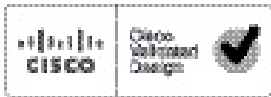




## FlexPod Datacenter with Microsoft Private Cloud Fast Track 4.0 and Cisco Nexus 9000 Series Switches

Deployment Guide for FlexPod Datacenter with Microsoft Private Cloud Fast Track 4.0 and Cisco Nexus 9300 Series Switches in Standalone Mode with NetApp FAS 8000 Series



Building Architectures to Solve Business Problems



# 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 [www.cisco.com/go/designzone](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)

© 2015 Cisco Systems, Inc. All rights reserved

## About the Authors

### **Mike Mankovsky, Technical Leader, Cisco Systems Inc.**

Mike Mankovsky is a Cisco Unified Computing System architect, focusing on Microsoft solutions with extensive experience in Microsoft Private Cloud, Hyper-V, storage systems, and Microsoft Exchange Server. Mike is a coauthor and architect of multiple FlexPod for Microsoft Private Cloud Fast Track Cisco Validated Designs.

### **Tim Cerling, Technical Marketing Engineer, Cisco Systems Inc.**

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

## Acknowledgements

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

- Haseeb Niazi, Cisco Systems Inc.
- Larry Roberts, Cisco Systems Inc.
- Glenn Sizemore, NetApp



# FlexPod Datacenter with Microsoft Private Cloud Fast Track 4.0 and Cisco Nexus 9000 Series Switches

---

## 1 Overview

Cisco Validated Designs consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of our customers.

The purpose of this document is to describe the Cisco and NetApp FlexPod solution, which is a validated approach for deploying Cisco and NetApp technologies as a shared cloud infrastructure.

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

The private cloud model provides much of the efficiency and agility of cloud computing, along with the increased control and customization that are achieved through dedicated private resources. With Private Cloud Fast Track, Microsoft and its hardware partners can help provide organizations both the control and the flexibility that are required to reap the potential benefits of the private cloud. Private Cloud Fast Track utilizes the core capabilities of the Windows Server, Hyper-V, and System Center to deliver a private cloud infrastructure as a service offering. These are also key software components that are used for every reference implementation.

### 1.1 Audience

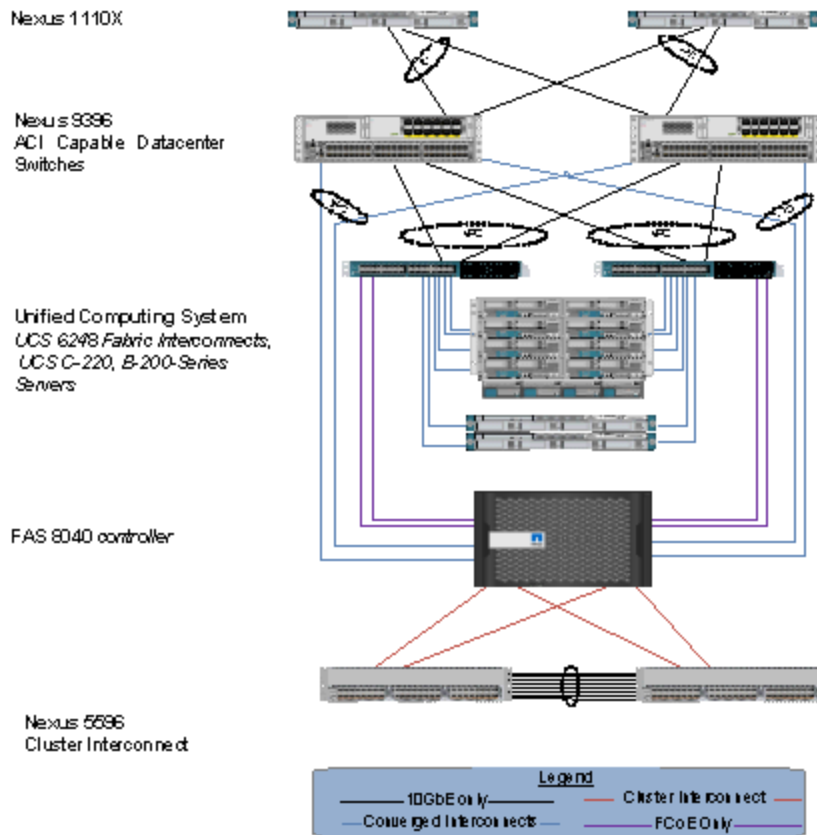
The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

## 2 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 v4 includes NetApp® FAS storage, Cisco Nexus® 9300 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 9396 switches
- Two Cisco Nexus 5596 switches

- Two Cisco UCS 6248 fabric interconnects
- Two Cisco Nexus 1110X appliances
- One chassis of Cisco UCS blades with two fabric extenders per chassis
- Eight Cisco USC B200M4 Servers
- One FAS8040 (HA pair)

Storage is provided by a NetApp FAS8040 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 for 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.

### 3 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	10
Native	VLAN to which untagged frames are assigned	2
CSV	VLAN for cluster shared volume	1004
Live Migration	VLAN designated for the movement of VMs from one physical host to another	1005
SMB	VLAN designated for SMB access to VHDX files on the NetApp storage array	1003
Database	VLAN for database access	1002
MF-Public	VLAN for Management Fabric application access	1001
AF-Public	VLAN for Application Fabric application access	1007

## 4 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.

## 5 Physical Infrastructure

### 5.1 FlexPod Cabling on Clustered Data ONTAP

Figure 2 shows the cabling diagram for a FlexPod configuration using clustered Data ONTAP.



Figure 2) FlexPod Cabling Diagram in Clustered Data ONTAP

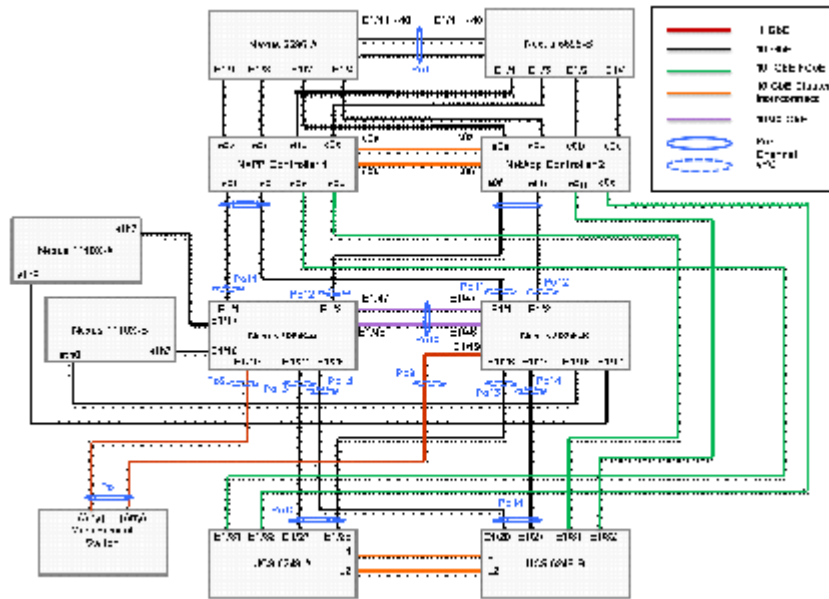


Table 2) Cisco Nexus 9396 A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9396 A	Eth1/1	10GbE	NetApp controller 1	e0e
	Eth1/2	10GbE	NetApp controller 2	eo
	Eth1/27	10GbE	Cisco UCS fabric interconnect A	Eth1/27
	Eth1/28	10GbE	Cisco UCS fabric interconnect B	Eth1/28
	Eth2/1*	10GbE	Cisco Nexus 9396 B	Eth2/1
	Eth2/2*	10GbE	Cisco Nexus 9396 B	Eth2/2
	Eth1/17	GbE	Cisco Nexus 1110-X A	LOM A
	Eth1/18	GbE	Cisco Nexus 1110-X B	LOM A
	Eth1/19	GbE	GbE management switch	Any
MGMT0	GbE	GbE management switch	Any	

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

**Table 3) Cisco Nexus 9396 B Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9396 B	Eth1/1	10GbE	NetApp controller 1	e0g
	Eth1/2	10GbE	NetApp controller 2	e0g
	Eth2/1*	10GbE	Cisco UCS Nexus 9396	Eth2/1
	Eth2/2*	10GbE	Cisco UCS Nexus 9396 B	Eth2/2
	Eth1/47*	10GbE	Cisco Nexus 9000 A	Eth1/47
	Eth1/48*	10GbE	Cisco Nexus 9000 A	Eth1/48
	Eth1/17	GbE	Cisco Nexus 1110-X A	LOM B
	Eth1/18	GbE	Cisco Nexus 1110-X B	LOM B
	Eth 1/19	GbE	GbE management switch	Any
	MGMT0	GbE	GbE management switch	Any

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

**Table 4) Cisco Nexus 5596 A Cluster Interconnect Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5596 A	Eth1/1	10GbE	NetApp controller 1	e0a
	Eth1/2	10GbE	NetApp controller 2	e0a
	Eth 1/3	10Gbe	NetApp controller 1	e0c
	Eth 1/4	10Gbe	NetApp controller 2	e0c
	Eth1/41	10GbE	Cisco Nexus 5596 B	Eth1/41
	Eth1/42	10GbE	Cisco Nexus 5596 B	Eth1/42
	Eth1/43	10GbE	Cisco Nexus 5596 B	Eth1/43
	Eth1/44	10GbE	Cisco Nexus 5596 B	Eth1/44
	Eth1/45	10GbE	Cisco Nexus 5596 B	Eth1/45
	Eth1/46	10GbE	Cisco Nexus 5596 B	Eth1/46
	Eth1/47	10GbE	Cisco Nexus 5596 B	Eth1/47
	Eth1/48	10GbE	Cisco Nexus 5596 B	Eth1/48
	MGMT0	GbE	GbE management switch	Any

**Table 5) Cisco Nexus 5596 B Cluster Interconnect Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5596 B	Eth1/1	10GbE	NetApp controller 1	e0b
	Eth1/2	10GbE	NetApp controller 2	e0b
	Eth 1/3	10Gbe	NetApp controller 1	e0d
	Eth 1/4	10Gbe	NetApp controller 2	e0d
	Eth1/41	10GbE	Cisco Nexus 5596 A	Eth1/41
	Eth1/42	10GbE	Cisco Nexus 5596 A	Eth1/42
	Eth1/43	10GbE	Cisco Nexus 5596 A	Eth1/43
	Eth1/44	10GbE	Cisco Nexus 5596 A	Eth1/44
	Eth1/45	10GbE	Cisco Nexus 5596 A	Eth1/45
	Eth1/46	10GbE	Cisco Nexus 5596 A	Eth1/46
	Eth1/47	10GbE	Cisco Nexus 5596 A	Eth1/47
	Eth1/48	10GbE	Cisco Nexus 5596 A	Eth1/48
	MGMT0	GbE	GbE management switch	Any

