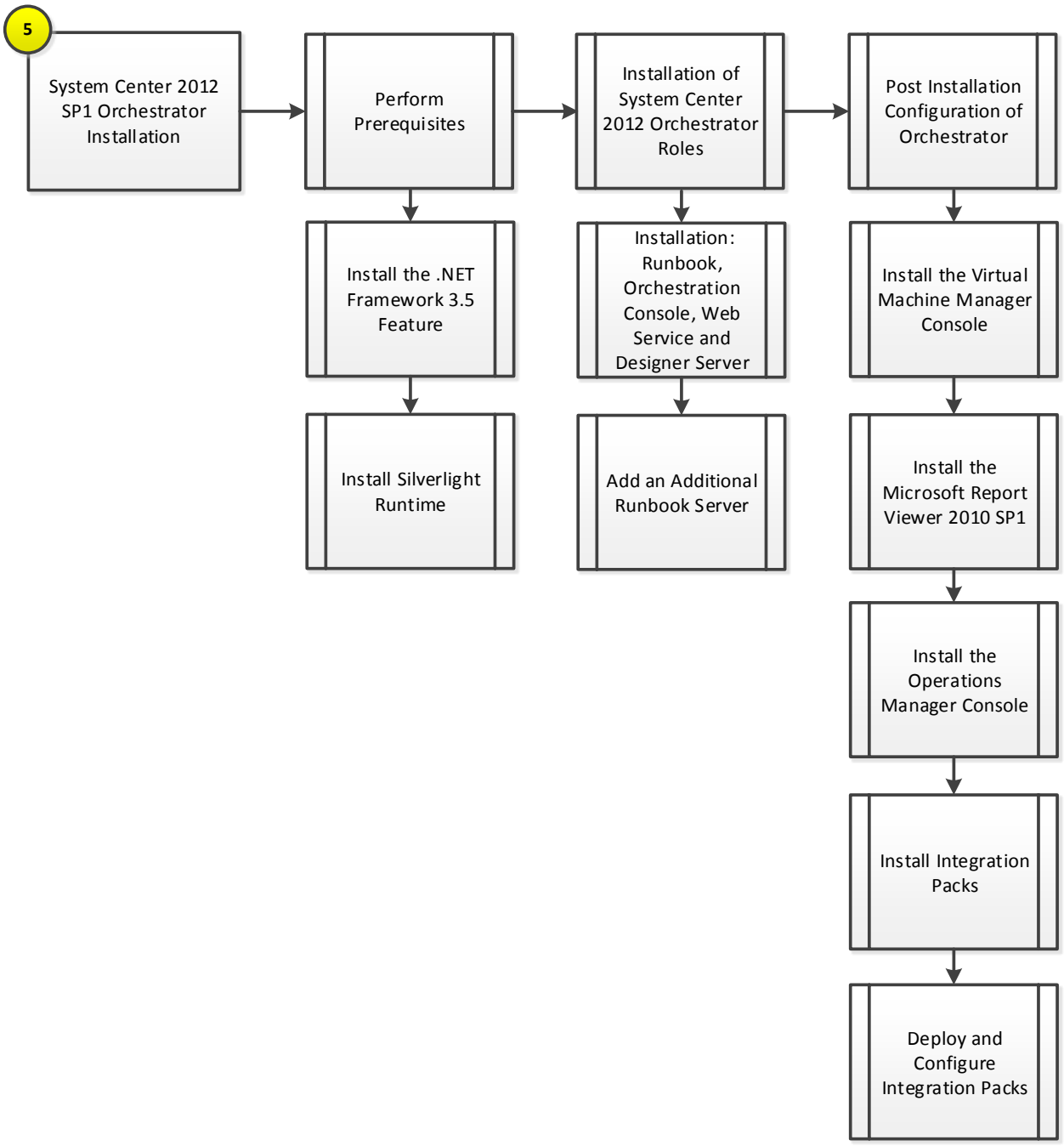
28. The wizard will display the progress while installing features.



29. When completed, the **Service Manger Setup Wizard** will display the **Setup completed successfully** dialog. Click **Close** to finish the installation. **Note**: The SMPortal link is provided in the dialog.	
30. From Microsoft Internet Explorer®, open the Service Manager self-service portal at https://<servername>/SMPortal. 31. Verify that the page loads completely and that all sections display as expected.	

20 Orchestrator

The Orchestrator installation process includes the following high-level steps:



20.1 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.

20.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security accounts have been created:

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 • Log on As a Service rights (User Rights) • *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-VMM-Admins

Groups

Verify that the following security groups have been created:

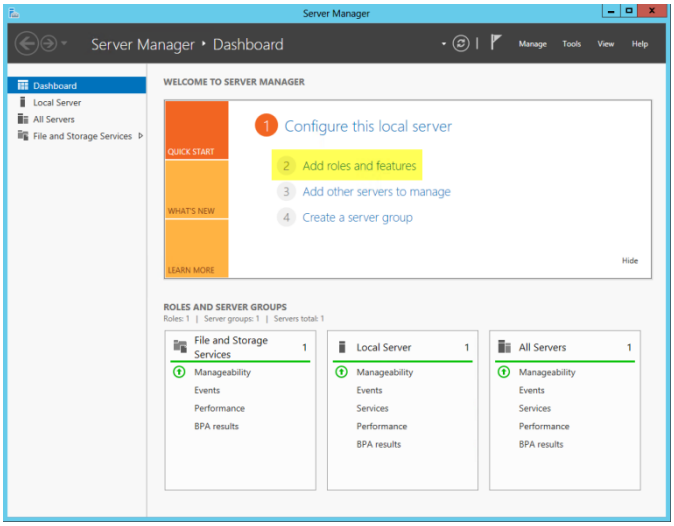
Security group name	Group scope	Members	Member of
<DOMAIN>\FT-SCO-Operators	Global		
<DOMAIN>\FT-SCO-Admins	Global	<DOMAIN>\FT-SCO-SVC	Local Administrators Target Active Directory domain BUILTIN\Distributed COM Users

Add the .NET Framework 3.5 Feature

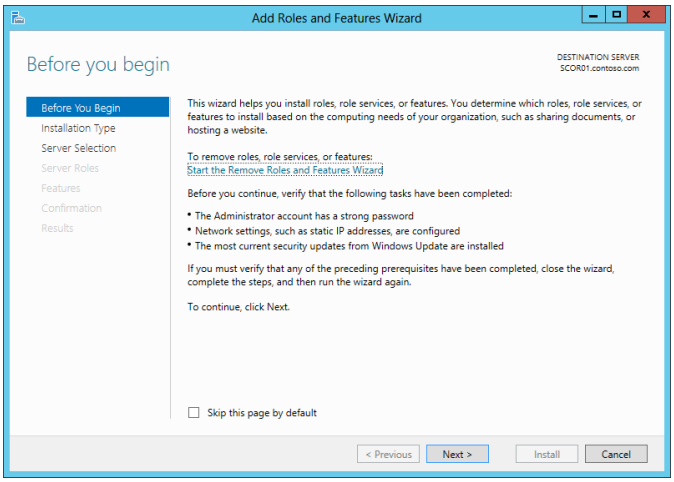
The Orchestrator installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5 Feature.

▶ Perform the following steps on all **Operations Manager** virtual machines.

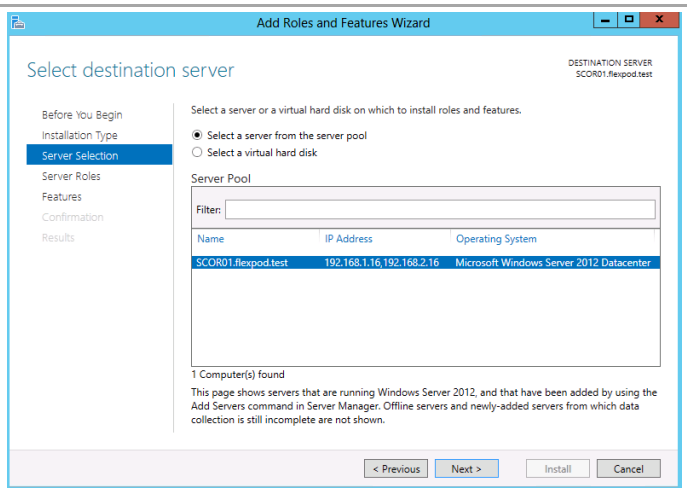
1. Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



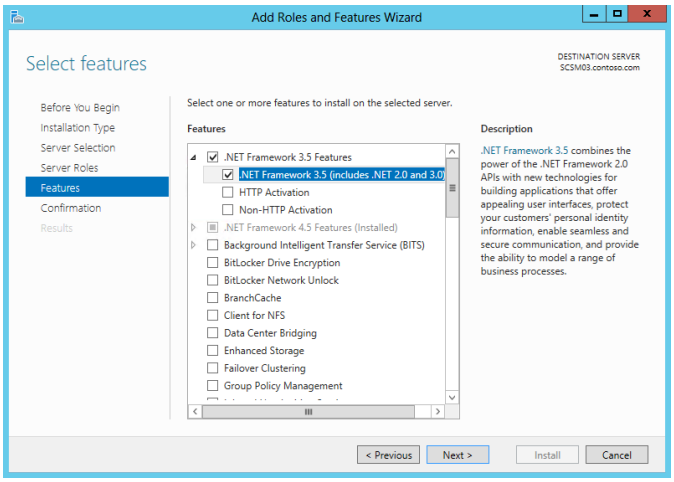
2. The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



3. 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.



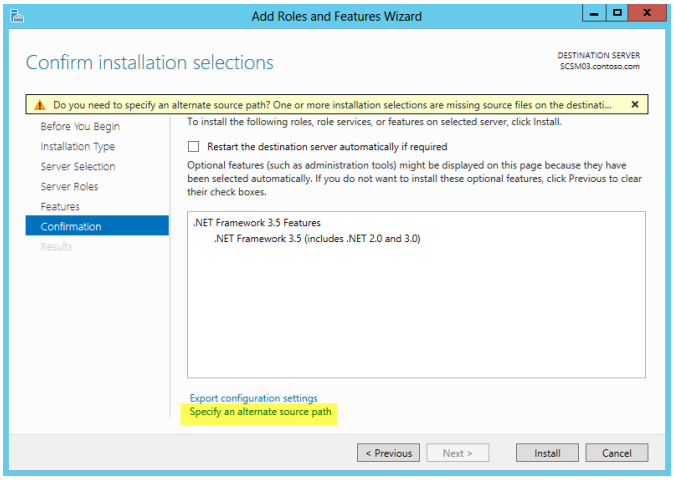
4. To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



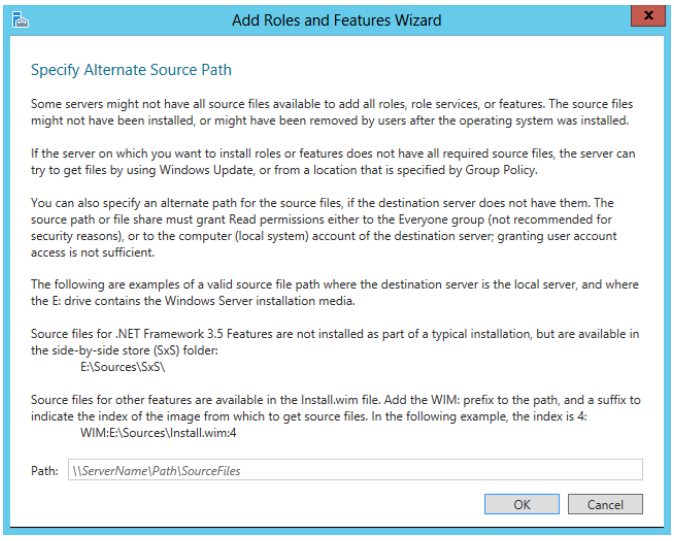
5. In the **Confirm installation selections** dialog verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

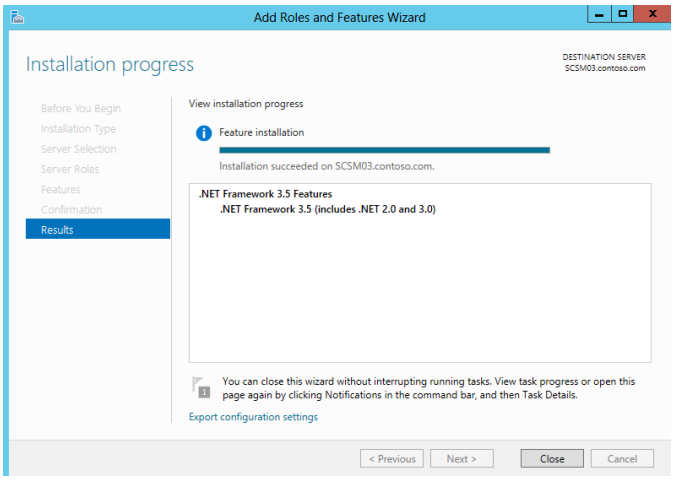
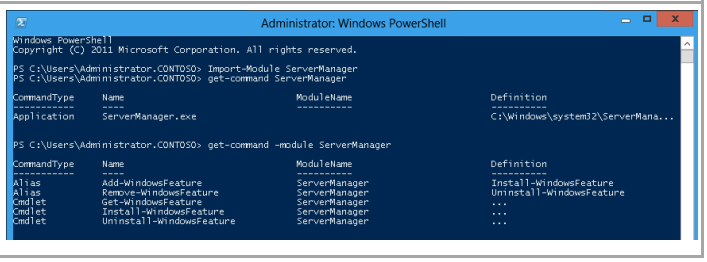
Note: The Export Configuration Settings option is available as a link on this dialog to export the options selected to XML. When exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features.

Also, if the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.



6. For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location must be specified for the installation.

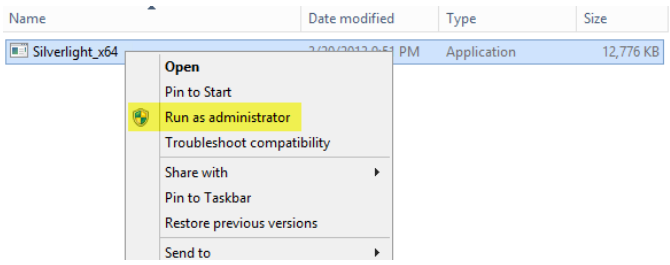


7. The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.	
Note: While the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.	

Install the Silverlight Runtime

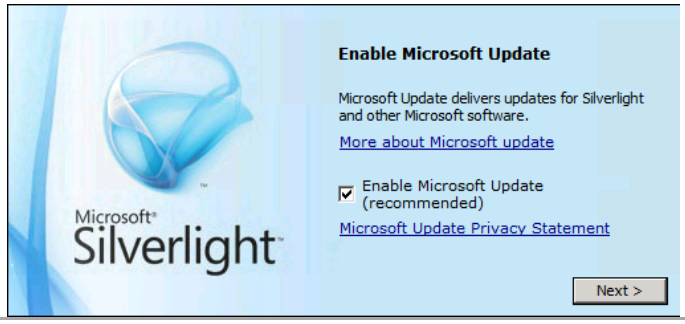
▶ Perform the following steps on the **Orchestrator** virtual machine.

1. From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.

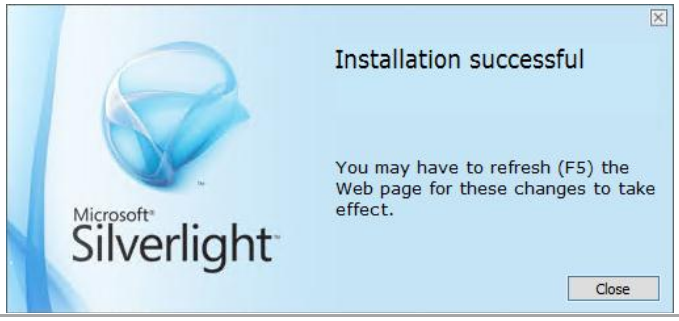


2. In the **Install Silverlight** dialog, click **Install now**.

3. In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.



4. In the **Installation Successful** dialog, click **Close** to exit the installation.



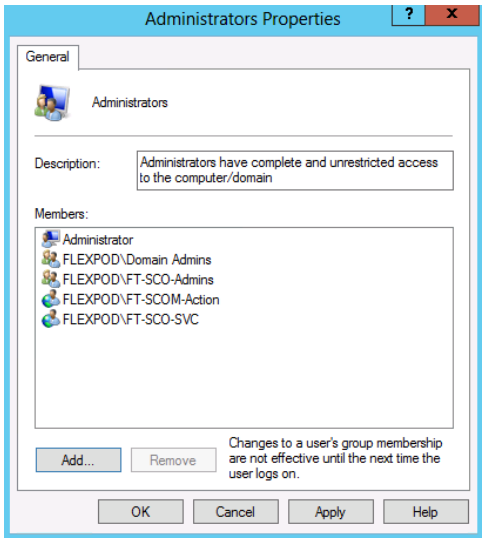
20.3 Installation

Install the Orchestrator Runbook, Web Service and Designer Server

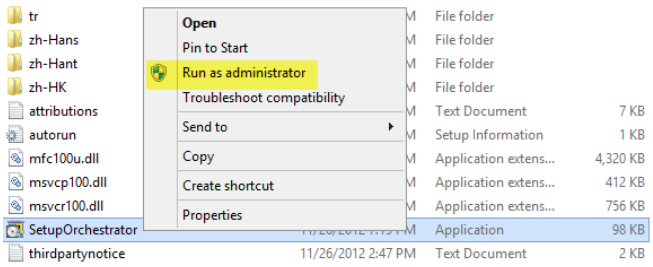
The following steps needs to be completed in order to install the Orchestrator Runbook Server component.

▶ Perform the following steps on the **Orchestrator** virtual machine.

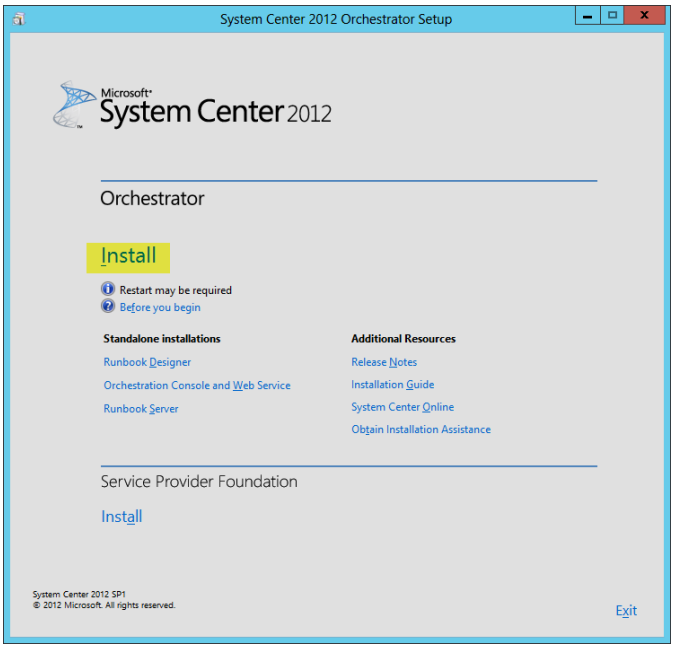
1. Log on to the Orchestrator virtual machine with a user with local admin rights.
2. Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:
    a. Orchestrator service account.
    b. Orchestrator Admins group.
    c. Operations Manager action account.



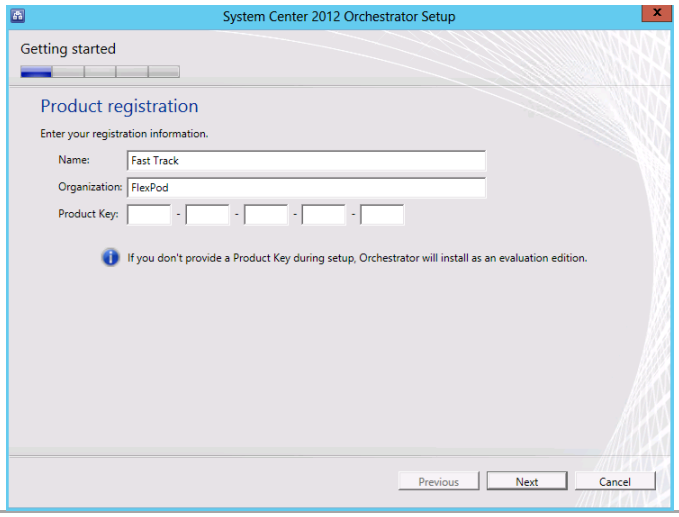
3. Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



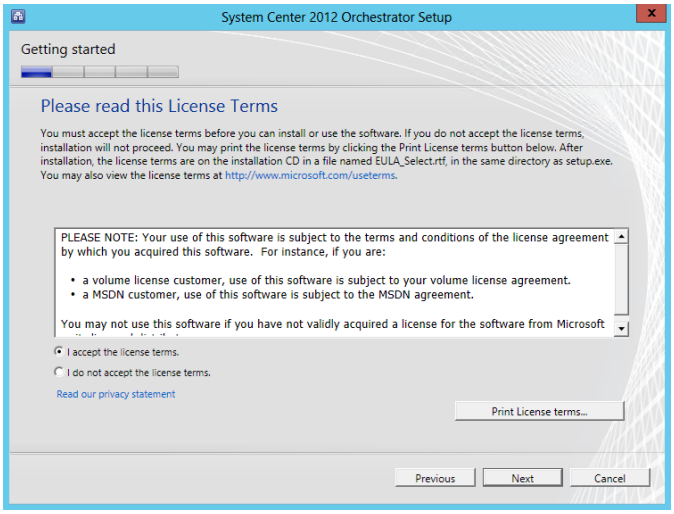
4. The Orchestrator installation wizard will begin. At the splash page, click **Install** to begin the Orchestrator server installation.



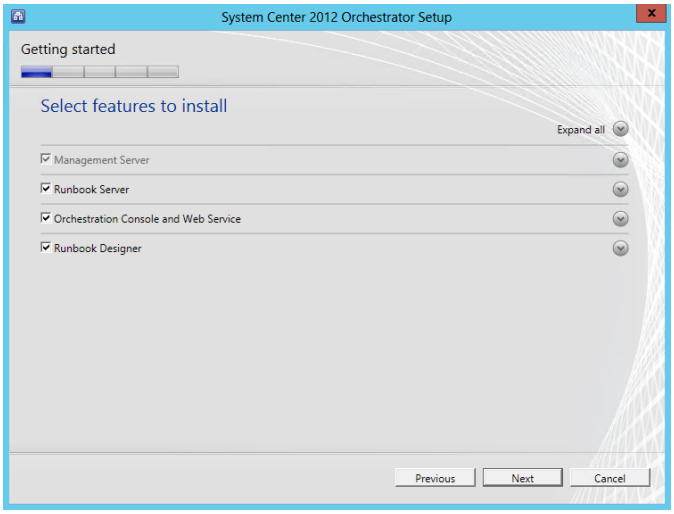
5. In the **Product registration information** dialog, provide the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** – *specify the name of the licensed organization.*
    c. **Product Key** – *provide a valid product key for installation of Orchestrator. If no key is provided, Orchestrator will be installed in evaluation mode.*
6. Click **Next** to continue.



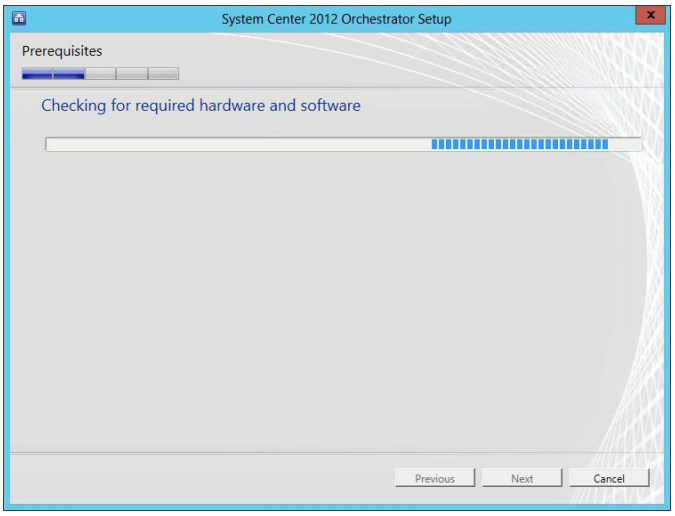
7. In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option checkbox is selected and click **Next** to continue.



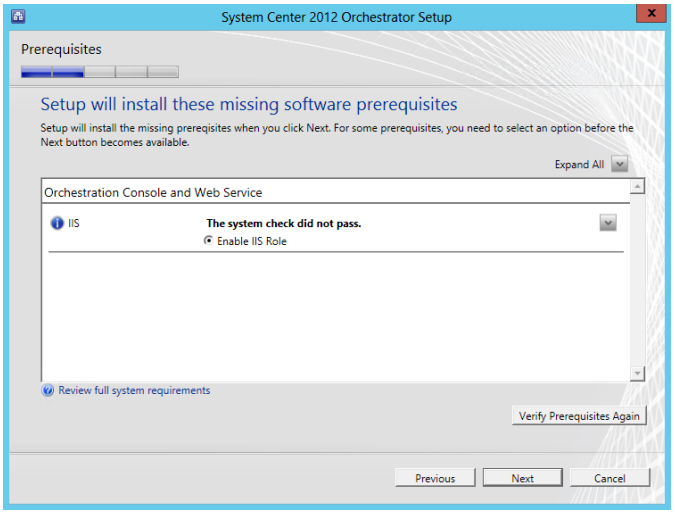
8. In the **Select Features to install** dialog, select the **Management Server** (default selected), **Runbook server**, **Orchestration console and web service**, **Runbook Designer** checkboxes and click **Next** to continue.

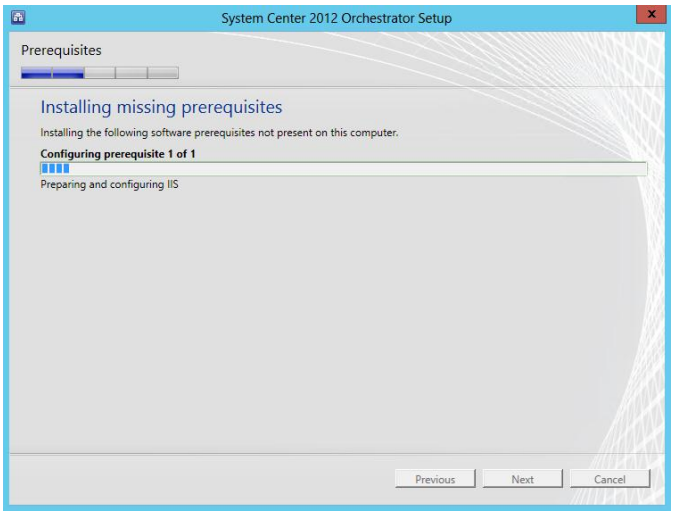


9. The **Checking for required hardware and software** dialog will appear to verify the installation prerequisites. When validation completes, click **Next** to continue.

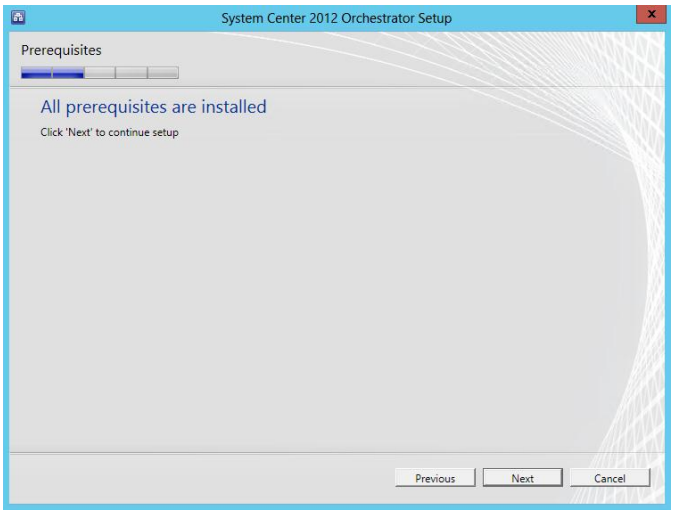


10. The Orchestrator setup will identify any prerequisite software required for the installation to complete. The **Setup will install these missing software prerequisites** dialog will attempt to perform the installation of missing prerequisites. When completed, click **Next** to continue.

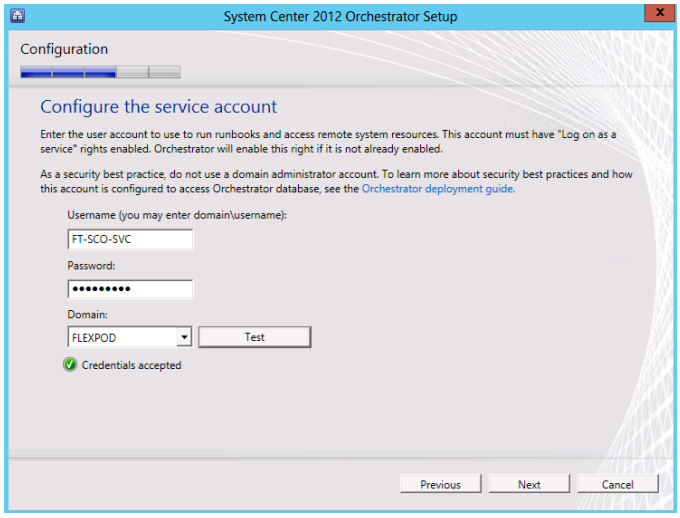




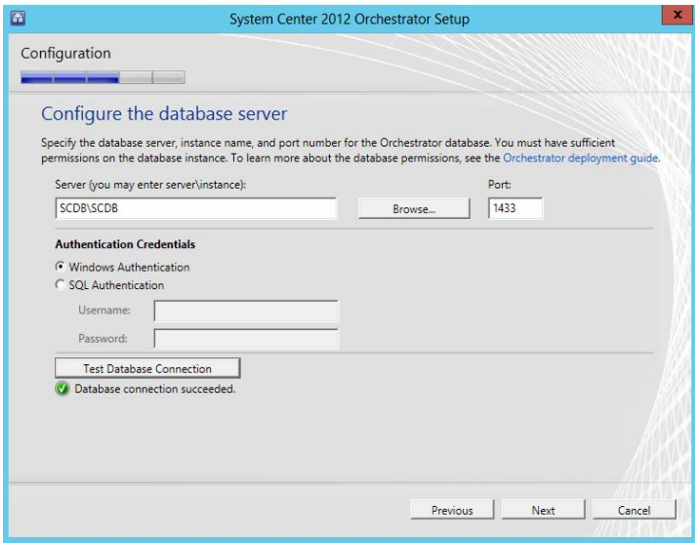
11. When the installation of the missing prerequisites is completed, click **Next** to continue.



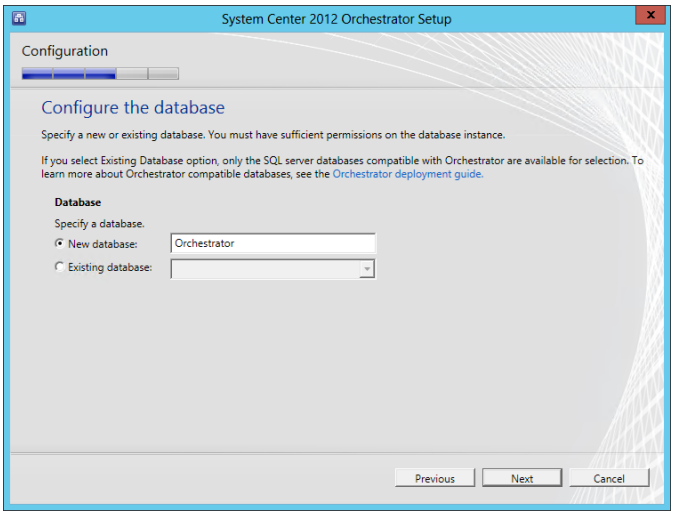
12. In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
13. Before proceeding, click the **Test** button to verify the credentials provided.
14. When successful, click **Next** to continue.



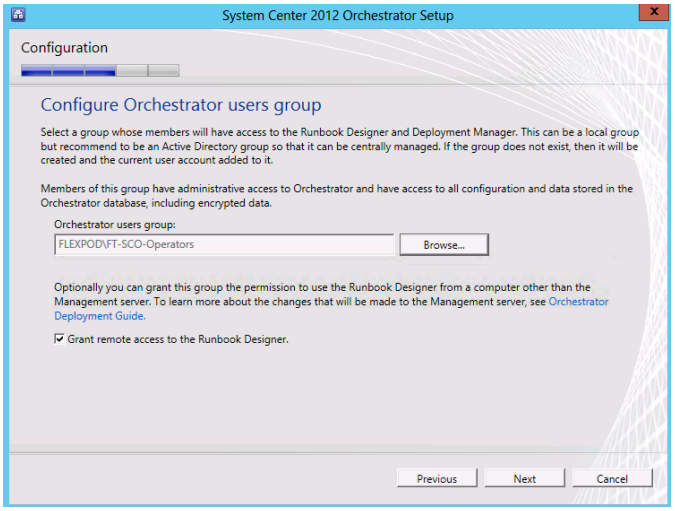
15. In the **Configure the database server** dialog, enter the following information in the provided text boxes:
    a. **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
    b. **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*
16. In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.
17. When successful, click **Next** to continue.



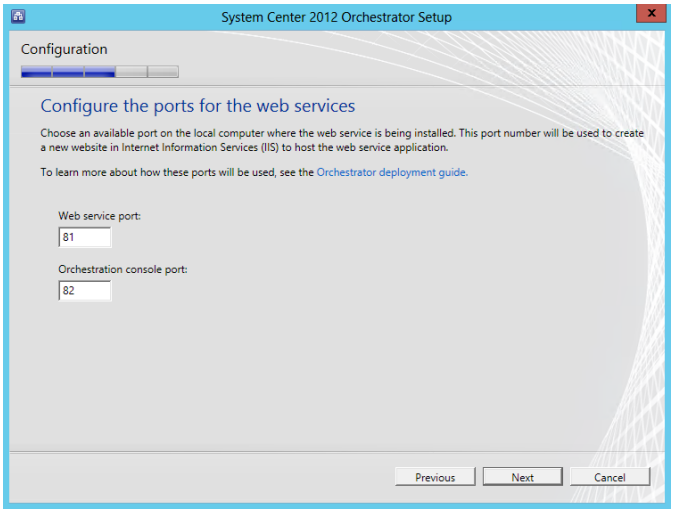
18. In the **Configure the database** dialog in the **Database** section, select the **New Database** option. Specify the default database name of *Orchestrator*.
19. Click **Next** to continue.



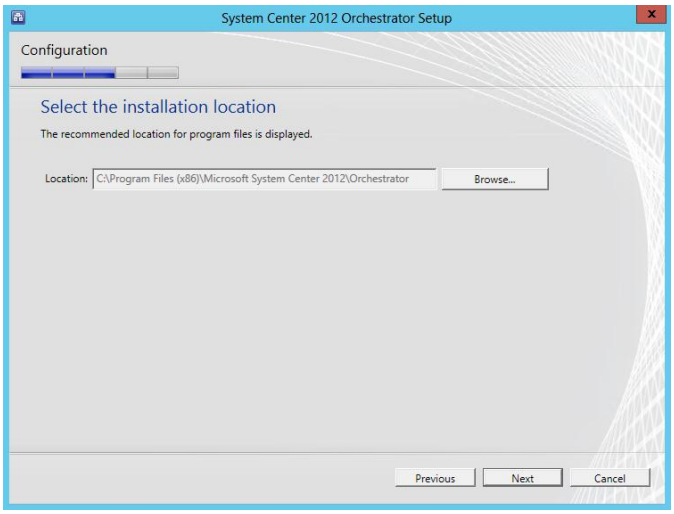
20. In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse…** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.
21. Verify that that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



22. In the **Configure the ports for the web services** dialog, provide the following information in the provided text boxes:
    a. **Web service port** – *specify the TCP port used for the Orchestrator Web Service. The default value of 81 is recommended.*
    b. **Orchestration console port** – *specify the TCP port used for the Orchestrator console port. The default value of 82 is recommended.*
23. When successful, click **Next** to continue.

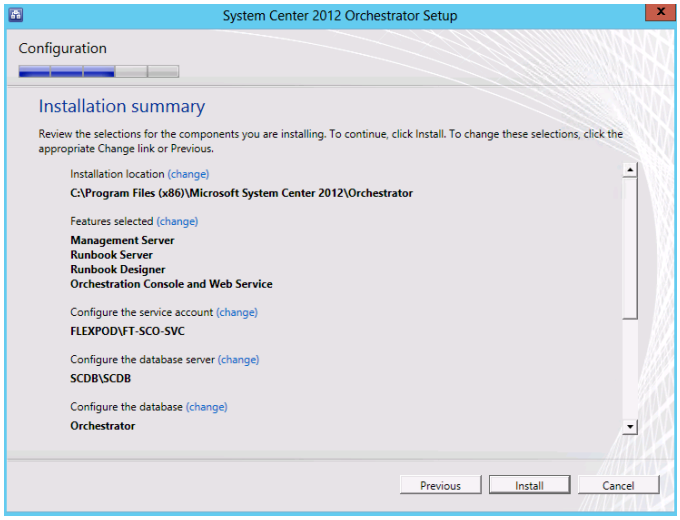


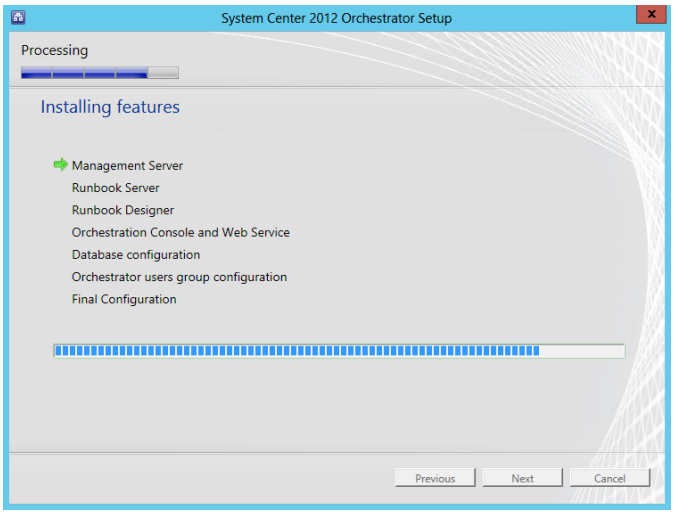
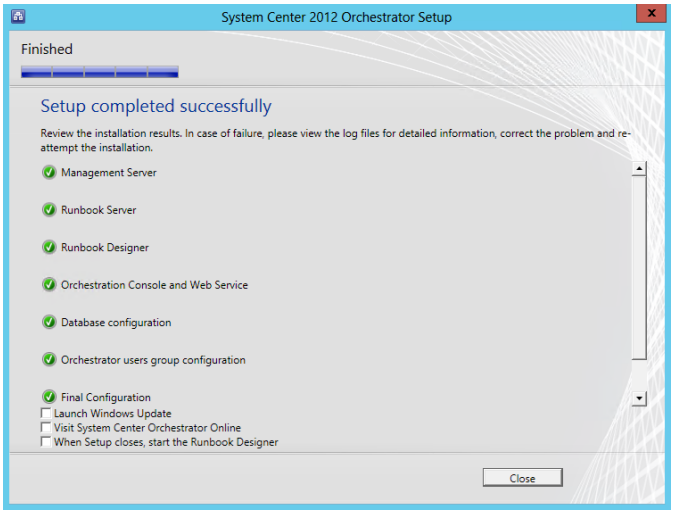
24. In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.

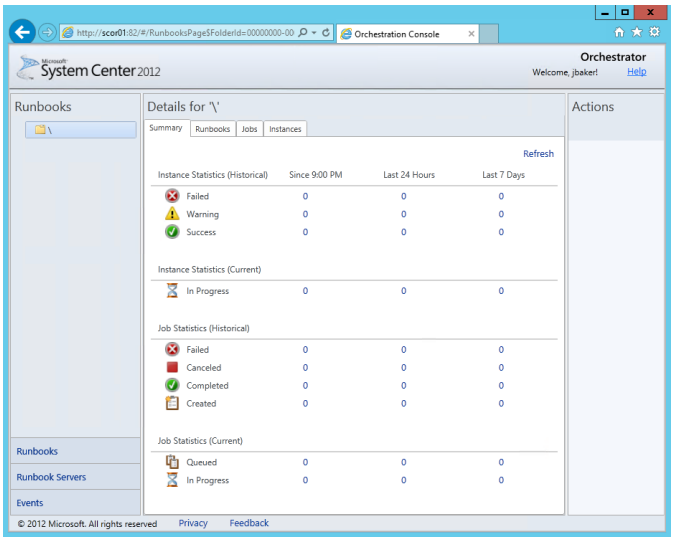
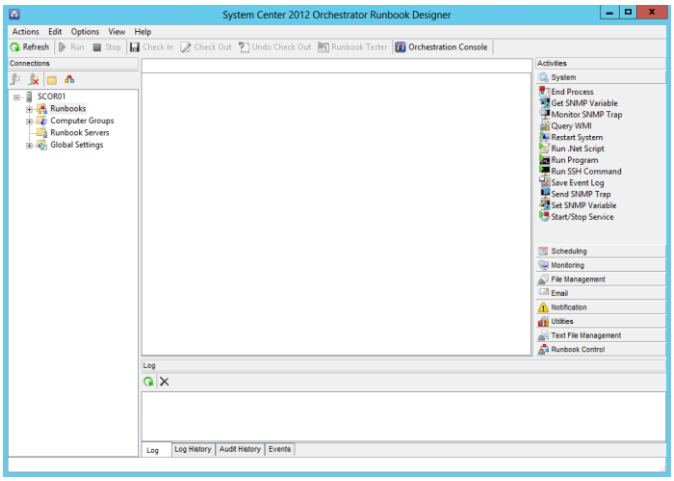


25. The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. These include:
    a. Customer Experience Improvement Program (CEIP)
    b. Error Reporting
26. Select the appropriate option based on your organization's policies and click **Next** to continue.

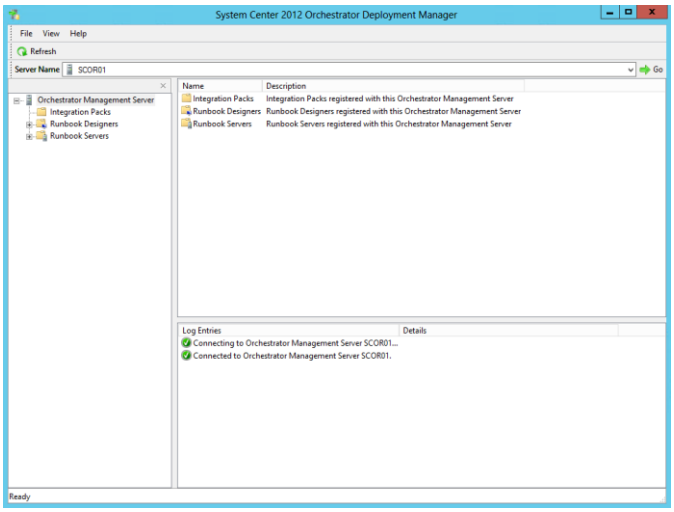
27. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



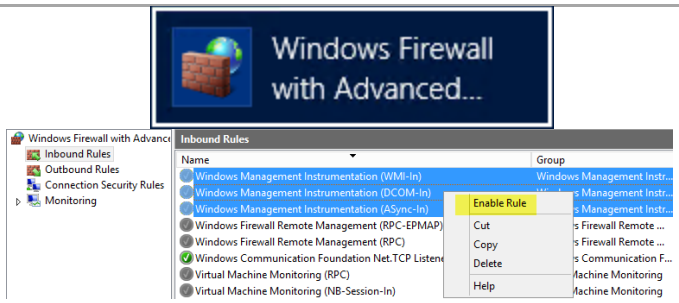
28. In the **Installing features** dialog, the installation will proceed and show progress.	
29. The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.	
30. When 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.	

31. Validate that the **Orchestration console** performs properly in Internet Explorer.	
32. From the **Start Menu**, then select the **Runbook Designer** tile.	
33. Launch the **Runbook Designer** console and verify that it performs properly.	
34. From the **Start Menu**, then select the **Deployment Manager** tile.	

35. Launch the **Deployment Manager** console and verify that it performs properly.

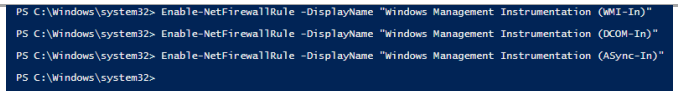


36. From the Start Screen, click on the Windows Firewall tile. Configure Windows Firewall for the first Orchestrator Runbook Server.[19]
37. If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:
    a. Windows Management Instrumentation (WMI-In).
    b. Windows Management Instrumentation (DCOM-In).
    c. Windows Management Instrumentation (ASync-In).
38. Right-click each rule and select **Enable Rule** from the context menu.



39. 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)"
```



[19] 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.

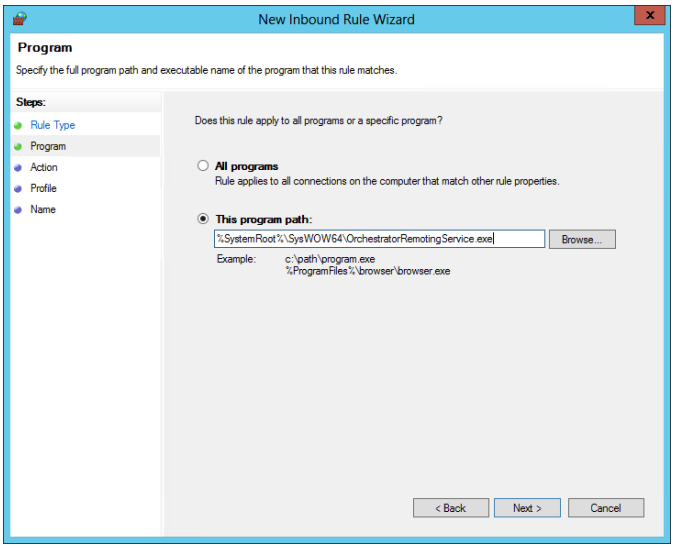
40. In Windows Firewall create a new Program rule using the following program path:

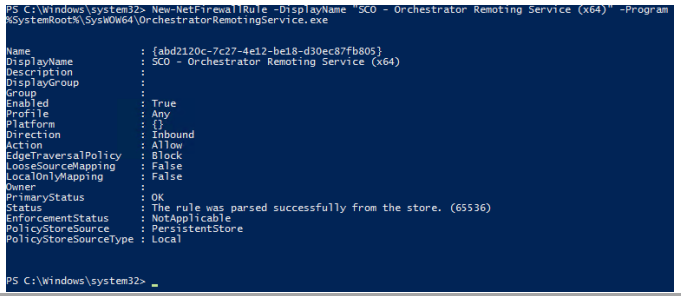
%SystemRoot%\SysWOW64\orchestratorRemotingService.exe

41. Name the rule **SCO – Orchestrator Remoting Service (x64)**.

42. Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO – Orchestrator Remoting Service (x64)" -Program C:\Windows\SysWOW64\OrchestratorRemotingService.exe
```

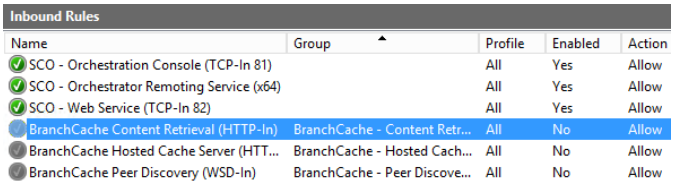




43. Since the first server runs the Orchestration console and web service, two additional ports (TCP 81 and 82) must be opened on the Windows Firewall as well. Create two additional firewall port rules named **SCO – Orchestration Console (TCP 81)** and **SCO – Web Service (TCP 82)** for each port and enable them.

44. 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)"
```



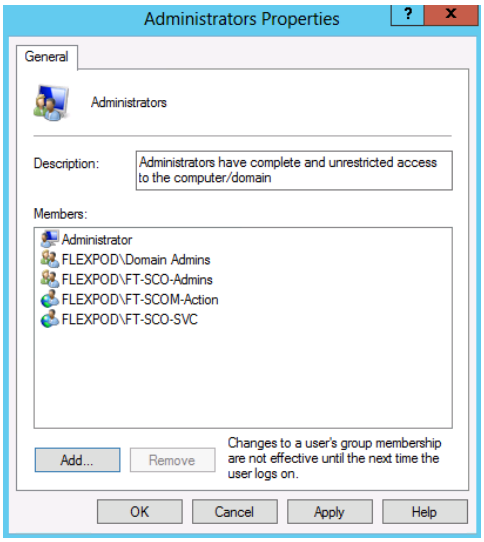
45. Restart the Orchestrator server.

Install an Additional Orchestrator Runbook Server

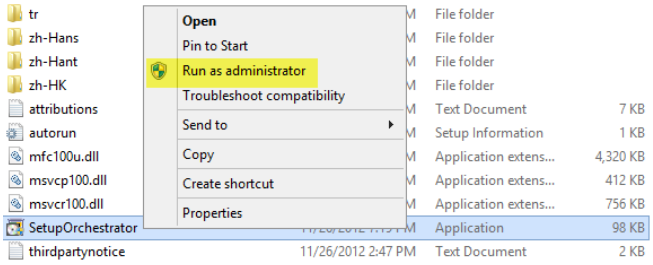
The following steps needs to be completed in order to install an additional Orchestrator Runbook Server.

▶ Perform the following steps on the **second Orchestrator Runbook Server** virtual machine.

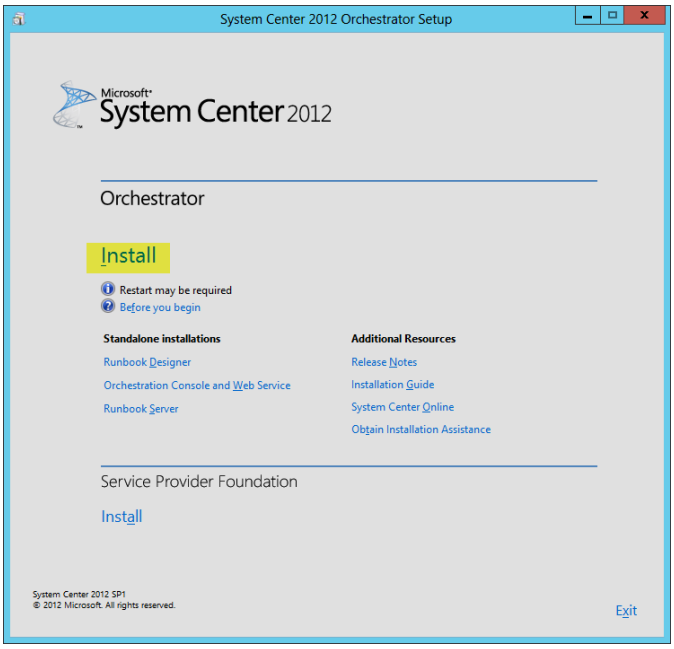
1. Log on to the Orchestrator virtual machine with a user with local admin rights.
2. Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:
   a. Orchestrator service account.
   b. Orchestrator Admins group.
   c. Operations Manager action account.



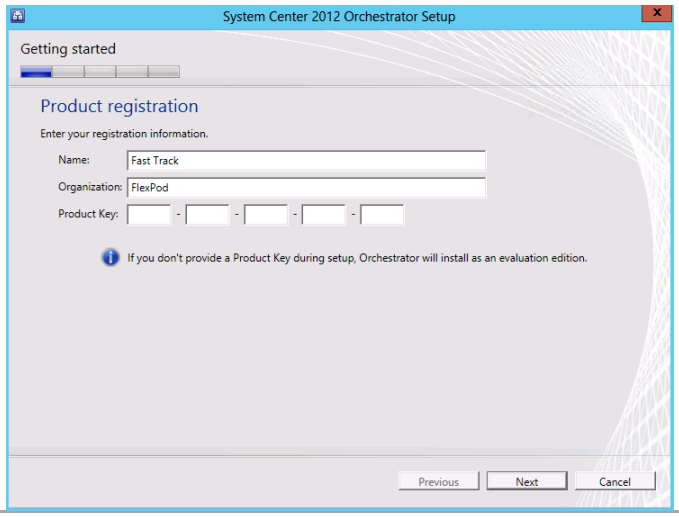
3. Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



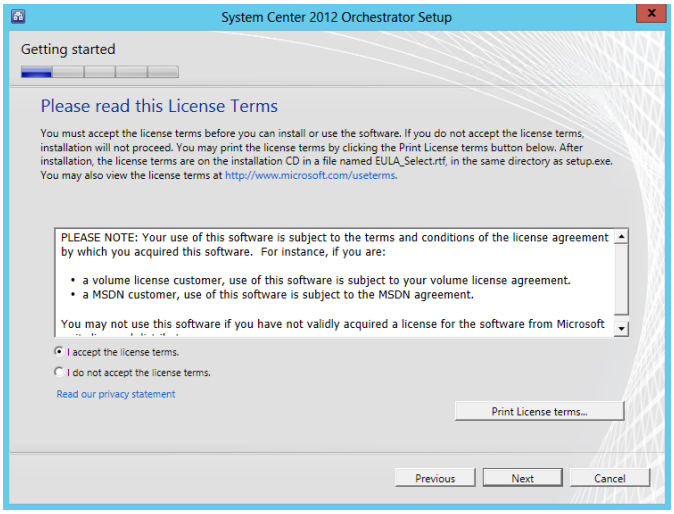
4. The Orchestrator installation wizard will begin. At the splash page, click **Install** begin the Orchestrator server installation.



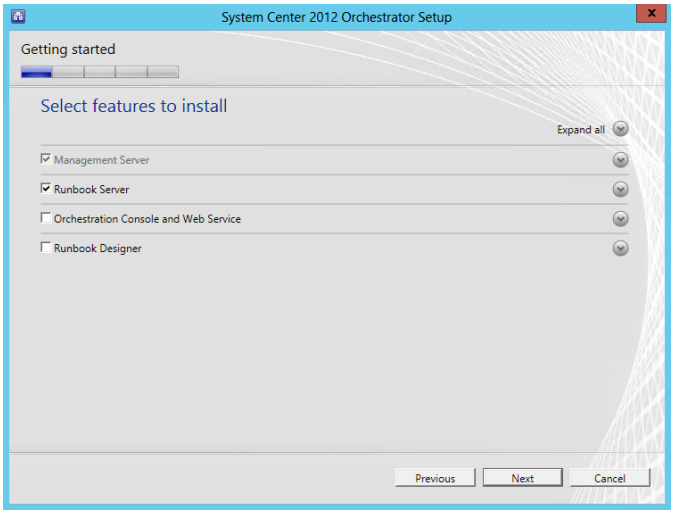
5. In the **Product registration information** dialog, enter the following information in the provided text boxes:
    a. **Name** – *specify the name of the primary user or responsible party within your organization.*
    b. **Organization** – *specify the name of the licensed organization.*
    c. **Product key** – *provide a valid product key for installation of Orchestrator. If no key is provided, Orchestrator will be installed in evaluation mode.*
6. Click **Next** to continue.



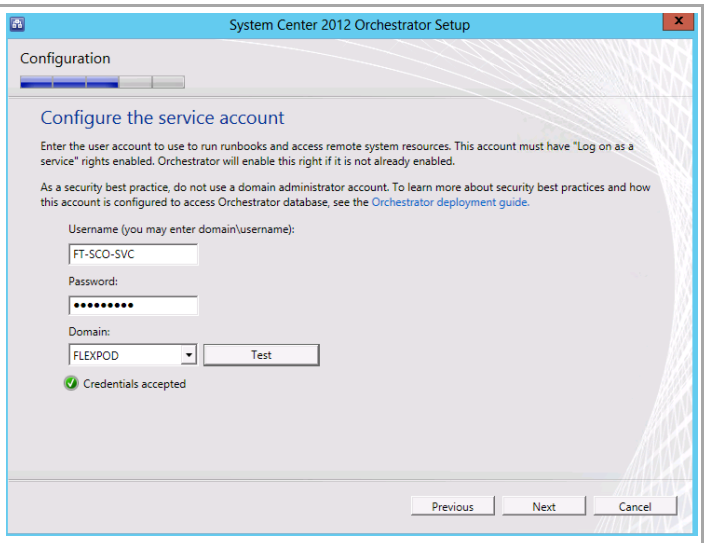
7. In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option checkbox is selected and click **Next** to continue.



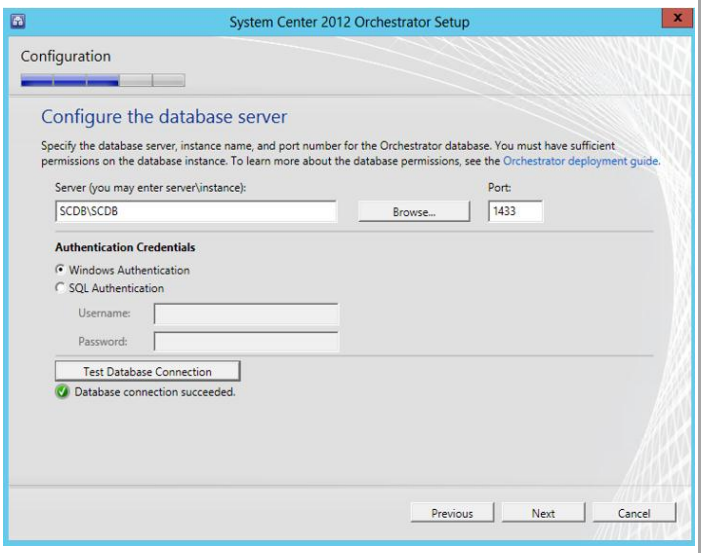
8. In the **Select Features to install** dialog, select the **Management Server** (default selected) and **Runbook server** checkboxes and click **Next** to continue.



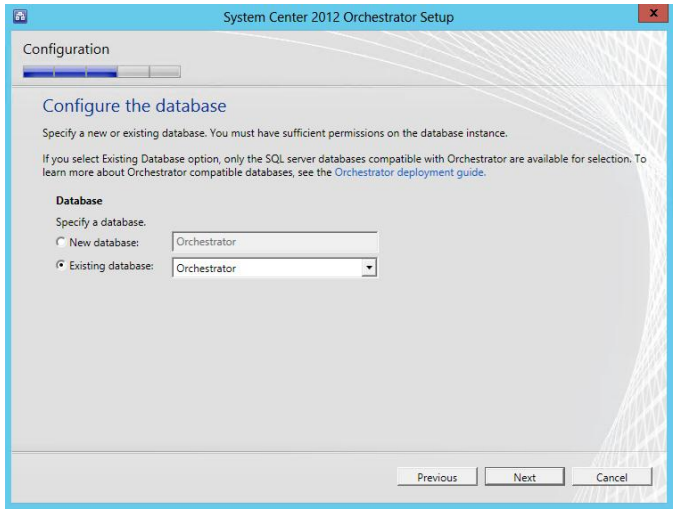
9. In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.
10. Before proceeding, click the **Test** button to verify the credentials provided.
11. When successful, click **Next** to continue.



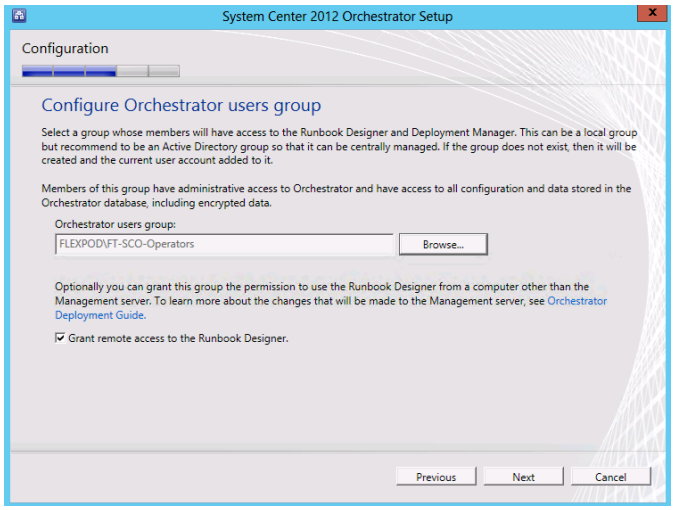
12. In the **Configure the database server** dialog, enter the following information in the provided text boxes:
    a. **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
    b. **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*
13. In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.
14. When successful, click **Next** to continue.



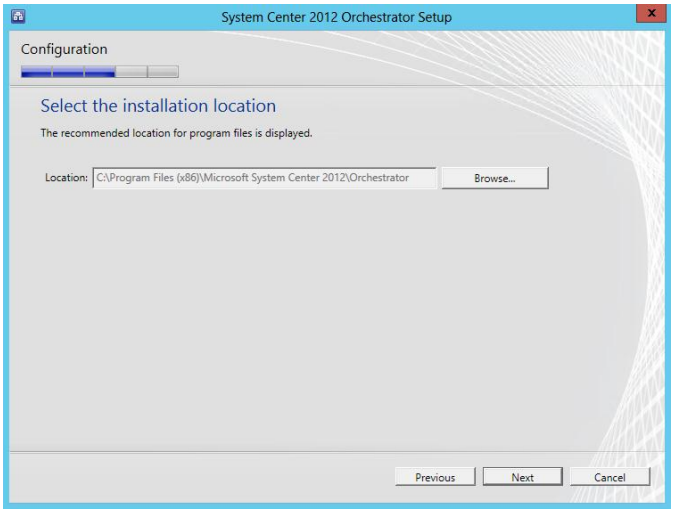
15. In the **Configure the database** dialog in the **Database** section, select the **Existing Database** option. Select the default database name of *Orchestrator* from the drop-down menu.
16. Click **Next** to continue.



17. 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.
18. Verify that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



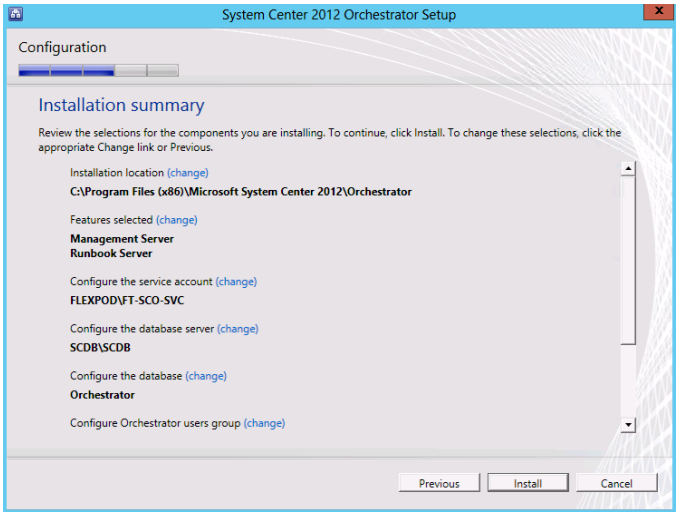
19. In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.



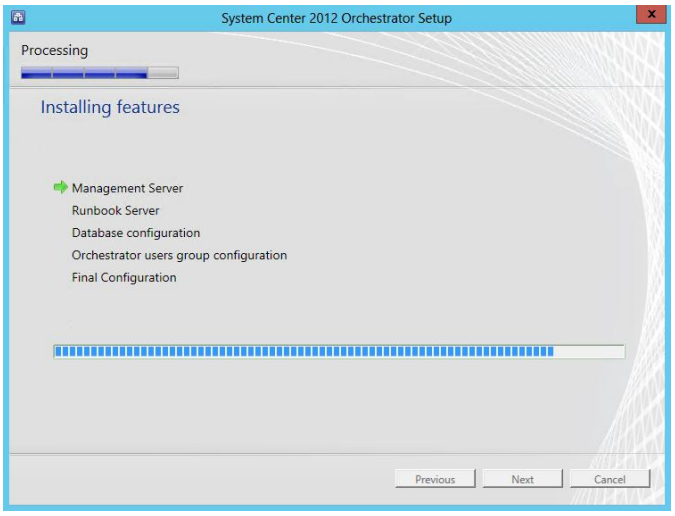
20. Depending on the current configuration of the server the Microsoft Updates Dialog may appear.
21. The **Microsoft Update** dialog provides options for participating in automatic updates for Orchestrator. Select the appropriate option based on your organization's policies and click **Next** to continue.

22. The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. This includes:
    a. Customer Experience Improvement Program (CEIP)
    b. Error Reporting
23. Select the appropriate option based on your organization's policies and click **Next** to continue.

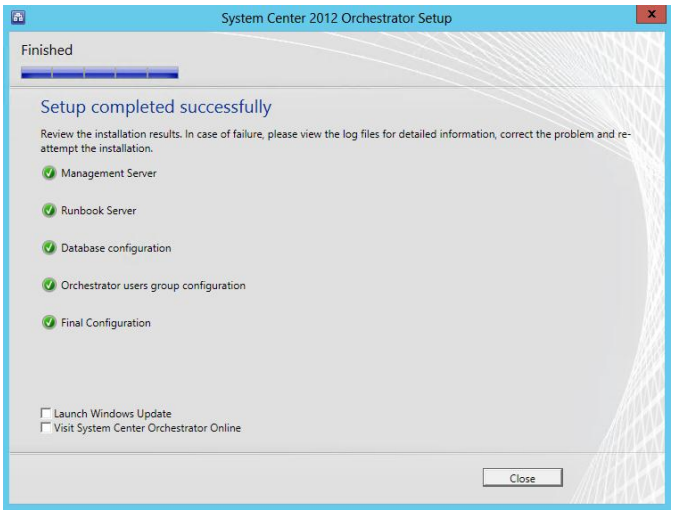
24. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



25. In the **Installing features** dialog, the installation will proceed and show progress.

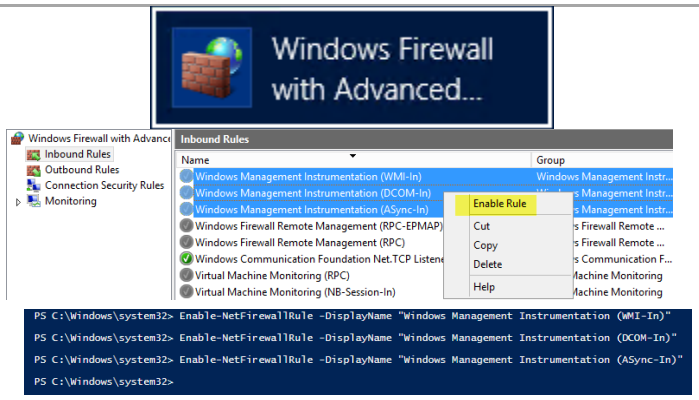


26. The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.



27. Configure Windows Firewall for the second Orchestrator Runbook Server.[20]
28. If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:
    a. Windows Management Instrumentation (WMI-In).
    b. Windows Management Instrumentation (DCOM-In).
    c. Windows Management Instrumentation (ASync-In).
    d. Right-click each rule and select **Enable Rule** from the context menu.
    e. 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)"
```



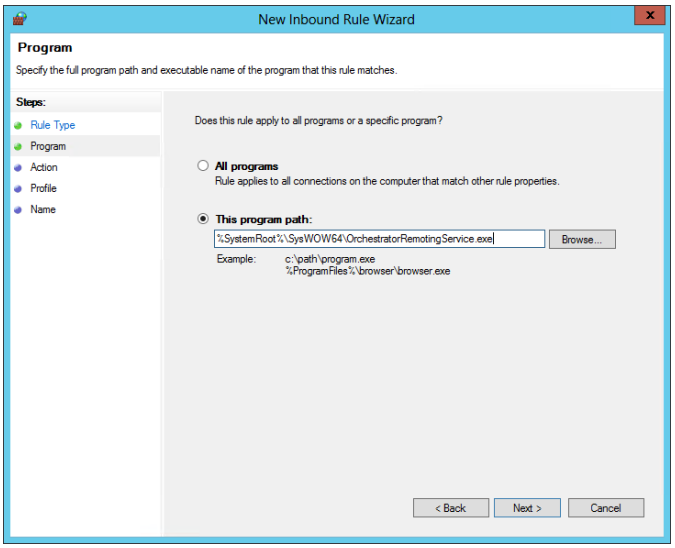
[20] Orchestrator guidance is provided from the following TechNet resources: Using Windows Firewall with Orchestrator - http://technet.microsoft.com/en-us/library/hh912321.aspx and TCP Port Requirements http://technet.microsoft.com/en-us/library/hh420382.aspx.

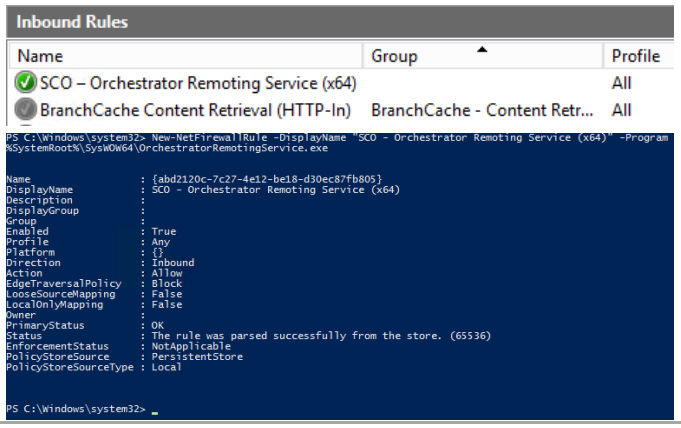
29. In Windows Firewall create a new Program rule using the following program path:

%SystemRoot%\SysWOW64\orchestratorRemotingService.exe

30. Name the rule **SCO – Orchestrator Remoting Service (x64)**.
31. Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO – Orchestrator Remoting Service (x64)" -Program C:\Windows\SysWOW64\OrchestratorRemotingService.exe
```

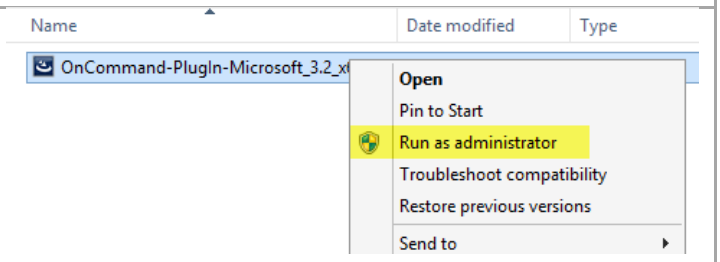
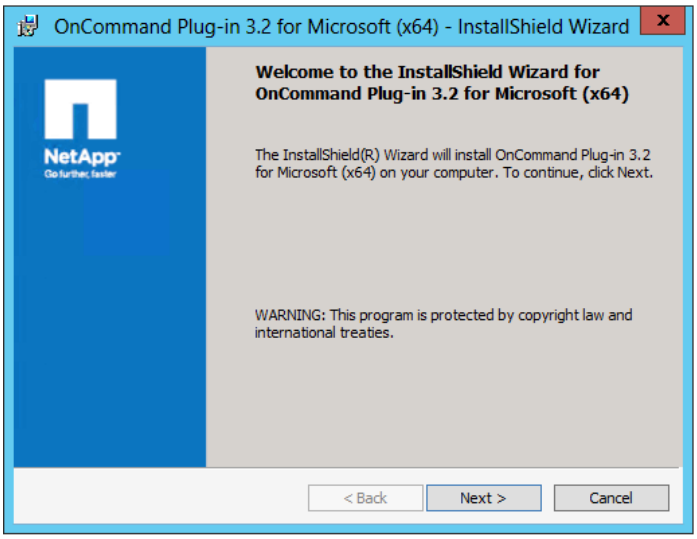




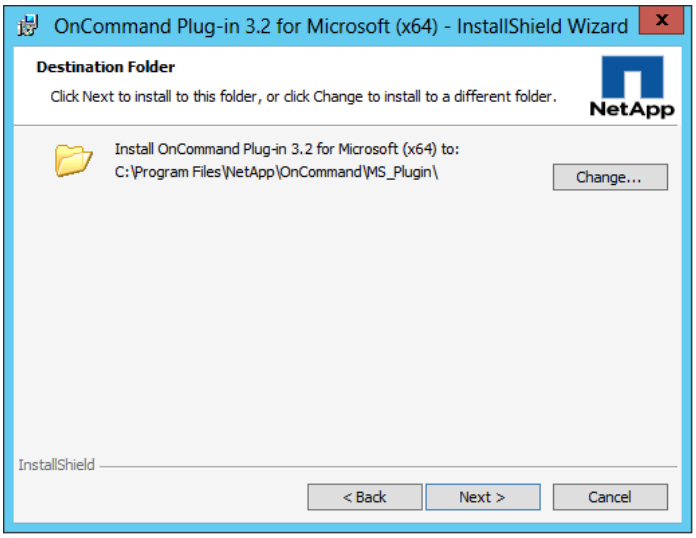
32. Restart the Orchestrator server.

20.4 Install NetApp Integration Pack

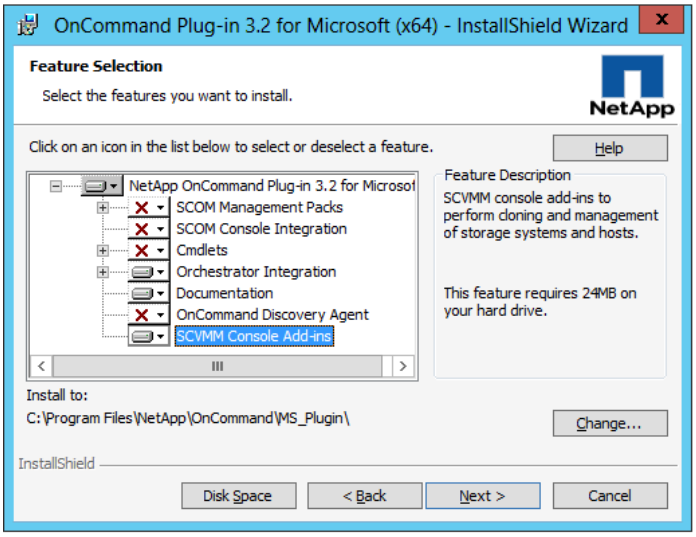
Complete the following steps to install the OCPM OIPs. Download the OCPM installer from http://support.netapp.com/NOW/download/software/appwatch_scom/3.2/OnCommand-PlugIn-Microsoft_3.2_x64_NetApp.exe.

▶ Perform the following steps on the **Orchestrator Runbook Server** virtual machine.	
<DOMAIN>\FT-OCPM-SVC	This account needs: • Full administrative permissions on all Hyper-V hosts to be managed. • Full administrative permissions on the Runbook servers. • Sysadmin on the SQL Server instance, or DBO rights to the OCPM database after it is created.
1. Log in to the SCO management server, right-click the **OCPM 3.2 installation package,** and select **Run as Administrator** to start the OCPM installation wizard.	
2. On the Welcome page, click **Next**.	

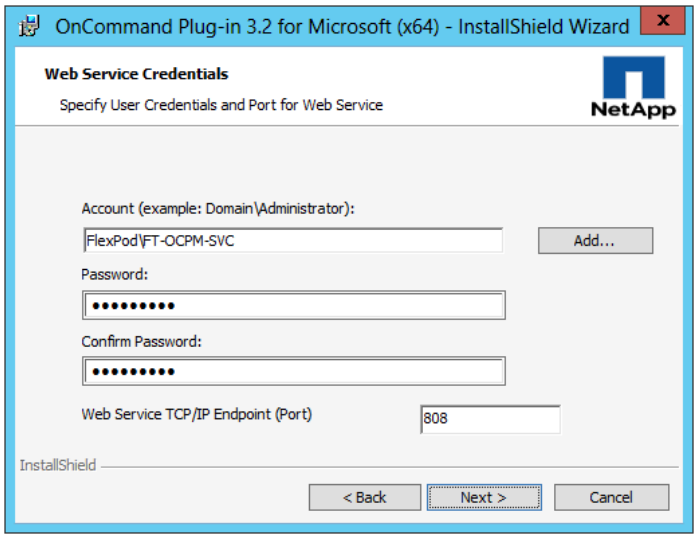
3. On the Destination Folder page, click Next to keep the default installation folder.



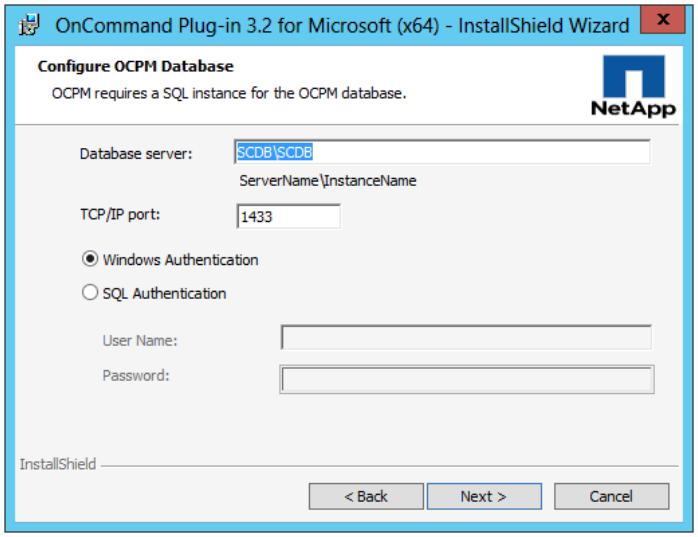
4. On the Feature Selection page, select the following features and click Next:
   a. Orchestrator Integration
   b. Documentation
   c. SCVMM Console Add-ins (if the SCVMM console is installed on the SCO server)



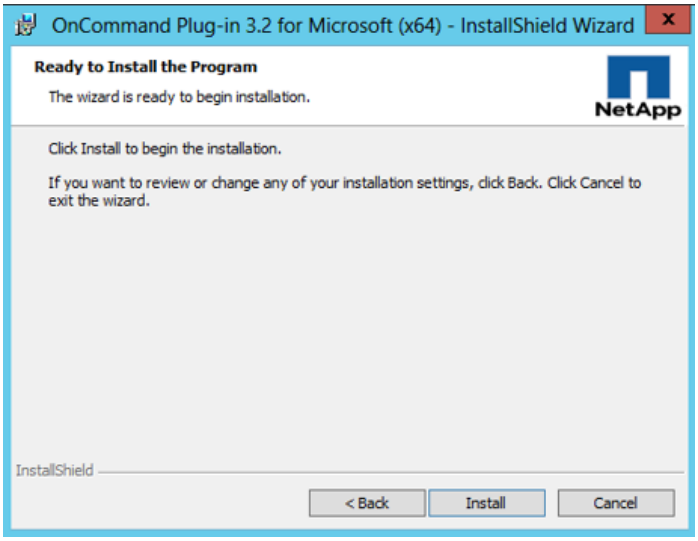
5. On the Web Service Credentials page, enter the following credentials and click Next:
   a. Account: Active Directory domain user account to be used for web service communication
   b. Password: Password of the domain user account
   c. Web Service TCP/IP Endpoint (Port): Leave the default value of 808, unless there is a port conflict or firewall configuration that requires a change in the port
6. All System Center servers running the OCPM web service must use the same port for communication.



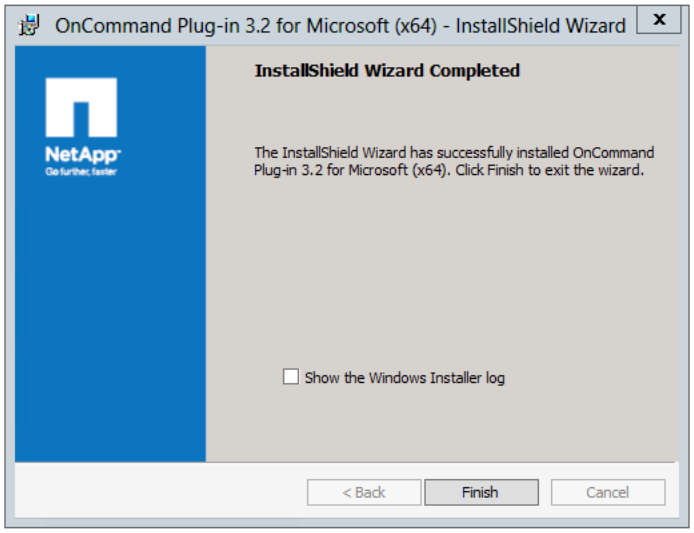
7. On the Configure OCPM Database page, complete the following steps and click Next:
    a. In the Database Server field, enter the name of the Microsoft SQL Server instance where OCPM can create a database.
    b. In the TCP/IP Port field, leave the default value of 1433 unless the SQL Server instance is using a different port for SQL Server client communication.
    c. Leave the default selection of Windows Authentication.
    d. The web service account must have a SQL Server login and SQL Server sysadmin role on the SQL Server instance.



8. Click Install to continue the installation.



9. On the InstallShield Wizard Completed page, click Finish to complete the installation.



20.5 Install Cisco UCS Integration Pack

The following steps needs to be completed in order to install the Cisco UCS Integration Pack. Download the integration pack from http://developer.cisco.com/web/unifiedcomputing/systemcenter

▶ Perform the following steps on the **Orchestrator** virtual machines.

20.6 Install Cisco UCS PowerTool

The Cisco UCS PowerTool should be installed on the FlexPod Management server.

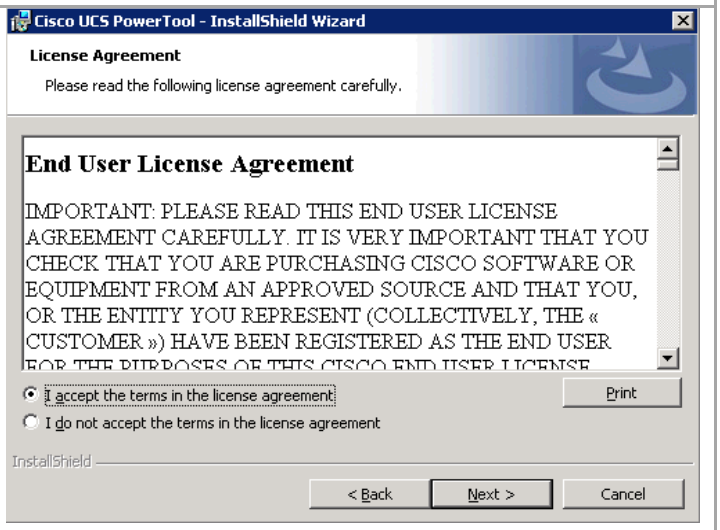
Download the Cisco UCS PowerTool version 0.9.9.0 or newer from the Cisco Developer Network. It can be found in the Microsoft Management section - http://developer.cisco.com/web/unifiedcomputing/microsoft.

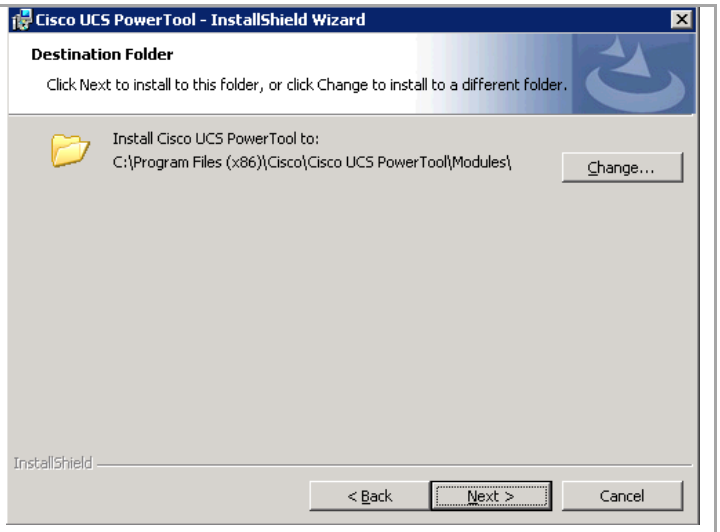
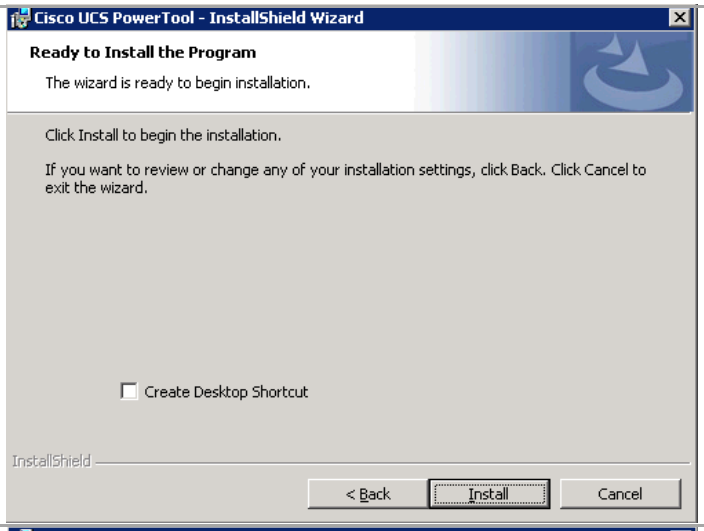
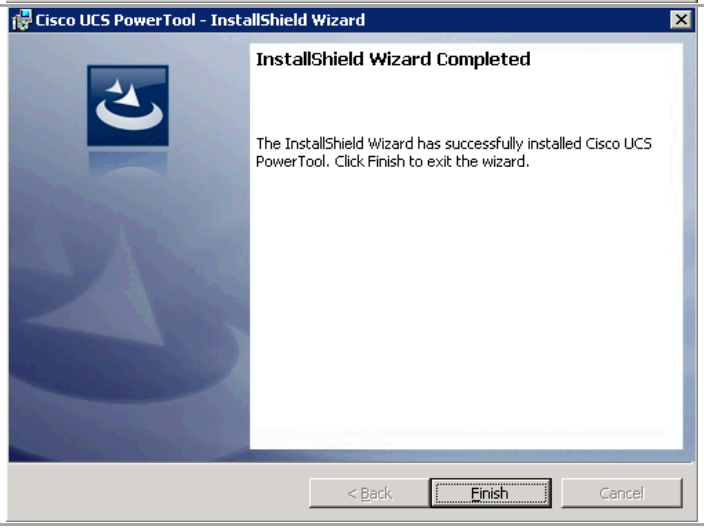
Extract the zip file and execute the extracted exe file.

▶ Perform the following steps on the **Orchestrator** virtual machines.

1. Launch the Cisco UCS PowerTool Installer. The **Setup Wizard** screen appears.

2. **Read and accept** the end user license agreement. Click **Next** to continue.



3. Select the **Destination Folder** and click **Next** to continue.	
4. Cisco UCS PowerTool is ready to install. Click **Next** to complete the installation.	
5. After the installation completes successfully click **Finish** to close the installation wizard.	

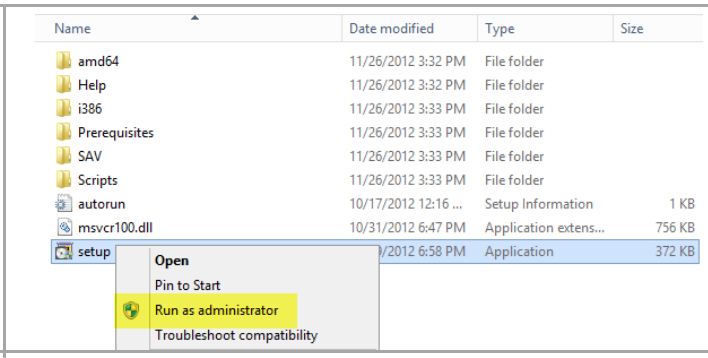
20.7 Post-Installation Tasks

When the installation is complete, install and configure Orchestrator Integration Packs on the target Runbook Servers.

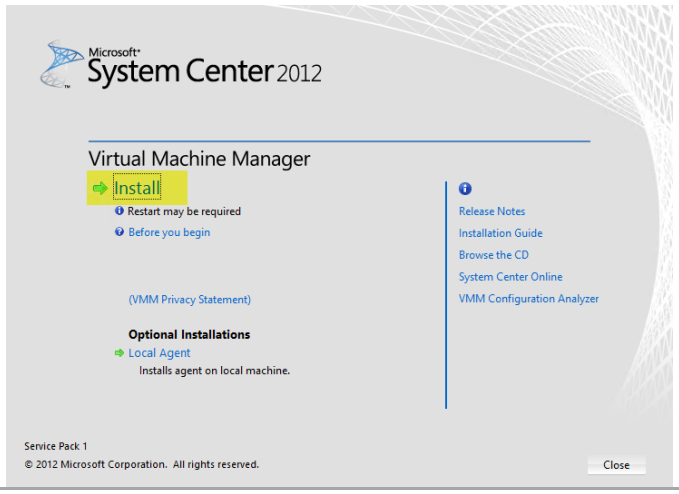
Install the Virtual Machine Manager Console

▶ Perform the following steps on the **Orchestrator** virtual machines.

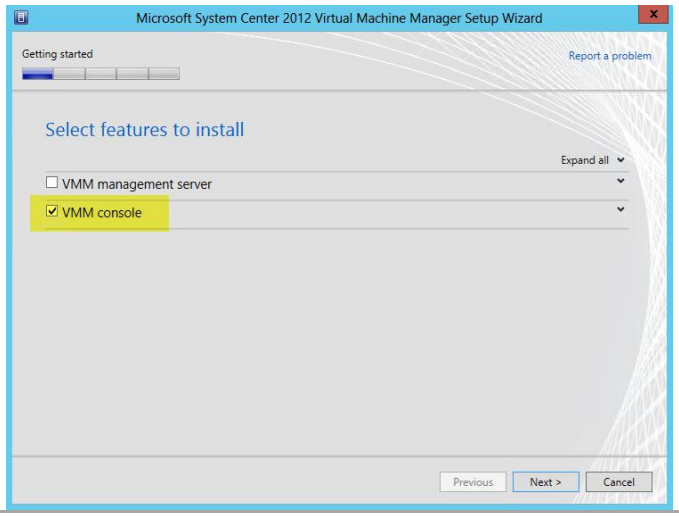
1. Log on to the Orchestrator server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

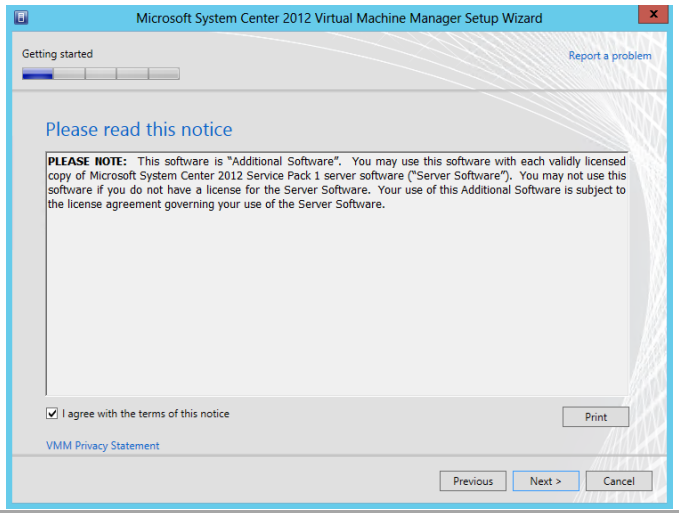
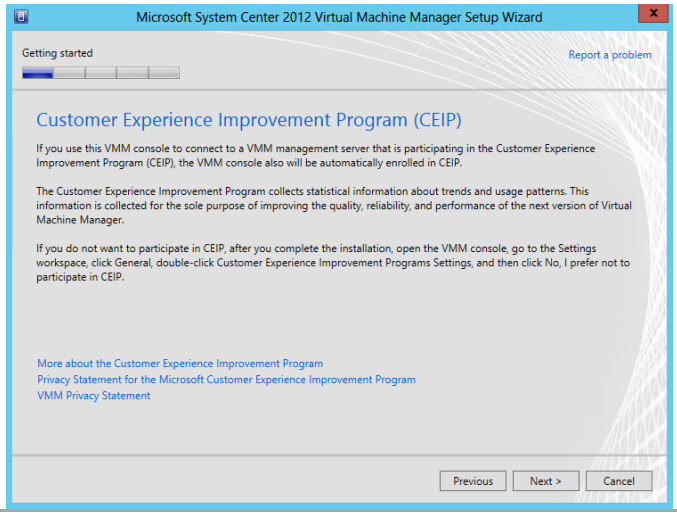


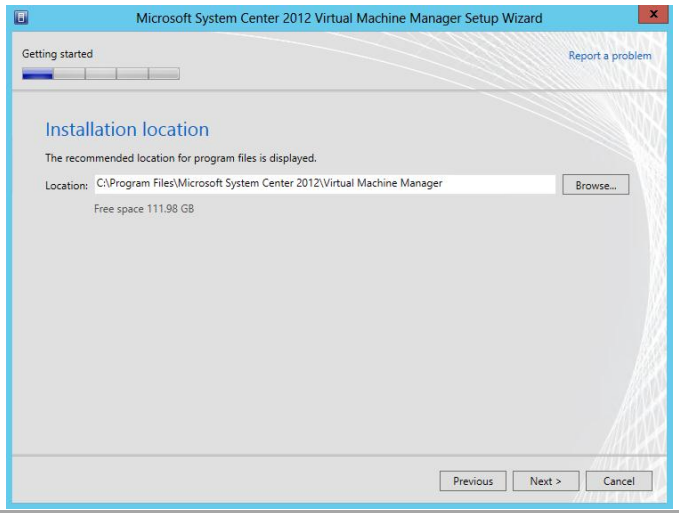
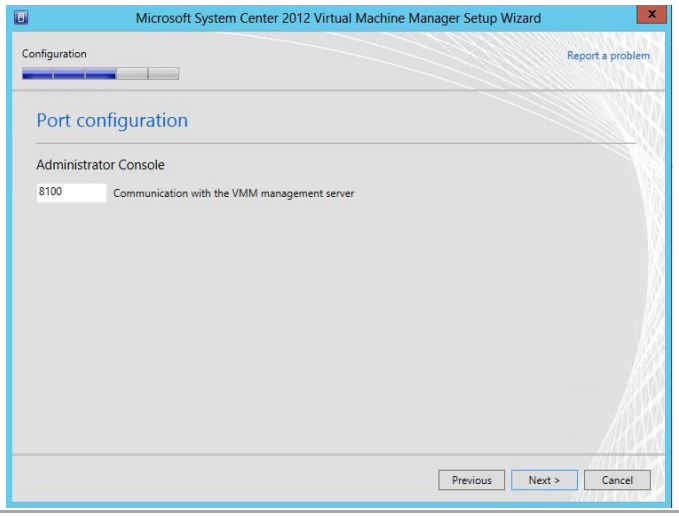
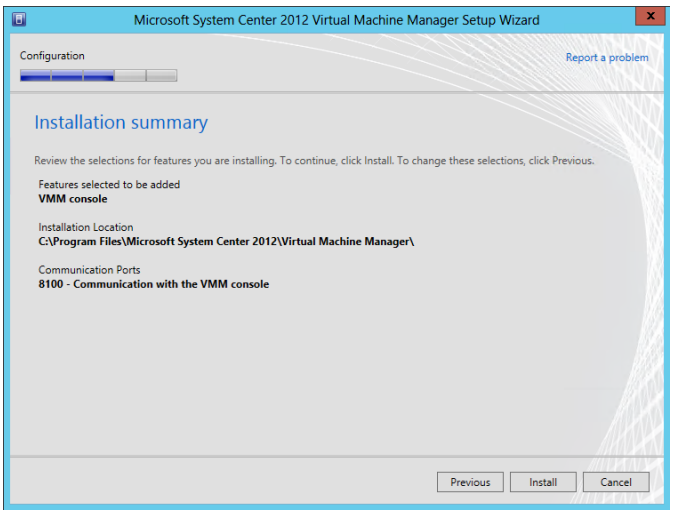
2. The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



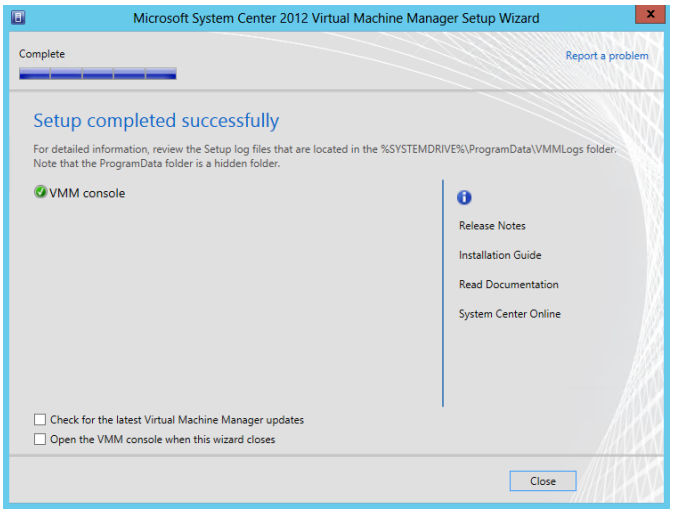
3. In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



4. 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.	
5. In the **Customer Experience Improvement Program** dialog, click **Next** to continue.	
6. 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.	

7. 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.	
8. 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.	
9. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

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

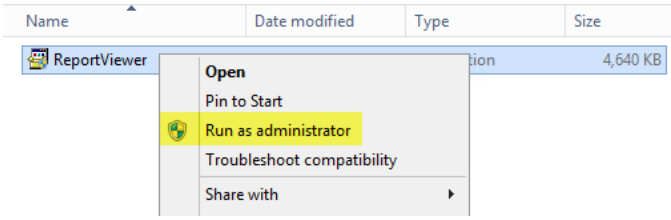


Install the Microsoft Report Viewer 2010 SP1

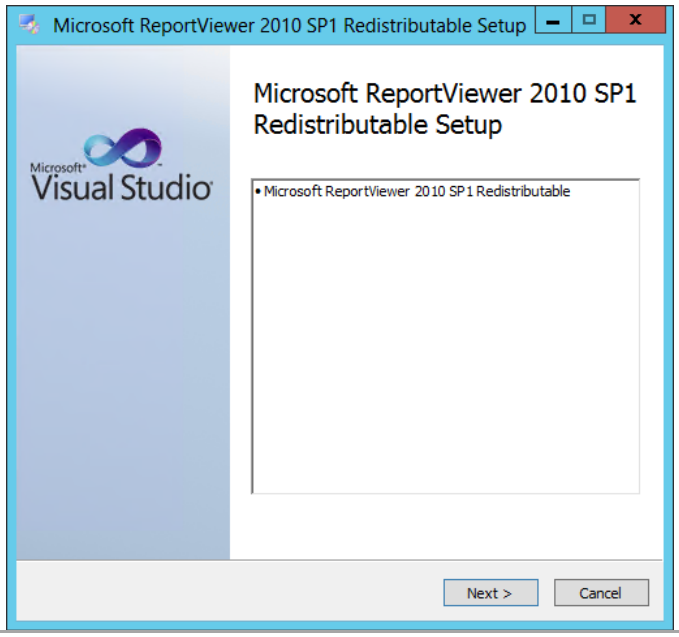
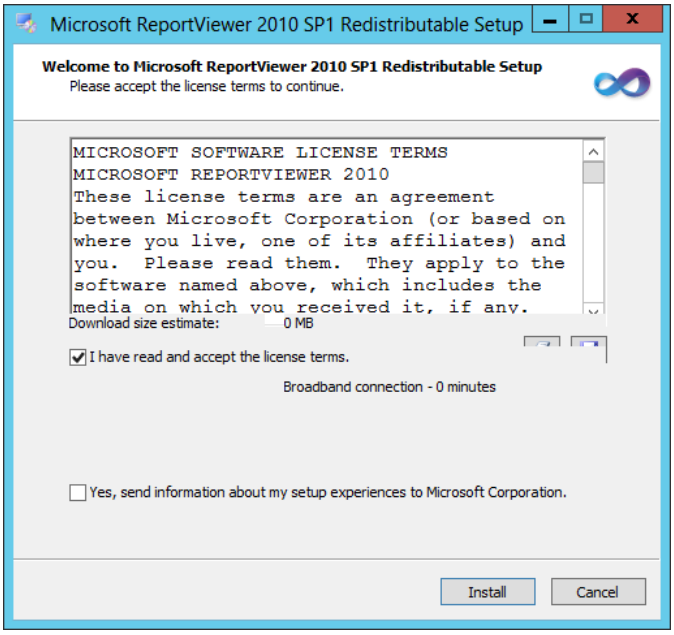
Additionally, inside Orchestrator the Operations Manager console is required, but this also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.[21] Follow the provided steps to install the SP1 package.

▶ Perform the following steps on both **Orchestrator** virtual machines.

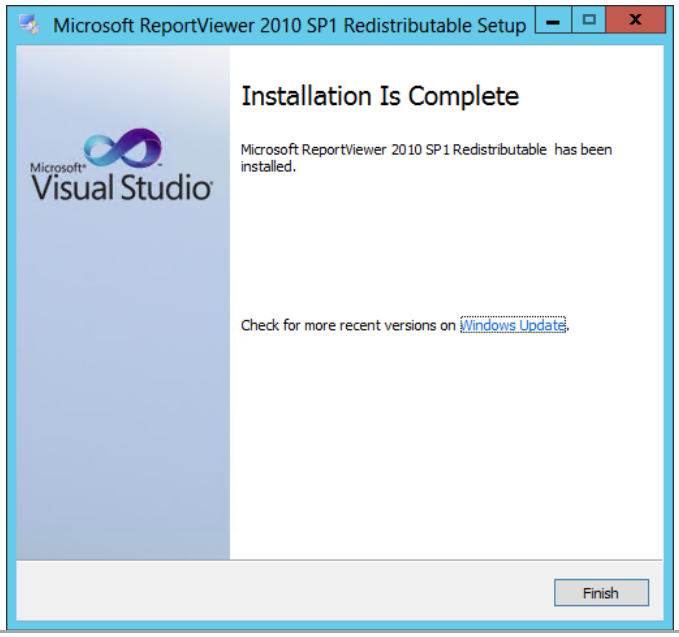
1. From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



[21] Microsoft Report Viewer 2010 SP1 Redistributable Package - http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en.

2. Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.	
3. Select the **I have read and accept the license terms** check box and click **Install.**	

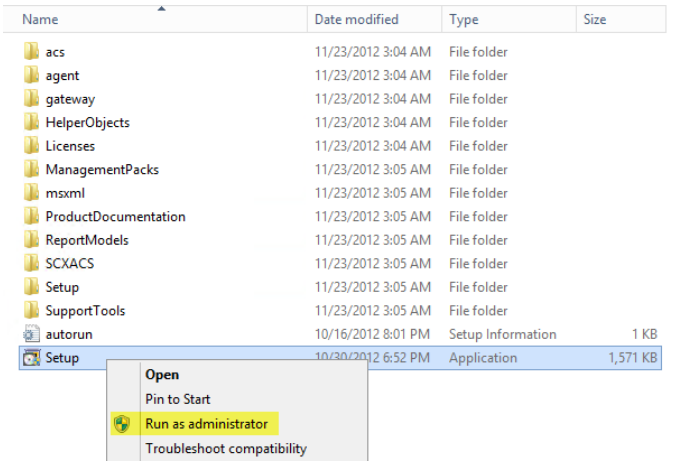
4. The installation progress will be displayed in the setup wizard. When completed, click **Finish** to exit the installation.

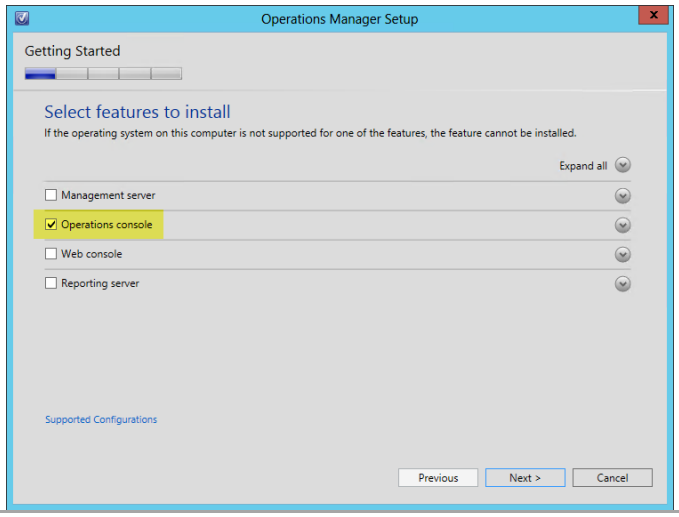
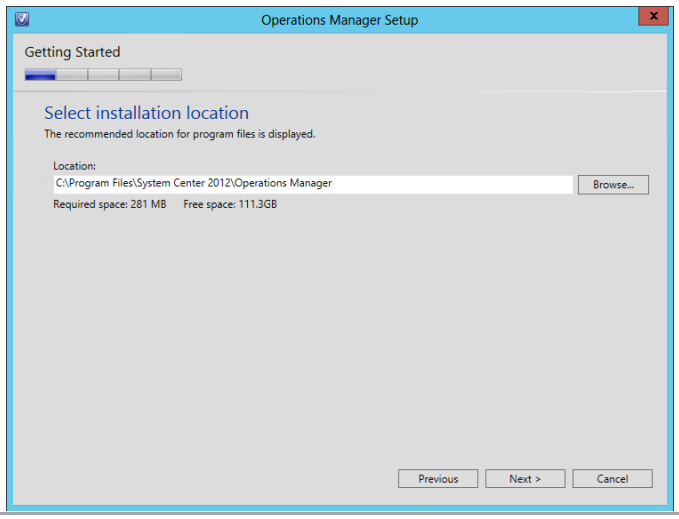


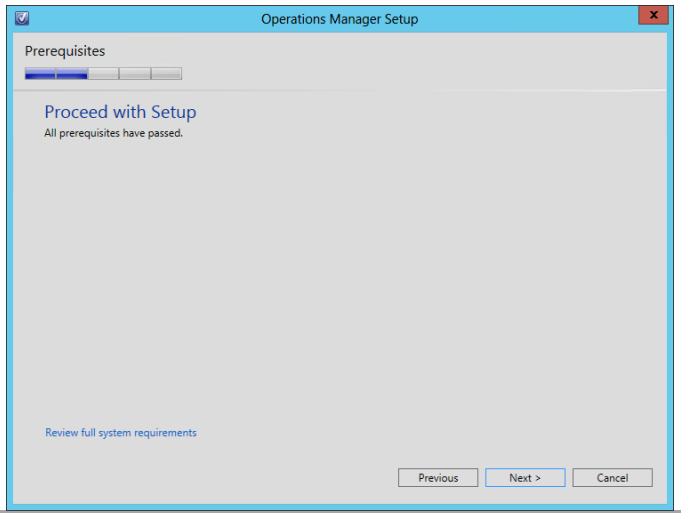
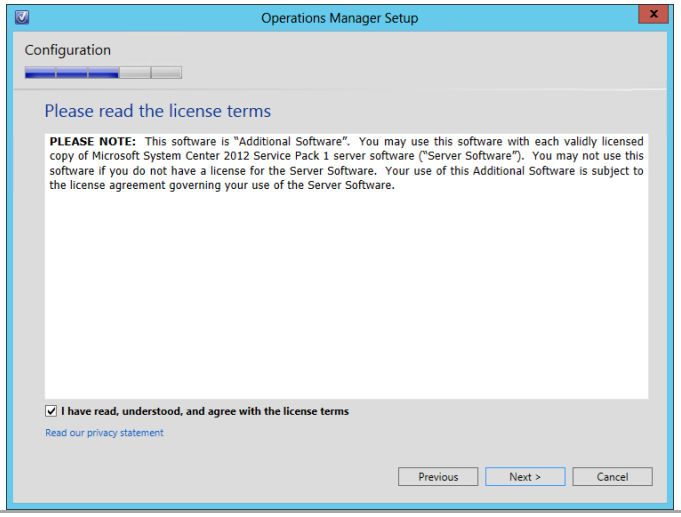
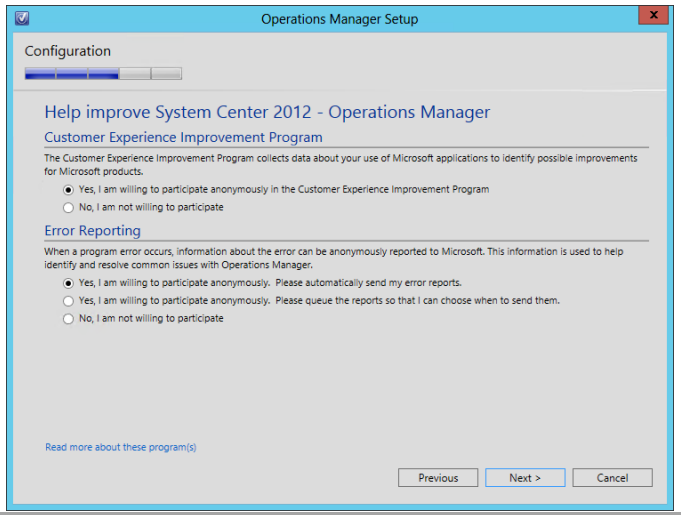
Install the Operations Manager Console

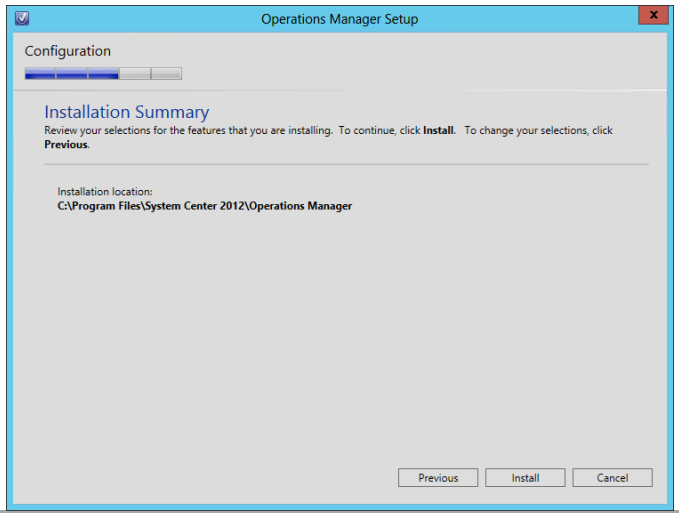
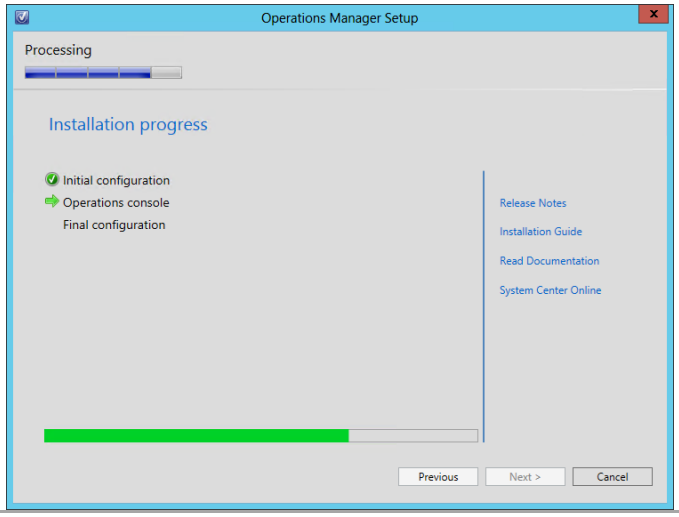
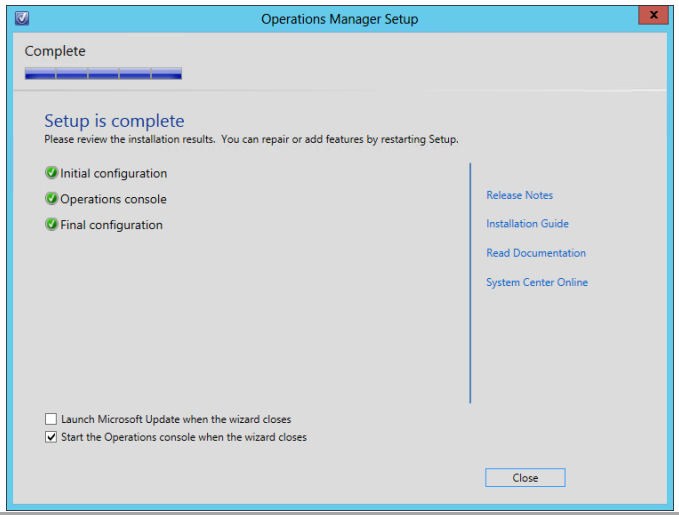
▶ Perform the following steps on both of the **Orchestrator** virtual machines.

1. From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

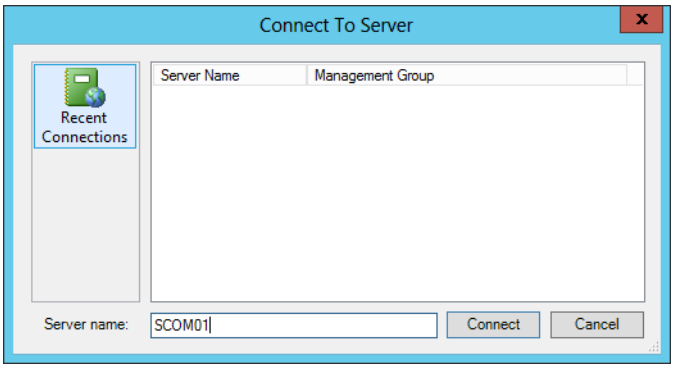


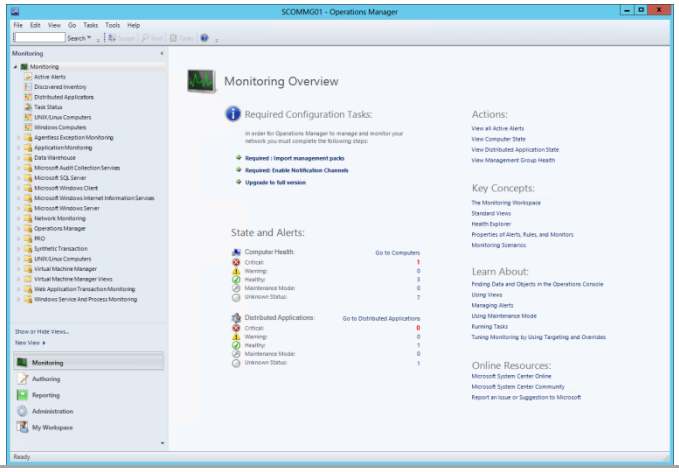
2. The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.	
3. In the **Select features to install** dialog, verify that the **Operations console** checkbox is selected. Click **Next** to continue.	
4. In the **Select 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.	

5. 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.	
6. 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 checkbox is selected and click **Next** to continue.	
7. The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include: a. Customer Experience Improvement Program (CEIP) b. Error Reporting 8. Select the appropriate option based on your organization's policies and click **Next** to continue.	