**Note:** When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

**Table 6) NetApp Controller 1 Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller 1	e0M	100MbE	100MbE management switch	Any
	e0i	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e0a	10GbE	Cisco Nexus 5596 A	Eth1/1
	e0b	10GbE	Cisco Nexus 5596 B	Eth1/1
	e0c	10GbE	Cisco Nexus 5596 A	Eth1/2
	e0d	10GbE	Cisco Nexus 5596 B	Eth1/2
	e0e	10GbE	Cisco Nexus 9000 A	Eth 1/1
	e0g	10GbE	Cisco Nexus 9000 B	Eth 1/1

**Table 7) NetApp Controller 2 Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller 2	e0M	100MbE	100MbE management switch	Any
	e0i	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e0a	10GbE	Cisco Nexus 5596 A	Eth1/3
	e0b	10GbE	Cisco Nexus 5596 B	Eth1/3
	e0c	10GbE	Cisco Nexus 5596 A	Eth1/4
	e0d	10GbE	Cisco Nexus 5596 B	Eth1/4
	e0e	10GbE	Cisco Nexus 9000 A	Eth 1/2
	e0g	10GbE	Cisco Nexus 9000 B	Eth 1/2

**Table 8) Cisco UCS Fabric Interconnect A Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/27	10GbE	Cisco Nexus 9000 A	Eth 1/27
	Eth1/28	10GbE	Cisco Nexus 9000 B	Eth 1/28
	Eth1/1	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX A	IOM 1/2
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

**Table 9) Cisco UCS Fabric Interconnect B Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	Eth1/28	10GbE	Cisco Nexus 9000 A	Eth 1/28
	Eth1/27	10GbE	Cisco Nexus 9000 B	Eth 1/27
	Eth1/1	10GbE	Cisco UCS Chassis Fabric Extender (FEX) B	IOM 2/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX B	IOM 2/2
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2

**Table 10) Cisco UCS C-Series 1**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 1	Port 0	10GbE	Cisco UCS fabric interconnect A	Eth 1/10
	Port 1	10GbE	Cisco UCS fabric interconnect B	Eth 1/10

**Table 11) Cisco UCS C-Series 2**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 2	Port 0	10GbE	Cisco UCS fabric interconnect A	Eth 1/11
	Port 1	10GbE	Cisco UCS fabric interconnect B	Eth 1/11

**Table 12) Cisco Nexus 1110-X A**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 1110-X A	Port 1	1 GbE	Management Switch	Any
Cisco Nexus 1110-X A	Port 2	1 GbE	Management Switch	Any
Cisco Nexus 1110-X A	Port 7	10 GbE	Cisco Nexus 9000 A	Eth 1/17
Cisco Nexus 1110-X A	Port 8	10 GbE	Cisco Nexus 9000 B	Eth 1/17

**Table 13) Cisco Nexus 1110-X B**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 1110-X B	Port 1	1 GbE	Management Switch	Any
Cisco Nexus 1110-X B	Port 2	1 GbE	Management Switch	Any
Cisco Nexus 1110-X B	Port 7	10 GbE	Cisco Nexus 9000 A	Eth 1/18
Cisco Nexus 1110-X B	Port 8	10 GbE	Cisco Nexus 9000 B	Eth 1/18

## 6 Cisco Nexus 9396PX Deployment Procedure

The following section provides a detailed procedure for configuring the Cisco Nexus 9396 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 9936PX running release Cisco NX-OS Firmware 6.1(2)I2(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.

## 6.1 Initial Cisco Nexus 9396PX Switch Configuration

These steps provide details for the initial Cisco Nexus 9396PX Switch setup.

### Cisco Nexus 9396 A

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

```
----- Basic System Configuration Dialog VDC: 1 -----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]:

  Create another login account (yes/no) [n]:

  Configure read-only SNMP community string (yes/no) [n]:

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : <<var_nexus_A_hostname>>

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address : <<var_nexus_A_mgmt0_ip>>

    Mgmt0 IPv4 netmask : <<var_nexus_A_mgmt0_netmask>>

  Configure the default gateway? (yes/no) [y]:

    IPv4 address of the default gateway : <<var_nexus_A_mgmt0_gw>>

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]:

  Enable the ssh service? (yes/no) [y]:

    Type of ssh key you would like to generate (dsa/rsa) [rsa]:

    Number of rsa key bits <1024-2048> [2048]:

  Configure the ntp server? (yes/no) [n]: y

    NTP server IPv4 address : <<var_global_ntp_server_ip>>

  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
switchname <<var_nexus_A_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_A_mgmt0_gw>>
exit
no feature telnet
```

```

ssh key rsa 2048 force
feature ssh
ntp server <<var_global_ntp_server_ip>>
copp profile strict
interface mgmt0
ip address <<var_nexus_A_mgmt0_ip>> <<var_nexus_A_mgmt0_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]:  Enter

Use this configuration and save it? (yes/no) [y]:  Enter

[#####] 100%
Copy complete.

```

## Cisco Nexus 9396 B

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

```

---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

  Create another login account (yes/no) [n]:

  Configure read-only SNMP community string (yes/no) [n]:

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : <<var_nexus_B_hostname>>

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address : <<var_nexus_B_mgmt0_ip>>

    Mgmt0 IPv4 netmask : <<var_nexus_B_mgmt0_netmask>>

  Configure the default gateway? (yes/no) [y]:

    IPv4 address of the default gateway : <<var_nexus_B_mgmt0_gw>>

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]:

  Enable the ssh service? (yes/no) [y]:

    Type of ssh key you would like to generate (dsa/rsa) [rsa]:

    Number of rsa key bits <1024-2048> [2048]:

  Configure the ntp server? (yes/no) [n]:  y

    NTP server IPv4 address : <<var_global_ntp_server_ip>>

```

```

Configure default interface layer (L3/L2) [L3]: L2

Configure default switchport interface state (shut/noshut) [shut]: Enter

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
switchname <<var_nexus_B_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_B_mgmt0_gw>>
exit
no feature telnet
ssh key rsa 2048 force
feature ssh
ntp server <<var_global_ntp_server_ip>>
copp profile strict
interface mgmt0
ip address <<var_nexus_B_mgmt0_ip>> <<var_nexus_B_mgmt0_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]: Enter

Use this configuration and save it? (yes/no) [y]: Enter

[#####] 100%
Copy complete.

```

## 6.2 Enable Appropriate Cisco Nexus Features

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

### Cisco Nexus A and Nexus B

1. Type `config t` to enter the global configuration mode.

```
config terminal
```

2. Use the following commands to enable the required features:

```
feature udld
feature lacp
feature vpc
```

## 6.3 Set Global Configurations

These steps provide details for setting global configurations.

### Cisco Nexus A and Nexus B

Perform the following configuration procedures on both Cisco Nexus switches.

#### **Configure Timezone**

1. Type `clock timezone <timezone abbreviation i.e. PST> <time offset i.e. -8 00>`.

```
clock timezone PST -8 00
```

**Note:** If you are using daylight savings or summer time, use the following command to configure the time offset.

2. Type `clock summer-time <timezone abbreviation e.g. PST>`.

```
clock summer-time PST
```



## Configure Spanning Tree

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
```

## 6.4 Create Necessary VLANs

These steps provide details for creating the necessary VLANs.

### Cisco Nexus A and Nexus B

1. Type the following commands:

```
vlan <<var_ib-mgmt_vlan_id>>
name Mgmt-VLAN

vlan <<var_native_vlan_id>>
name Native-VLAN

vlan <<var_CSV_vlan_id>>
name CSV-VLAN

vlan <<var_SMB_vlan_id>>
name SMB-VLAN

vlan <<var_Live-Migration_vlan_id>>
name Live-Migration-VLAN

vlan <<var_vm_database_vlan_id>>
name VM-Database-VLAN

vlan <<var_vm_MF-Public_vlan_id>>
name VM-MF-Public-VLAN

vlan <<var_vm_AF-Public_vlan_id>>
name VM-AF-Public-VLAN

vlan <<var_vm_AF_Cluster_Comm_vlan_id>>
name VM-AF-Cluster_Comm-VLAN
```

2. Type copy run star.t

3. Type show vlan.

VLAN	Name	Status	Ports
1	default	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/16, Eth1/17 Eth1/18, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth1/25, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/35 Eth1/36, Eth1/37, Eth1/38 Eth1/39, Eth1/40, Eth1/41 Eth1/42, Eth1/43, Eth1/44 Eth1/45, Eth1/46, Eth1/47 Eth1/48, Eth2/1, Eth2/2, Eth2/3 Eth2/4, Eth2/5, Eth2/6, Eth2/7 Eth2/8, Eth2/9, Eth2/10, Eth2/11 Eth2/12
2	Native-VLAN	active	
10	Mgmt-VLAN	active	

```

1001 MF-Public-VLAN          active
1002 SC-Database-VLAN      active
1003 SMB-VLAN              active
1004 CSV-VLAN              active
1005 Live-Migration-VLAN   active
1006 AF-Cluster-Comm-VLAN  active
1007 AF-Public-VLAN        active

```

```

VLAN Type      Vlan-mode
-----
1   enet        CE
2   enet        CE
10  enet        CE
1001 enet        CE
1002 enet        CE
1003 enet        CE
1004 enet        CE
1005 enet        CE
1006 enet        CE
1007 enet        CE

```

```

Remote SPAN VLANs
-----

```

```

Primary Secondary Type      Ports
-----

```

## 6.5 Configure Virtual Port Channel Domain

### Cisco Nexus 9396 A

To configure virtual port channels (vPCs) for switch A, complete the following steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make Cisco Nexus 9000A the primary vPC peer by defining a low priority value:

```
role priority 10
```

3. Use the management interfaces on the supervisors of the Cisco Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source <<var_nexus_A_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
auto-recovery
```

5. Show the running vPC configuration:

```

N9396-A(config)# show run vpc

!Command: show running-config vpc
!Time: Mon Sep 15 11:28:53 2014

version 6.1(2)I2(3)
feature vpc

vpc domain 100
  peer-switch
  role priority 10
  peer-keepalive destination 10.10.0.19 source 10.10.0.18

```

```
delay restore 150
peer-gateway
auto-recovery
```

#### 6. Show the vPC status:

```
N9396-A(config)# show vpc
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 100
Peer status              : peer link not configured
vPC keep-alive status   : peer is alive
Configuration consistency status : failed
Per-vlan consistency status : failed
Configuration inconsistency reason: vPC peer-link does not exist
Type-2 consistency status : failed
Type-2 inconsistency reason : vPC peer-link does not exist
vPC role                 : none established
Number of vPCs configured : 0
Peer Gateway             : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status     : Enabled (timeout = 240 seconds)
```

### Cisco Nexus 9396 B

To configure vPCs for switch B, complete the following steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make Cisco Nexus 9000 B the secondary vPC peer by defining a higher priority value than that of the Nexus 9000 A:

```
role priority 20
```

3. Use the management interfaces on the supervisors of the Cisco Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source <<var_nexus_B_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
auto-recovery
delay restore 150
peer-gateway
auto-recovery
```

5. Show the running vPC configuration:

```
N9396-B(config)# show run vpc

!Command: show running-config vpc
!Time: Mon Sep 15 11:32:43 2014

version 6.1(2)I2(3)
feature vpc

vpc domain 100
 peer-switch
 role priority 20
 peer-keepalive destination 10.10.0.18 source 10.10.0.19
 delay restore 150
 peer-gateway
 auto-recovery
```

6. Show the vPC status:

```

N9396-B(config)# show vpc
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 100
Peer status             : peer link not configured
vPC keep-alive status  : peer is alive
Configuration consistency status : failed
Per-vlan consistency status : failed
Configuration inconsistency reason: vPC peer-link does not exist
Type-2 consistency status : failed
Type-2 inconsistency reason : vPC peer-link does not exist
vPC role                : none established
Number of vPCs configured : 0
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status    : Enabled (timeout = 240 seconds)

```

## Configure Network Interfaces for the VPC Peer Links

### Cisco Nexus 9396 A

1. Define a port description for the interfaces connecting to VPC Peer <<var\_nexus\_B\_hostname>>.