9. The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
10. The installation progress will be displayed during the installation.	
11. 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.	

12. 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.



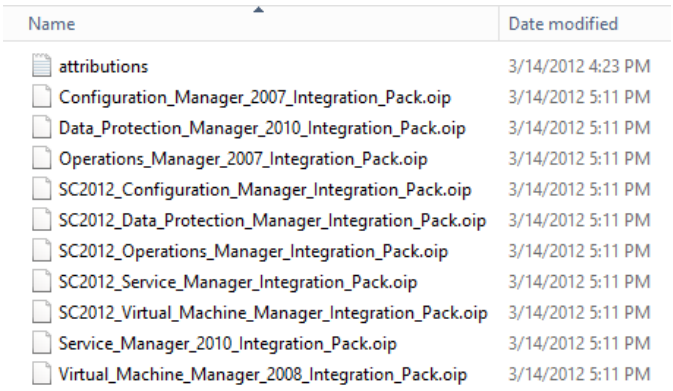


Install System Center 2012 SP1, NetApp, and Cisco UCS Integration Packs

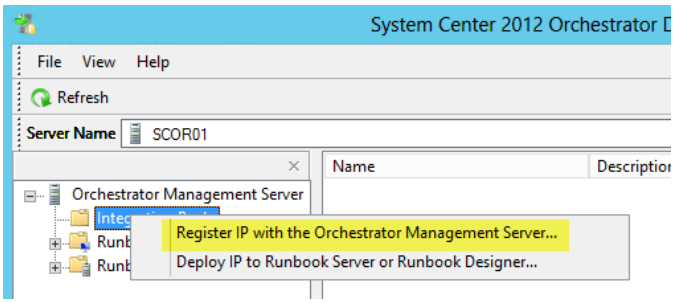
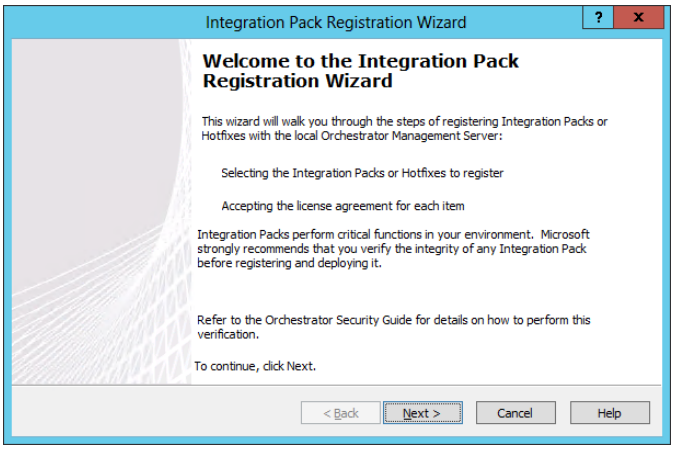
The following steps needs to be completed in order to install the Orchestrator Integration Packs.

▶ Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

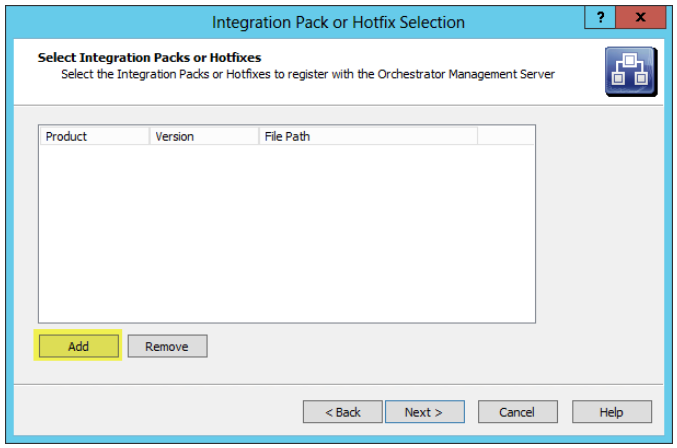
1. Download the System Center 2012 SP1 Integration Packs from http://www.microsoft.com/en-us/download/details.aspx?id=34611
2. and expand them to a single location so the Orchestrator Integration Pack files are expanded.

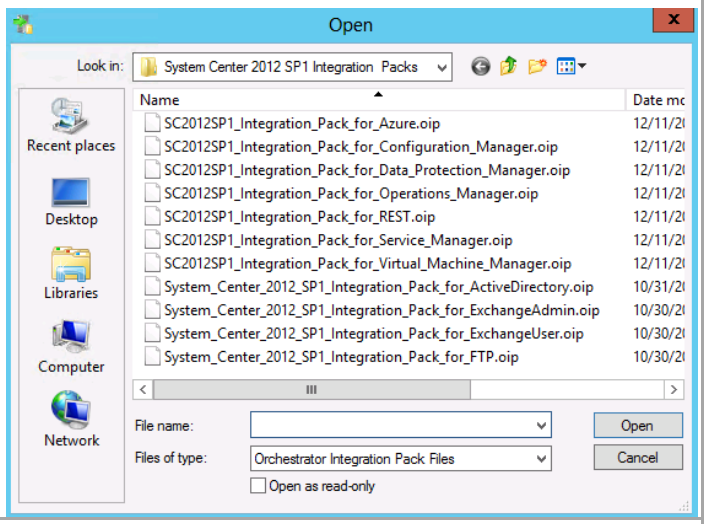


3. From the **Start** screen, click the **Deployment Manager** tile.

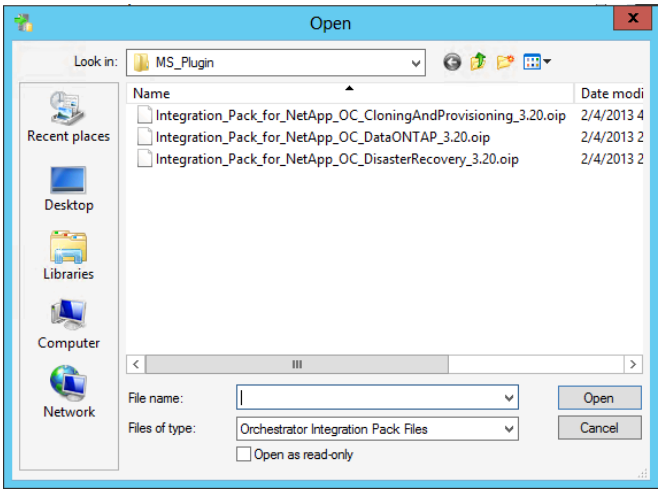
4. In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Register IP with the Orchestrator Management Server...** option from the context menu.	
5. The **Integration Pack Registration Wizard** will appear. Click **Next** to continue.	

6. 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**:
    a. System Center 2012 SP1 Configuration Manager.
    b. System Center 2012 SP1 Data Protection Manager.
    c. System Center 2012 SP1 Operations Manager.
    d. System Center 2012 SP1 Service Manager.
    e. System Center 2012 SP1 Virtual Machine Manager.

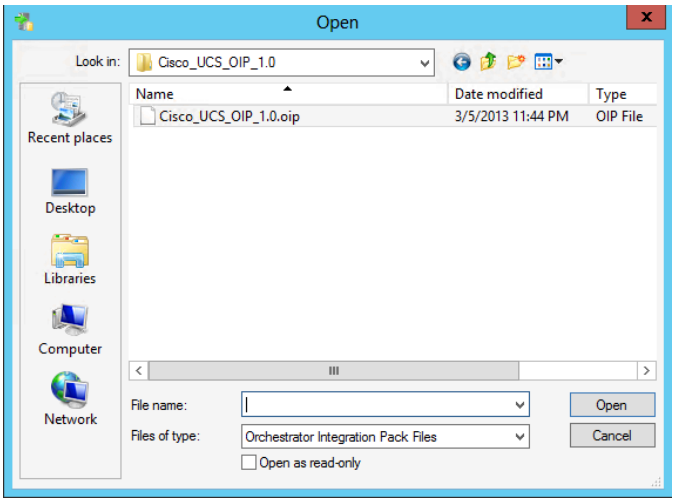




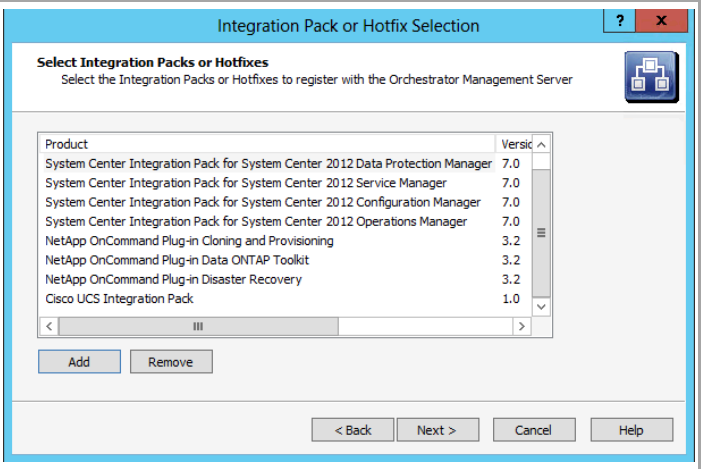
7. In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the OCPM installation directory and select the following integration packs and click **Open**.



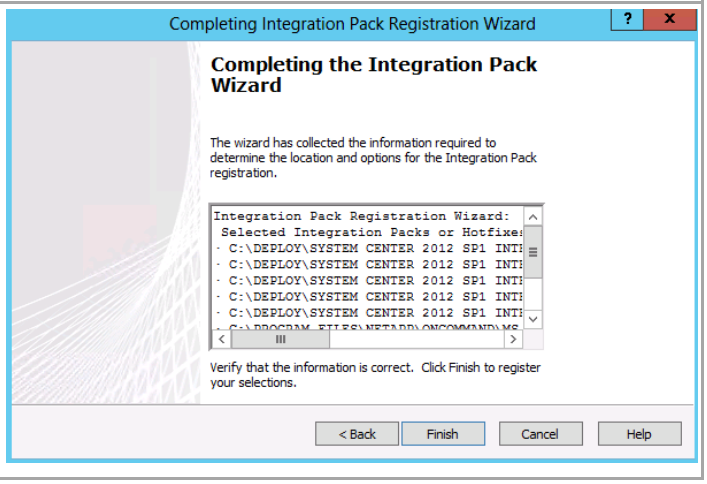
8. In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the location where the Cisco UCS OIP was extracted and select the following integration packs and click **Open**.
9. Cisco UCS OIP 1.0

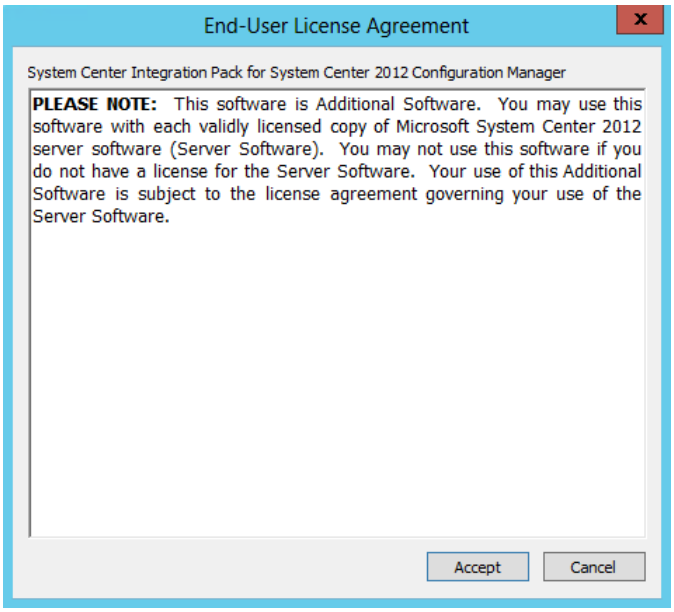
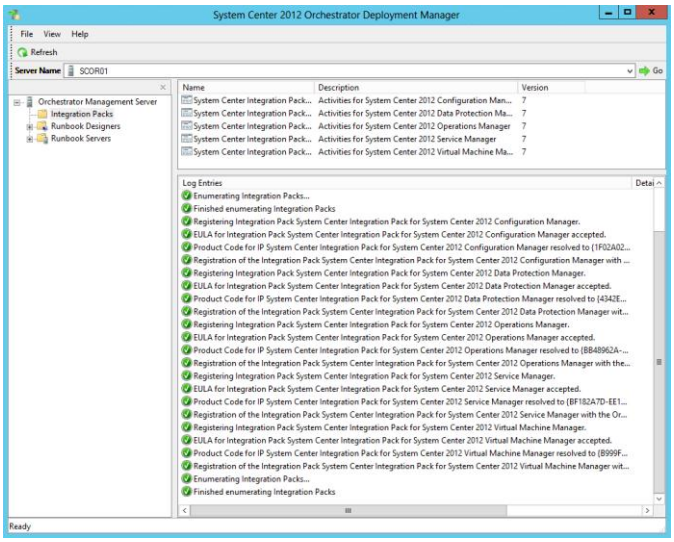


10. When all integration packs are selected, click **Next** to continue.



11. The **Completing the Integration Pack Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



12. During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.	
13. When complete, each integration pack will be displayed in the Deployment Manager interface.	

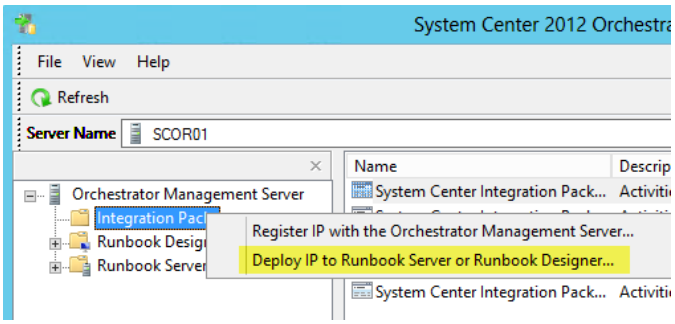
Deploy Integration Packs

The following steps need to be completed in order to install the Orchestrator Integration Packs.[22]

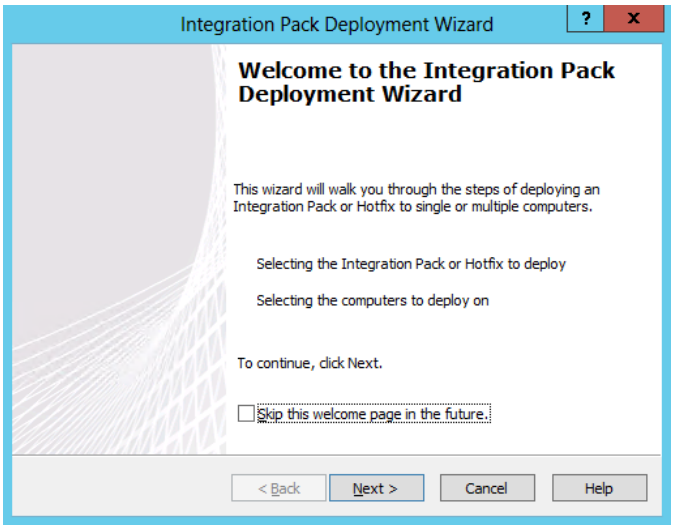
▶ Perform the following steps on the **Orchestrator Runbook Server** virtual machine.	
1. From the **Start** screen, click the **Deployment Manager** tile.	

[22] System Center 2012 SP1 – Orchestrator Component Add-ons and Extensions - http://www.microsoft.com/en-us/download/details.aspx?id=34606

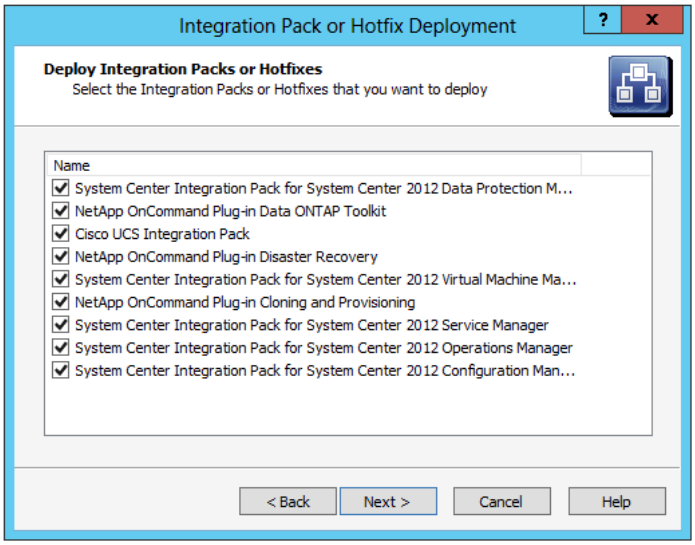
2. In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer...** option from the context menu.

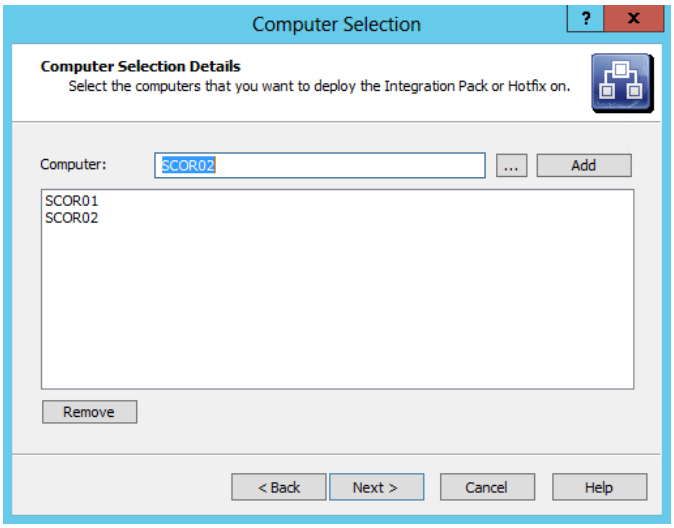
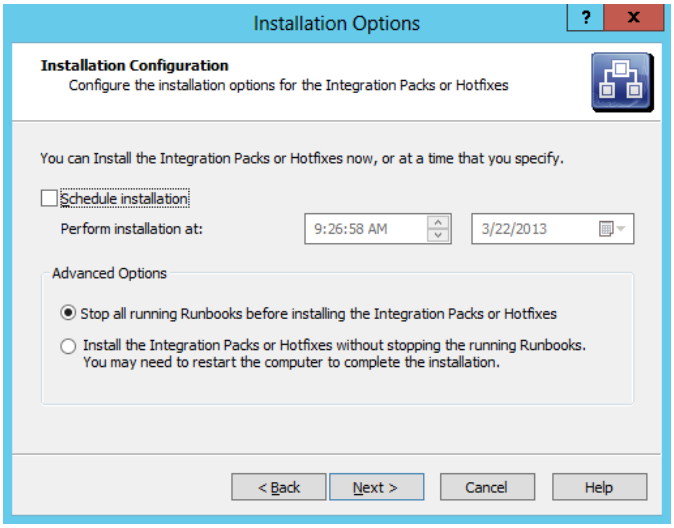
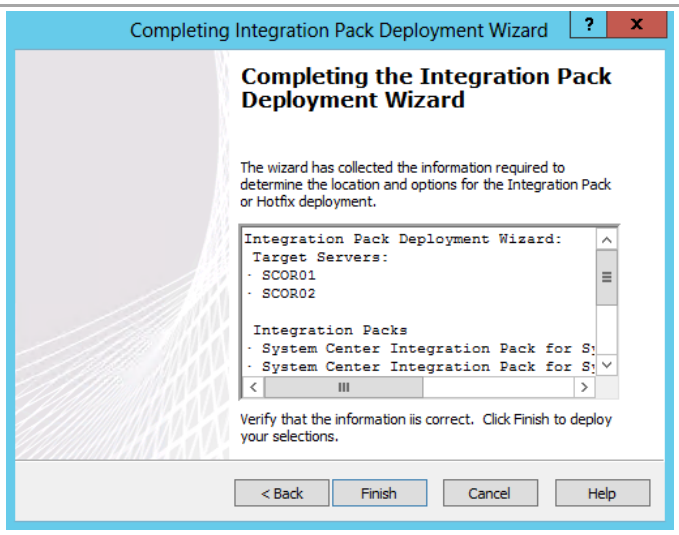


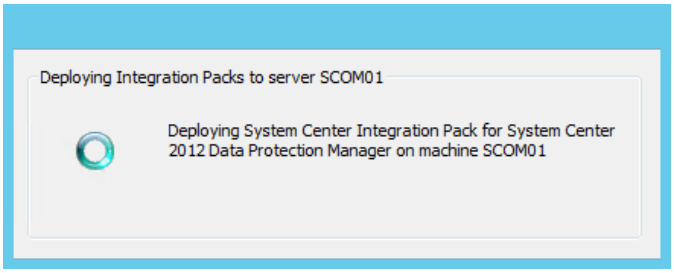
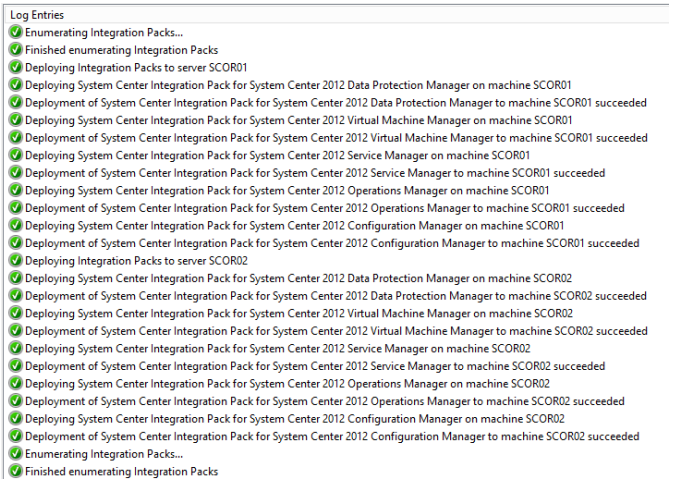
3. The **Integration Pack Deployment Wizard** will appear. Click **Next** to continue.

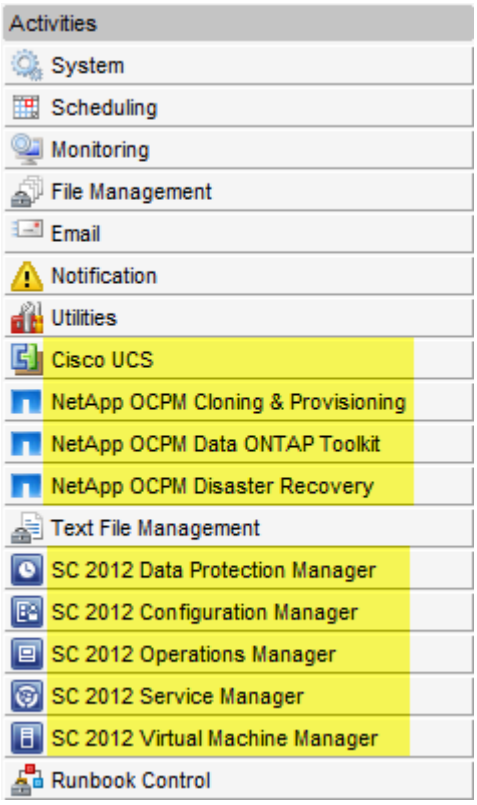
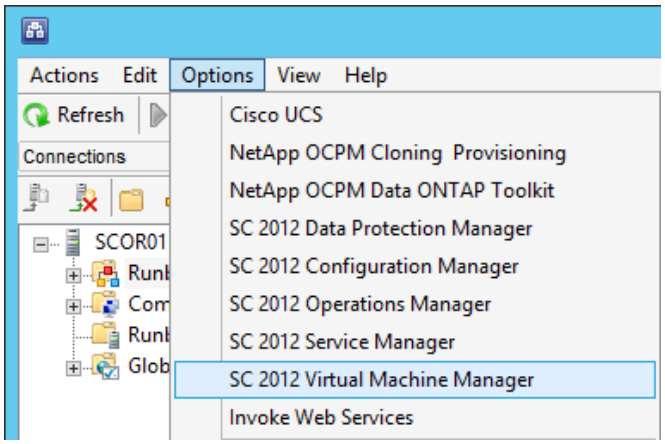


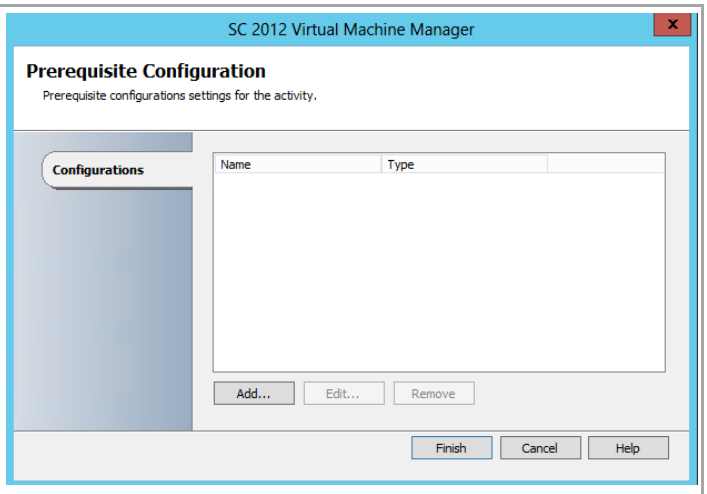
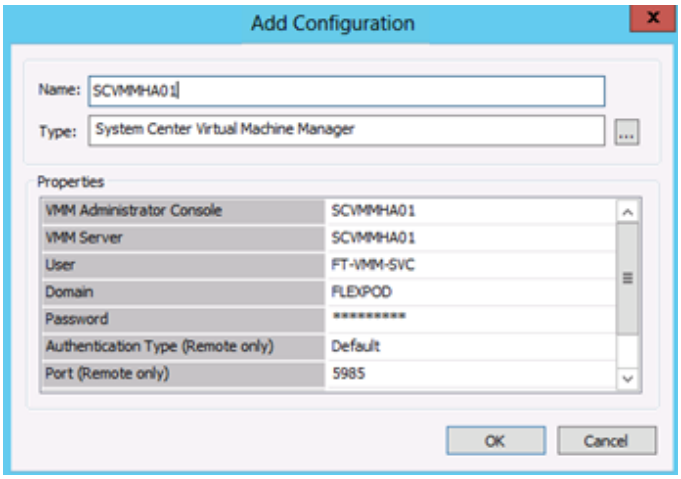
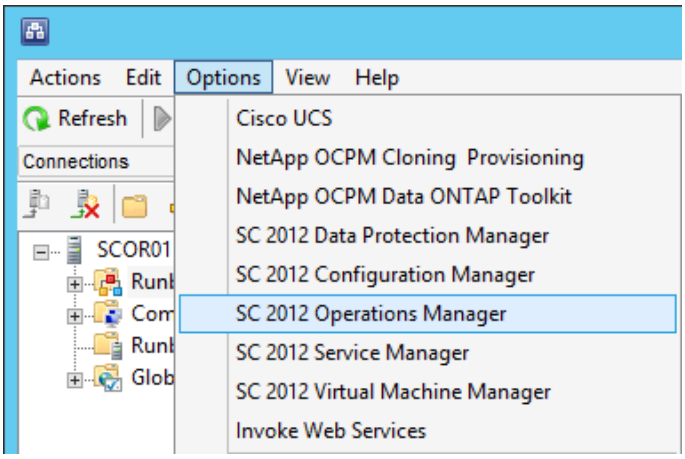
4. In the **Deploy Integration Packs or Hotfixes** dialog, select the check boxes integration packs folder created earlier and select the following integration packs:
    a. System Center 2012 Configuration Manager.
    b. System Center 2012 Data Protection Manager.
    c. System Center 2012 Operations Manager.
    d. System Center 2012 Service Manager.
    e. System Center 2012 Virtual Machine Manager.
    f. NetApp OnCommand Plug-In Data ONTAP Toolkit
    g. NetApp OnCommand Plug-In Disaster Recovery
    h. NetApp OnCommand Plug-In Cloning and Provisioning
    i. Cisco UCS Integration Pack
5. When complete, click **Next** to continue.



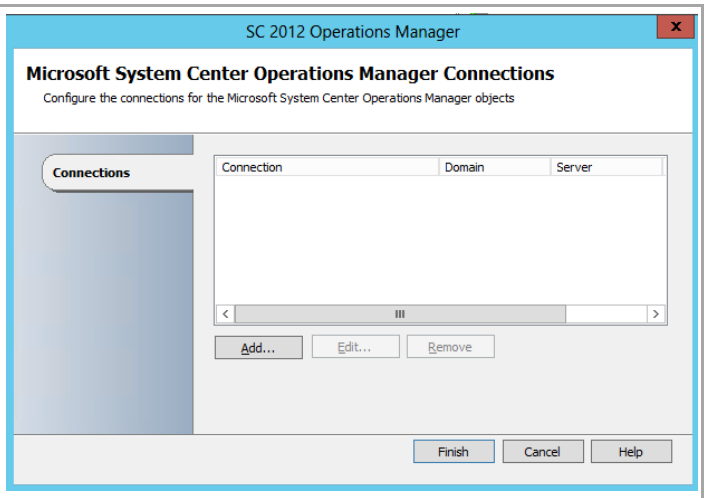
6. In the **Computer Selection Details**, type the name of the Orchestrator management server and click **Add**. When added, click **Next** to continue.	
7. In the **Installation Configuration** dialog, in the **Advanced Options** pane select **Stop all running Runbooks before installing the Integration Packs or Hotfixes** option. Click **Next** to continue.	
8. The **Completing the Integration Pack Deployment Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.	

9. During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.	 
10. From the **Start** screen, click the **Runbook Designer** tile.	

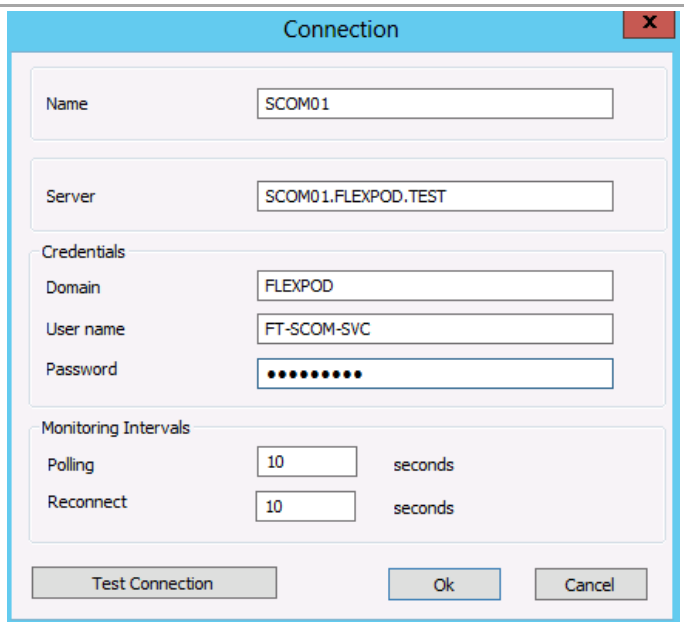
11. When complete, each integration pack will be displayed in the Runbook Designer interface.	
12. To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Virtual Machine Manager** option.	

13. In the Prerequisite Configuration dialog, click **Add.**	
14. 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.	
15. While still in the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Operations Manager** option.	

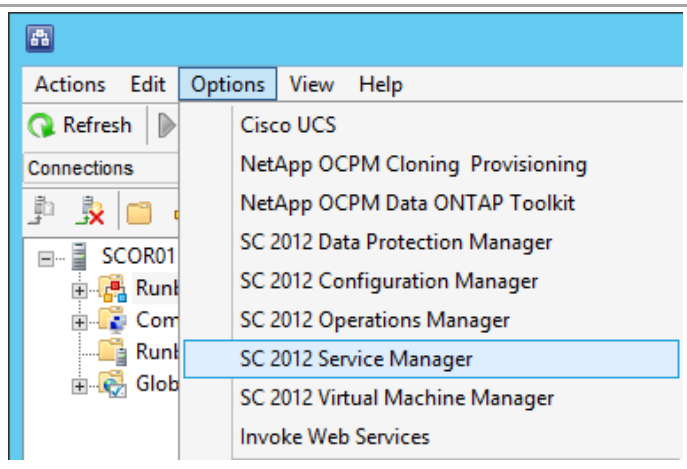
16. In the **Microsoft System Center Operations Manager Connections** dialog, click **Add.**



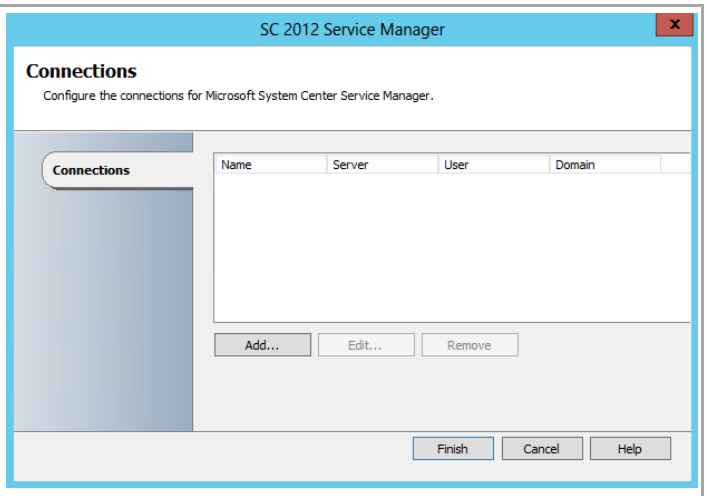
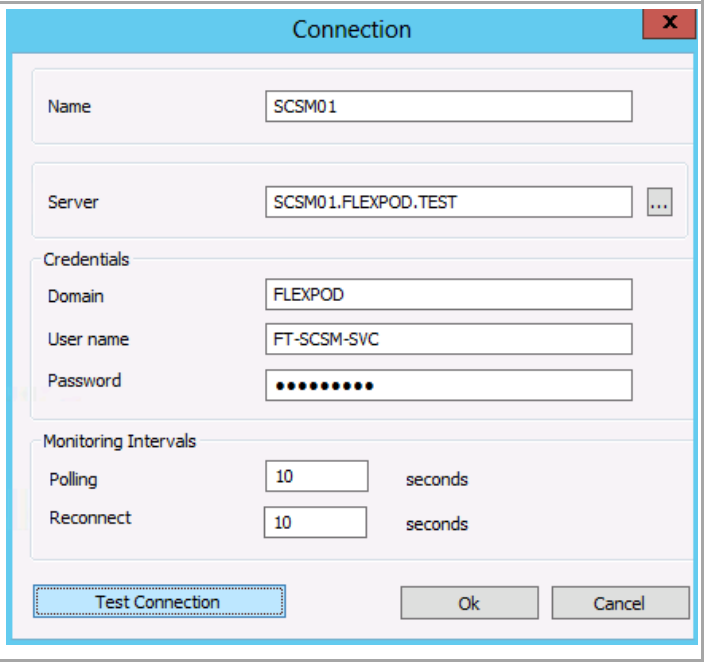
17. In the **MS System Center Operations Manager Connection Settings** dialog, fill in the required information for the Operations Manager management server and click **Test Connection**[23]. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.



18. In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **SC 2012 Service Manager** option.

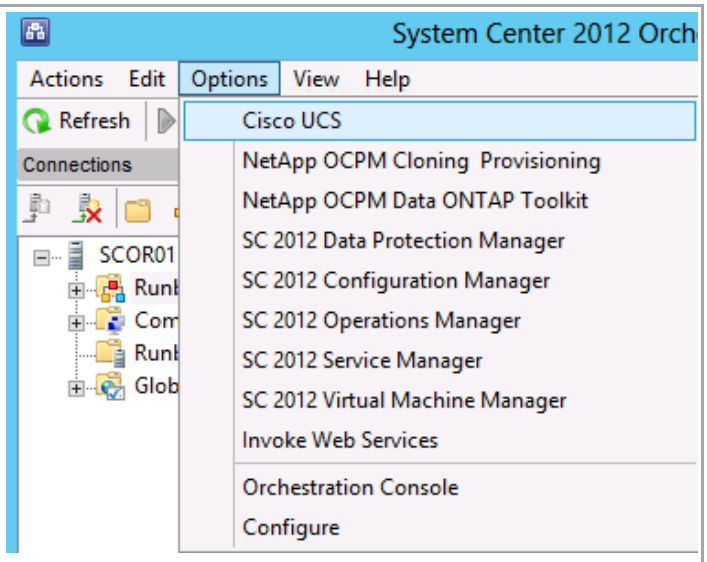


[23] The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

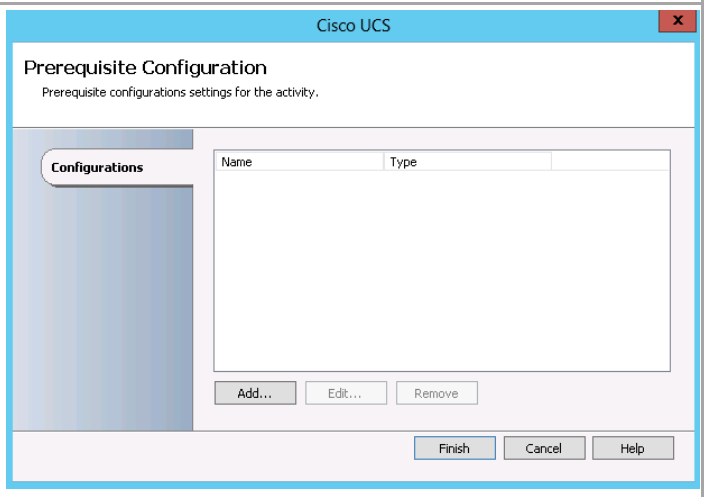
19. In the **Connections** dialog, click **Add.**	
20. In the **Connection** dialog, fill in the required information for the Operations Manager management server[24] and click **Test Connection**. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.	

[24] The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

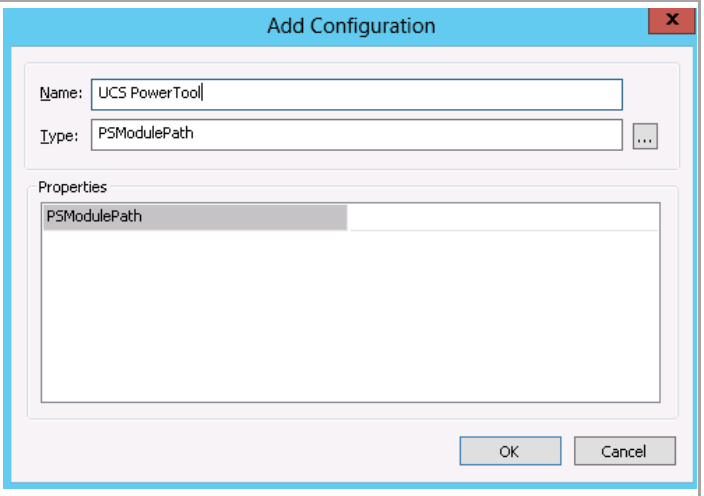
21. In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **Cisco UCS** option.

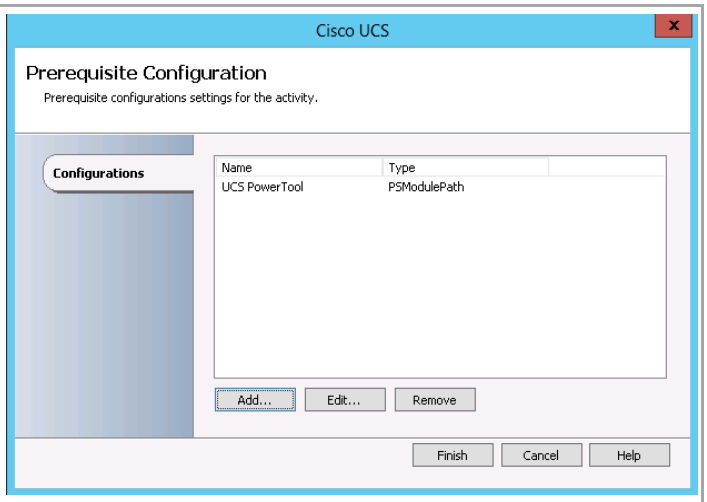


22. The Cisco UCS **Prerequisite Configuration** window opens. Click the **Add** button.



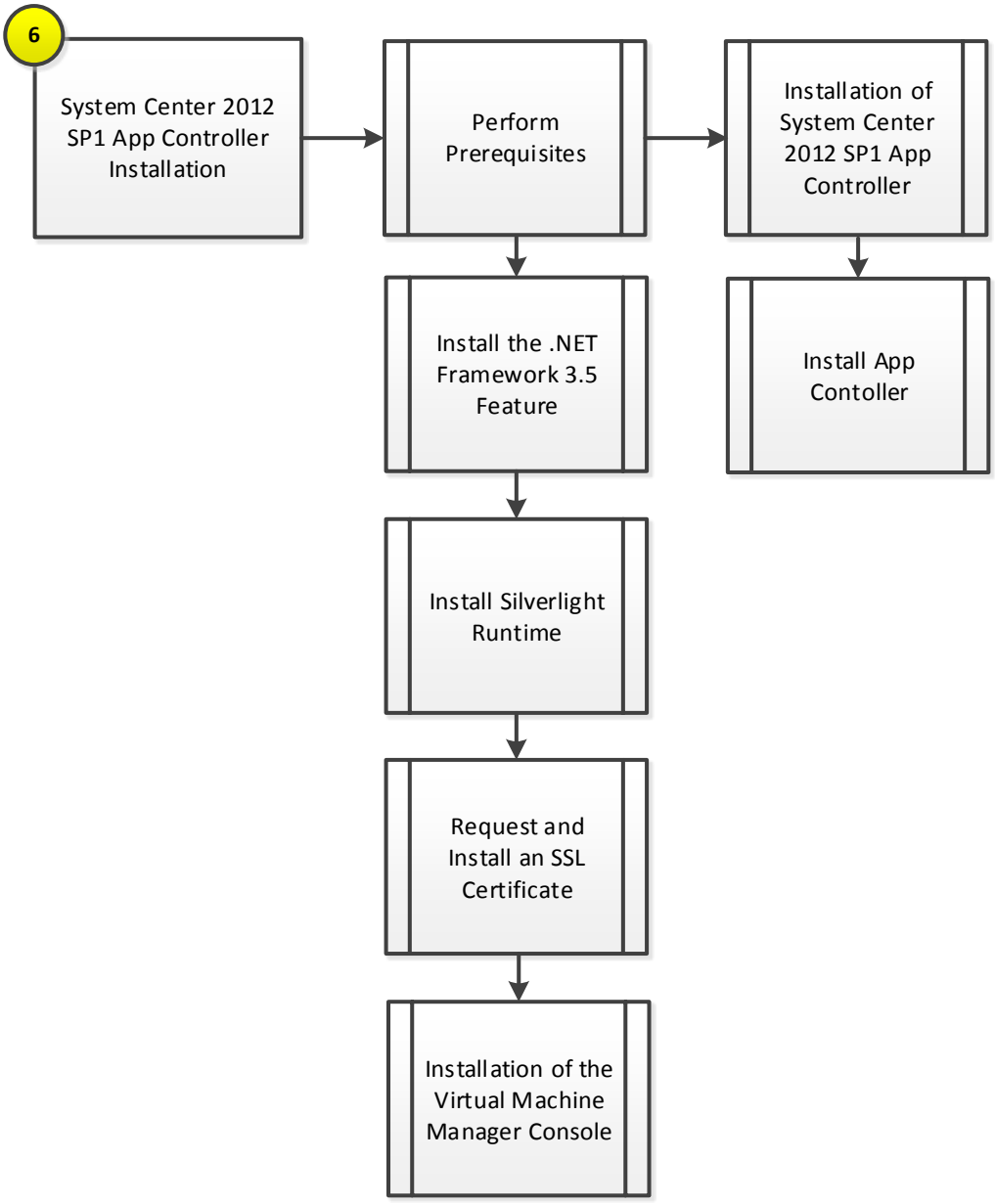
23. Type the configuration **name**. Click the "..." button and select **PSModulePath**. Click **OK** to accept the settings and close the windows.
24. Leave **PSModulePath** property blank to use default PowerTool installation or provide custom path of **CiscoUcsPS.psd1** file. Click OK to close the window.



25. Click **Finish** the save the setting and close the window.	

21 App Controller

The App Controller installation process includes the following high-level steps:


6
System Center 2012 SP1 App Controller Installation
Perform Prerequisites
Installation of System Center 2012 SP1 App Controller
Install the .NET Framework 3.5 Feature
Install App Contoller
Install Silverlight Runtime
Request and Install an SSL Certificate
Installation of the Virtual Machine Manager Console

21.1 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.

21.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

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-VMM-Admins

Groups

Verify that the following security groups have been created:

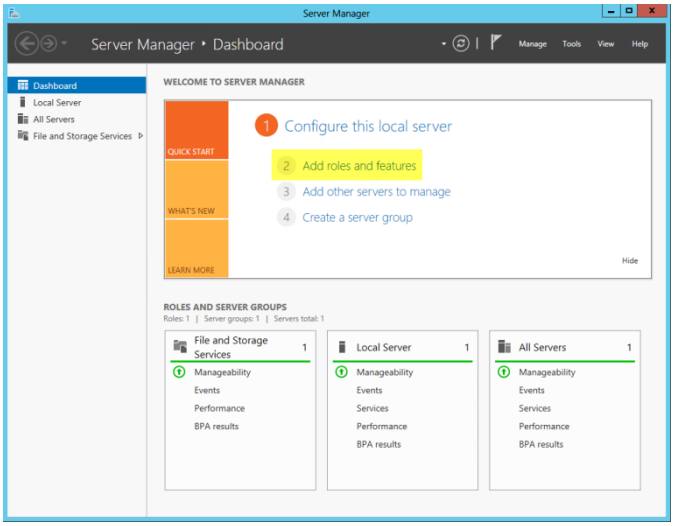
Group name	Purpose	Members
<DOMAIN>\ FT-SCAC-Admins	App Controller Admin group	<DOMAIN>\ FT-SCAC-SVC <DOMAIN>\ FT-VMM-Admins

Install the .NET Framework 3.5 Feature

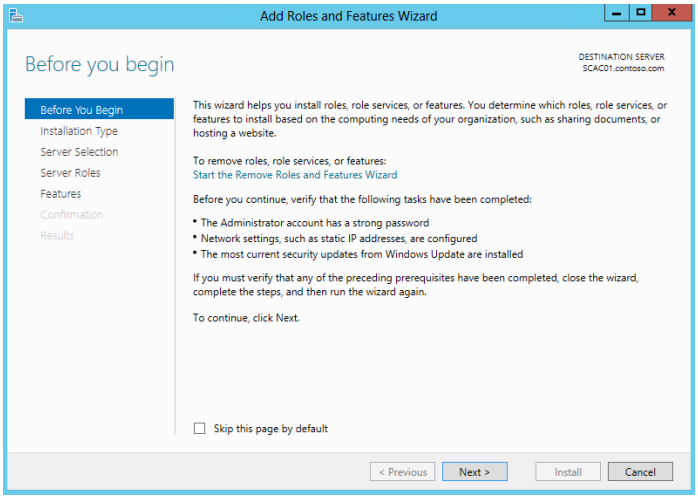
The App Controller installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

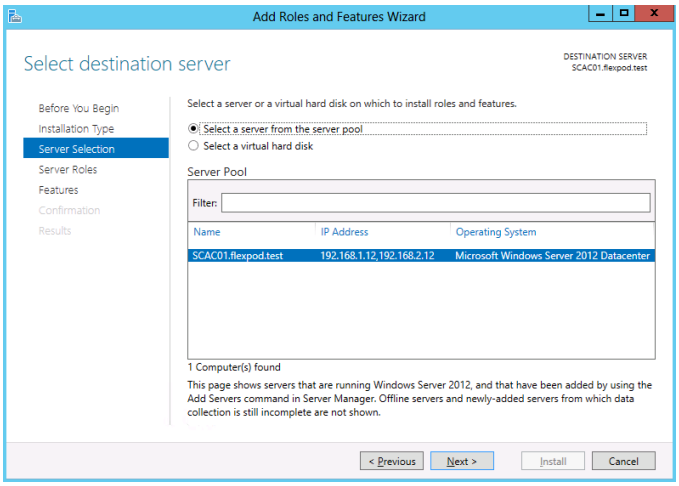
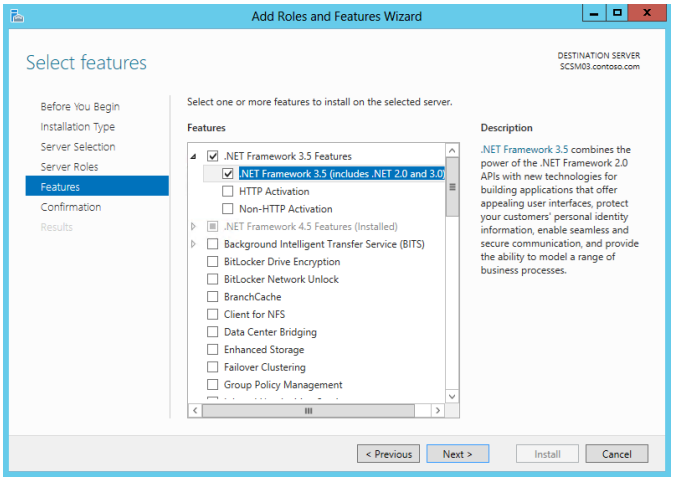
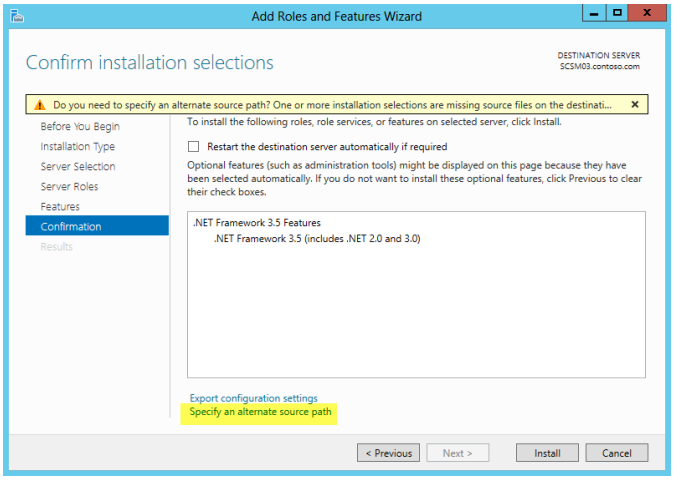
▶ Perform the following steps on the **App Controller** virtual machine.

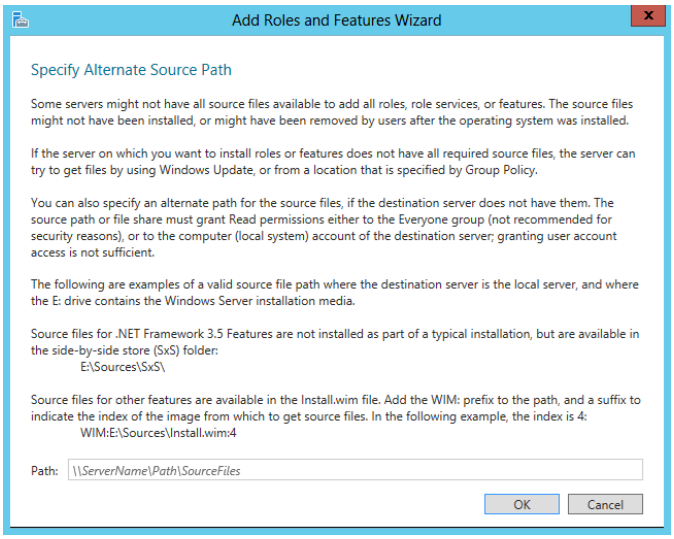
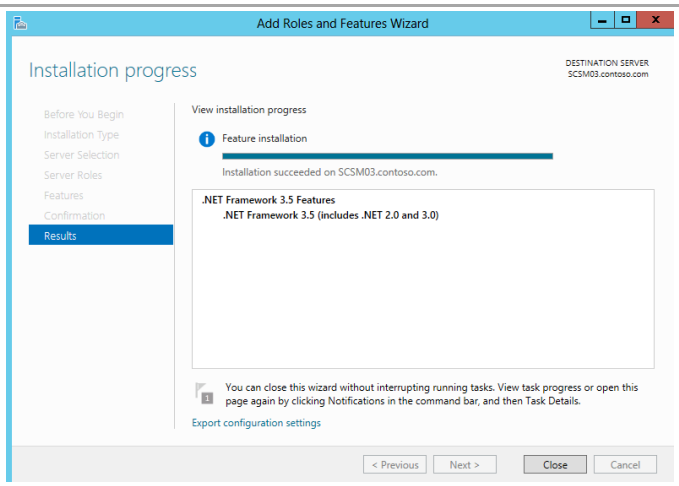
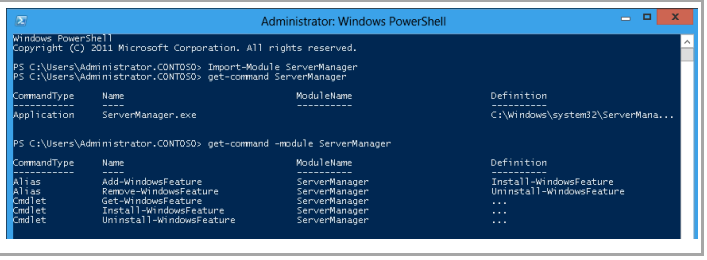
1. Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



2. 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.



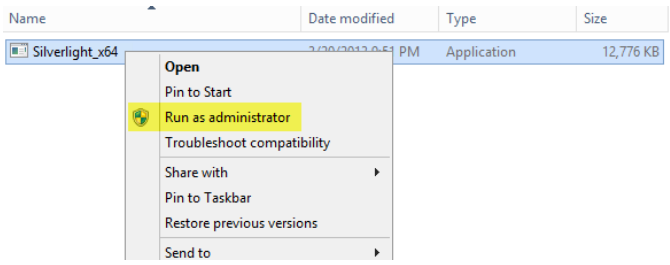
3. In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click Next for this installation, click the **Features** menu option to continue.	
4. To add the .NET Framework 3.5 Feature, in the **Select Features** 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.	
5. 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. When exported, this can be used in conjunction with the Server Manager PowerShell module to automate the installation of roles and features. Also, if the server does not have internet access an alternate source path can be specified by clicking the Specify and alternate source patch link.	

6. For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location must be specified for the installation.	
7. The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.	
8. 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

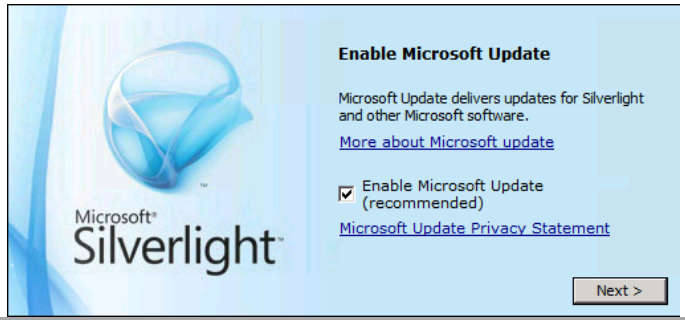
▶ Perform the following steps on the **App Controller** virtual machine.

1. From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.

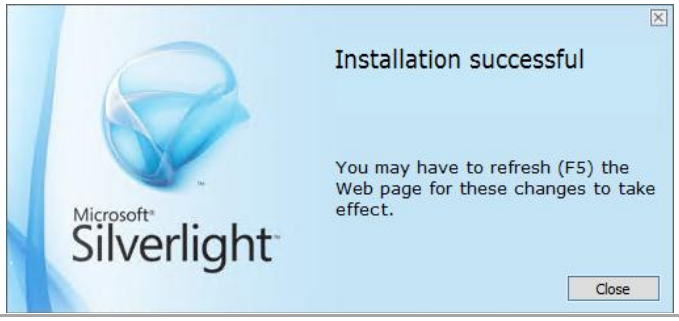


2. In the **Install Silverlight** dialog, click **Install now**.

3. In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.



4. In the **Installation Successful** dialog, click **Close** to exit the installation.

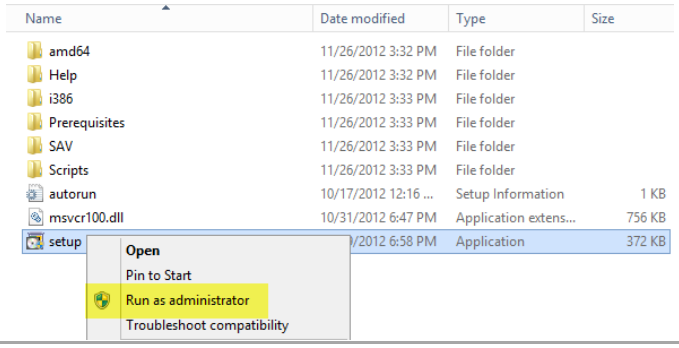


Install the Virtual Machine Manager Console

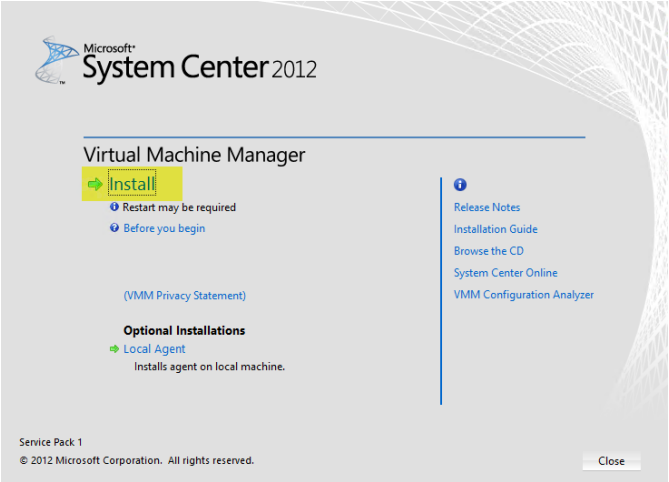
The following steps needs to be completed in order to install the Virtual Machine Manager console on the target App Controller virtual machine.

▶ Perform the following steps on the **App Controller** virtual machines.

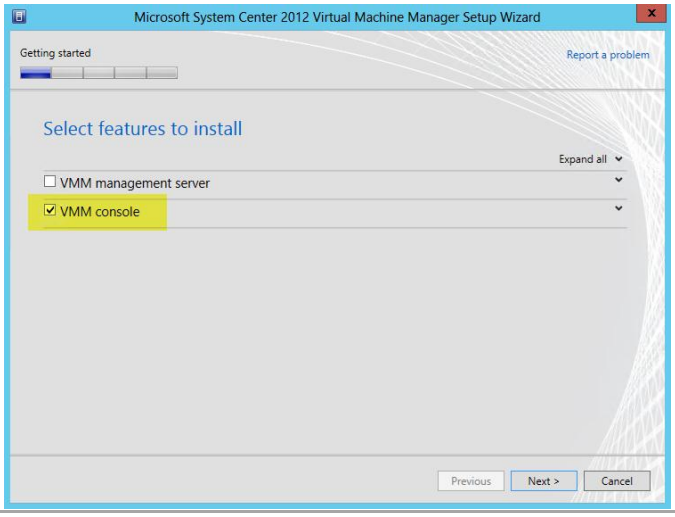
1. Log on to the App Controller server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

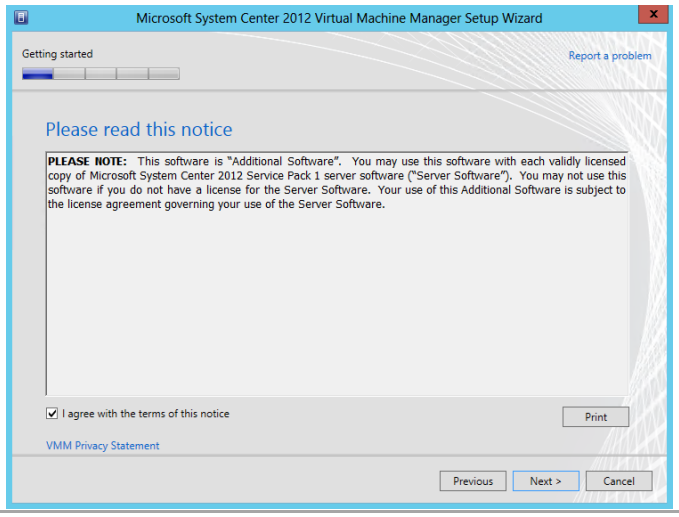
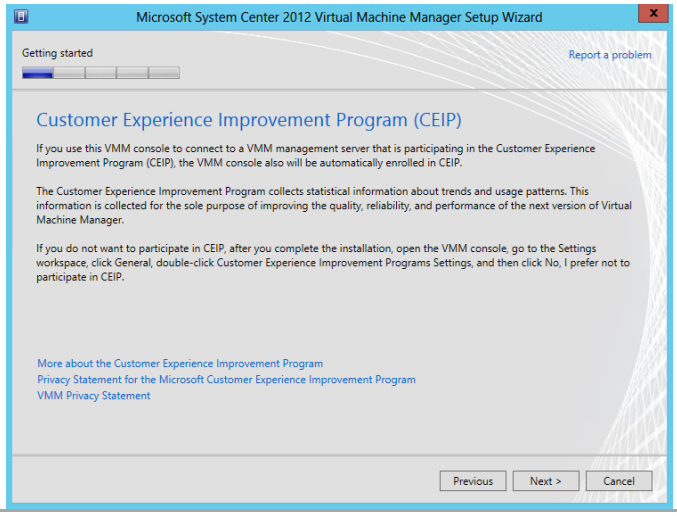


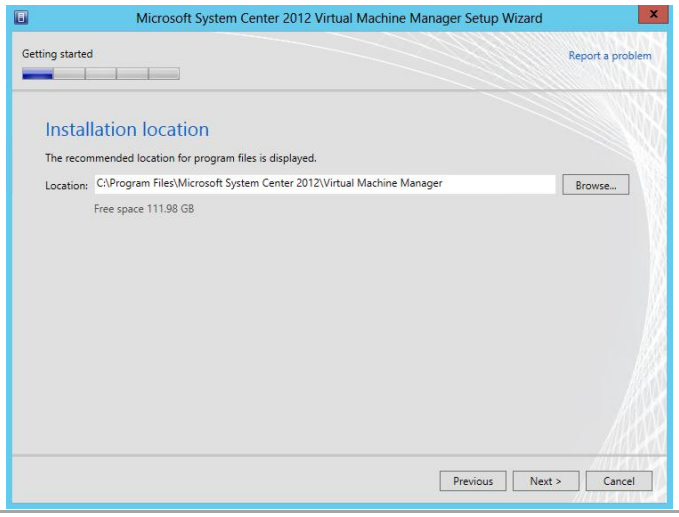
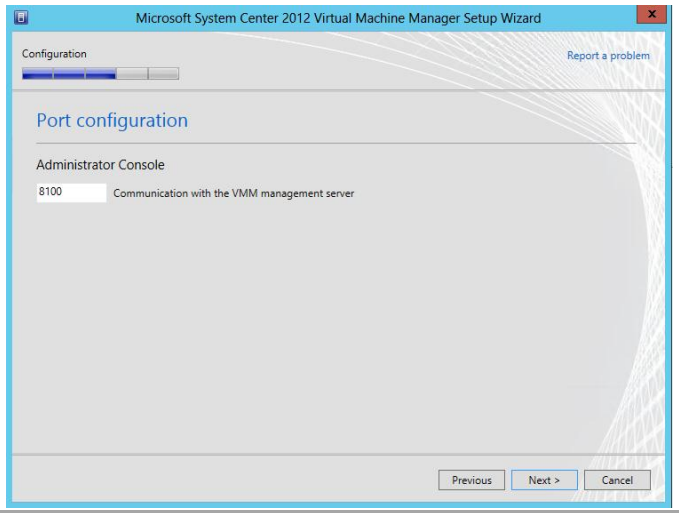
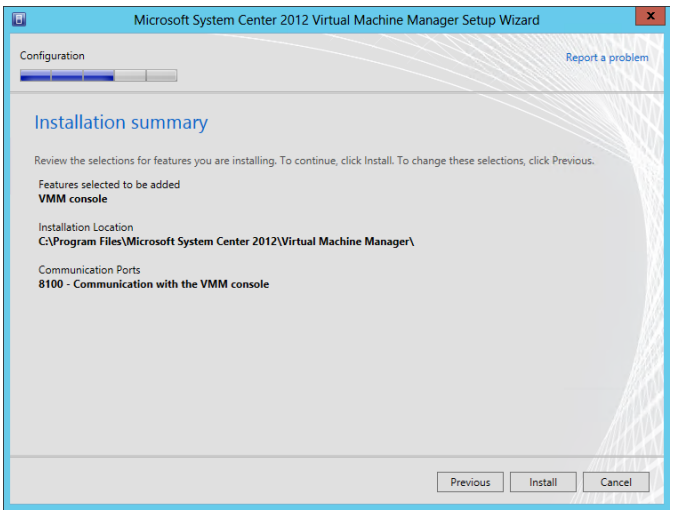
2. The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



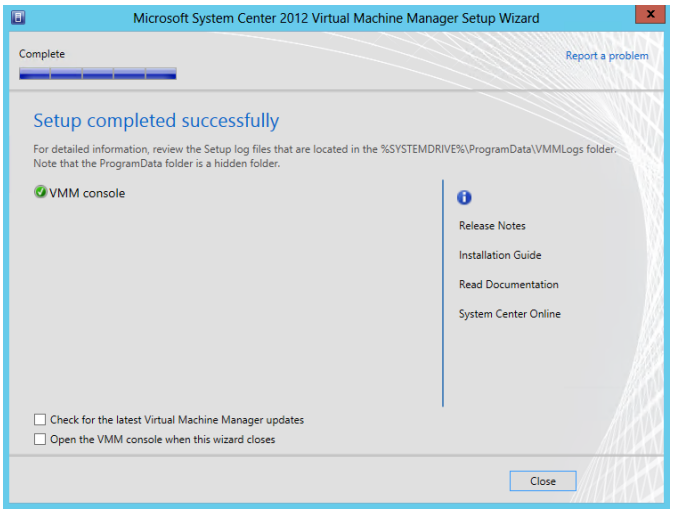
3. In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



4. 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.	
5. In the **Customer Experience Improvement Program** dialog, click **Next** to continue.	
6. 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.	

7. 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.	
8. 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.	
9. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	

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



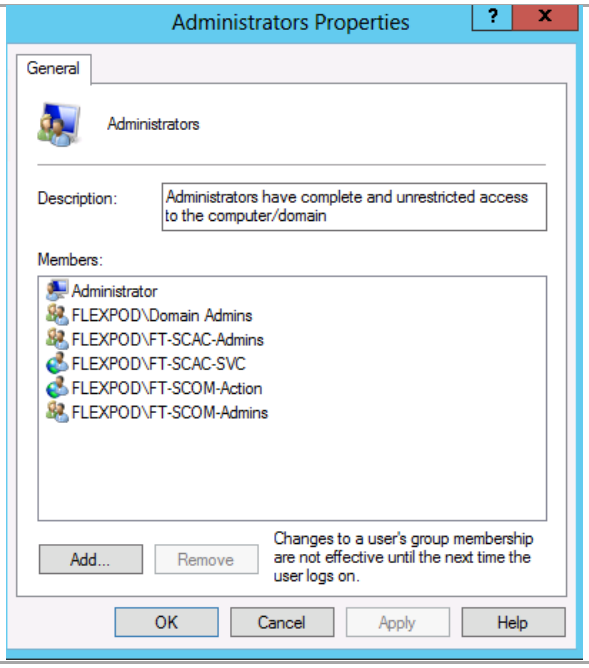
21.3 Installation

Install the App Controller Portal Server

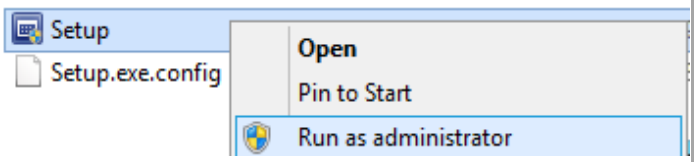
The following steps need to be completed in order to install App Controller.

▶ Perform the following steps on the **App Controller** virtual machine.

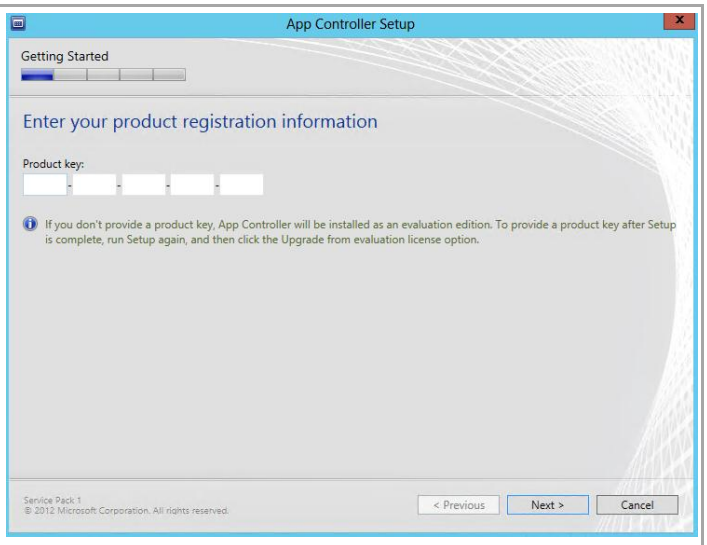
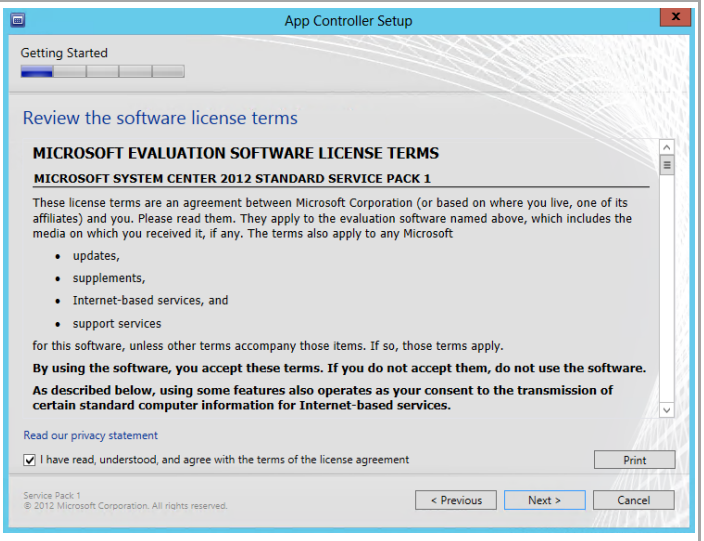
1. Log on to the App Controller virtual machine with a user with local admin rights.
2. Verify the following accounts and/or groups are members of the Local Administrators group on the App Controller portal virtual machine:
   - Fast Track Operations Manager action account.
   - Fast Track Operations Manager Admins group.
   - Fast Track App Controller service account.
   - Fast Track App Controller Admins group.



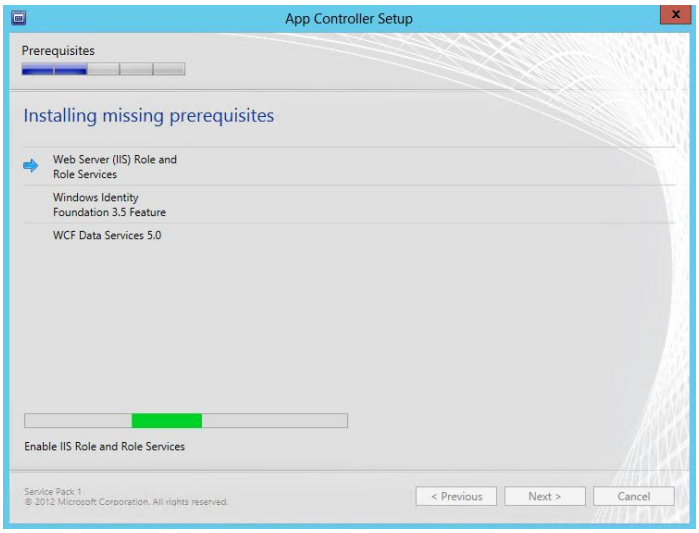
3. Log on to System Center App controller server. From the **System Center App Controller** installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



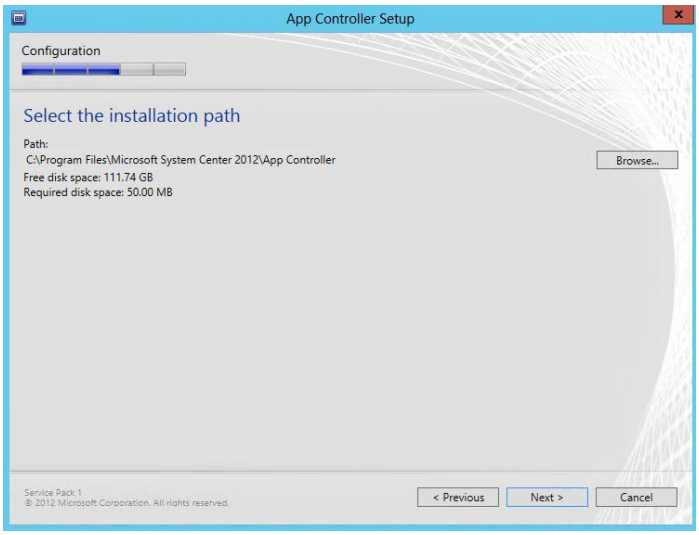
4. The **App Controller Setup** wizard will begin. At the splash page, click **Install** begin the App Controller server installation.

5. 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.	
6. 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.	
7. 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.	

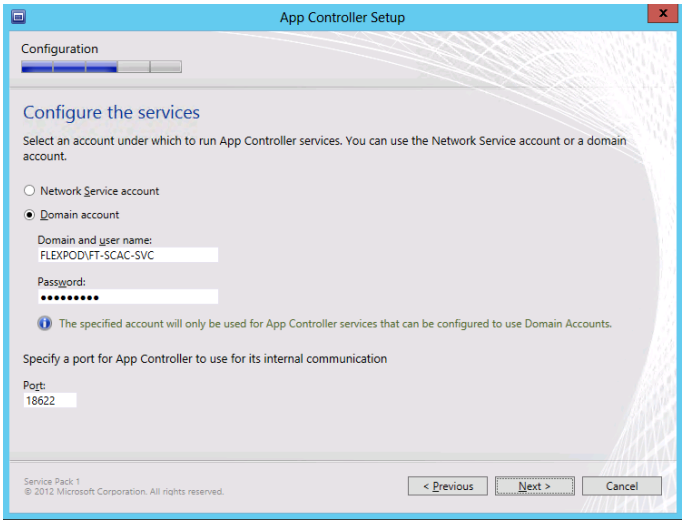
8. The wizard will detect missing roles and software and attempt installing the missing prerequisites.



9. 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.



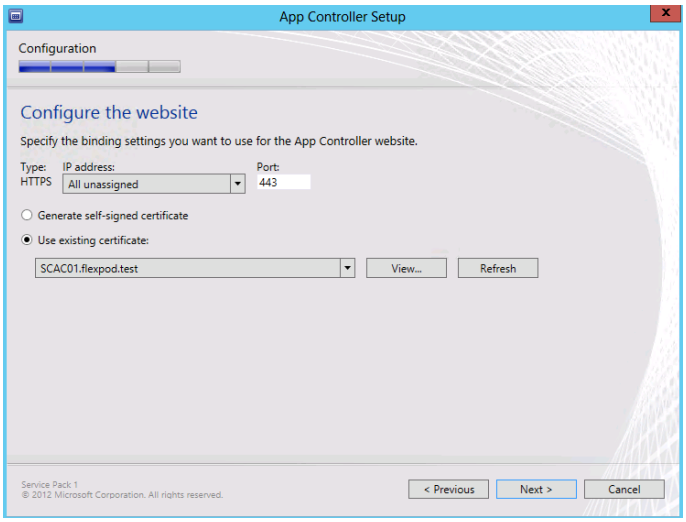
10. In the **Configure the services** dialog, verify that the **Domain account** option is selected and specify the App Controller service account in the **Domain and user name** text box. Provide the associated **Password** in the supplied text box.
11. In the **Port** text box, accept the default TCP port of 18622 or change the port to meet your organization's requirements. In most cases the default port selection should be kept.
12. When complete, click **Next** to continue.



13. 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.

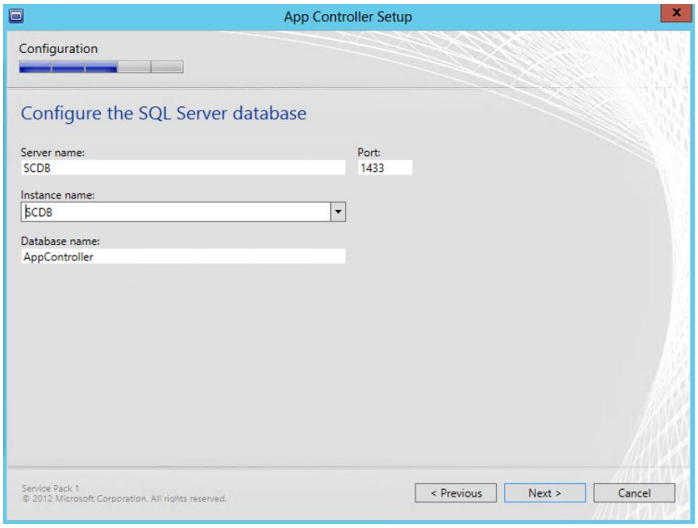
14. When complete, click **Next** to continue.

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.



15. 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.*

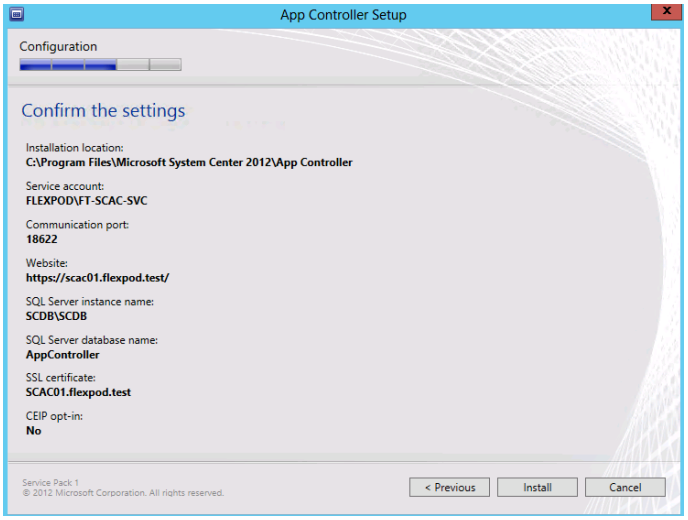
16. Click **Next** to continue.



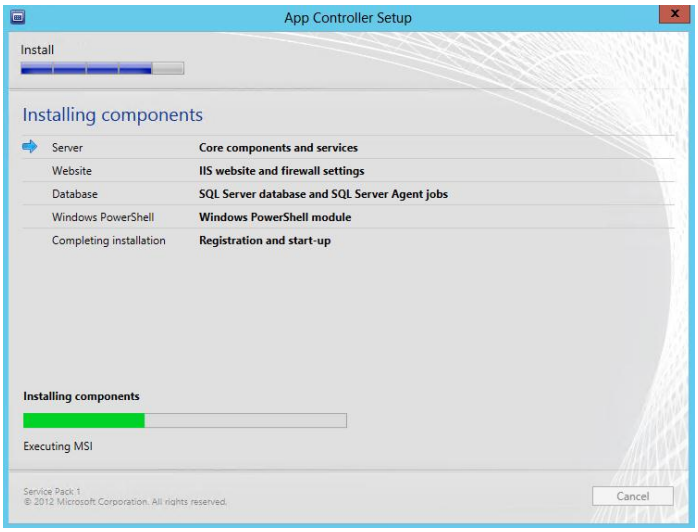
17. The **Help Improve App Controller for System Center 2012** dialog provides options for participating in various product feedback mechanisms. These include:
    - **Customer Experience Improvement Program (CEIP)**
    - **Microsoft Update**

18. Select the appropriate option based on your organization's policies and click **Install** to continue.

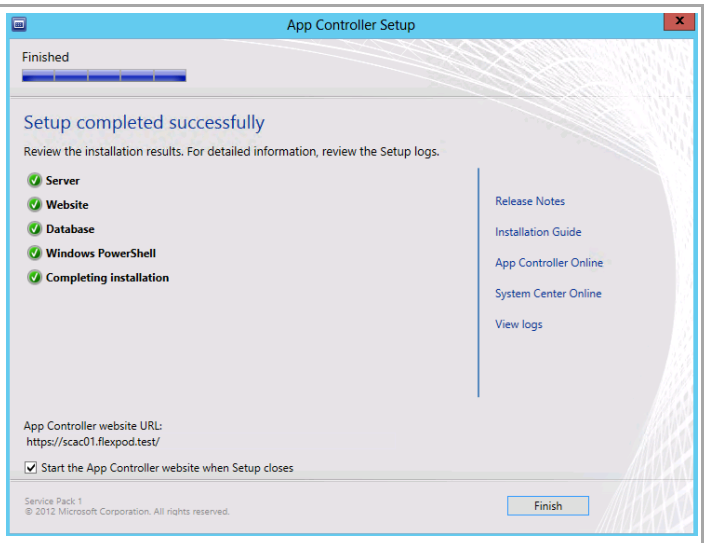
19. In the **Confirm the settings** dialog, verify the settings provided during the installation wizard and click **Install** to begin the installation.



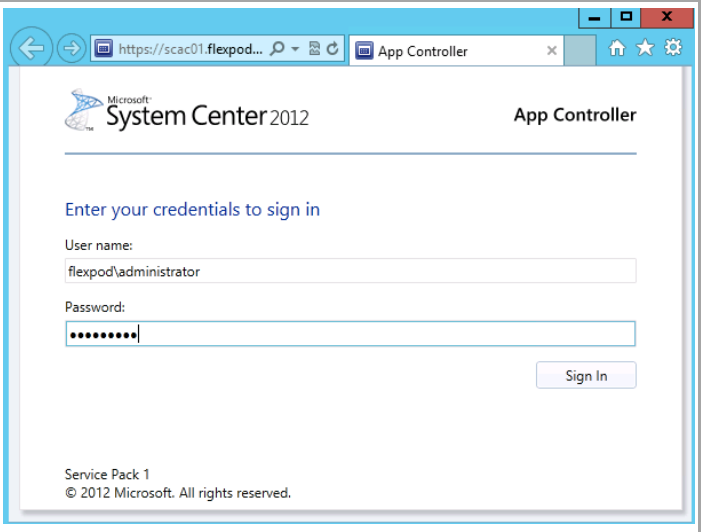
20. The required components will install and progress of the installation will be provided in the wizard.



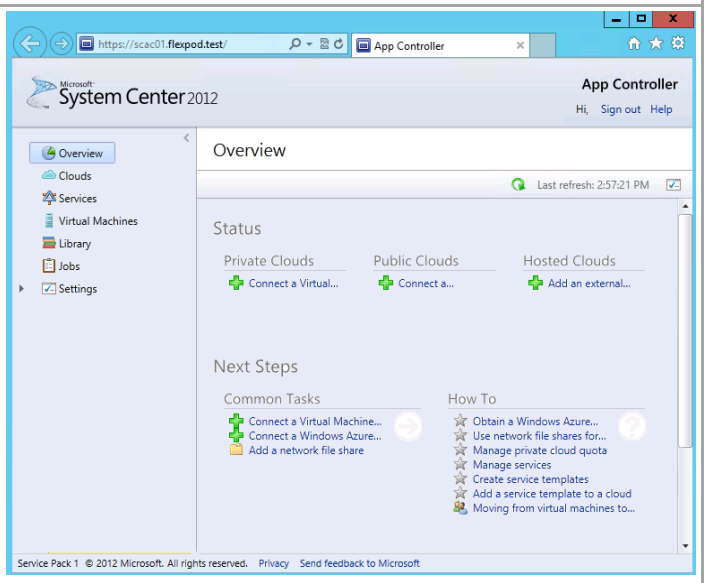
21. When complete, the **Setup completed successfully** dialog will appear with progress of each component. Verify that each component successfully. Note the App Controller website in the provided text box.
22. Verify that the **Start the App Controller website when Setup closes** check box is selected and click **Finish**.



23. 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). When complete, click **Sign in**.

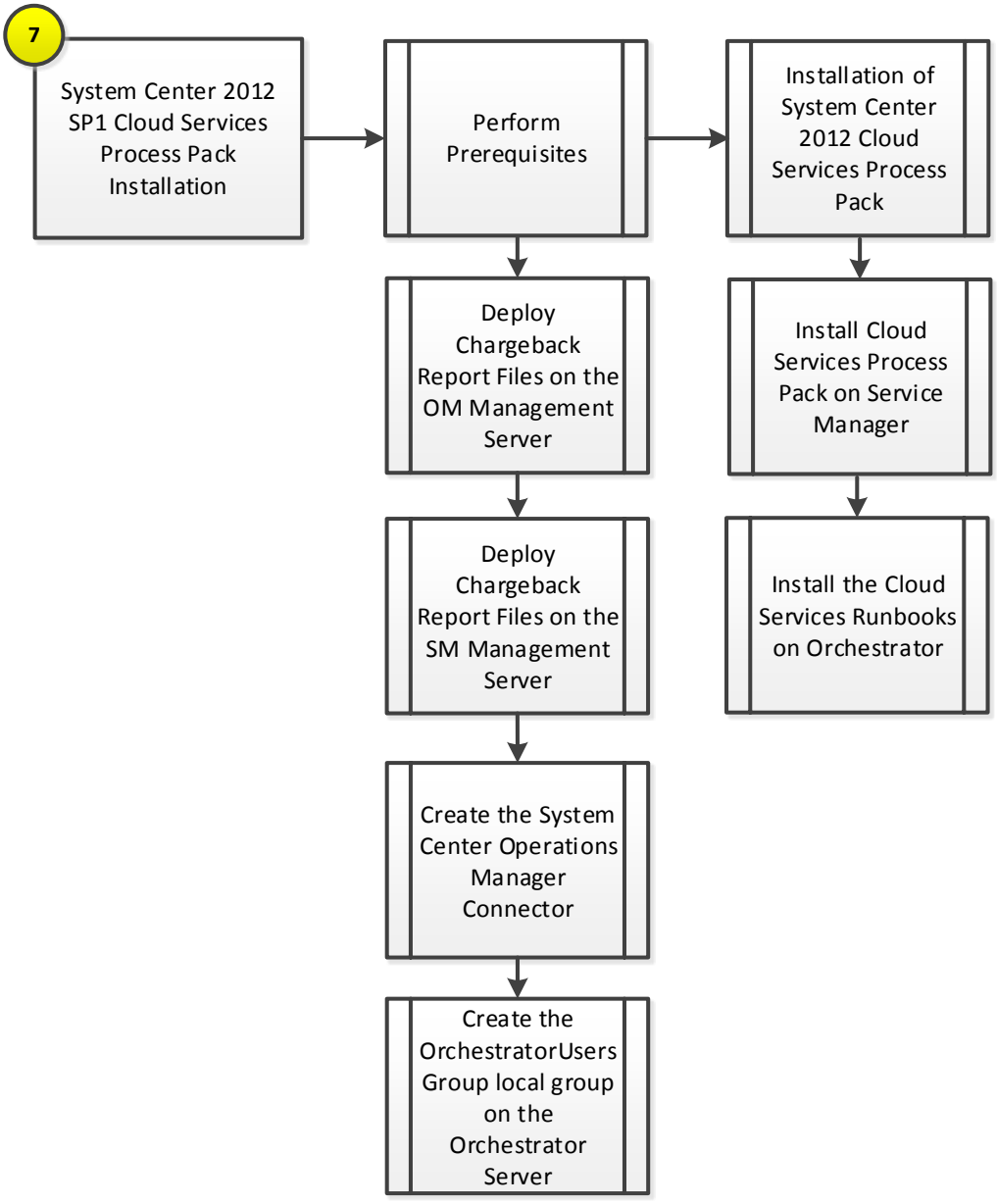


24. The App Controller portal will appear. After validating functionality, the App Controller installation is considered complete.



22 System Center Cloud Services Process Pack

The Cloud Services Process Pack installation process includes the following high-level steps:



22.1 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.

22.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

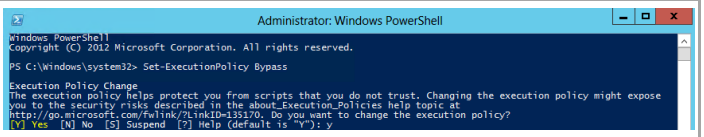
Deploy Chargeback Report Files on the Operations Manager Management Server

▶ Perform the following steps on the **Operations Manager management server** virtual machine.

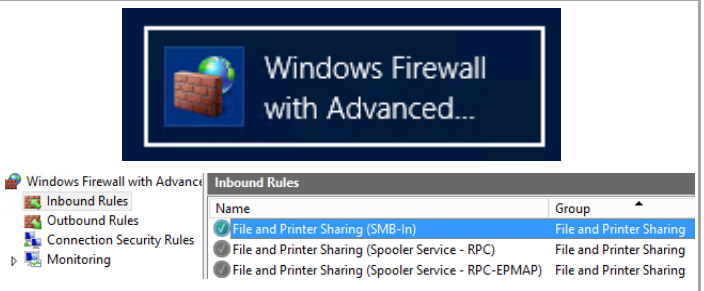
1. From an elevated PowerShell prompt, configure the execution policy to Bypass.

```
Set-ExecutionPolicy Bypass
```

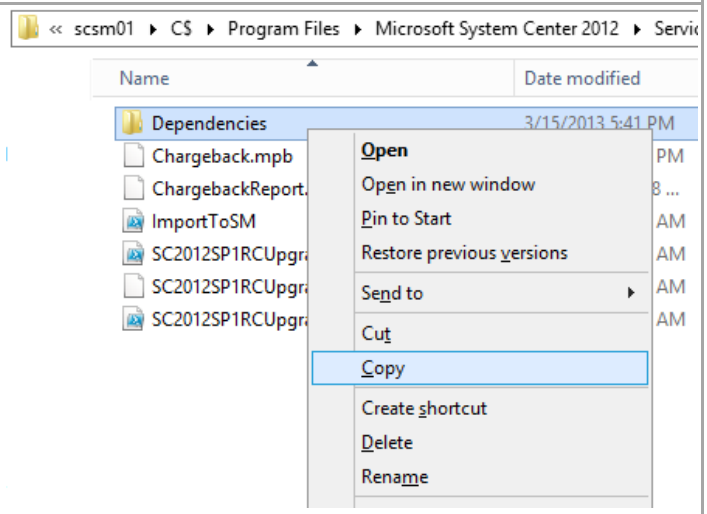
Note: When installation is complete, execution policy should be configured to a more secure level within the organization.

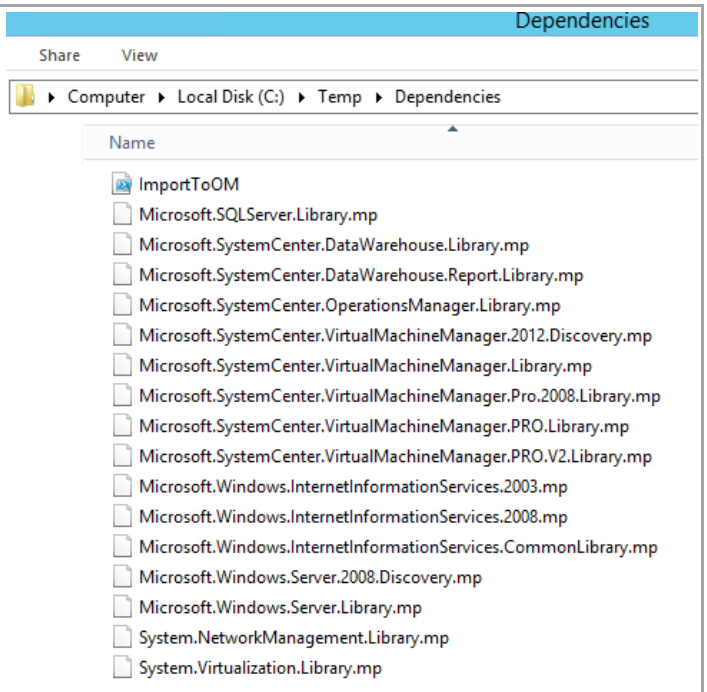
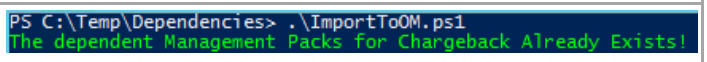


2. Open the **Windows Firewall with Advanced Security** MMC console.
3. Within the W**indows Firewall with Advanced Security** MMC console, select the **Inbound Rules** node and enable the **File and Printer Sharing (SMB-In)** rule from the action pane.



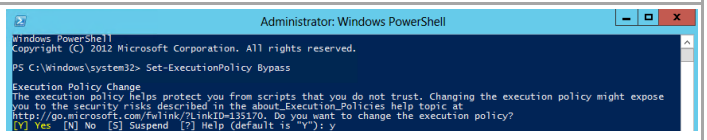
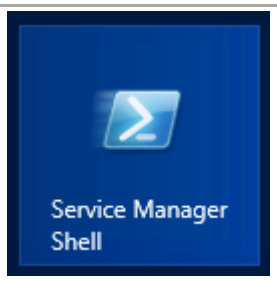
4. Connect to the administrative share where %ProgramFiles% resides on the Service Manager management server. Copy the **Dependencies** folder from the %ProgramFiles%\Microsoft System Center 2012\Service Manager\ Chargeback installation folder on the remote Service Manager management server.

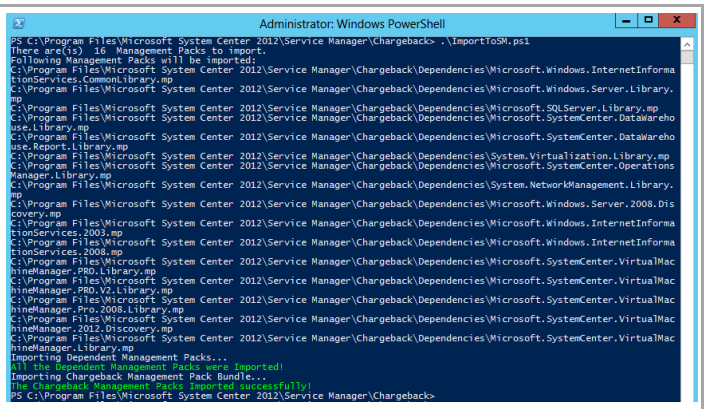
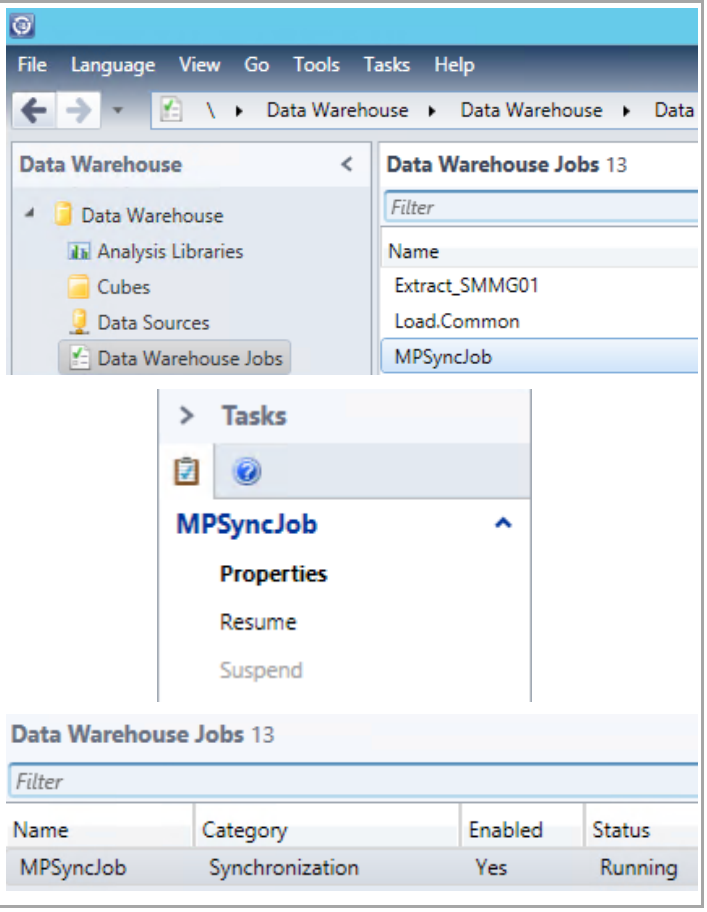


5. Copy the **Dependencies** folder to a temporary directory on the Operations Manager management server.	
6. From the same elevated PowerShell session, navigate to the **Dependencies** folder which was copied locally and execute the ImportToOM.ps1 PowerShell script. In some cases the dependent management 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** (SCSM01) virtual machine.

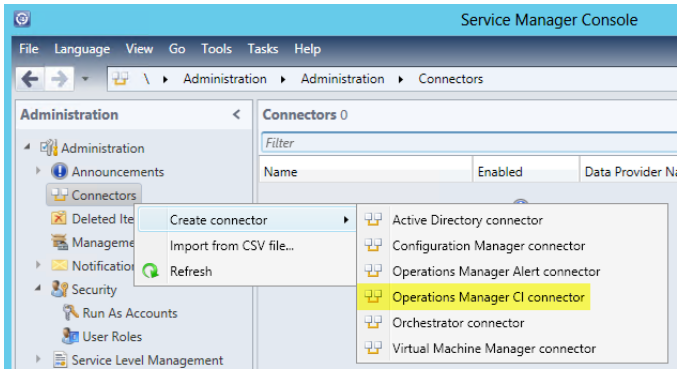
1. From an elevated PowerShell prompt, configure the execution policy to Bypass. `Set-ExecutionPolicy Bypass` **Note**: When installation is complete, execution policy should be configured to a more secure level within the organization.	
2. From the **Start** screen, select the **Service Manager Shell** tile and run this as an administrator.	

3. In the elevated **Service Manager Shell** dialog, navigate to %ProgramFiles%\Microsoft System Center 2012\Service Manager\Chargeback and execute the **ImportToSM.ps1** script. When completed, close the console.	
4. 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.	

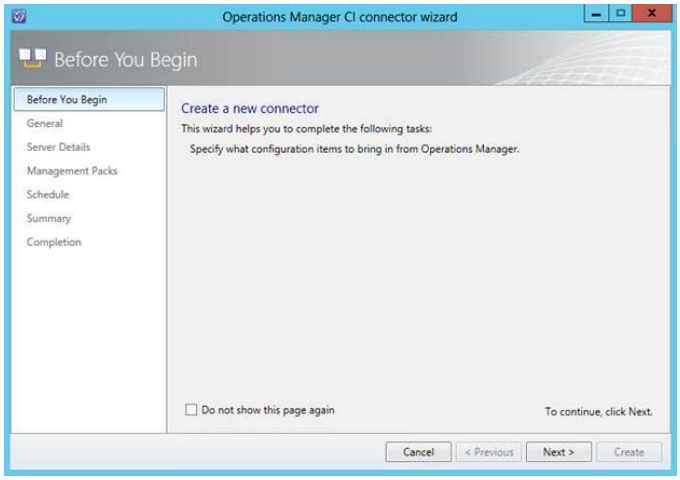
Create the System Center Operations Manager Connector

▶ Perform the following steps on the **Service Manager management server** virtual machine.

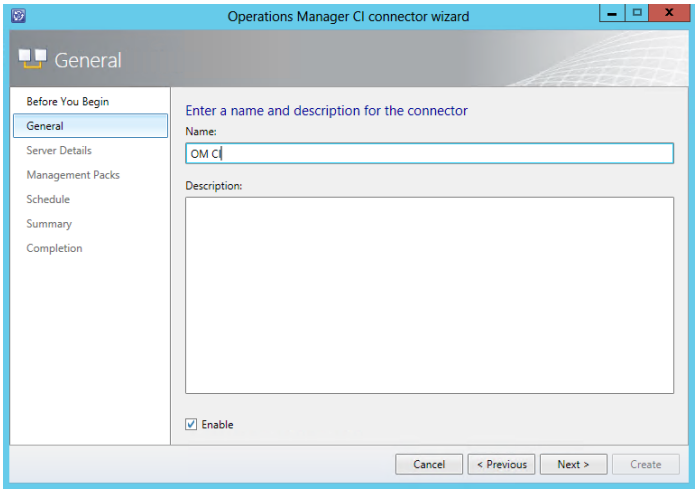
1. Open the **Service Manager Console**, select **Administration** from the navigation tree and navigate to the **Cloud Services** node.
2. In the Getting Started pane, click **Create an Operations Manager Connector**.



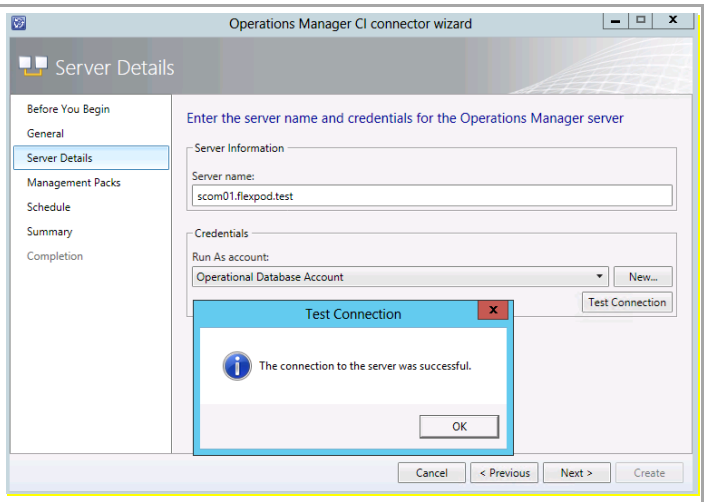
3. In the **Befor you Begin** dialog, click **Next** to continue.



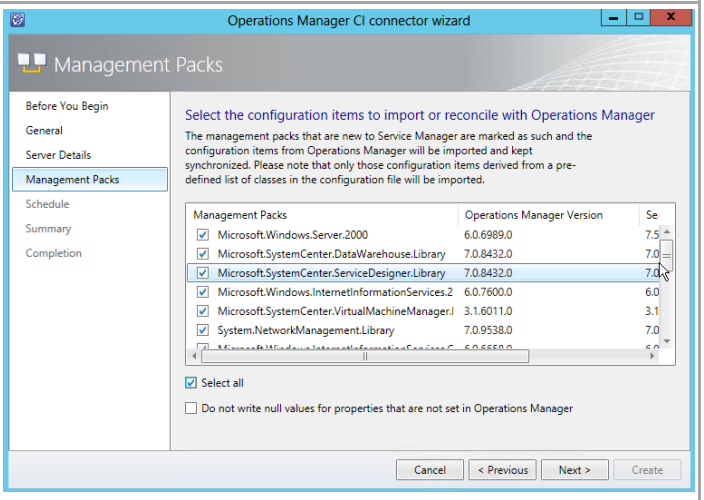
4. The **Operations Manager CI connector** wizard will appear. In the **General** dialog, type a descriptive name for the connector in the **Name** textbox. Verify the **Enable** checkbox is selected. Click **Next** to continue.



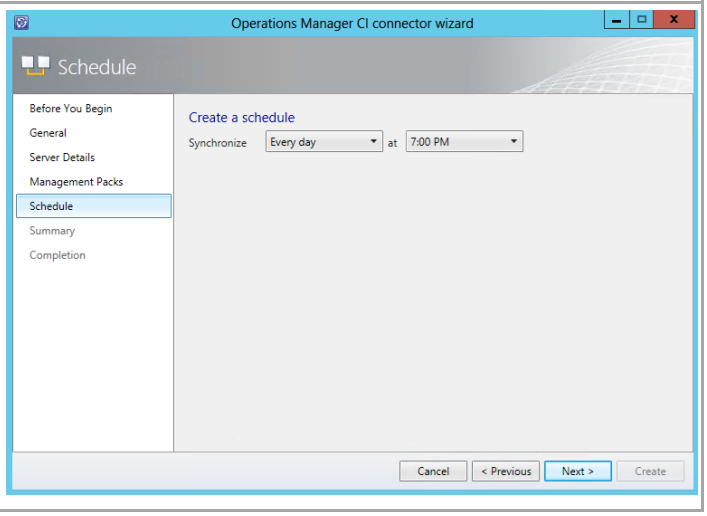
5. In the **Server Details** dialog, type the FQDN of the Operations Manager server in the **Server Name** textbox. In the **Credentials** section, click the **New...** button and create a Run As account using the **FT-SCOM-SVC** account. Click Test Connection to verify the connection. Click **Next** to continue.

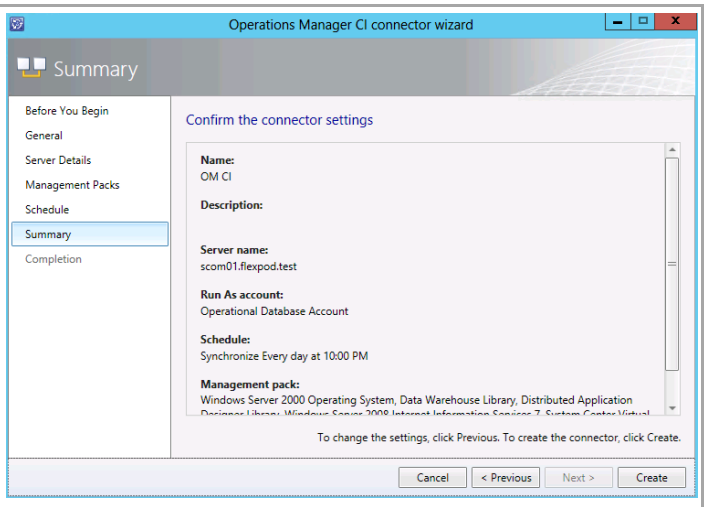
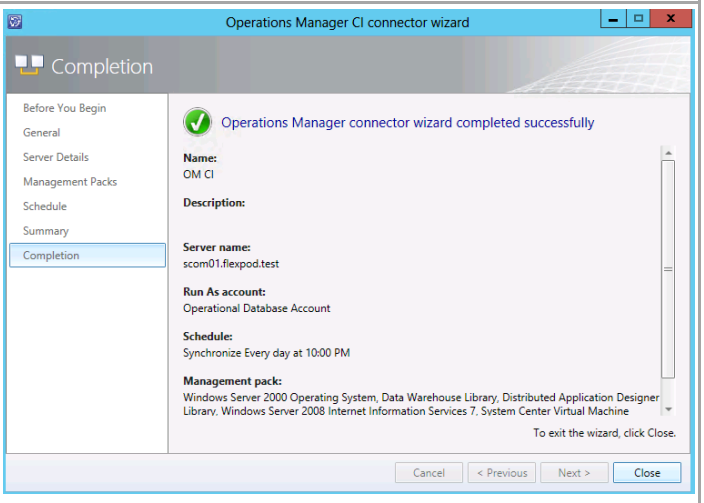
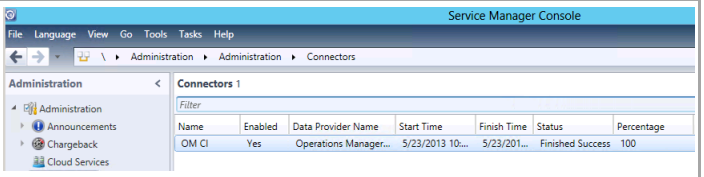
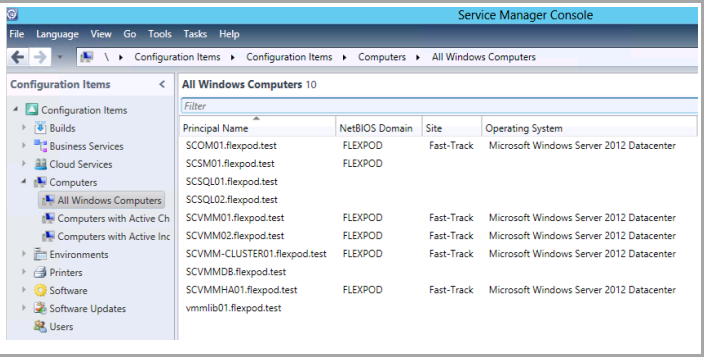


6. In the **Management Packs** dialog, select the **Select All** checkbox. Click **Next** to continue.



7. In the **Schedule** dialog, create a schedule for the connector or leave the defaults. Click **Next** to continue.



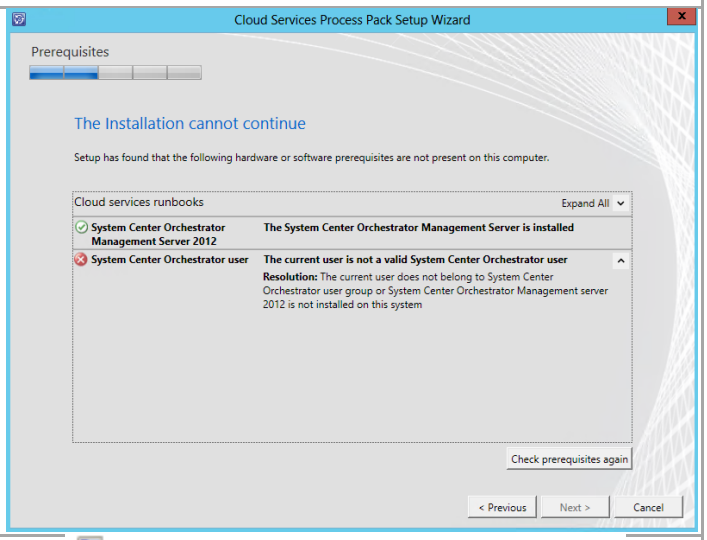
8. In the **Summary** dialog, verify the selections made and click **Create** to create the connector.	
9. In the **Completion** dialog, verify the process completes successfully and click **Close**.	
10. When created, verify the Connector has a successful run by checking that there is a time listed in the **Finish Time** column.	
11. 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

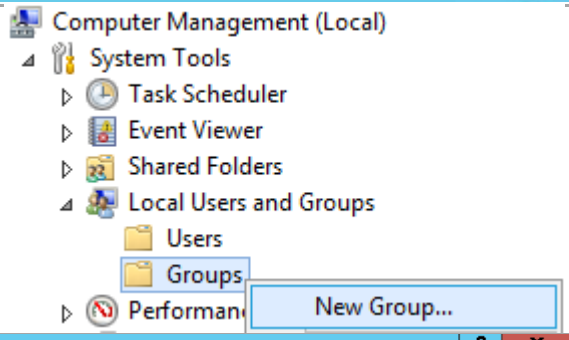
Perform the following steps to avoid issues related to CSPP setup on Orchestrator.

▶ Perform the following steps on both **Orchestrator** virtual machines.

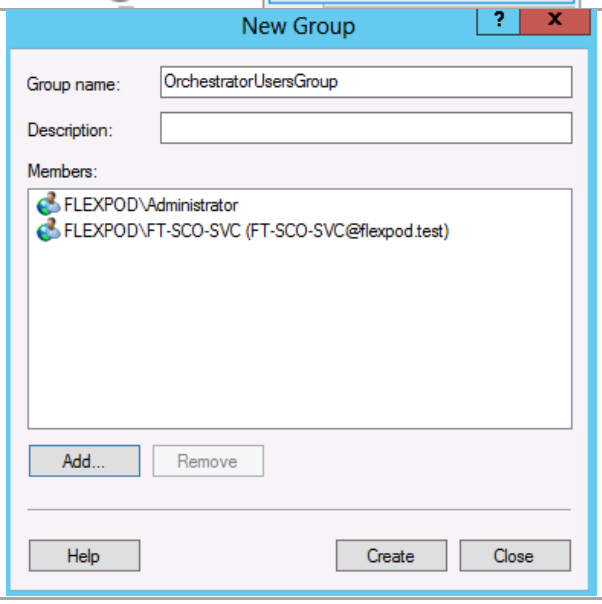
1. The pre-requisite checker in CSPP validates settings in Orchestrator, but during its process it verifies if the logged in user is directly a member of a local security group called "**OrchestratorUsersGroup**", regardless of how security for Orchestrator is configured. Per the recommended configuration 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[25].



2. 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.



3. 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.



25 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

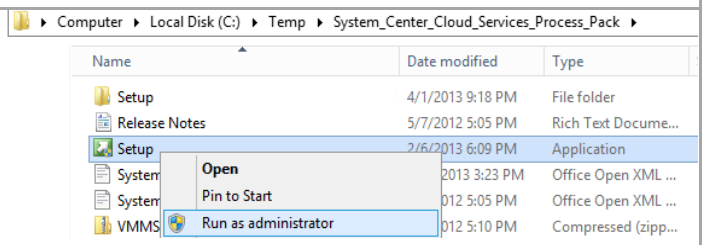
22.3 Installation

Install the Cloud Services Process Pack

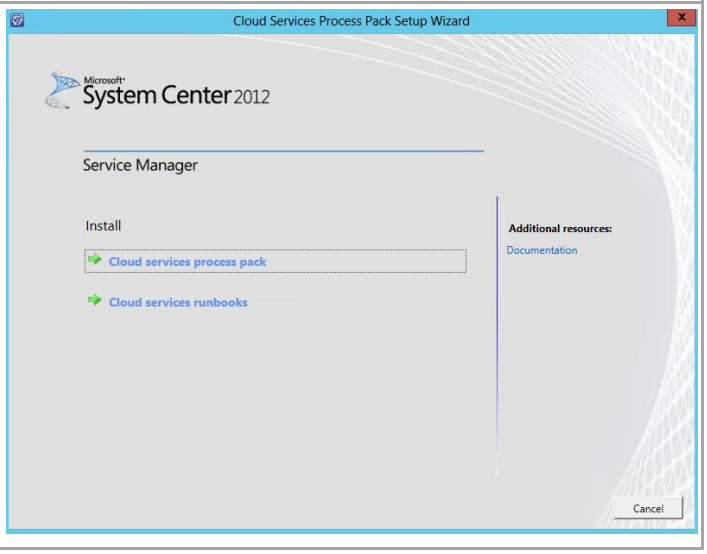
The following steps needs to be completed in order to install the Cloud Services Process Pack.

▶ Perform the following steps on the **Service Manager management server** (SCSM01) virtual machine.

1. Log on to the Service Manager management server virtual machine with a user with local admin rights.
2. Verify the account has the following rights:
   - A Service Manager administrator.
   - An administrator on the server that is running Service Manager.
3. After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and run **Setup.exe** as an Administrator.

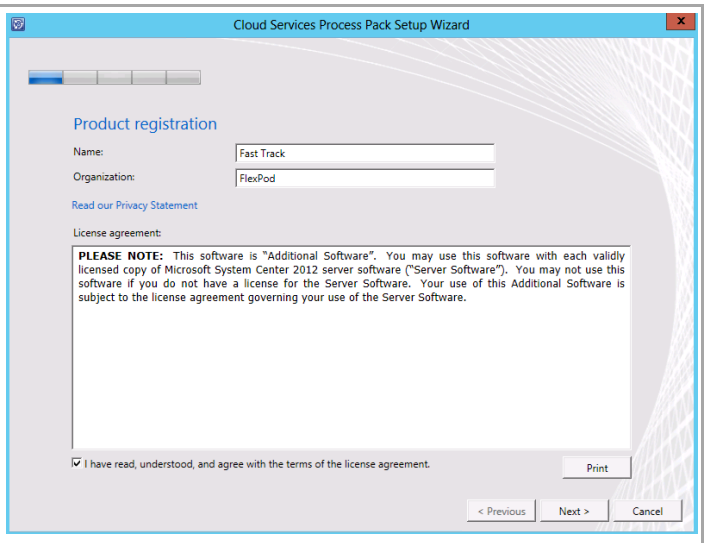


4. The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud services process pack.

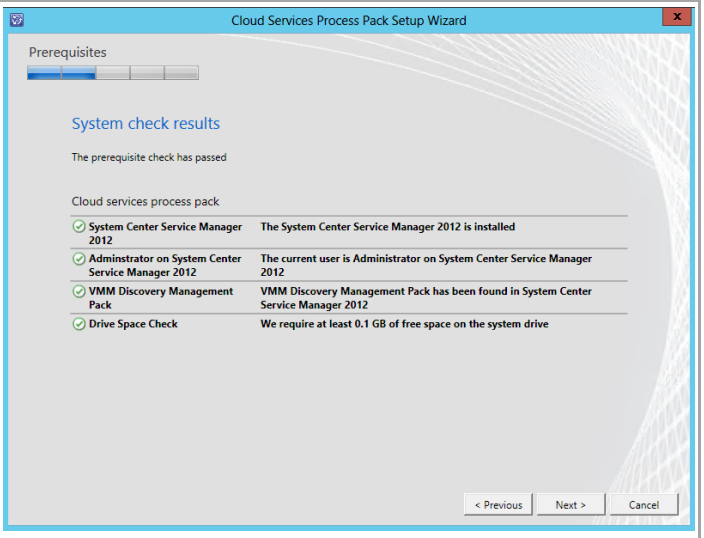


5. In the **Product registration information** dialog, enter the following information in the provided text boxes:
   - **Name** – *specify the name of the primary user or responsible party within your organization.*
   - **Organization** - *specify the name of the licensed organization.*

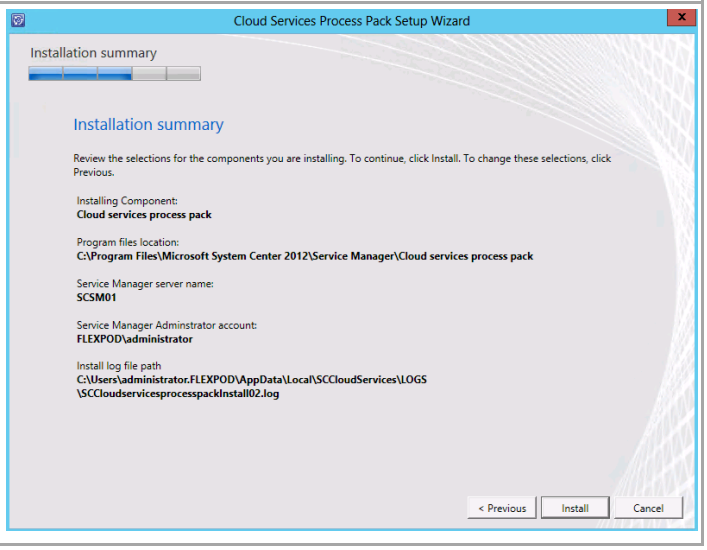
6. Click **Next** to continue.



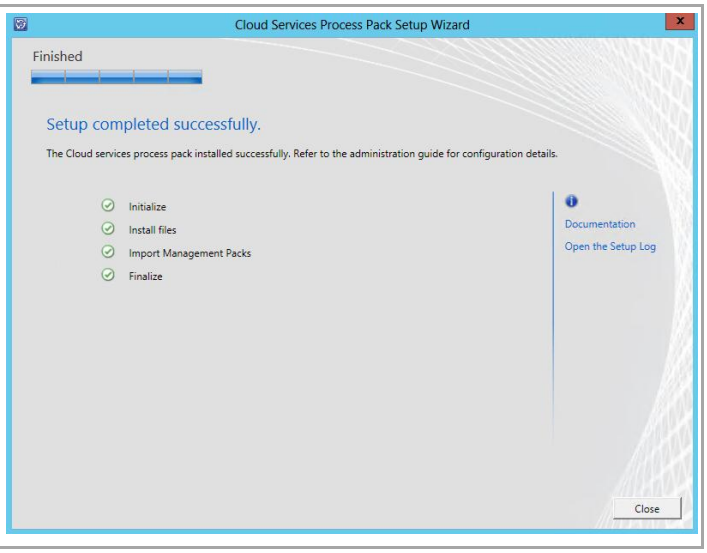
7. The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



8. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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

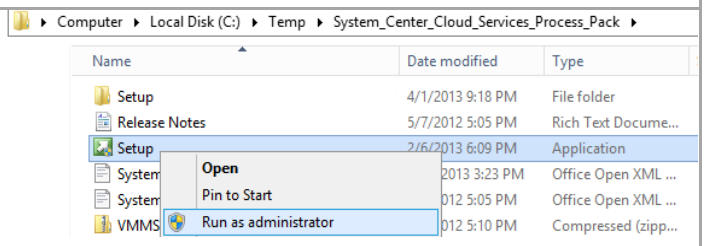


Install the Cloud Services Process Pack Runbooks

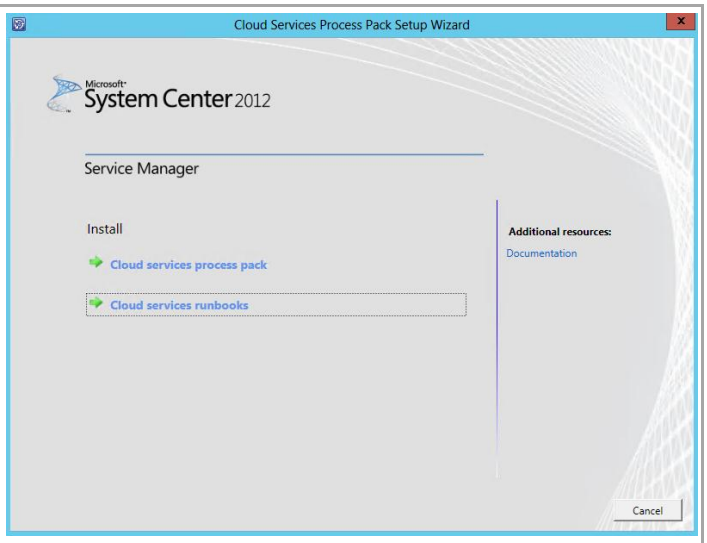
The following steps needs to be completed in order to install the Cloud Services Process Pack Orchestrator runbooks.

▶ Perform the following steps on the **Orchestrator** virtual machine.

1. Log on to the Orchestrator management server virtual machine with a user with local admin rights.
2. 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.
3. After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and click **Setup.exe** as an Administrator.

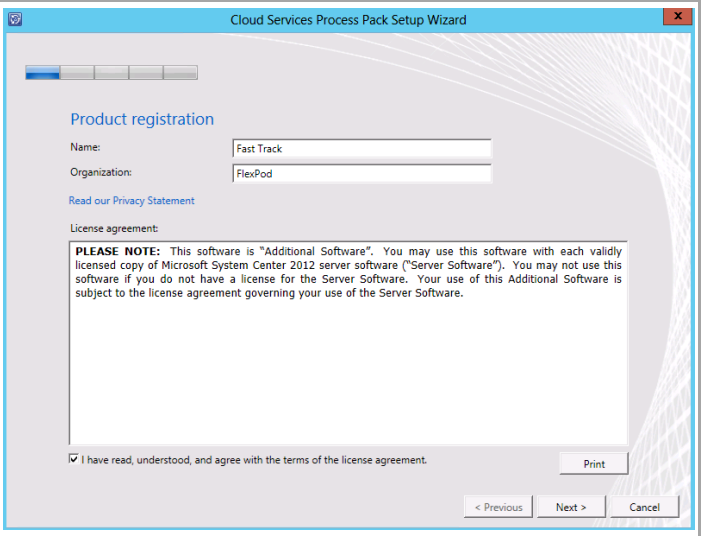


4. The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud services process pack.

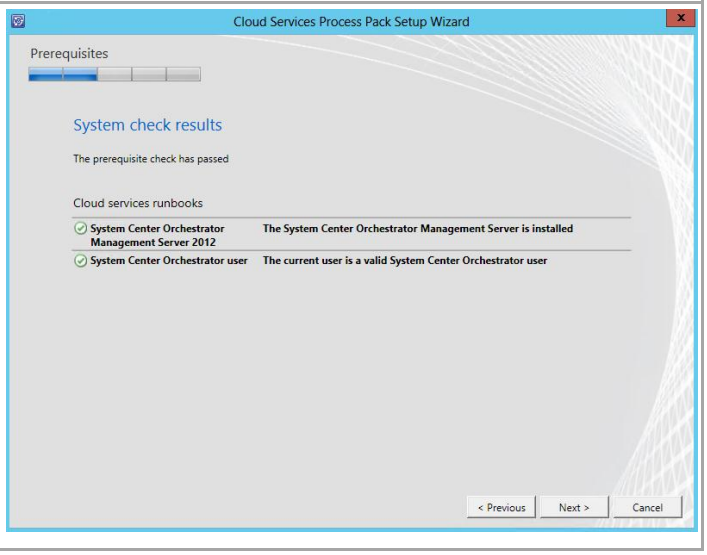


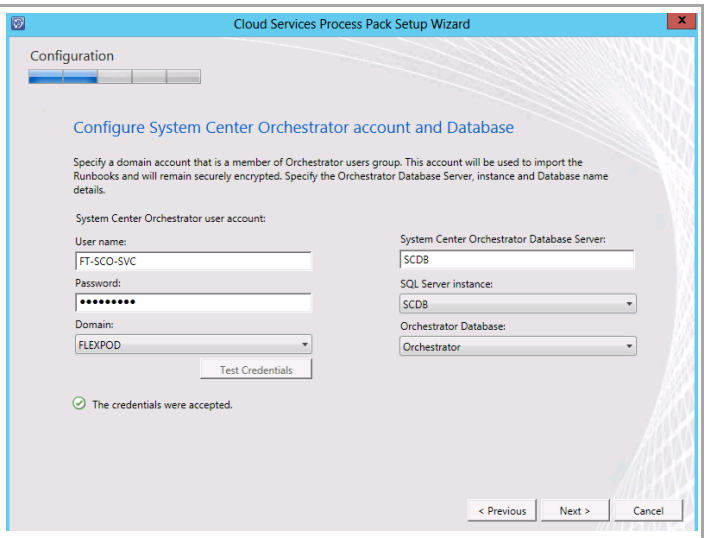
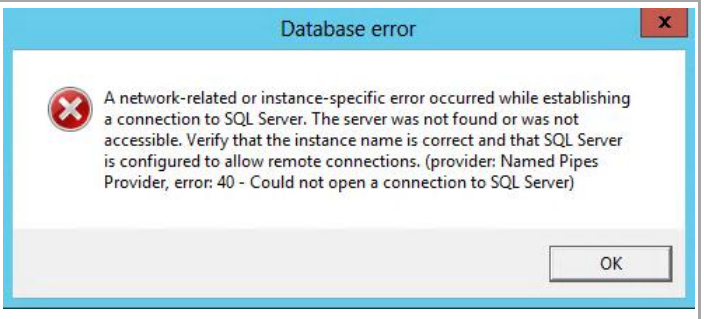
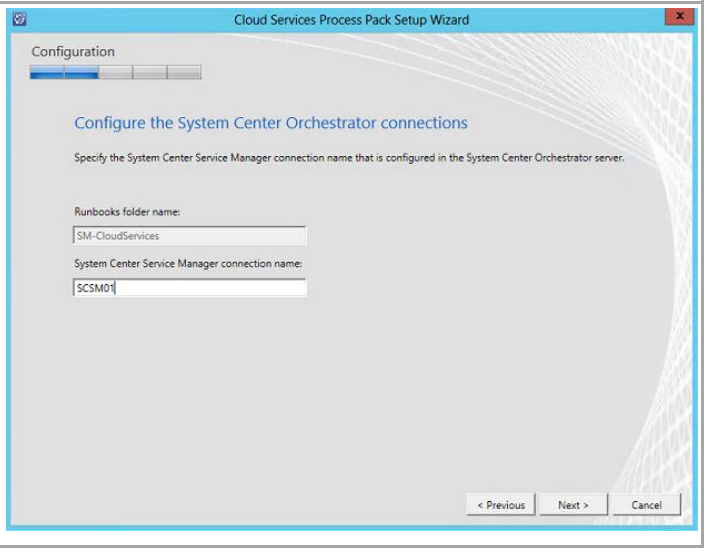
5. In the **Product registration information** dialog, enter the following information in the provided text boxes:
   - **Name** – *specify the name of the primary user or responsible party within your organization.*
   - **Organization** - *specify the name of the licensed organization.*

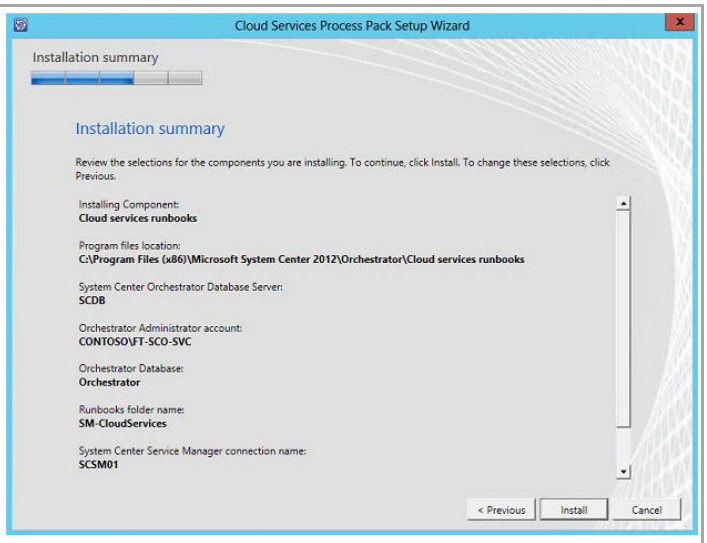
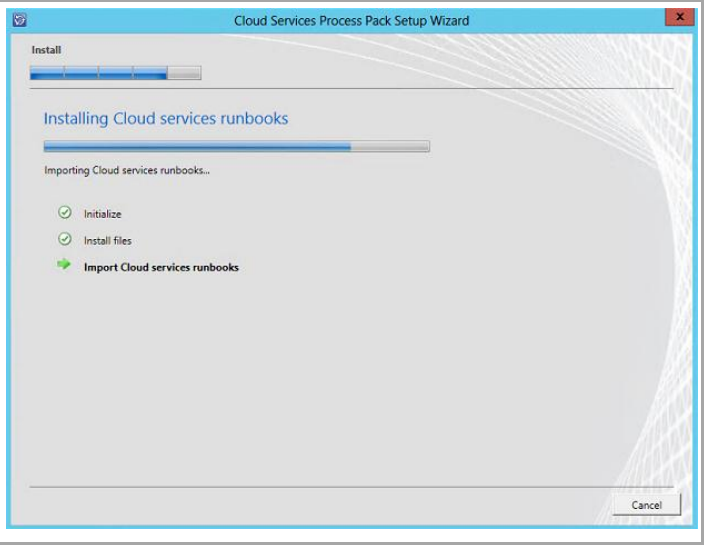
6. Click **Next** to continue.



7. 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.



8. 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.	
9. 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.	

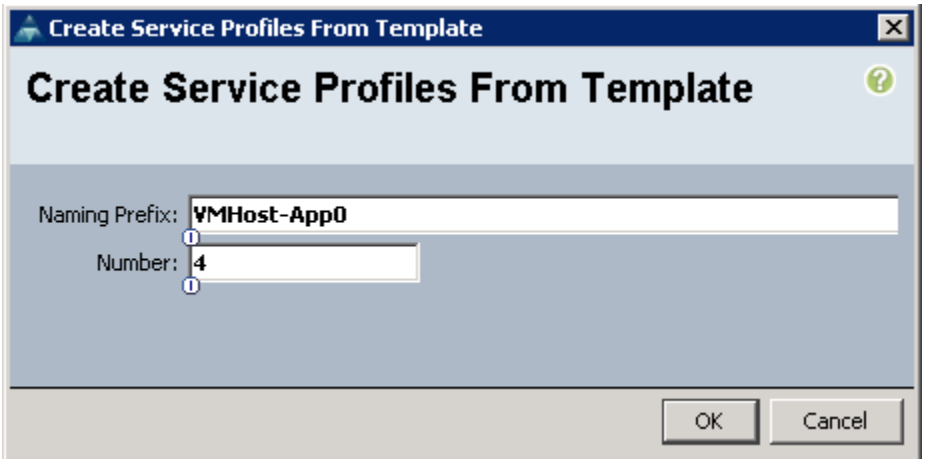
10. The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.	
11. When the installation completes, the wizard will display the **Setup completed successfully** dialog. 12. Click **Close** to complete the installation	

23 Deploy App Cluster

23.1 Create Service Profiles

These steps provide details for creating a service profile from a template.

1. In Cisco UCS Manager, Select the `Servers` tab at the top left of the window.
2. Select `Service Profile Templates VMHost-Mgmt-Fabric-A`
3. Right-click `and select Create Service Profile From Template.`
4. Enter `VMHost-App0` for the service profile prefix.
5. Enter `3` for the number of service profiles to create.
6. Click `OK` to create the service profile.



7. Click `OK` in the message box.

23.2 Gather Necessary Information

After the Cisco UCS service profiles have been created (in the previous steps), the infrastructure blades in the environment each have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blades.

Table 13 vHBA WWPNs for Fabric A and Fabric B.

Cisco UCS Service Profile Name	Fabric-A WWPN	Fabric-B WWPN
VMHost-App01		
VMHost-App02		
VMHost-App03		
VMHost-App04		

Note: To gather the information in the table above, launch the Cisco UCS Manager GUI, and in the left pane select the `Servers` tab. From there, expand `Servers > Service Profiles > root >`. Click each service profile and then click the `Storage` tab on the right. While doing so, record the WWPN information in the right display window for both vHBA_A and vHBA_B for each service profile in the table above.

23.3 Create Device Aliases

These steps provide details for configuring device aliases for the boot path.

Cisco Nexus 5548 A

1. Create device alias.