```

interface Eth2/11
description VPC Peer <<var_nexus_B_hostname>>:2/11

interface Eth2/12
description VPC Peer <<var_nexus_B_hostname>>:2/12

```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```

interface Eth2/11,Eth2/12
channel-group 10 mode active
no shutdown

```

3. Define a description for the port-channel connecting to <<var\_nexus\_B\_hostname>>.

```

interface Po10
description vPC peer-link

```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, SMB, and VM traffic, packet control VLANs, and the native VLAN.

```

switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>, <<var_CSV_vlan_id>>

```

5. Make this port-channel the VPC peer link and bring it up.

```

vpc peer-link
no shutdown

```

6. Show the running vPC configuration:

```

!Command: show running-config vpc
!Time: Fri Sep 19 13:47:28 2014

version 6.1(2)I2(3)
feature vpc

vpc domain 100
  peer-switch
  role priority 20
  peer-keepalive destination 10.10.0.18 source 10.10.0.19

```

```
delay restore 150
peer-gateway
auto-recovery

interface port-channel10
vpc peer-link
```

## Cisco Nexus 9396 B

1. Define a port description for the interfaces connecting to VPC peer <<var\_nexus\_A\_hostname>>.

```
interface Eth2/11
description VPC Peer <<var_nexus_A_hostname>>:2/11

interface Eth2/12
description VPC Peer <<var_nexus_A_hostname>>:2/12
```

2. Apply a port channel to both VPC peer links and bring up the interfaces.

```
interface Eth2/11,Eth2/12
channel-group 10 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var\_nexus\_A\_hostname>>.

```
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, SMB, and VM traffic, packet control VLANs, and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>, <<var_csv_vlan_id>>
```

5. Make this port-channel the VPC peer link and bring it up.

```
vpc peer-link
no shutdown
```

6. Show the running vPC configuration.

```
!Command: show running-config vpc
!Time: Fri Sep 19 13:47:28 2014

version 6.1(2)I2(3)
feature vpc

vpc domain 100
peer-switch
role priority 20
peer-keepalive destination 10.10.0.18 source 10.10.0.19
delay restore 150
peer-gateway
auto-recovery

interface port-channel10
vpc peer-link
```

## Cisco Nexus 9000 A and B

### 1. Show the vPC status.

```
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 100
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role              : secondary
Number of vPCs configured : 0
Peer Gateway          : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status  : Enabled (timeout = 240 seconds)

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po10  up     10,1001-1007,1011
```

## 6.6 Configure Network Interfaces to NetApp Storage for Data Traffic

### Cisco Nexus 9396 A

#### 1. Define a description for the port-channel connecting to <<var\_node01>>.

```
interface Po11
description <<var_node01>>
```

#### 2. Make the port-channel a switchport, and configure a trunk to allow SMB and native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_smb_vlan_id>>
```

#### 3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

#### 4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

#### 5. Make this a VPC port-channel and bring it up.

```
vpc 11
no shutdown
```

#### 6. Show the port-channel 11 configuration.

```
!Command: show running-config interface port-channel11
!Time: Sat Sep 20 18:48:50 2014

version 6.1(2)I2(3)

interface port-channel11
  description fascluster01-01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  spanning-tree port type edge trunk
```

#### 7. Define a port description for the interface connecting to <<var\_node01>>.

```
interface Eth1/1
description <<var_node01>>:e0f
```

8. Apply it to a port channel and bring up the interface.

```
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 1003
mtu 9216
channel-group 11 mode active
no shutdown
```

9. Show the port eth1/1 configuration

```
!Command: show running-config interface Ethernet1/1
!Time: Sat Sep 20 19:01:24 2014

version 6.1(2)I2(3)

interface Ethernet1/1
  description fascluster01-01:e0f
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  mtu 9216
  channel-group 11 mode active
```

10. Define a description for the port-channel connecting to <<var\_node02>>.

```
interface Po12
description <<var_node02>>
```

11. Make the port-channel a switchport, and configure a trunk to allow SMB and native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_smb_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```
vpc 12
no shutdown
```

15. Show the port-channel 12 configuration.

```
!Command: show running-config interface port-channel12
!Time: Sat Sep 20 19:06:33 2014

version 6.1(2)I2(3)

interface port-channel12
  description fascluster01-01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
```

16. Define a port description for the interface connecting to <<var\_node02>>.

```
interface Eth1/2
description <<var_node02>>:e0f
```

## 17. Apply it to a port channel and bring up the interface

```
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 1003
mtu 9216
channel-group 12 mode active
no shutdown
```

## 18. Show the port eth1/2 configuration

```
!Command: show running-config interface Ethernet1/2
!Time: Sat Sep 20 19:13:28 2014

version 6.1(2)I2(3)

interface Ethernet1/2
  description fascluster01-02:e0f
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  mtu 9216
  channel-group 12 mode active
```

## Cisco Nexus 9000 B

### 1. Define a description for the port-channel connecting to <<var\_node01>>.

```
interface Po11
description <<var_node01>>
```

### 2. Make the port-channel a switchport, and configure a trunk to allow SMB and native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_smb_vlan_id>>
```

### 3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

### 4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

### 5. Make this a VPC port-channel and bring it up.

```
vpc 11
no shutdown
```

### 6. Show the port-channel 11 configuration.

```
! !Command: show running-config interface port-channel11
!Time: Sat Sep 20 19:24:33 2014

version 6.1(2)I2(3)

interface port-channel11
  description fascluster01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  spanning-tree port type edge trunk
  mtu 9216
```

### 7. Define a port description for the interface connecting to <<var\_node01>>.

```
interface Eth1/1
description <<var_node01>>:e0h
```



8. Apply it to a port channel and bring up the interface.

```
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 1003
mtu 9216
channel-group 11 mode active
no shutdown
```

9. Show the port eth1/1 configuration.

```
!Command: show running-config interface Ethernet1/1
!Time: Sat Sep 20 19:32:13 2014

version 6.1(2)I2(3)

interface Ethernet1/1
  description fascluster01:e0h
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  mtu 9216
  channel-group 11 mode active
```

10. Define a description for the port-channel connecting to <<var\_node02>>.

```
interface Po12
description <<var_node02>>
```

11. Make the port-channel a switchport, and configure a trunk to allow SMB and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_smb_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```
vpc 12
no shutdown
```

15. Show the port-channel 11 configuration.

```
Command: show running-config interface port-channel12
Time: Sat Sep 20 19:40:26 2014

ersion 6.1(2)I2(3)

nterface port-channel12
  description fascluster02
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
```

16. Define a port description for the interface connecting to <<var\_node02>>.

```
interface Eth1/2
description <<var_node02>>:e0h
```

17. Apply it to a port channel and bring up the interface.

```
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 1003
spanning-tree port type edge trunk
mtu 9216
channel-group 12 mode active
no shutdown
```

#### 18. Show the port eth1/2 configuration.

```
!Command: show running-config interface Ethernet1/2
!Time: Sat Sep 20 19:44:49 2014

version 6.1(2)I2(3)

interface Ethernet1/2
  description fascluster02:e0h
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 1003
  mtu 9216
  channel-group 12 mode active
```

## 6.7 Configure Network Interfaces to Cisco UCS Fabric Interconnects

### Cisco Nexus 9000 A

1. Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-A.

```
interface Po13
description <<var_ucs_clustername>>-A
```

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, SMB, VM traffic, and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 13
no shutdown
```

6. Show the port-channel 13 configuration.

```
!Command: show running-config interface port-channel13
!Time: Mon Sep 22 11:26:38 2014

version 6.1(2)I2(3)

interface port-channel13
  description MSPCFT-UCS01-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
```

7. Define a port description for the interface connecting to <<var\_ucs\_clustername>>-A.

```
interface Eth1/27
description <<var_ucs_clustername>>-A:1/27
```

8. Apply it to a port channel and bring up the interface.

```
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>
mtu9216
channel-group 13 mode active
no shutdown
```

9. Show the port eth1/27 configuration.

```
!Command: show running-config interface Ethernet1/27
!Time: Mon Sep 22 11:41:21 2014

version 6.1(2)I2(3)

interface Ethernet1/27
  description MSPCFT-UCS01-A:1/27
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  mtu 9216
  channel-group 13 mode active
```

10. Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-B.

```
interface Po14
description <<var_ucs_clustername>>-B
```

11. Make the port-channel a switchport, and configure a trunk to allow InBand management, SMB, and VM traffic VLANs and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>,
<<var_sc_database_vlan_id>>, <<var_csv_vlan_id>>, <<var_af_public_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```
vpc 14
no shutdown
```

15. Show the port-channel 14 configuration.

```
!Command: show running-config interface port-channel14
!Time: Mon Sep 22 11:47:20 2014

version 6.1(2)I2(3)

interface port-channel14
  description MSPCFT-UCS01-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  spanning-tree port type edge trunk
  mtu 9216
```

```
vpc 14
```

16. Define a port description for the interface connecting to <<var\_ucs\_clustername>>-B.

```
interface Eth1/28
description <<var_ucs_clustername>>-B:1/28
```

17. Apply it to a port channel and bring up the interface.

```
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>
mtu9216
channel-group 14 mode active
no shutdown
```

18. Show the port eth1/28 configuration.

```
!Command: show running-config interface Ethernet1/28
!Time: Mon Sep 22 11:52:16 2014

version 6.1(2)I2(3)

interface Ethernet1/28
  description MSPCFT-UCS01-A:1/28
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  mtu 9216
  channel-group 14 mode active
```

## Cisco Nexus 9396 B

1. Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-B.

```
interface Po14
description <<var_ucs_clustername>>-B
```

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, SMB, and VM traffic VLANs and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>,
<<var_sc_database_vlan_id>>, <<var_csv_vlan_id>>, <<var_af_public_vlan_id>>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 14
no shutdown
```

6. Show the port-channel 14 configuration.

```
!Command: show running-config interface port-channel14
!Time: Mon Sep 22 13:39:43 2014

version 6.1(2)I2(3)

interface port-channel14
  description fascluster01-B
  switchport mode trunk
```

```
switchport trunk native vlan 2
switchport trunk allowed vlan 10,1001-1007
spanning-tree port type edge trunk
mtu 9216
vpc 14
```

7. Define a port description for the interface connecting to <<var\_ucs\_clustername>>-B.

```
interface Eth1/27
description <<var_ucs_clustername>>-B:1/27
```

8. Apply it to a port channel and bring up the interface.

```
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>,
<<var_sc_database_vlan_id>>,<<var_csv_vlan_id>>, <<var_af_public_vlan_id>>

mtu 9216
channel-group 14 mode active
no shutdown
```

9. Show the port eth1/27 configuration

```
!Command: show running-config interface Ethernet1/27
!Time: Mon Sep 22 13:42:27 2014

version 6.1(2)I2(3)

interface Ethernet1/27
  description fascluster01-B:1/27
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  mtu 9216
  channel-group 14 mode active
```

10. Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-A.

```
interface Po13
```

```
description <<var_ucs_clustername>>-A
```

11. Make the port-channel a switchport, and configure a trunk to allow in-band management, SMB, and VM traffic VLANs and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>,
<<var_sc_database_vlan_id>>,<<var_csv_vlan_id>>, <<var_af_public_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```
vpc 13
no shutdown
```

15. Show the port-channel 14 configuration.

```
!Command: show running-config interface port-channel13
```

```

!Time: Mon Sep 22 13:46:22 2014

version 6.1(2)I2(3)

interface port-channel13
  description fascluster01-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13

```

16. Define a port description for the interface connecting to <<var\_ucs\_clustername>>-A.

```

interface Eth1/28
description <<var_ucs_clustername>>-A:1/28

```

17. Apply it to a port channel and bring up the interface.

```

switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_smb_vlan_id>>,
<<var_Live_Migration_vlan_id>>, <<var_mf_public_vlan_id>>,
<<var_sc_database_vlan_id>>,<<var_csv_vlan_id>>, <<var_af_cluster_comm_vlan_id>>,
<<var_af_public_vlan_id>>
mtu 9216
channel-group 13 mode active
no shutdown

```

18. Show the port eth1/28 configuration

```

!Command: show running-config interface Ethernet1/28
!Time: Mon Sep 22 13:53:39 2014

version 6.1(2)I2(3)

interface Ethernet1/28
  description fascluster01-A:1/28
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  mtu 9216
  channel-group 13

```

## Cisco Nexus 9000 A and B

1. Show the vPC status.

```

Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 100
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 4
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Enabled (timeout = 240 seconds)

vPC Peer-link status
-----
id  Port   Status Active vlans
--  ---
1   Po10   up     10,1001-1007,1012

```

```
vPC status
-----
```

id	Port	Status	Consistency	Reason	Active vlans
11	Pol1	down*	success	success	-
12	Pol2	down*	success	success	-
13	Pol3	down*	success	success	-
14	Pol4	down*	success	success	-

## 6.8 Configure Ports for Cisco Nexus 1110-X Virtual Appliances

### Cisco Nexus 9000 A

To configure the ports in switch A that are connected to the Cisco Nexus 1110-X, complete the following steps:

1. Define a port description for the interface connecting to Cisco Nexus 1110-X-A.

```
interface Eth1/17
description <<var_nexus_1110x-1>>:Eth1
```

2. Define a port description for the interface connecting to Cisco Nexus 1110-X-B.

```
interface Eth1/18
description <<var_nexus_1110x-2>>:Eth1
```

3. Configure both Nexus 1110-X ports to be trunks carrying the in-band management and packet control VLANs.

```
interface Eth4/17, Eth1/18
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_mf_public_vlan_id>>
```

4. Make the interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

5. Bring it up the interfaces.

```
no shutdown
```

6. Save the configuration.

```
copy running-config startup-config
[#####] 100%
Copy complete.
```

### Cisco Nexus 9000 B

To configure the ports in switch B that are connected to the Cisco Nexus 1110-X, complete the following steps:

1. Define a port description for the interface connecting to Cisco Nexus 1110-X-1.

```
interface Eth1/17
description <<var_nexus_1110x-A>>:Eth2
```

2. Define a port description for the interface connecting to Cisco Nexus 1110-X-2.

```
interface Eth1/18
description <<var_nexus_1110x-B>>:Eth2
```

3. Configure both Nexus 1110-X ports to be trunks carrying the in-band management and Packet Control VLANs.

```
interface Eth1/17, Eth1/18
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_mf_public_vlan_id>>
```

4. Make the interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

5. Bring it up the interfaces.

```
no shutdown
```

6. Save the configuration.

```
copy running-config startup-config
[#####] 100%
Copy complete.
```

## 6.9 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, Cisco recommends using vPCs to uplink the Cisco Nexus 9396 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.

## 7 Cisco Nexus 1110-X Appliance Deployment Procedure

The Cisco Nexus 1110-X Appliance runs the NetScaler 1000V network loadbalancer. The Nexus 1110-X connects to Nexus 9396PX switches and the Out-of-Band networks switches. These steps provide details for the initial Cisco Nexus 1110-X configuration.

### 7.1 Cisco Nexus 1110-X Appliance CIMC Configuration

#### Cisco Nexus 1110-A A and B

1. Connect to the Nexus 1100-X Appliance Console using a monitor and keyboard or a KVM Console.
2. During the appliance boot process, hit the F8 key to enter the Cisco IMC (CIMC) configuration.





```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,  
<F12> Network Boot
```

```
Bios Version : C220M3.2.0.3.0.080120140402  
Platform ID  : C220M3
```

```
Cisco IMC IPv4 Address  : 10.10.0.21  
Cisco IMC MAC Address  : 44:03:A7:4A:D7:3A
```

```
| Loading LSI EFI SAS Driver  
Total Memory = 64 GB Effective Memory = 64 GB  
Memory Operating Speed 1600 Mhz
```

```
Entering CIMC Configuration Utility...
```

3. In the CIMC configuration screen configure the following parameters to enable CIMC communication on the Out-Of-Band network:
  - a. Select Dedicated NIC Mode
  - b. Enter the IP Address, CIMC IP Address, and Gateway.
  - c. Set the appropriate VLAN ID for the Out-Of-Band network.
  - d. Select the NIC redundancy base on the cabling topology.
  - e. Hit the F10 key to save the configuration.
  - f. After 45 seconds hit F5 to refresh the configuration.

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                NIC redundancy
Dedicated:             [X]      None:                   [X]
Shared LOM:            [ ]      Active-standby:        [ ]
Cisco Card:            [ ]      Active-active:         [ ]
Shared LOM Ext:        [ ]

IP (Basic)
IPV4:                  [X]      IPV6:                   [ ]
DHCP enabled           [ ]
CIMC IP:               10.10.0.21
Prefix/Subnet:         255.255.255.0
Gateway:               10.10.0.1
Pref DNS Server:      0.0.0.0

VLAN (Advanced)
VLAN enabled:          [ ]
VLAN ID:               1
Priority:               0

*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings

```

4. Hit the ESC key to exit and reboot the system.

## 7.2 Configure the Cisco Nexus 1110-X

### Cisco Nexus 1110-X A

1. Use an SSH console to connect to the IP address of CIMC on the first Nexus1110-X appliance. Setup will start automatically.

```

----- Basic System Configuration Dialog -----

Log in with the CIMC account and password.

login as: admin
admin@10.10.0.21's password:

```

2. Connect to the VSA by typing connect host.

```

N1110-X-A# connect host

----- System Admin Account Setup -----

```

3. Begin the initial configuration by entering the password for the admin account.

```

Enter the password for "admin":
Confirm the password for "admin":

```

4. Enter Primary for the HA role.

```
Enter HA role[primary/secondary]: primary
```

5. Enter the VSA domain ID.

```
Enter the domain id<1-4095>: 100
```

6. Enter the control VLAN ID.

```
Enter control vlan <1-3967, 4048-4093>: 10
Control Channel Setup.
```

7. Type "0" to create a new port channel.

```
Choose Uplink: < Gig:1,2,3,4,5,6 10Gig:7,8 NewPortChannel:0 >[0]:
```

8. Type HA for the port channel type.

```
Choose type of portchannel <ha/lacp>[ha]: ha
```

9. Select interfaces 1 and 2 for the uplinks.

```
PortChannel1 - Choose uplinks < Gig:1,2,3,4,5,6 10Gig:7,8 >[1,2]: 1,2
```

10. Select VLAN 10 for the management VLAN ID.

```
Enter management vlan <1-3967, 4048-4093>: 10
Management Channel setup
```

11. Select the same port channel created in step 7.

```
Choose Uplink: < Gig:3,4,5,6 10Gig:7,8 Po1:9 NewPortChannel:0 >[9]:
Saving boot configuration. Please wait...

[#####] 100%
Copy complete, now saving to disk (please wait)...

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
```

of the system.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

## 12. Select not to create another account.

Create another login account (yes/no) [n]:

## 13. Configure read-only SNMP and set the community string.

Configure read-only SNMP community string (yes/no) [n]: yes

SNMP community string : FlexPod

## 14. Enter the VSA name.

Enter the VSA name : FlexPod-VSA

## 15. Select the option to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

## 16. Select IPv4.

Mgmt0 IP address type V4/V6? (V4): V4

## 17. Enter the IP address, netmask, and gateway.

Mgmt0 IPv4 address : 10.10.0.23

Mgmt0 IPv4 netmask : 255.255.255.0

Configure the default gateway? (yes/no) [y]:

IPv4 address of the default gateway : 10.10.0.1

## 18. Select not to configure the advanced IP options.

Configure advanced IP options? (yes/no) [n]: n

## 19. Select to disable telnet services.

Enable the telnet service? (yes/no) [n]: n

## 20. Enable SSH services and configure the SSH key.

```
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <768-2048> [1024]: 1024
```

## 21. Enable HTTP-Server.

```
Enable the http-server? (yes/no) [y]: y
```

## 22. Enable and configure the NTP server.

```
Configure the ntp server? (yes/no) [n]: yes
NTP server IPv4 address : 10.10.0.9
```

## 23. Review the configuration and save it.

```
The following configuration will be applied:
snmp-server community FlexPod ro
switchname FlexPod-VSA
interface mgmt0
ip address 10.10.0.23 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.10.0.1
ssh key rsa 1024 force
ssh server enable
feature http-server
ntp server 10.10.0.9

Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y

[#####] 100%
Copy complete, now saving to disk (please wait)...
System is going to reboot to configure network uplinks
```

## 24. Wait for the appliance to reboot. This may take a few minutes.

## 25. Login to the VSA (Virtual Service Appliance).

```
Cisco VSA
login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

## 26. List the configured port channels.