```
device-alias database.
  device-alias name VMHost-App01_A pwwn <Fabric-A WWPN>
  device-alias name VMHost-App02_A pwwn <Fabric-A WWPN>
  device-alias name VMHost-App03_A pwwn <Fabric-A WWPN>
  device-alias name VMHost-App04_A pwwn <Fabric-A WWPN>
exit.
device-alias commit.
copy running-config startup-config
```

Cisco Nexus 5548 B

1. Create device alias.

```
device-alias database.
  device-alias name VMHost-App01_B pwwn <Fabric-B WWPN>.
  device-alias name VMHost-App02_B pwwn <Fabric-B WWPN>.
  device-alias name VMHost-App03_B pwwn <Fabric-B WWPN>.
  device-alias name VMHost-App04_B pwwn <Fabric-B WWPN>.
exit
device-alias commit.
copy running-config startup-config
```

23.4 Create Zones for Each Service Profile

These steps provide details for configuring the zones for the boot path.

Cisco Nexus 5548 A

1. Create the Zones and Add Members.

```
zone name VMHost-App01_A vsan <Fabric  VSAN ID>
  member device-alias VMHost-App01_A
  member device-alias controller_A_2a
  member device-alias controller_B_2a
exit
zone name VMHost-App02_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App02_A
  member device-alias controller_A_2a
  member device-alias controller_B_2a
exit
zone name VMHost-App03_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App03_A
  member device-alias controller_A_2a
  member device-alias controller_B_2a
exit
zone name VMHost-App04_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App04_A
  member device-alias controller_A_2a
  member device-alias controller_B_2a
exit
```

2. Create the Zoneset and Add the Necessary Members

```
zoneset name Flexpod vsan <Fabric A VSAN ID>
  member VMHost-App01_A
  member VMHost-App02_A
```

```
  member VMHost-App03_A
  member VMHost-App04_A
exit
```

3. Activate the Zoneset

```
zoneset activate name flexpod vsan < Fabric A VSAN ID>
exit
copy run start
```

Cisco Nexus 5548 B

1. Create the Zones and Add Members.

```
zone name VMHost-App01_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App01_B
  member device-alias controller_A_2b
  member device-alias controller_B_2b
exit
zone name VMHost-App02_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App02_B
  member device-alias controller_A_2b
  member device-alias controller_B_2b
exit
zone name VMHost-App03_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App03_B
  member device-alias controller_A_2b
  member device-alias controller_B_2b
exit
zone name VMHost-App04_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App04_B
  member device-alias controller_A_2b
  member device-alias controller_B_2b
exit
```

2. Create the Zoneset and Add the Necessary Members.

```
zoneset name Flexpod vsan <Fabric B VSAN ID>
  member VMHost-App01_B
  member VMHost-App02_B
  member VMHost-App03_B
  member VMHost-App04_B
exit
```

3. Activate the Zoneset.

```
zoneset activate name flexpod vsan < Fabric B VSAN ID>
exit
copy run start
```

23.5 FlexClone Boot LUN

These steps provide details for cloning the boot lun from the goldmaster.

1. Start a Windows PowerShell session on the administrative host and import the Data ONTAP PowerShell Toolkit module.

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NaController <<var_ntap_A_hostname>> -credential root
```

3. Create a new Qtree to hold the boot LUN.

```
New-NaQtree /vol/ucs_boot/VMHost-App01
New-NaQtree /vol/ucs_boot/VMHost-App02
New-NaQtree /vol/ucs_boot/VMHost-App03
New-NaQtree /vol/ucs_boot/VMHost-App03
```

4. Create igroups.

```
New-NaIgroup -Name VMHost-App01 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>

New-NaIgroup -Name VMHost-App02 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>

New-NaIgroup -Name VMHost-App03 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>
New-NaIgroup -Name VMHost-App03 -Protocol fcp -Type windows |
   Add-NaIgroupInitiator -Initiator <vHBA_A WWPN> |
   Add-NaIgroupInitiator -Initiator <vHBA_B WWPN>
```

5. Clone the boot LUN form the goldmaster boot LUN.

```
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-App01/boot.lun
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-App02/boot.lun
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-App03/boot.lun
Start-NaClone -SourcePath /vol/ucs_boot/goldmaster/goldmaster.lun `
    -DestinationPath /vol/ucs_boot/VMHost-App04/boot.lun
```

6. Change the GUID of the LUN using the following command.

```
Set-NaLunSignature /vol/ucs_boot/VMHost-App01/boot.lun
Set-NaLunSignature /vol/ucs_boot/VMHost-App02/boot.lun
Set-NaLunSignature /vol/ucs_boot/VMHost-App03/boot.lun
Set-NaLunSignature /vol/ucs_boot/VMHost-App04/boot.lun
```

7. Map the boot LUN to the new iGroup.

```
Add-NaLunMap -Path /vol/ucs_boot/VMHost-App01/boot.lun -InitiatorGroup VMHost-App01
Add-NaLunMap -Path /vol/ucs_boot/VMHost-App02/boot.lun -InitiatorGroup VMHost-App02
Add-NaLunMap -Path /vol/ucs_boot/VMHost-App03/boot.lun -InitiatorGroup VMHost-App03
Add-NaLunMap -Path /vol/ucs_boot/VMHost-App03/boot.lun -InitiatorGroup VMHost-App03
```

23.6 Boot Service Profiles

Complete the following steps to boot each new service profile.

All Hosts

1. Back in USCM right-click on Service profile and select Associate with Server Pool.
2. From the Pool Assignment box, select the Infra_Pool and click OK, and OK again to acknowledge.
3. Right-click the <Hyper-V hostname> and select KVM Console.
4. Click Boot Server, the service profile will then pull a server from the VM-Host-Infra, and configure the hardware per the service profile.
5. Back in USCM right-click <Hyper-V Hostname>, and select KVM Console.
6. Click Boot Server, the service profile will then pull a server from the Infra_Pool, and configure the hardware per the service profile.

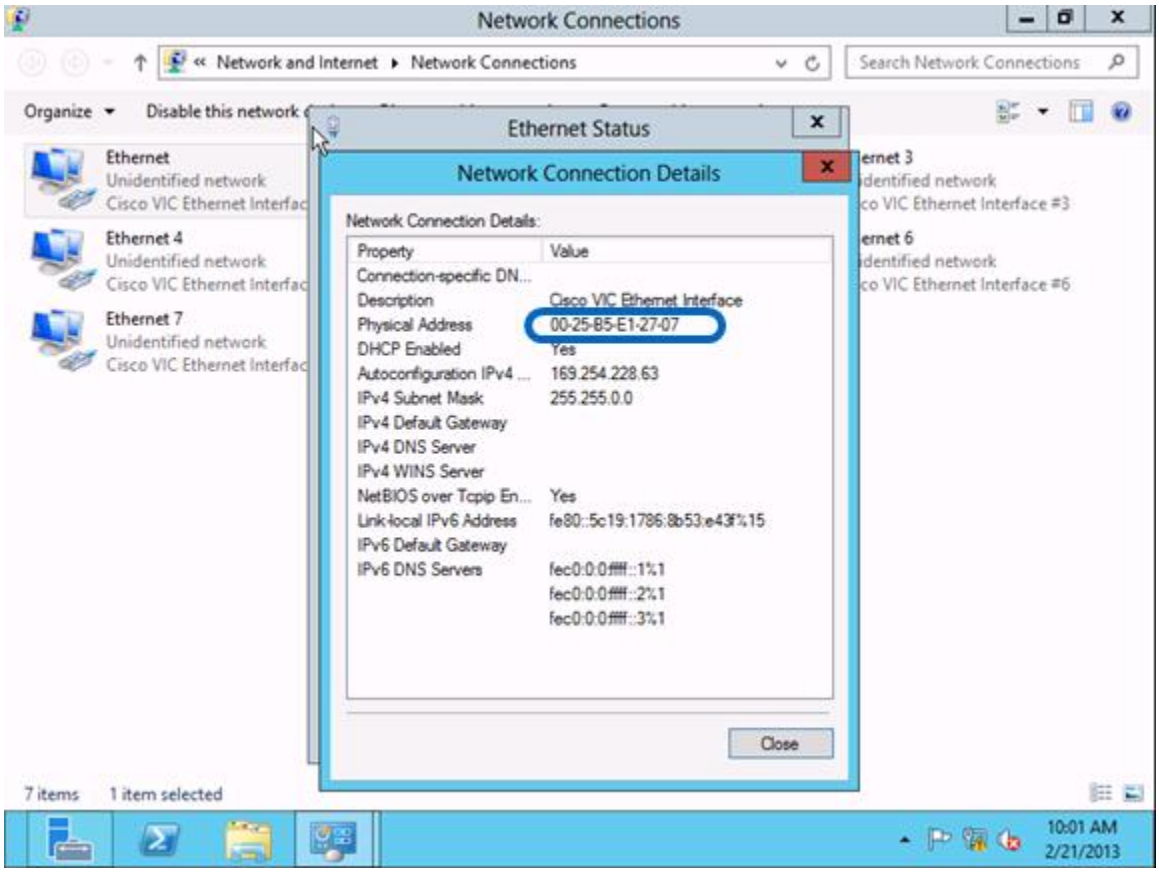
7. When the server has fully booted Windows will enter the out of box experience. Accept the EULA, and click Accept.
8. Enter the region and language settings and Click Next.
9. Enter a new Administrator Password, and click Finish.
10. Repeate for each service profile.

23.7 Configure Windows Networking for FlexPod

The following steps describe how to rename the network for each Hyper-V host.

All Hosts

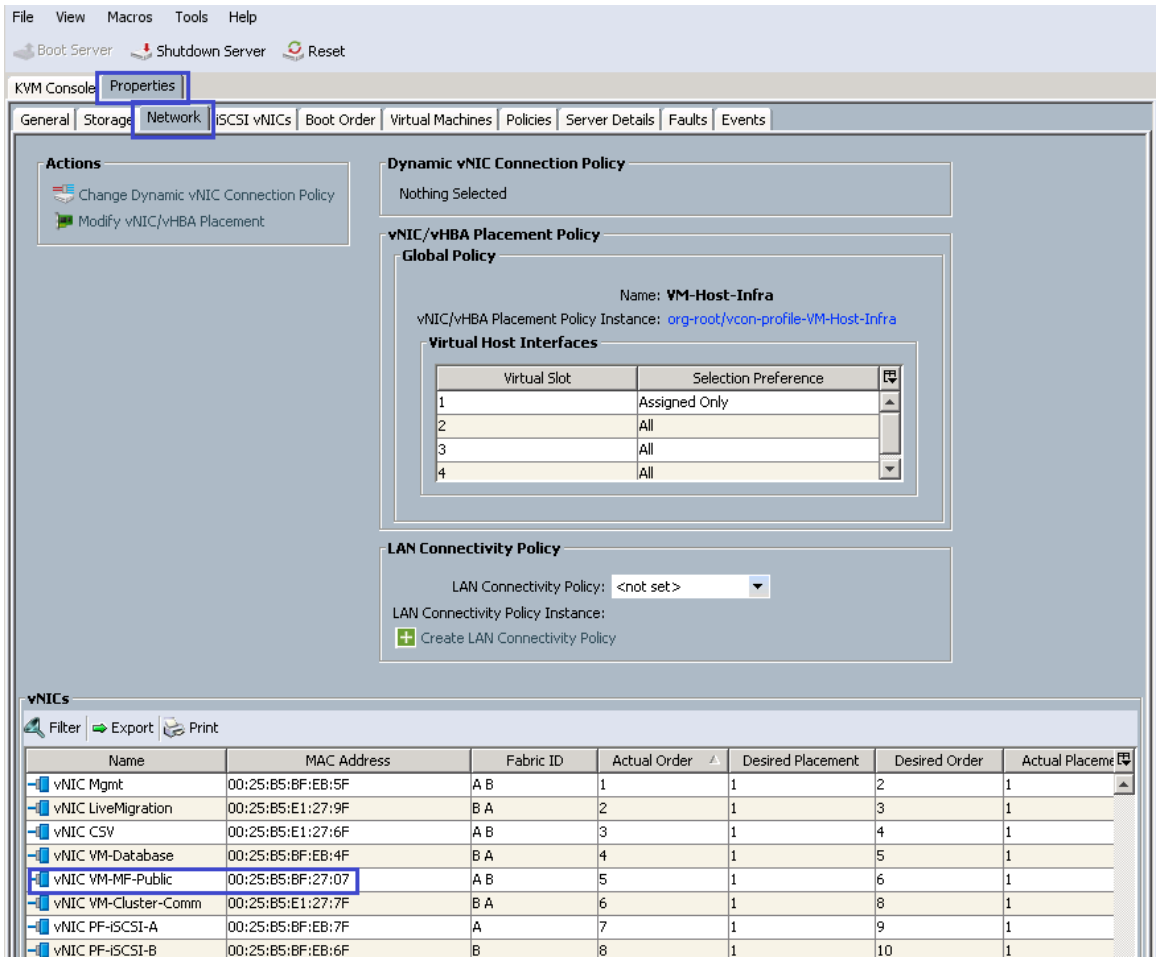
1. In server Manger select Local Server on the left.
2. Click on the `IPv4 address assigned by DHCP, IPv6 enabled` link to launch the network connections control panel.
3. One at a time, right-click on each eNIC, and select Status.
4. Click Details, and note the Physical Address.



Note: The following PowerShell command provides a list of the adapters with their associated MAC addresses it can be used instead of performing steps 3 through 5 for each NIC.

```
Get-NetAdapter | ft name, MacAddress -AutoSize
```

5. In the KVM console select Properties -> Network. Locate the vNIC

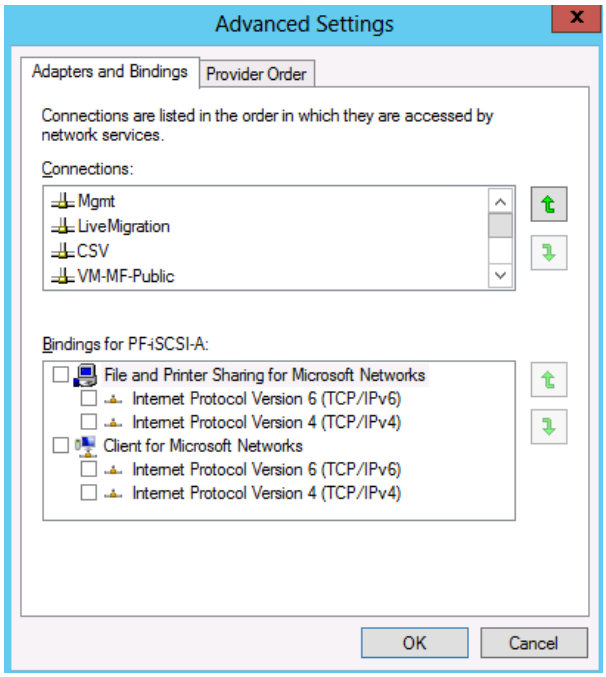


6. Identify the vNIC with the MAC Address noted in step 3.
7. Back in windows rename the LAN adapter to reflect the network it is associated with.
8. Set the appropriate IP settings for that adapter.

Note: Assign IP Addresses to the LiveMigration, CSV, and Mgmt adapters.

9. Repeat for each eNIC in windows.
10. In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings
11. Select the adapter and use the arrows to move it up or down in binding order.
12. The recommended binding order is:
    - Mgmt
    - LiveMigration
    - CSV
    - VM-Database
    - VM-MF-Public
    - VM-Cluster-Comm
    - PF-iSCSI-A
    - PF-iSCSI-B

13. Select the PF-iSCSI-A connection.
14. In the Bindings for PF-iSCSI-A list box, clear the check box next to File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
15. Repeat steps 13 and 14 for the PF-iSCSI-B connection.



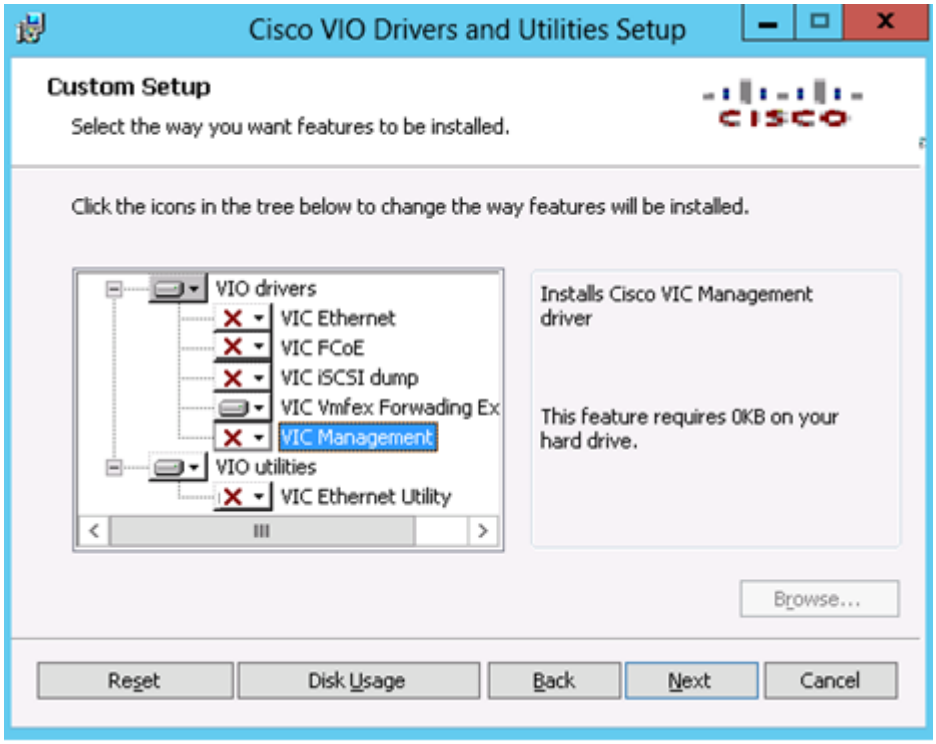
23.8 Install Cisco Virtual Switch Forwarding Extensions for Hyper-V

Cisco Virtual Switch Forwarding Extensions for Hyper-V enable SR-IOV capability when using VM-FEX for Hyper-V. The installation package is located on the UCS drivers ISO image starting with version 2.1. The installation package file name is CSCO_VIO_INSTALLER_64_2.x.x.msi. It is located in the Windows\installers\Cisco\MLOM\W2K12\x64 directory.

All Hosts

1. Run CSCO_VIO_INSTALLER_64_2.x.x.msi with administrator rights.
2. Click `Next` in the welcome screen.
3. `Accept the EULA` and click `Next`.
4. Select `Custom setup`.
5. Deselect the following options:
   - VIC Ethernet
   - VIC FCoE
   - VIC iSCSI Dump
   - VIC Management
   - VIC Ethernet Utility

Note: Only the option VIC VMfex Forwarding Extension should be installed.



6. Click `Next`.
7. Click `Install`.
8. Click `Finish` to complete the installation.

23.9 Create Hyper-V Virtual Network Switches

All Hosts

1. Open a powershell command window.
2. Create the Hyper-V virtual switches with the following parameters:

Virtual Network Name	Connection Type	Enable SR-IOV	Interface Name	Share Network with Management Host
VM-Cluster-Comm	External	No	VM-Cluster-Comm	No
VF-iSCSI-A	External	Yes	PF-iSCSI-Fabric-A	No
VF-iSCSI-B	External	Yes	PF-iSCSI-Fabric-B	No

Note: Do not create a virtual network switch for the Mgmt, Database, and MF-Public network. The MF-Public Nexus 1000V logical switch will be created using Virtual Machine Manager later in this section. The Mgmt and Database virtual switches are not needed in the App Fabric cluster.

3. Create virtual switch VM-Cluster-Comm.

```
New-vmswitch -name VM-Cluster-Comm -NetAdapterName VM-Cluster-Comm -AllowManagementOS
$false
```

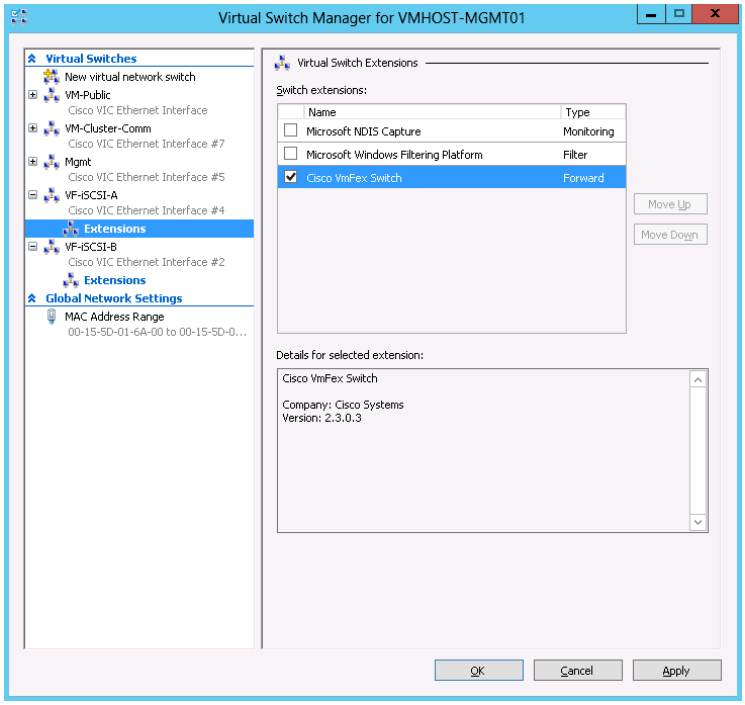
4. Create virtual switch VF-iSCSI-A.

```
New-vmswitch -name VF-iSCSI-A -NetAdapterName PF-iSCSI-A -AllowManagementOS $false -
EnableIov $true
```

5. Create virtual switch VF-iSCSI-B.

```
New-vmswitch -name VF-iSCSI-B -NetAdapterName PF-iSCSI-B -AllowManagementOS $false -
EnableIov $true
```

6. Open Hyper-V Manager
    a. Select Hyper-V Virtual Switch Manger in the action pane.
    b. Expand the VF-iSCSI-A virtual switch.
    c. Select Extensions under the VF-iSCSI-A virtual switch.
7. Check the box next to Cisco VMFex Switch



8. Click Apply.
9. Repeat for virtual switch VF-iSCSI-B

23.10 Prepare Nodes for Clustering

The following section describes how to prepare each node to be added to the Hyper-V cluster.

All Hosts

1. Install windows feature

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

2. Rename the Host.

```
Rename-Computer -NewName <hostname> -restart
```

3. Add the host to Active Directory.

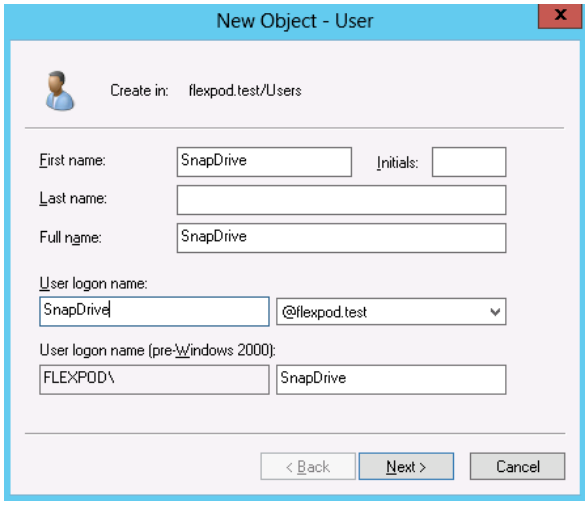
```
Add-Computer -DomainName <domain_name> -Restart
```

23.11 Install NetApp SnapDrive

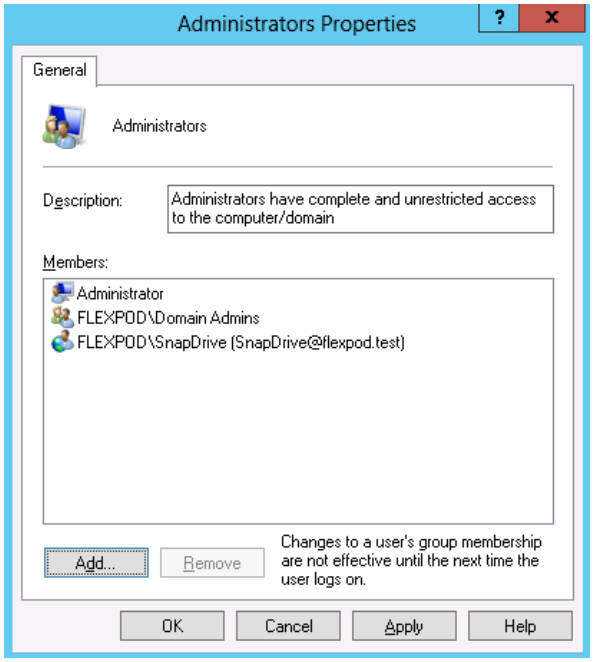
The following section describes how to installation of the NetApp SnapDrive Windows. For detailed information regarding the installation see the Administration and Installation Guide.

Service Account preparation

1. In active directory create a SnapDrive service account note this account requires no special delegation.



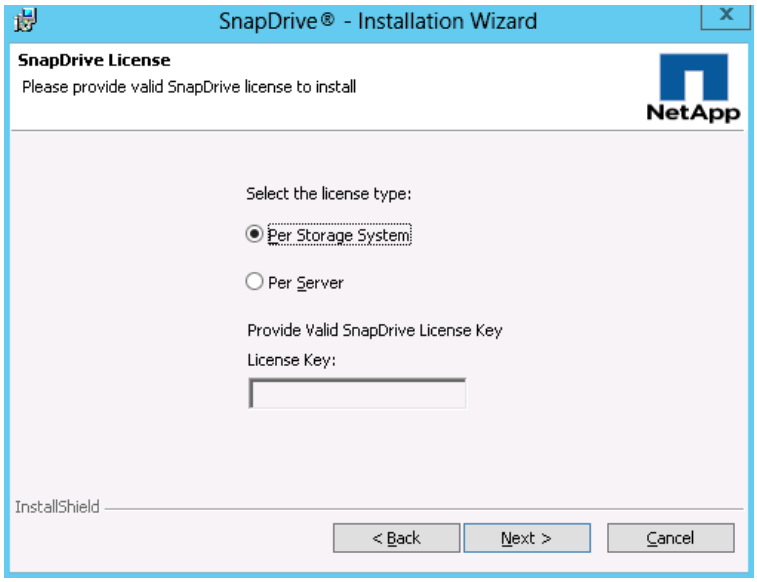
2. Add the SnapDrive service account to the local Administrators group in Windows.



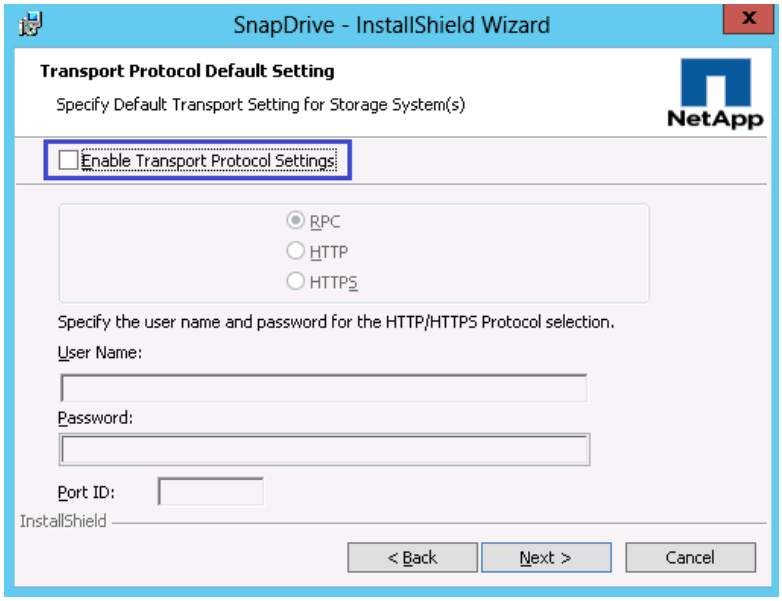
All Hosts

1. Download SnapDrive installer http://support.netapp.com/NOW/download/software/snapdrive_win/6.5/SnapDrive6.5_x64.exe
2. Launch the Installer, click `Next`.
3. `Accept the EULA` and click `Next`.

4. Select the Storage based Licensing method and click Next.



5. Enter your User Name, and Organization information, and click `Next`.
6. Validate the installation path and click `Next`.
7. Check the `Enable SnapDrive to communicate through the Windows Firewall` checkbox and click `Next`.
8. Enter the Account information for the Snapdrive service account, Click `Next`.
9. Click `Next`, through the SnapDrive Web Service Configuration.
10. Uncheck the `Enable Transport Protocol Settings`, and click `Next`



11. Leave `Enable Protection Manger Integration` Unchecked, and click `Next`.
12. Click `Install`.
13. After the installation is finished. Launch a NEW PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.

Note: A new prompt is required to register the sdcli executable.

14. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_controller1>> -IP <<var_controller1_e0m_ip>>
sdcli preferredIP set -f <<var_controller2>> -IP <<var_controller2_e0m_ip>>
```

15. Configure SnapDrive transport protocol authentication configuration for each controller.

```
sdcli transport_protocol set -f <<var_controller1>> -type https -user root -pwd
<<var_admin_passwd>>
sdcli transport_protocol set -f <<var_controller2>> -type https -user root -pwd
<<var_admin_passwd>>
```

23.12 Install NetApp SnapManager for Hyper-V

The following section describes how to installation of the NetApp SnapManger for Hyper-V. For detailed information regarding the installation see the Administration and Installation Guide.

Service Account preparation

1. In active directory create a SMHV service account note this account requires no special delegation.
2. Add the SMHV service account to the local Administrators group in Windows.

All Hosts

1. Download the SnapManger for Hyper-V installer from http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/1.2/SMHV1.2_NetApp_x64.exe
2. Launch the Installer, click Next.
3. Accept the EULA and click Next.
4. Select the Storage based Licensing method and click Next.
5. Enter your User Name, and Organization information, and click Next.
6. Validate the installation path and click Next.
7. Enter the Account information for the SMHV service account, Click Next.
8. Click Next, through the SMHV Web Service Configuration.
9. Click Install.

23.13 Install VM-FEX Port Profile Management Utilities in Hyper-V

All Hosts

1. Run the VM-FEX Port Profile Management Utilities installation package VMFEX_ToolS_64_2.3.2.msi.
2. Click **Next** on the welcome screen.
3. Accept the license agreement and click **Next**.
4. Click the **Custom** installation button.
5. Click **Next**.
6. Click **Install**.
7. Click **Finish** to complete the installation.

23.14 Create a Cluster

One Server Only

1. Launch a PowerShell prompt with administrative permissions, by right clicking on the PowerShell icon and selecting Run as Administrator.
2. Create a new cluster.

```
New-Cluster -Name <cluster_name> -Node <Node1>, <Node2>, <node3>, <node4> -NoStorage -
StaticAddress <cluster_ip_address>
```

3. Rename Cluster Networks

```
Get-ClusterNetworkInterface | ? Name -like *CSV* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'CSV'}
Get-ClusterNetworkInterface | ? Name -like *LiveMigration* | Group Network| %{ (Get-
ClusterNetwork $_.Name).Name = 'LM'}
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Mgmt'}
```

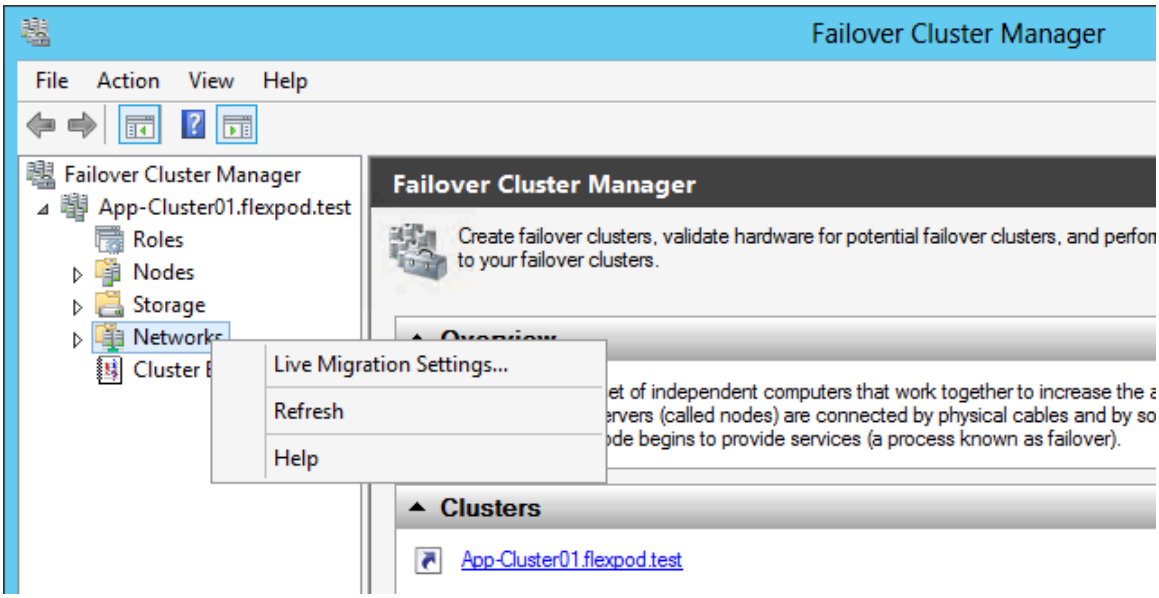
4. Designate the CSV network.