```
FlexPod-VSA(config)# show network port-channel database
PortChannel1
  Last membership update is successful
  2 ports in total, 2 ports up
  First operational port is Ethernet1
  Ports:   Ethernet1           [up]
          Ethernet2           [up]
```

## 27. Configure VLAN 10 to be the native VLAN for the management port channel.

```
FlexPod-VSA(config)# interface portChannel 1
FlexPod-VSA(config-if)# native vlan 10
Interface carries control traffic on new native vlan, new native vlan will get in effect
after reload
Warning! Mandatory reload needed for change to take effect.
Save configuration before reload, else Nexus1010 HA will break!
```

## 28. Save the configuration and reboot the device.

```
FlexPod-VSA(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
FlexPod-VSA(config-if)# reload
This command will reboot the system. (y/n)? [n] y
```

**Note:** Wait for the appliance to reboot. This may take a few minutes.

## Cisco Nexus 1110-X B

1. Use an SSH console to connect to the IP address of CIMC on the first Cisco Nexus1110-X appliance. Setup will start automatically.

```
----- System Admin Account Setup -----

Enter the password for "admin":
Confirm the password for "admin":
Enter HA role[primary/secondary]: secondary

Enter the domain id<1-4095>: 100

Enter control vlan <1-3967, 4048-4093>: 1

Control Channel Setup.
Choose Uplink: < Gig:1,2,3,4,5,6 10Gig:7,8 NewPortChannel:0 >[0]:
Choose type of portchannel <ha/lacp>[ha]: ha

PortChannel1 - Choose uplinks < Gig:1,2,3,4,5,6 10Gig:7,8 >[1,2]: 1,2

Enter management vlan <1-3967, 4048-4093>: 1

Management Channel setup

Choose Uplink: < Gig:3,4,5,6 10Gig:7,8 Po1:9 NewPortChannel:0 >[9]:
```

```
Saving boot configuration. Please wait...

[#####] 100%
Copy complete, now saving to disk (please wait)...
```

## 2. After the appliance reboots, login to the VSA.

```
Cisco VSA
login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# show network port-channel database
PortChannel1
  Last membership update is successful
  2 ports in total, 2 ports up
  First operational port is Ethernet1
  Ports:   Ethernet1           [up]
          Ethernet2           [up]

switch(config)# interface portChannel 1
switch(config-if)# native vlan 1
Interface carries control traffic on new native vlan, new native vlan will get in effect
after reload
Warning! Mandatory reload needed for change to take effect.
Save configuration before reload, else Nexus1010 HA will break!
switch(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
switch(config-if)# reload
This command will reboot the system. (y/n)? [n] y
```

**Note:** Wait for the appliance to reboot. This may take a few minutes.

### 1110-X A

1. Login to the VSA (Virtual Service Appliance).
2. Verify that the Appliance is operating in HA mode.

```
Cisco VSA
FlexPod-VSA login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
```

owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at

<http://www.opensource.org/licenses/gpl-2.0.php> and

<http://www.opensource.org/licenses/lgpl-2.1.php>

FlexPod-VSA# show system redundancy status

Redundancy role

-----

administrative: primary  
operational: primary

Redundancy mode

-----

administrative: HA  
operational: HA

This supervisor (sup-1)

-----

Redundancy state: Active  
Supervisor state: Active  
Internal state: Active with HA standby

Other supervisor (sup-2)

-----

Redundancy state: Standby  
Supervisor state: HA standby  
Internal state: HA standby

### 3. Create VLANs.

FlexPod-VSA# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

FlexPod-VSA(config)# vlan 2

FlexPod-VSA(config-vlan)# name Native

FlexPod-VSA(config-vlan)# vlan 1001

FlexPod-VSA(config-vlan)# name MF-Public

FlexPod-VSA(config-vlan)# show vlan

VLAN Name	Status	Ports
-----------	--------	-------

-----

1	default	active
2	Native	active
1001	VLAN1001	active

VLAN Type	Vlan-mode
-----------	-----------

-----

1	enet	CE
2	enet	CE
1001	enet	CE

Remote SPAN VLANs



Primary	Secondary	Type	Ports

## 8 NetScaler 1000V Deployment

The NetScaler 1000V network loadbalancer is deployed on the highly available Cisco Nexus 1110-X appliances that were deployed in the previous procedure.

### 1. Login to the VSA.

```
FlexPod-VSA# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

### 2. Create the virtual service blade with the desired name.

```
FlexPod-VSA(config)# virtual-service-blade FlexPod-NSVSB01
```

### 3. Deploy the NetScaler image into the service blade. The NetScaler OVA file should already be download to the Nexus 1110-X.

```
FlexPod-VSA(config-vs-b-config)# virtual-service-blade-type new
Netscaler1000V-NEXUS-10.5-53.9_nc.ova
```

Note: It can take awhile to finish OVA extract operation. Please be patient..

### 4. Assign VLANs to virtual interfaces.

```
FlexPod-VSA(config-vs-b-config)# interface ns_intf_0 vlan 10
FlexPod-VSA(config-vs-b-config)# interface ns_intf_1 vlan 2
FlexPod-VSA(config-vs-b-config)# interface ns_intf_2 vlan 2
FlexPod-VSA(config-vs-b-config)# interface ns_intf_3 vlan 2
FlexPod-VSA(config-vs-b-config)# interface ns_intf_4 vlan 2
FlexPod-VSA(config-vs-b-config)# interface ns_intf_5 vlan 2
FlexPod-VSA(config-vs-b-config)# interface ns_intf_6 vlan 1001
FlexPod-VSA(config-vs-b-config)# interface ns_intf_7 vlan 1001
```

### 5. Assign physical interfaces and PortChannels to virtual interfaces.

```
FlexPod-VSA(config-vs-b-config)# interface ns_intf_0 uplink PortChannel
1
FlexPod-VSA(config-vs-b-config)# interface ns_intf_1 uplink PortChannel
1
FlexPod-VSA(config-vs-b-config)# interface ns_intf_2 uplink PortChannel
1
FlexPod-VSA(config-vs-b-config)# interface ns_intf_3 uplink PortChannel
1
FlexPod-VSA(config-vs-b-config)# interface ns_intf_4 uplink PortChannel
1
FlexPod-VSA(config-vs-b-config)# interface ns_intf_5 uplink PortChannel
1
```

```
FlexPod-VSA(config-vs-b-config)# interface ns_intf_6 uplink Ethernet 7
FlexPod-VSA(config-vs-b-config)# interface ns_intf_7 uplink Ethernet 8
```

## 6. Disable unused NetScaler virtual interfaces.

```
FlexPod-VSA(config-vs-b-config)# interface VsbEthernet 1/3
FlexPod-VSA(config-if)# shutdown
FlexPod-VSA(config-if)# interface VsbEthernet 1/4
FlexPod-VSA(config-if)# shutdown
FlexPod-VSA(config-if)# interface VsbEthernet 1/5
FlexPod-VSA(config-if)# shutdown
FlexPod-VSA(config-if)# interface VsbEthernet 1/6
FlexPod-VSA(config-if)# shutdown
FlexPod-VSA(config-if)# interface VsbEthernet 1/7
FlexPod-VSA(config-if)# shutdown
```

## 7. Configure the basic parameters for the NetScaler 1000V.

```
FlexPod-VSA(config-vs-b-config)# enable
Enter vsb image: [Netscaler1000V-NEXUS-10.5-53.9_nc.ova]
NS HA [true/false]: [true]
Management IP version [V4|V6]: [V4]
Enter Primary IPv4 address: 10.10.0.24
Enter Primary subnet mask: 255.255.255.0
Primary IPv4 address of the default gateway: 10.10.0.1
Enter Secondary IPv4 address: [0.0.0.0]
Enter Secondary subnet mask: [0.0.0.0]
Enter secondary IPv4 address of the default gateway: [0.0.0.0]
Enter Primary HostName: FlexPod-NLB-Primary
Enter Secondary HostName: FlexPod-NLB-Secondary
Enter the password for 'nsroot': *****
----Details entered----
NS HA [true/false]: : true
Management IP version [V4|V6]: : V4
Enter Primary IPv4 address: : 10.10.0.24
Enter Primary subnet mask: : 255.255.255.0
Primary IPv4 address of the default gateway: : 10.10.0.1
Enter Secondary IPv4 address: : 10.10.0.25
Enter Secondary subnet mask: : 255.255.255.0
Enter secondary IPv4 address of the default gateway: : 10.10.0.1
Enter Primary HostName: : FlexPod-NLB-Primary
Enter Secondary HostName: : FlexPod-NLB-Secondary
Enter the password for 'nsroot': : *****
Do you want to continue installation with entered details (Y/N)? [Y] Y

Note: VSB installation is in progress, please use show virtual-service-
blade commands to check the installation status
```

**Note:** VSB installation may take up to 5 minutes.

## 8. Show the Virtual Blade Deployment Status.

```
FlexPod-VSA(config-vs-b-config)# do show virtual-service-blade summary
```

```

-----
-----
Name          HA-Role    HA-Status  Status
Location
-----
-----
FlexPod-NSVSB01  PRIMARY   NONE       VSB DEPLOY IN PROGRESS
PRIMARY
FlexPod-NSVSB01  SECONDARY NONE       VSB NOT PRESENT
SECONDARY

```

9. After the primary instance is deployed and powered on, the secondary instance deployment begins.

```

FlexPod-VSA(config-vsbs-config)# do show virtual-service-blade summary
-----
-----
Name          HA-Role    HA-Status  Status
Location
-----
-----
FlexPod-NSVSB01  PRIMARY   STANDBY    VSB POWERED ON
PRIMARY
FlexPod-NSVSB01  SECONDARY NONE       VSB DEPLOY IN PROGRESS
SECONDARY

```

10. The primary and secondary node will be in a Powered On state at the completion of the NetScaler virtual service blade deployment.

```

FlexPod-VSA(config-vsbs-config)# do show virtual-service-blade summary
-----
-----
Name          HA-Role    HA-Status  Status
Location
-----
-----
FlexPod-NSVSB01  PRIMARY   ACTIVE     VSB POWERED ON
PRIMARY
FlexPod-NSVSB01  SECONDARY STANDBY    VSB POWERED ON
SECONDARY

```

11. Verify that the NetScaler 1000V is Operating in High Availability Mode.

```

FlexPod-VSA(config-vsbs-config)# show virtual-service-blade name
FlexPod-NSVSB01
virtual-service-blade FlexPod-NSVSB01
Description:
Slot id:      1
Host Name:    FlexPod-NLB-Primary
Management IP: 10.10.0.24
VSB Type Name : NetScaler1000V-105539.1
Configured vCPU:      2

```

```

Operational vCPU:          2
Configured Ramsize:       2048
Operational Ramsize:      2048
Disksize:                 20
Configured CryptoOffload Bandwidth: 0
Operational CryptoOffload Bandwidth: 0
Configured CryptoOffload VF: 0
Operational CryptoOffload VF: 0
Heartbeat:                166680

```

Legends: P - Passthrough

```

-----
Interface                Type          MAC           VLAN   State  Uplink-Int
                          Pri  Sec Oper  Adm
-----
VsbEthernet1/1          ns_intf_0    0002.3d70.6402   1    up    up Po1    Po1
  internal              NA           NA              NA    up    up
VsbEthernet1/3          ns_intf_1    0002.3d70.6403   2    down  down Po1    Po1
VsbEthernet1/4          ns_intf_2    0002.3d70.6404   2    down  down Po1    Po1
VsbEthernet1/5          ns_intf_3    0002.3d70.6405   2    down  down Po1    Po1
VsbEthernet1/6          ns_intf_4    0002.3d70.6406   2    down  down Po1    Po1
VsbEthernet1/7          ns_intf_5    0002.3d70.6407   2    down  down Po1    Po1
VsbEthernet1/8          ns_intf_6    0002.3d70.6408 1001   up    upEth7  Eth7
VsbEthernet1/9          ns_intf_7    0002.3d70.6409 1001   up    upEth8  Eth8

```

HA Role: Primary

HA Status: ACTIVE

Status: VSB POWERED ON

Location: PRIMARY

SW version: NetScaler NS10.5: Build 53.9.nc, Date: Oct 30 2014,  
20:22:52

HA Role: Secondary

HA Status: STANDBY

Status: VSB POWERED ON

Location: SECONDARY

SW version: NetScaler NS10.5: Build 53.9.nc, Date: Oct 30 2014,  
20:22:52

VSB Info:

Netscaler VPX

## 12. SSH to the NetScaler, login, and accept the license agreement.

```

login as: nsroot
Using keyboard-interactive authentication.
Password:

```

```

Do you agree License Agreement (Y/N)?: Yes
Done

```

## 13. Verify the Netscaler node configuration.

```

> show node
1)      Node ID:      0
        IP:          10.10.0.24 (FlexPod-NLB-Primary)

```

```

Node State: UP
Master State: Primary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: ENABLED
Propagation: ENABLED
Enabled Interfaces : 0/1 0/2 1/1 1/2 1/3 1/4 1/5 1/6 1/7
Disabled Interfaces : None
HA MON ON Interfaces : 0/1 0/2 1/1 1/2 1/3 1/4 1/5 1/6 1/7
Interfaces on which heartbeats are not seen : 0/2 1/1 1/2 1/3
1/4 1/5
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT
Hello Interval: 200 msec
Dead Interval: 3 secs
Node in this Master State for: 0:0:13:0 (days:hrs:min:sec)
2) Node ID: 1
IP: 10.10.0.25
Node State: UP
Master State: Secondary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: SUCCESS
Propagation: ENABLED
Enabled Interfaces : 0/1 0/2 1/1 1/2 1/3 1/4 1/5 1/6 1/7
Disabled Interfaces : None
HA MON ON Interfaces : 0/1 0/2 1/1 1/2 1/3 1/4 1/5 1/6 1/7
Interfaces on which heartbeats are not seen : 0/2 1/1 1/2 1/3
1/4 1/5
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT

Local node information:
Critical Interfaces: 0/1 0/2 1/1 1/2 1/3 1/4 1/5 1/6 1/7
Done

```

#### 14. Disable the unused interfaces 1/1 through 1/5.

```

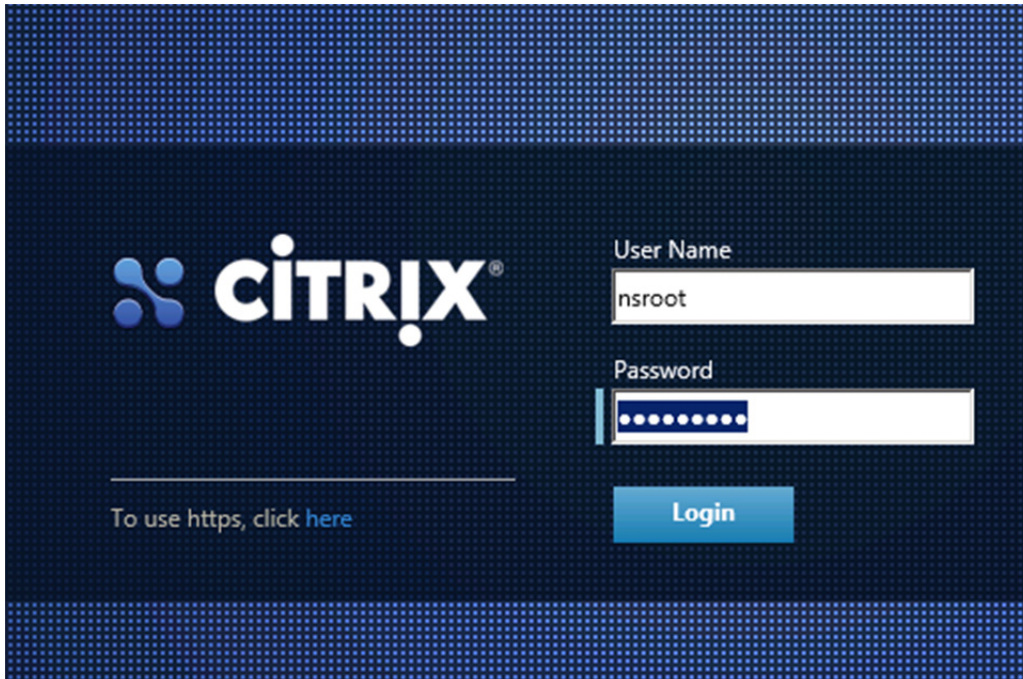
> disable interface 1/[1-5]
interface "1/1" disabled
interface "1/2" disabled
interface "1/3" disabled
interface "1/4" disabled
interface "1/5" disabled
Done

```

## 8.1 Configure the NetScaler Loadbalancer

To configure the NetScaler Loadbalancer, complete the following steps:

1. Open a web browser to the NetScaler primary IP address.



2. Click Subnet IP Address in the Configuration tab.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout

Dashboard **Configuration** Reporting Documentation Downloads

**Welcome!**

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: 10.10.0.24 Netmask: 255.255.255.0	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: Not configured	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: FlexPod-NLB-Primary DNS IP Address: Not configured Time Zone: CoordinatedUniversalTime	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	

The Subnet IP Address is the loadbalancer source address for client proxy communication. This address is also used for to perform health checks of the backend servers. This address is on the same subnet as on the MF-Public subnet where the Windows Azure Pac server interfaces are connected.

3. Enter the Subnet IP Address and click Done.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

### Subnet IP Address

A subnet IP address is used by the NetScaler to communicate with the backend servers. NetScaler uses this subnet IP address as a source IP address to proxy the client connections as well as to send monitor probes to check the health of the backend servers.

The infographic shows the usage of SNIP in client server communication.

Depending on your network topology, you might have to configure additional subnet IP addresses.

For more information about subnet IP addresses, [click here](#).

VIP = Virtual IP address  
SNIP = Subnet IP address

Subnet IP Address\*  
192 . 198 . 1 . 252

Netmask\*  
255 . 255 . 255 . 0

Done Do It Later

4. Click the Host Name, DNS IP Address, and Time Zone to configure the timezone.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

### Welcome!

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: 10.10.0.24 Netmask: 255.255.255.0	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: 192.168.1.252	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: FlexPod-NLB-Primary DNS IP Address: Not configured Time Zone: CoordinatedUniversalTime	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	

5. Enter the appropriate timezone and click Done.



### Host Name, DNS IP Address, and Time Zone

Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler is located.

Host Name	FlexPod-NLB-Primary
DNS IP Address	. . . +
Time Zone*	GMT-08:00-PST-Pacific/Pitcairn
<input type="button" value="Done"/> <input type="button" value="Back"/>	

6. Click Licenses TAB to install the appropriate NetScaler Licenses.

### Welcome!

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: 10.10.0.24   Netmask: 255.255.255.0	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: 192.168.1.252	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: FlexPod-NLB-Primary   DNS IP Address: Not configured   Time Zone: GMT-08:00-PST-Pacific/Pitcairn	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	

7. Install the NetScaler Licenses.



### Licenses

If a license is already present on your local computer, you can upload it to this NetScaler. Alternatively, you can use the serial number of this NetScaler or the license activation code (sent through email by Citrix) to allocate licenses from the Citrix licensing portal.

Upload license files from a local computer

8. Click Continue to go to proceed to the NetScaler configuration.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard **Configuration** Reporting Documentation Downloads

**Welcome!**

Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: <b>10.10.0.24</b>   Netmask: <b>255.255.255.0</b>	✓
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: <b>192.168.1.252</b>	✓
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: <b>FlexPod-NLB-Primary</b>   DNS IP Address: <i>Not configured</i>   Time Zone: <b>GMT-08:00-PST-Pacific/Pitcairn</b>	✓
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	—

**Continue**

9. Click System in the configuration tab to expand the System tree.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard **Configuration** Reporting Documentation Downloads

**System**

- Licenses
- Settings
- Diagnostics
- High Availability
- NTP Servers
- Reports
- Profiles
- + User Administration
- + Authentication
- + Auditing
- + SNMP
- + AppFlow
- + Cluster
- + EdgeSight Monitoring
- + Network
- + Web Interface
- + AppExpert
- + Traffic Management
- + Optimization
- + Security
- Show Unlicensed Features

NetScaler > System > System Information

System Information | System Sessions

Upgrade Wizard | Reboot | Statistics | Call Home

System Information	
NetScaler IP Address	10.10.0.24
Netmask	255.255.255.0
Node	Primary
Time Zone	GMT-08:00-PST-Pacific/Pitcairn
System Time	Tue, 20 Jan 2015 04:37:56 PST
Last Config Changed Time	Mon, 19 Jan 2015 21:55:04 PST
Last Config Saved Time	Fri, 16 Jan 2015 20:50:18 PST
Hardware Information	
Platform	NetScaler Virtual Appliance Nexus 1010 450110
Manufactured on	9/2/2013
CPU	2000 MHZ
Host Id	00023d706402
Serial no	HE2JU29DEN
Encoded serial no	HE2JU29DEN