```
(Get-ClusterNetwork -Name CSV).Metric = 900
```

23.15 Configure Live Migration Network

One Server Only

1. Open Failover Cluster Manger from Server Manager select Tools -> Failover Cluster Manger.
2. Expand the Cluster tree on the left, and right click on Networks, select Live Migration Settings…



3. Deselect all but the LiveMigration network and click OK.

23.16 Configure Quorum LUN

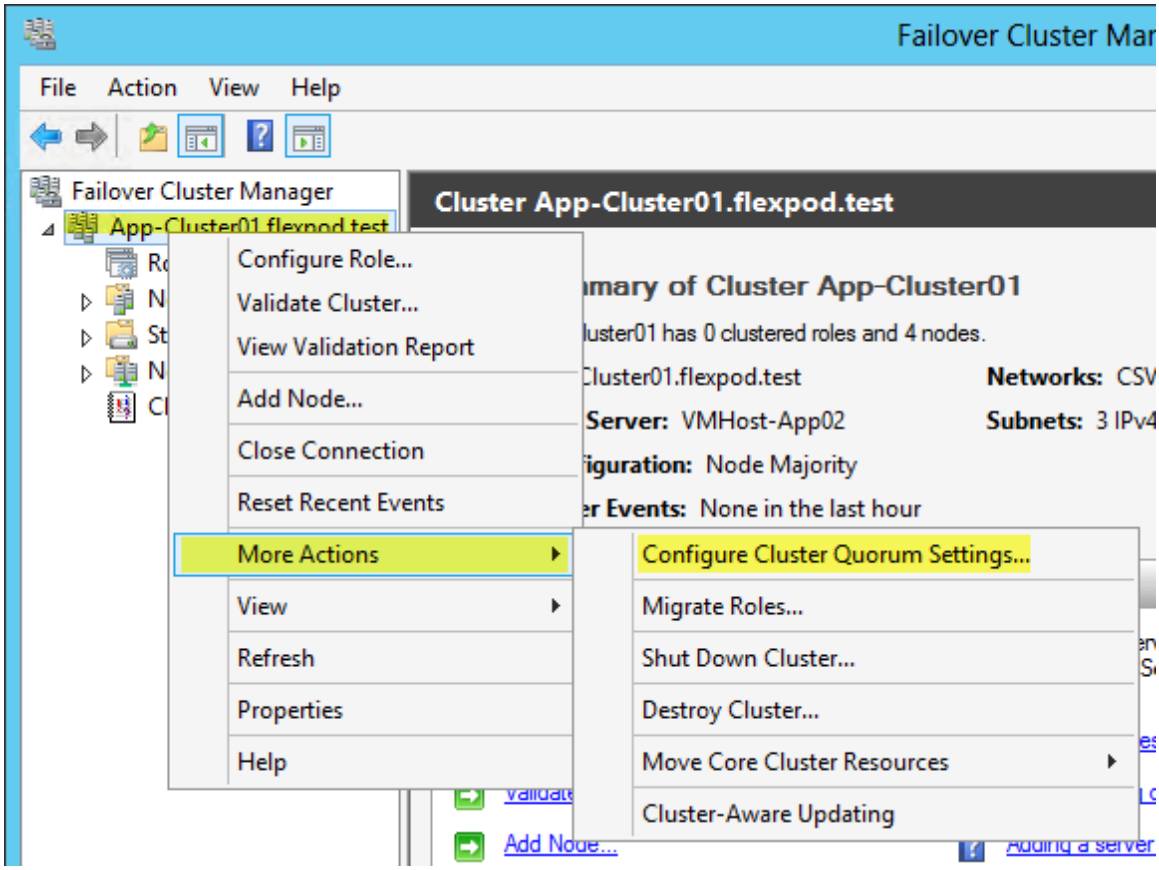
The following section will describe now to create the quorum disk, and configure the cluster to use the quorum witness.

One Server Only

1. Open a PowerShell prompt and move the Available Storage cluster group by running.

```
Move-ClusterGroup "Available Storage" -Node $env:COMPUTERNAME | Start-ClusterGroup
```

2. Open SnapDrive from the start screen to configure cluster storage.
3. From SnapDrive, Open the Server name, then Open the Disks Icon.
4. Right-click the Disks Icon and choose to **Create Disk**.
5. Type in the IP Address of the controller that contains the quroum Volume.
6. When connected, open the controller tree and select the quroum Volume.
7. Type in the name of the LUN in the LUN NAME box, click **Next**.
8. Select **Shared (Microsoft Cluster Services only)** and click **Next**.
9. Validate that all nodes of the cluster are shown and click **Next**.
10. Select **Set the Drive letter to Q:**,and set the LUN size to be **1GB** and click **Next**.
11. Click **Next** through the Volume properties confirmation.
12. **Select the FCP WWPN** to Map the LUN to click **Next**.
13. Select **Automatic** igroup management and Click **Next**.
14. Select **Select the cluster group Availavle Storage**, and click **Next**.
15. Click **Finish**.
16. In Cluster Manager, Click the Cluster object and Select **More Actions** -> **Configure Cluster Quorum Settings**.



.

17. In the Welcome screen Click **Next.**
18. Select **Add or Change the Quorum Witness,** and click **Next.**
19. Select **Configure a disk witness,** and click **Next.**
20. Select **Disk Q**:, and click **Next**.
21. Click **Next**.
22. Click **Finish**.

23.17 Create CSVs LUN for VM Storage

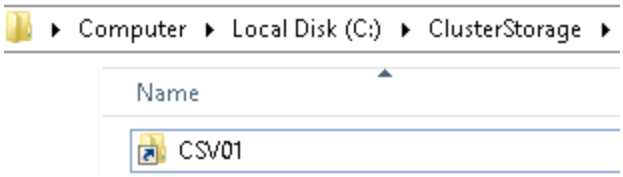
The following section will describe now to create the application CSVs. NetApp recommends that at least one CSV be created per Node in the cluster.

One Server Only

1. Open a PowerShell prompt and move the Available Storage cluster group by running.

```
Move-ClusterGroup "Available Storage" -Node $env:COMPUTERNAME | Start-ClusterGroup
```

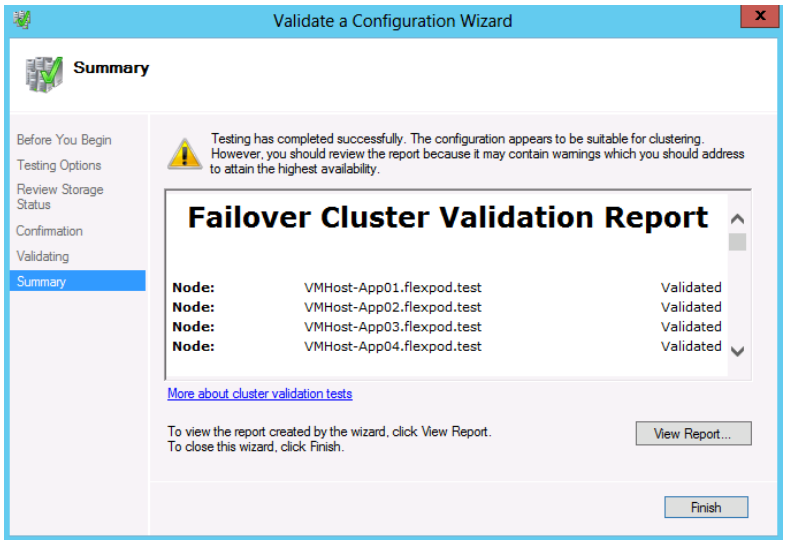
2. Open SnapDrive from the start screen to configure cluster storage.
3. From SnapDrive, Open the Server name, then Open the Disks Icon.
4. Right-click the Disks Icon and choose to **Create Disk**.
5. Type in the IP Address of the controller that contains the infra CSV Volume.
6. When connected, open the controller tree and select the infra CSV Volume.
7. Type in the name of the LUN in the LUN NAME box, click **Next**.
8. Select **Shared (Microsoft Cluster Services only)** and click **Next**.
9. Validate that all nodes of the cluster are shown and click **Next**.
10. Select **Do not assign a Drive letter or Volume Mount Point**, set the LUN size to be **1tb** and click **Next**.
11. Click **Next** through the Volume properties confirmation.
12. **Select the FCP WWPN** to Map the LUN to click **Next**.
13. Select **Automatic** igroup management and Click **Next**.
14. Select **Add to cluster shared volumes**, and click **Next**.
15. Click Finish.
16. In Cluster Manager, Click the Storage node in the tree view and select the disk object.
17. Right click the newly created CSV disk and select properties.
18. Change the name of the CSV disk to one you prefer.
19. Click okay to accept the new name.
20. Use Explore to rename the new CSV disk.



23.18 Validated the Cluster

Run the cluster validation wizard to verify that the cluster is operating correctly.

1. Open Failover Cluster Manager.
2. Click Validate Cluster… In the action pane.
3. Proceed through the wizard and select the option to run all tests.



4. Review and correct any failures that are listed in the validation report.

Note: The following warnings are expected to be reported by the validation wizard. These warning can safely be disregarded.

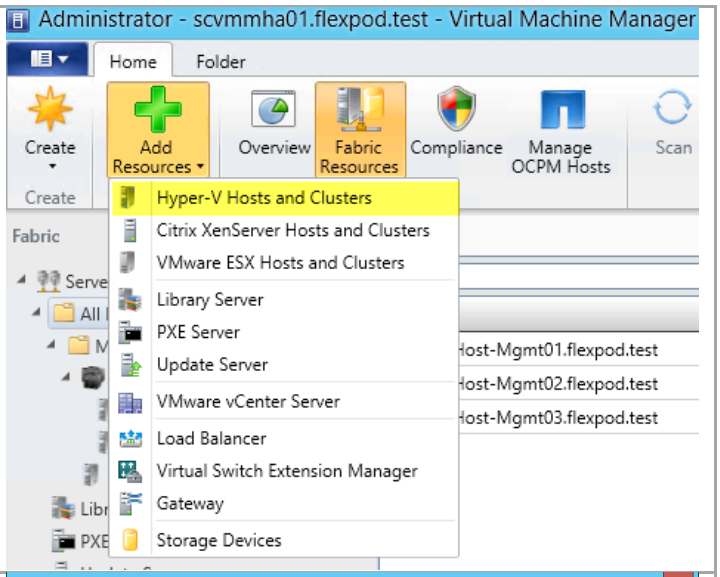
Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node VMHost-App01.flexpod.test.

Test Disk 0 does not support SCSI-3 Persistent Reservations commands needed to support clustered Storage Pools. Some storage devices require specific firmware versions or settings to function properly with failover clusters. Please contact your storage administrator or storage vendor to check the configuration of the storage to allow it to function properly with failover clusters.

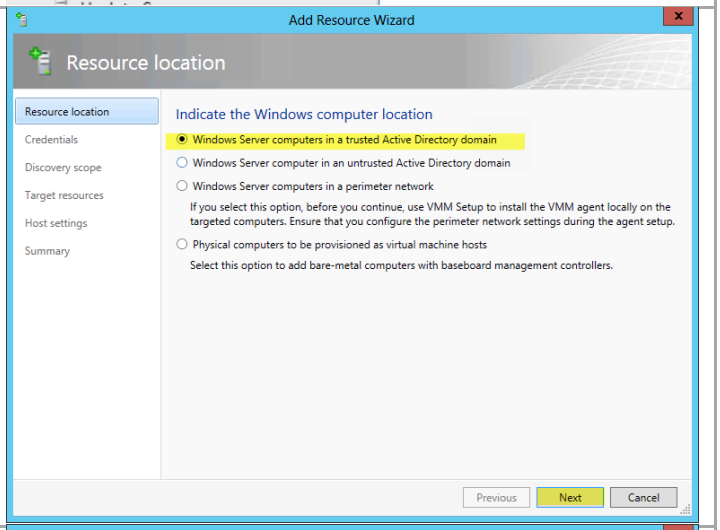
23.19 Add the Cluster to SCVMM

▶ Perform the following steps on the SCVMM server.

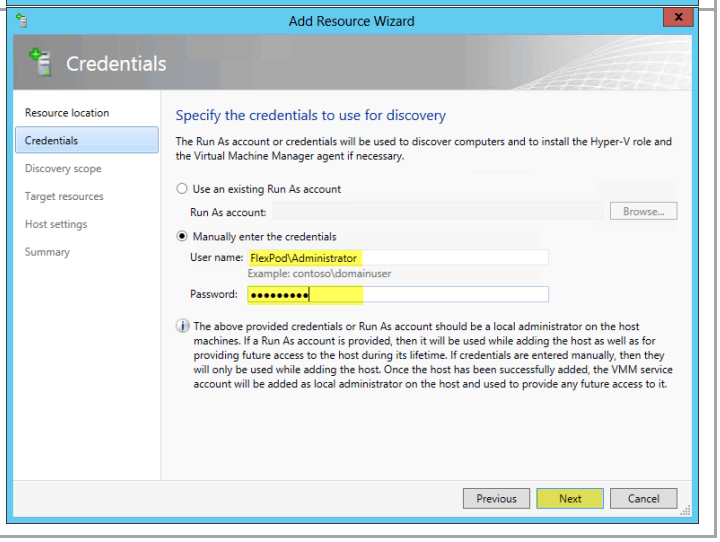
1. In the **Virtual Machine Manger** console, navigate to the **Fabric** pane.
2. Select Add Resources, Hyper-V Hosts and Clusters.



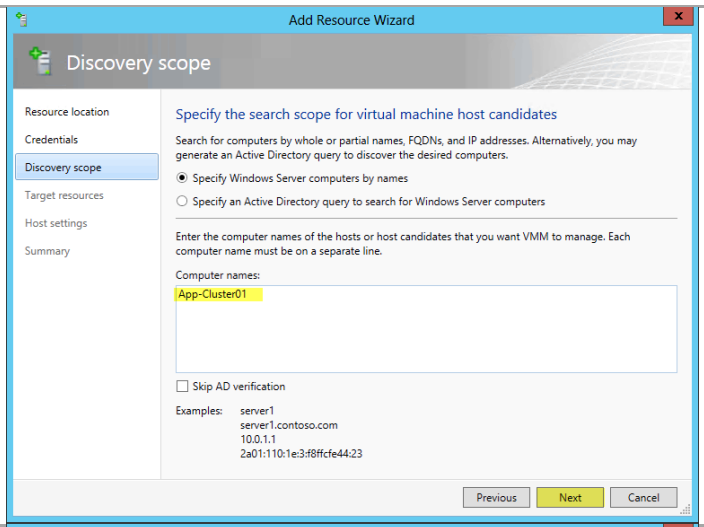
3. Select Windows Server Computers in a trusted Active Directory domain, and click Next.



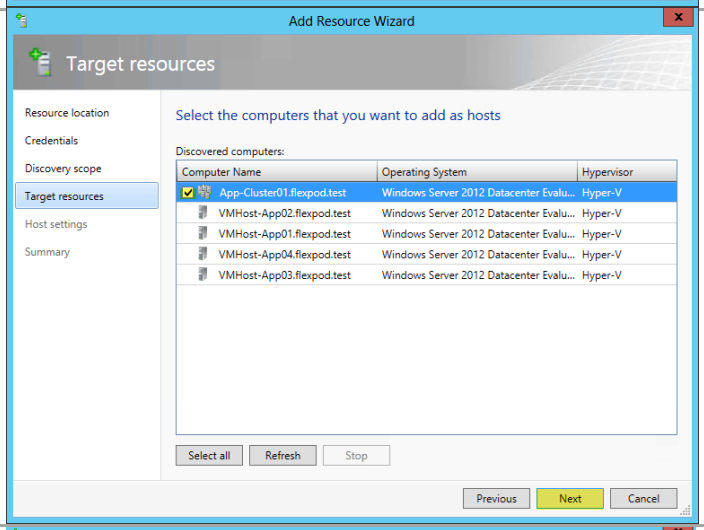
4. **Enter an account** that has permission on the cluster and click **Next**.



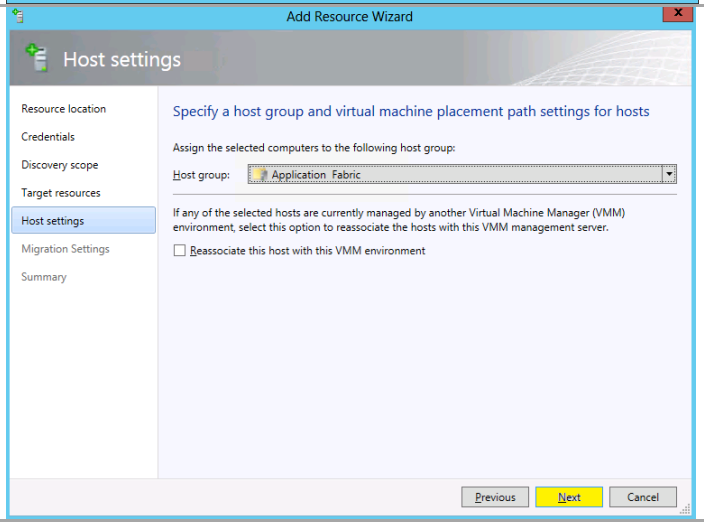
5. **Enter the cluster name** and click **Next**.



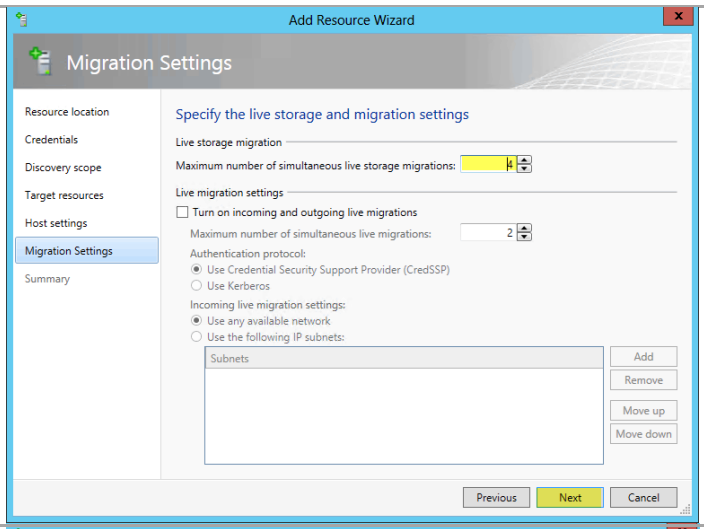
6. **Select the cluster object** and click **Next**



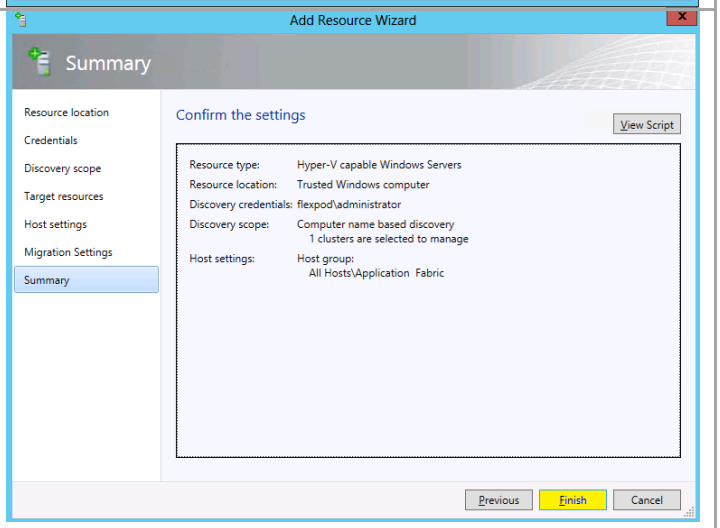
7. Select the host group and click **Next**



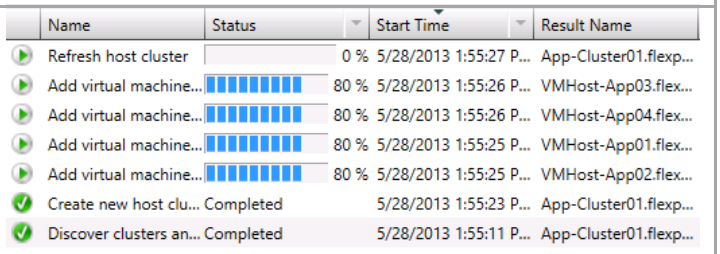
8. Set the **Live Storage Migrations to 4, click Next.**



9. Click **Finish.**

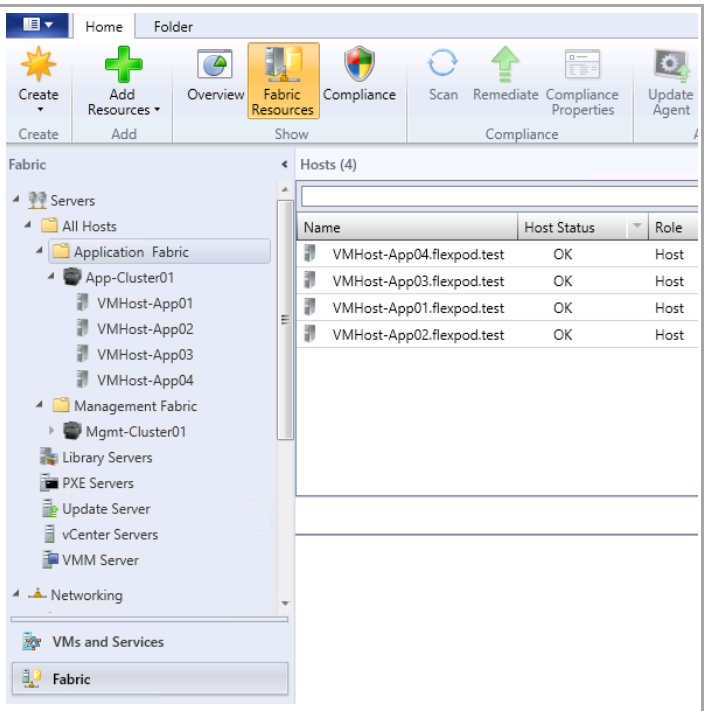
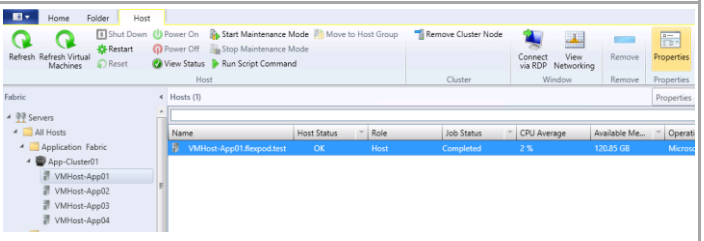
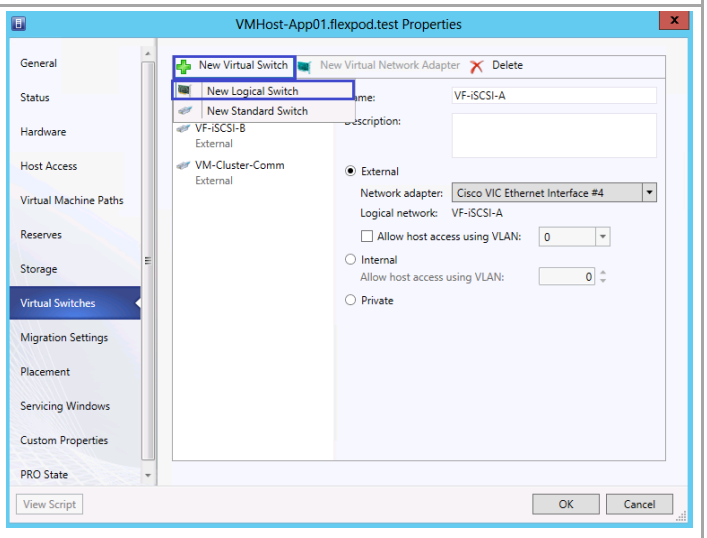


10. Monitor the job status and verify the cluster addition jobs complete successfully.

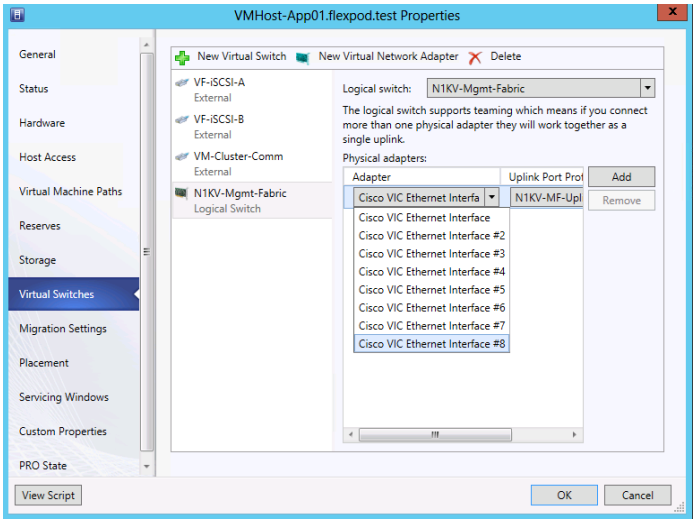


23.20 Creating the Logical Switch on the Hyper-V Hosts

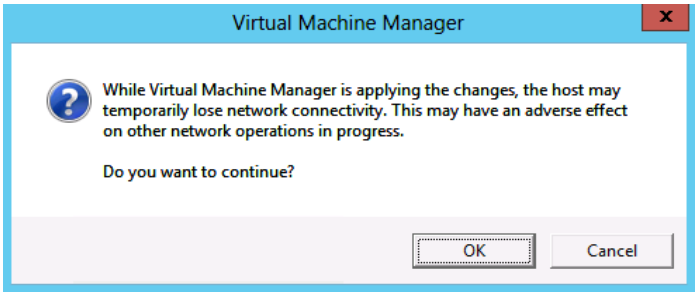
▶ Perform the following procedure on each App Fabric Cluster node.

1. In the active Virtual Machine Manager instance, select Fabric. Expand All Hosts and Management Fabric.	
2. Select the first management fabric host and click **Properties**.	
3. Select Virtual Switch in the left pane and New Virtual Switch. Select New Logical Switch.	

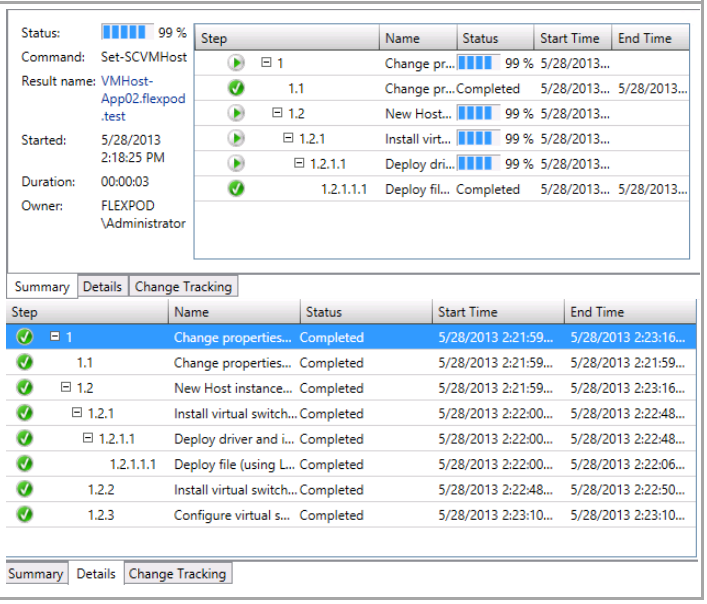
4. Select the new logical switch in the middle pane and in the right pane select the Ethernet adapter for the N1KV-Mgmt-Fabric network. Click OK.

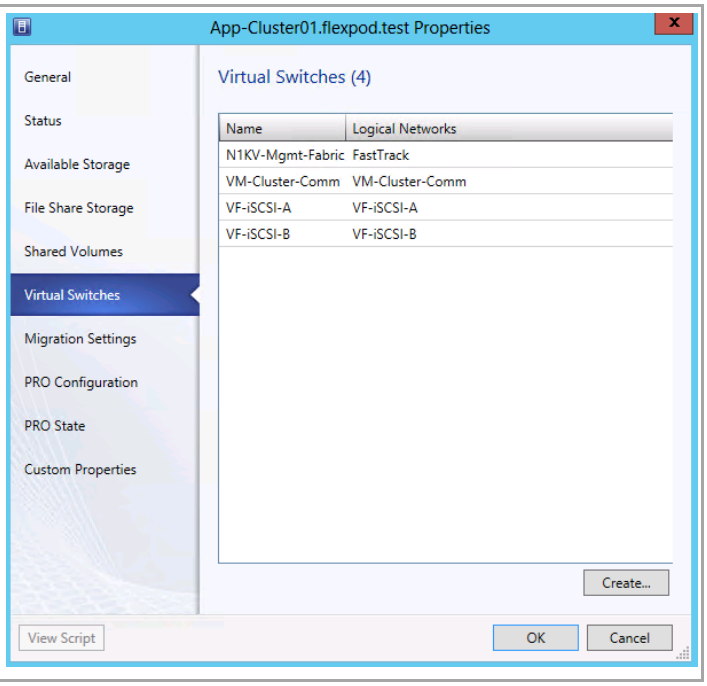


5. Click OK to invoke the configuration change.
6. Repeat this procedure on the remaining management fabric hosts.



7. Click Jobs and monitor the job progress. The job will complete with info until the logical swith is installed on all of the hosts in the cluster.
8. Repeat this procedure on all cluster nodes.



9. Open the Mgmt-Cluster01 properties and verify that the N1KV-Mgmt-Fabric Switch is in the list of switch installed on all cluster nodes.	

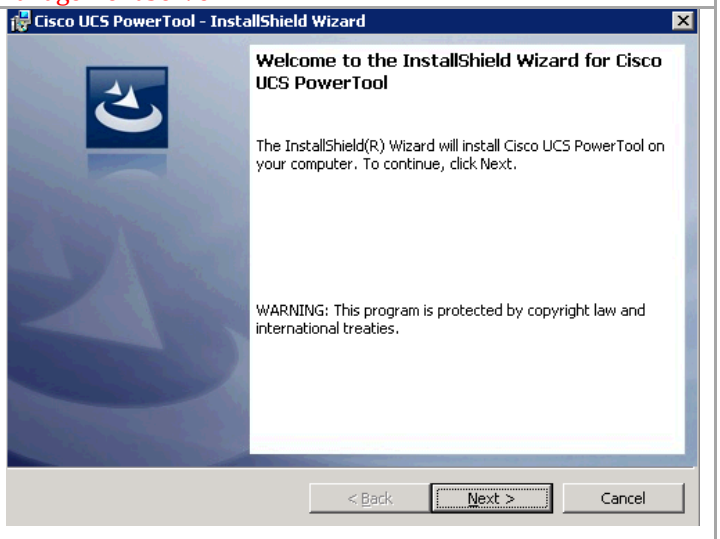
APPENDIX A: Installing Cisco UCS PowerTool

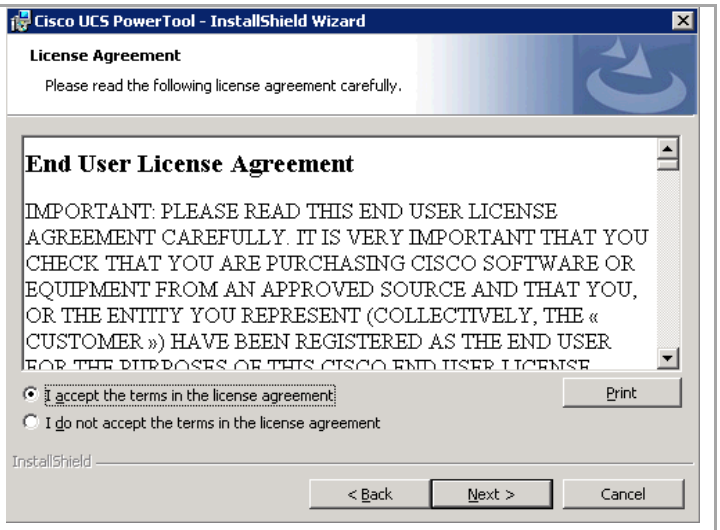
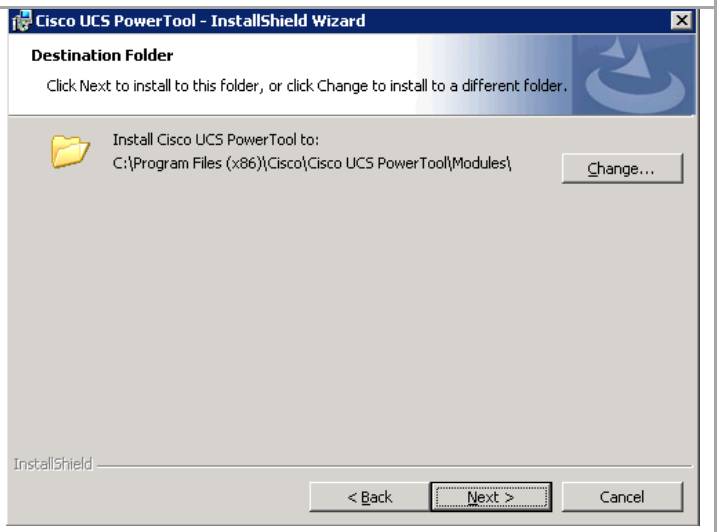
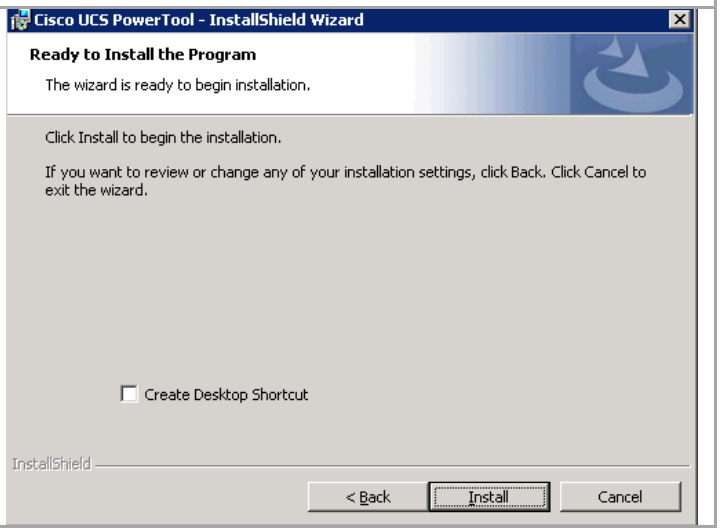
The Cisco UCS PowerTool should be installed on the FlexPod Management server.

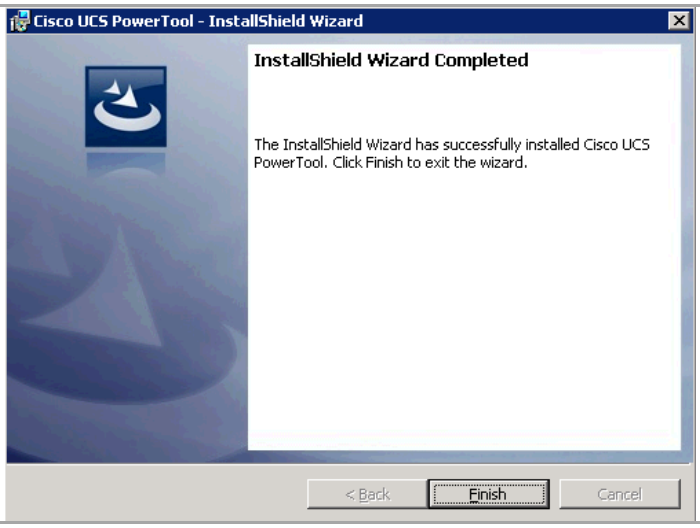
Download the Cisco UCS PowerTool version 0.9.9.0 or newer from the Cisco Developer Network. It can be found in the Microsoft Management section - http://developer.cisco.com/web/unifiedcomputing/microsoft.

Extract the zip file and execute the extracted exe file.

▶ Perform the following steps on the FlexPod management server.

1. Launch the Cisco UCS PowerTool Installer. The **Setup Wizard** screen appears.	

2. **Read and accept** the end user license agreement. Click **Next** to continue.	
3. Select the **Destination Folder** and click **Next** to continue.	
4. Cisco UCS PowerTool is ready to install. Click **Next** to complete the installation.	

5. After the installation completes successfully click **Finish** to close the installation wizard.	

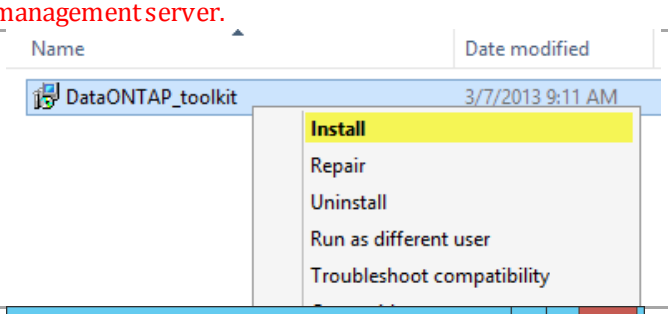
APPENDIX B: Installing the Data ONTAP PowerShell Toolkit.

The Data ONTAP PowerShell Toolkit should be installed on the FlexPod Management Server.

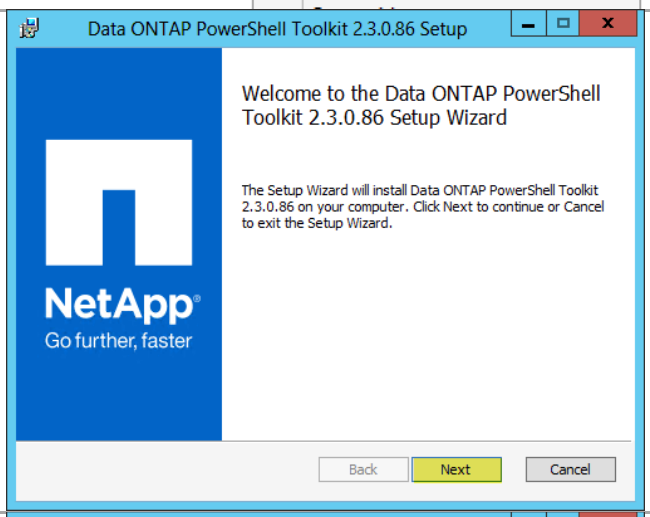
Download the Data ONTAP PowerShell toolkit from NetApp Communities: https://communities.netapp.com/community/products_and_solutions/microsoft/powershell.

▶ Perform the following steps on the FlexPod management server.

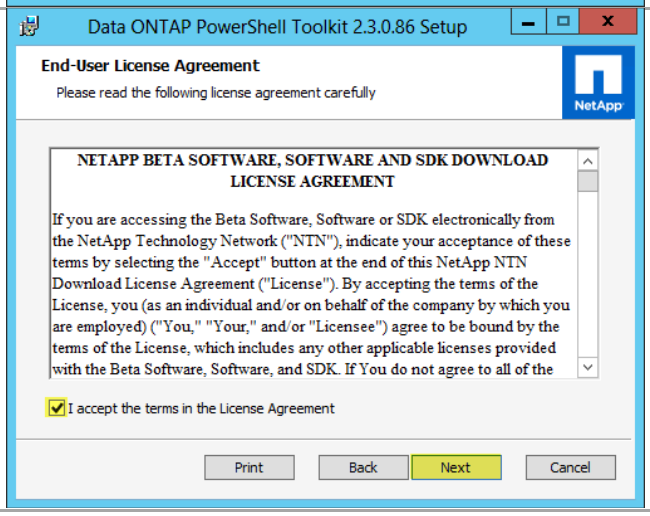
1. Run the Data ONTAP Windows installation package.

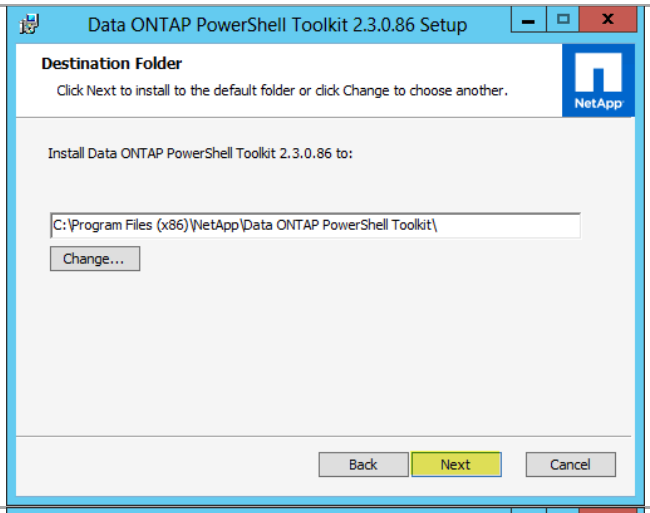
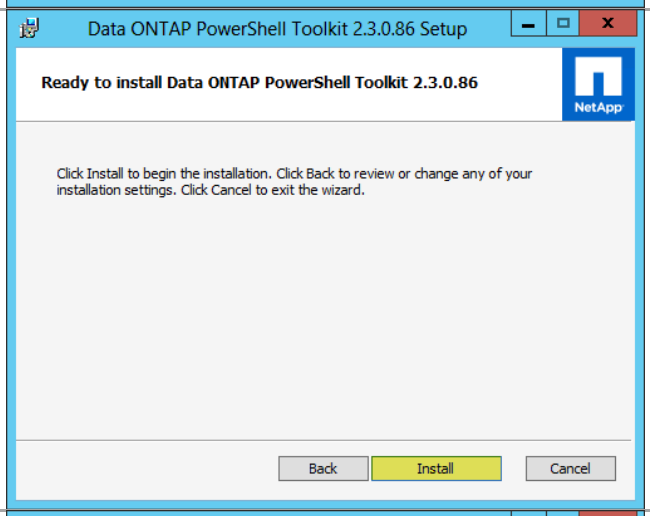


2. On the Welcome page, click **Next**.



3. Accept the EULA and click Next.



4. Validate the Installation path and click **Next**.	
5. Click Install.	
6. Click Finish.