10. Click Network to expand the Network tree and click Interfaces.

NetScaler > System > Network > Interfaces

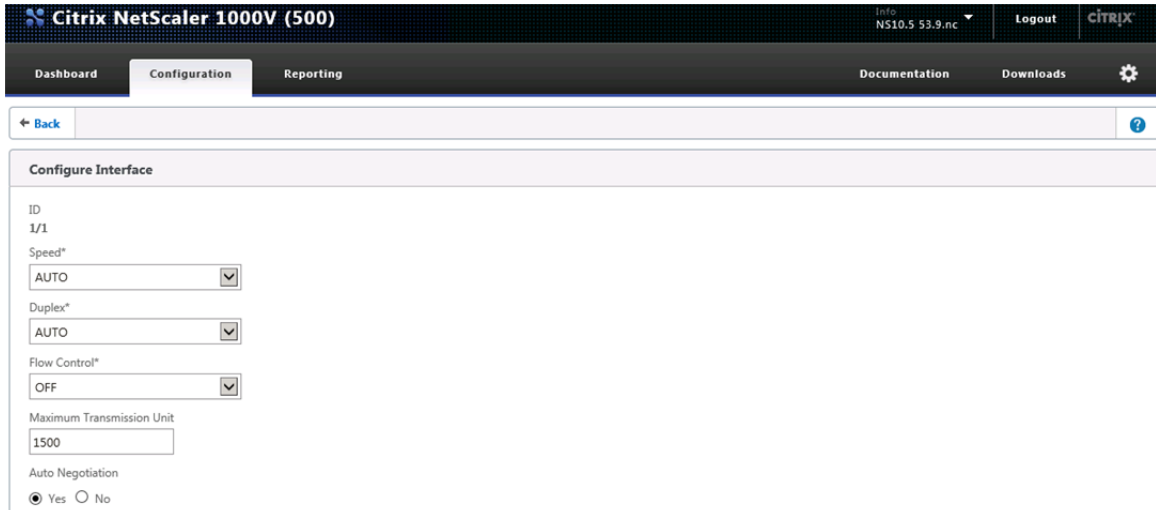
Interface	Description	Alias Name	MAC	Uptime	Downtime	VMAC	Enabled	State	H
0/1	(NetScaler Virtual Interface) #0		00:02:3d:70:64:02	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
0/2	(NetScaler Virtual Interface) #1		52:54:00:00:11:01	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
1/1	(NetScaler Virtual Interface) #2		00:02:3d:70:64:03	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/2	(NetScaler Virtual Interface) #3		00:02:3d:70:64:04	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/3	(NetScaler Virtual Interface) #4		00:02:3d:70:64:05	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/4	(NetScaler Virtual Interface) #5		00:02:3d:70:64:06	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/5	(NetScaler Virtual Interface) #6		00:02:3d:70:64:07	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/6	(NetScaler Virtual Interface) #7		00:02:3d:70:64:08	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
1/7	(NetScaler Virtual Interface) #8		00:02:3d:70:64:09	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
LO/1	(NetScaler Loopback interface) #9		00:02:3d:70:64:02	3d 7h 47m 59s		-N/A-	✓	Up	O

11. Turn off HA monitoring for the disabled interfaces 1/1 through 1/5 by right clicking each disabled interface and clicking Edit.

NetScaler > System > Network > Interfaces

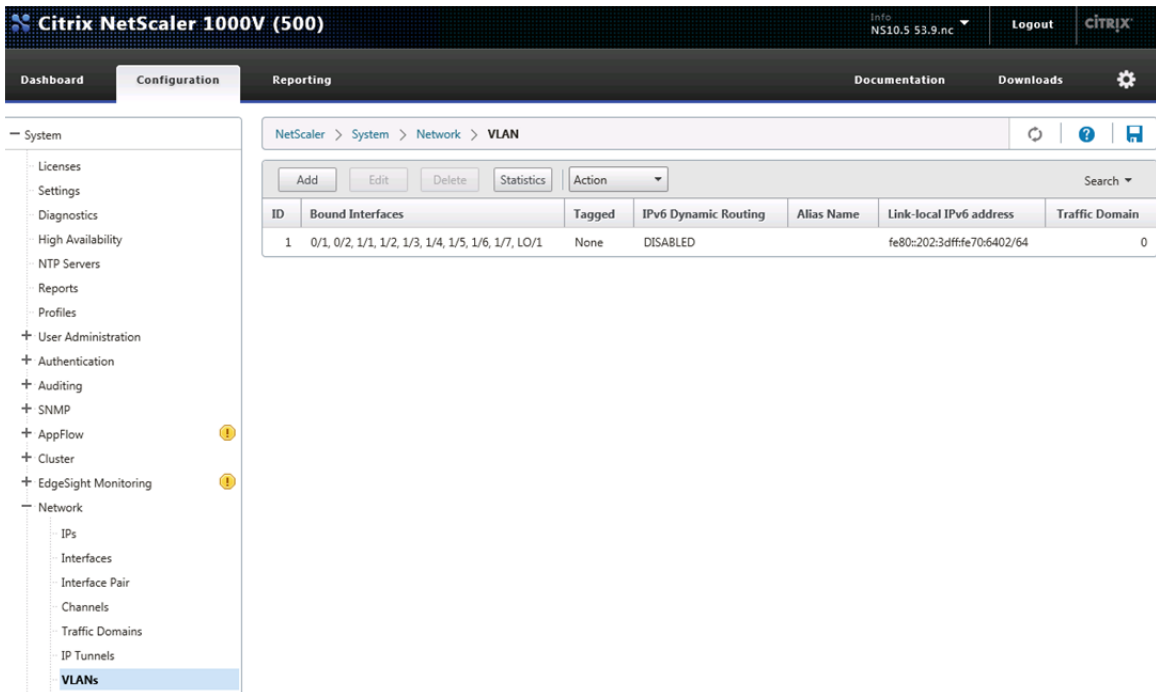
Interface	Description	Alias Name	MAC	Uptime	Downtime	VMAC	Enabled	State	H
0/1	(NetScaler Virtual Interface) #0		00:02:3d:70:64:02	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
0/2	(NetScaler Virtual Interface) #1		52:54:00:00:11:01	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
1/1	(NetScaler Virtual Interface) #2		00:02:3d:70:64:03	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/2	(NetScaler Virtual Interface) #3		00:02:3d:70:64:04	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/3	(NetScaler Virtual Interface) #4		00:02:3d:70:64:05	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/4	(NetScaler Virtual Interface) #5		00:02:3d:70:64:06	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/5	(NetScaler Virtual Interface) #6		00:02:3d:70:64:07	22m 36s	3d 7h 25m 13s	-N/A-	✗	Down (pwr off)	O
1/6	(NetScaler Virtual Interface) #7		00:02:3d:70:64:08	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
1/7	(NetScaler Virtual Interface) #8		00:02:3d:70:64:09	3d 7h 47m 49s	0m 10s	-N/A-	✓	Up	O
LO/1	(NetScaler Loopback interface) #9		00:02:3d:70:64:02	3d 7h 47m 59s		-N/A-	✓	Up	O

12. Select OFF for the HA Monitoring option and click OK at the bottom of the screen.



13. Repeat this procedure to disable HA monitoring for disabled interface 1/2 through 1/5.

14. Configure the VLAN for the NLB interfaces by clicking VLAN in the Network tree.



15. Click Add to add a VLAN. Enter the VLAN ID, VLAN Alias. Select Interface 1/6 and 1/7 in the interface binding tab. Do not check the Tagged box next to these interfaces.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back ?

### Create VLAN

VLAN ID\*  
1001

Alias Name  
MF-Public

Maximum Transmission Unit

IPv6 Dynamic Routing

Interface Bindings IP Bindings

<input type="checkbox"/>	1/3	<input type="checkbox"/>
<input type="checkbox"/>	1/4	<input type="checkbox"/>
<input type="checkbox"/>	1/5	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/6	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/7	<input type="checkbox"/>

Warning: "Associating interfaces" may cause this client to lose connectivity with Appliance. It is **recommended** that this command be issued from the Appliance console using the command line interface.

Create Close

16. Click the IP Bindings tab and check the box for the previously configured Subnet IP address.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back ?

### Create VLAN

VLAN ID\*  
1001

Alias Name  
MF-Public

Maximum Transmission Unit

IPv6 Dynamic Routing

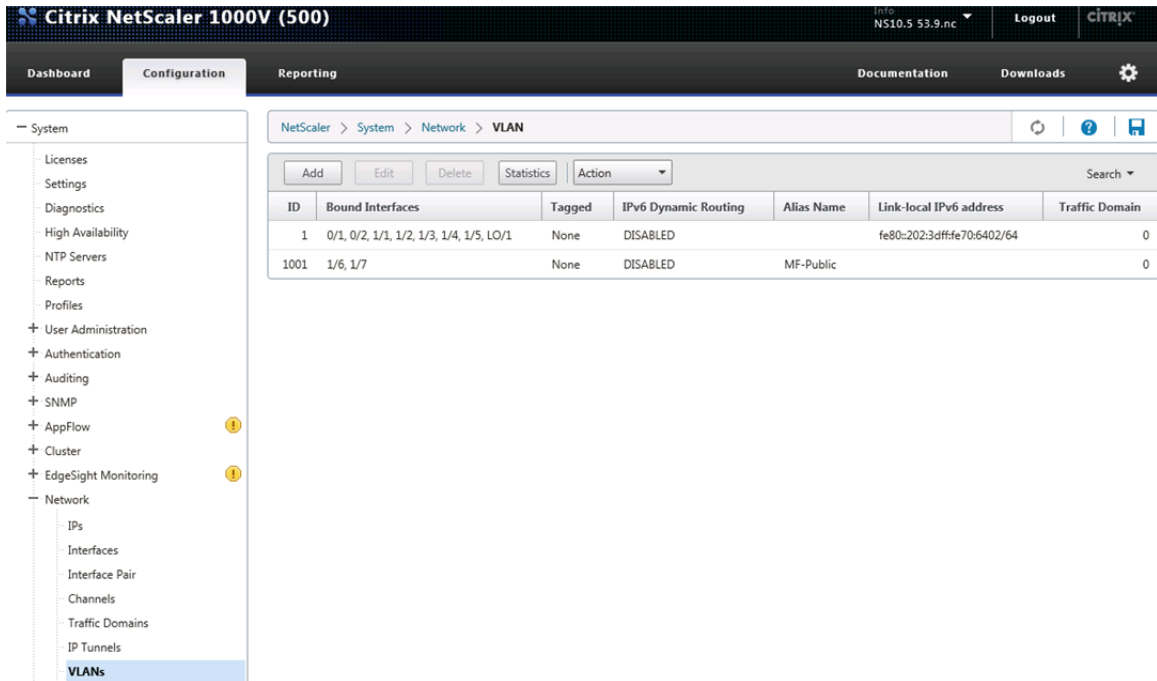
Interface Bindings IP Bindings

	IP Address	Traffic Domain	Type	Netmask
<input checked="" type="checkbox"/>	192.168.1.252	0	Subnet IP	255.255.255.0

Warning: "Associating interfaces" may cause this client to lose connectivity with Appliance. It is **recommended** that this command be issued from the Appliance console using the command line interface.

Create Close

17. Click Create to create the VLAN.



**Note:** The NetScaler Network Loadbalancer configuration will be completed after the Windows Azure Pack servers are installed.

## 9 Storage Configuration

### 9.1 Controller FAS80xx Series

Refer to the [Site Requirements Guide](#) for planning the physical location of the storage systems. From the downloaded guide, refer to the sections listed below:

- Site Preparation
- System Connectivity Requirements
- Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements
- 80xx Series Systems

#### NetApp Hardware Universe

The NetApp Hardware Universe provides supported hardware and software components for the specific Data ONTAP version. It provides configuration information for all NetApp storage appliances currently supported by the Data ONTAP software. It also provides a table of component compatibilities.

1. Make sure that the hardware and software components are supported with the version of Data ONTAP that you plan to install by checking the [NetApp Hardware Universe](#) at the [NetApp Support](#) site.
2. Access the [Hardware Universe](#) Application to view the System Configuration guides. Click the “Controllers” tab to view the compatibility between Data ONTAP software versions and NetApp storage appliances with the desired specifications.

- Alternatively, to compare components by storage appliance, click “Compare Storage Systems”.

### Controllers

Follow the physical installation procedures for the controllers in the [FAS80xx documentation](#) at the [NetApp Support](#) site.

## 9.2 Disk Shelves

NetApp storage systems support a wide variety of disk shelves and disk drives. The complete list of [disk shelves](#) that are supported is available at the [NetApp Support](#) site.

When using the SAS disk shelves with the NetApp storage controllers, refer to the [SAS Disk Shelves Universal SAS and ACP Cabling Guide](#) for the cabling guidelines.

## 9.3 Cisco NX5596 Cluster Network Switch Configuration

Table 14) Cisco Nexus 5596 Cluster Network Switch Configuration Prerequisites

Description
<ul style="list-style-type: none"><li>• Rack and connect power to the new Cisco Nexus 5596 switches</li><li>• Provide a terminal session that connects to the switch's serial console port (9600, 8, n, 1)</li><li>• Connect the <code>mgmt0</code> port to the management network and be prepared to provide IP address information</li><li>• Obtain password for admin</li><li>• Determine switch name</li><li>• Identify SSH key type (dsa, rsa, or rsa1)</li><li>• Set up an e-mail server for Cisco Smart Call Home and IP connectivity between the switch and the e-mail server</li><li>• Provide SNMP contact information for Cisco Smart Call Home (name, phone, street address)</li><li>• Identify a CCO ID associated with an appropriate Cisco SMARTnet<sup>®</sup> Service contract for Cisco Smart Call Home</li><li>• Enable Cisco SMARTnet Service for the device to be registered for Cisco Smart Call home</li></ul>

### Initial Setup of Cisco Nexus 5596 Cluster Interconnect

The first time a Cisco Nexus 5596 cluster interconnect is accessed, it runs a setup program that prompts the user to enter an IP address and other configuration information needed for the switch to communicate over the management Ethernet interface. This information is required to configure and manage the switch. If the configuration must be changed later, the setup wizard can be accessed again by running the `setup` command in EXEC mode.

To set up the Cisco Nexus 5596 cluster interconnect, complete the following steps. These steps will need to be completed on both cluster interconnects.

1. Provide applicable responses to the setup prompts displayed on the Cisco Nexus 5596 cluster interconnect.

```
Do you want to enforce secure password standard (yes/no): yes
Enter the password for the "admin": <password>
```

```

Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <switchname>
Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <ic_mgmt0_ip>
Mgmt0 IPv4 netmask: <ic_mgmt0_netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <ic_mgmt0_gw>
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa): rsa
Number of key bits <768-2048> : 1024
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <ntp_server_ip>
Enter basic FC configurations (yes/no) [n]: Enter

```

2. At the end of the setup, the configuration choices are displayed. Verify the information and save the configuration at this time.

```

Would you like to edit the configuration? (yes/no) [n]: <n>
Use this configuration and save it? (yes/no) [y]: <y>

```

## Download and Install NetApp Cluster Switch Software

When the Cisco Nexus 5596 is being used as a cluster network switch with Data ONTAP 8.2.2, it should be running NX-OS version 5.2(1)N1(1). The `show version` command from the switch command line interface will show the switch version currently running on the switch. If the currently running version is not 5.2(1)N1(1), go to the [NetApp Support](#) site and download and install NX-OS 5.2(u1)N1(1) for the Cisco Nexus 5596 switch. Make sure both cluster interconnects are running NX-OS version 5.2(1)N1(1).

## Download and Merge of NetApp Cluster Switch Reference Configuration File

Cluster network and management network switches are shipped without the configuration files installed. These files must be downloaded to the switches during deployment. Configuration files must be downloaded when the cluster network and management network switches are first installed or after the Cisco switch software is updated or reinstalled.

After the initial setup is complete, the NetApp cluster network switch reference configuration must be transferred to the switch and merged with the existing configuration. Instructions for this task and the reference configuration files for the appropriate switches are available on the [NetApp Support](#) site.

To download configuration files to a host and install them on a Cisco Nexus 5596 switch, complete the following steps on both cluster interconnects:

1. Obtain a console connection to the switch. Verify the existing configuration on the switch by running the `show run` command.
2. Log in to the switch. Make sure that the host recognizes the switch on the network (for example, use the ping utility).
3. Enter the following command:

```
copy <transfer_protocol>: bootflash: vrf management
```

4. Verify that the configuration file is downloaded.



5. Merge the configuration file into the existing `running-config`. Run the following command, where `<config file name>` is the file name for the switch type. A series of warnings regarding PortFast is displayed as each port is configured.

```
copy <config file name> running-config
```

6. Verify the success of the configuration merge by running the `show run` command and comparing its output to the contents of the configuration file (a `.txt` file) that was downloaded.
  - a. The output for both installed-base switches and new switches should be identical to the contents of the configuration file for the following items:
    - `banner` (should match the expected version)
    - Switch port descriptions such as `description Cluster Node x`
    - The new ISL algorithm `port-channel load-balance Ethernet source-dest-port`
  - b. The output for new switches should be identical to the contents of the configuration file for the following items:
    - Port channel
    - Policy map
    - System QoS
    - Interface
    - Boot
  - c. The output for installed-base switches should have the flow control receive and send values `on` for the following items:
    - Interface port-channel 1 and 2Ethernet interface 1/41 through Ethernet interface 1/48.
7. Copy the `running-config` to the `startup-config`.

```
copy running-config startup-config
```

### Cisco Smart Call Home Setup

To configure Smart Call Home on a Cisco Nexus 5596 switch, complete the following steps:

1. Enter the mandatory system contact using the `snmp-server contact` command in global configuration mode. Then run the `callhome` command to enter callhome configuration mode.

```
NX-5596#config t
NX-5596 (config)#snmp-server contact <sys-contact>
NX-5596 (config)#callhome
```

2. Configure the mandatory contact information (phone number, e-mail address, and street address).

```
NX-5596 (config-callhome)#email-contact <email-address>
NX-5596 (config-callhome)#phone-contact <+1-000-000-0000>
NX-5596 (config-callhome)#streetaddress <a-street-address>
```

3. Configure the mandatory e-mail server information. The server address is an IPv4 address, IPv6 address, or the domain-name of a SMTP server to which Call Home will send e-mail messages. Optional port number (default=25) and VRF may be configured.

```
NX-5596 (config-callhome)#transport email smtp-server <ip-address> port 25 use-vrf <vrf-name>
```

4. Set the destination profile CiscoTAC-1 e-mail address to [callhome@cisco.com](mailto:callhome@cisco.com)

```
NX-5596(config-callhome)#destination-profile CiscoTAC-1 email-addr callhome@cisco.com vrf management
```

5. Enable periodic inventory and set the interval.

```
NX-5596(config-callhome)#periodic-inventory notification
NX-5596(config-callhome)#periodic-inventory notification interval 30
```

6. Enable callhome, exit, and save the configuration.

```
NX-5596(config-callhome)#enable
NX-5596(config-callhome)#end
NX-5596#copy running-config startup-config
```

7. Send a callhome inventory message to start the registration process.

```
NX-5596#callhome test inventory
trying to send test callhome inventory message
successfully sent test callhome inventory message
```

8. Watch for an e-mail from Cisco regarding the registration of the switch. Follow the instructions in the e-mail to complete the registration for Smart Call Home.

## SNMP Monitoring Setup

1. Configure SNMP by using the following example as a guideline. This example configures a host receiver for SNMPv1 traps and enables all link up/down traps.

```
NX-5596(config)# snmp-server host <ip-address> traps { version 1 } <community> [udp_port <number>]
NX-5596(config)# snmp-server enable traps link
```

## 9.4 Clustered Data ONTAP 8.2.2

### Node 1

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. From the Loader-A prompt:

```
printenv
```

3. If the `last-OS-booted-ver` parameter is not set to 8.2.2, proceed to step 4 to load Data ONTAP 8.2.2 software. If Data ONTAP 8.2.2 is already loaded, proceed to step 16.
4. Allow the system to boot up.

```
boot_ontap
```

5. Press Ctrl-C when the Press Ctrl-C for Boot Menu message appears.

**Note:** If Data ONTAP 8.2.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, then select option 8 and `yes` to reboot the node. Then proceed with step 15.

6. To install new software, first select option 7.

```
7
```

7. Answer `yes` to perform a nondisruptive upgrade.

```
y
```

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

```
e0M
```

9. Select yes to reboot now.

```
y
```

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

```
<<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>>
```

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

**Note:** This Web server must be pingable.

```
<<var_url_boot_software>>
```

12. Press Enter for the user name, indicating no user name.

```
Enter
```

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

```
y
```

14. Enter yes to reboot the node.

```
y
```

**Note:** When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the LOADER prompt. If these actions occur, the system might deviate from this procedure.

15. Press Ctrl-C to exit autoboot when you see this message:

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

16. From the LOADER-A prompt, enter:

```
printenv
```

**Note:** If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

17. If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdpportname e0M
```

18. At the LOADER-A prompt, enter:

```
autoboot
```

19. When you see Press Ctrl-C for Boot Menu:

```
Ctrl - C
```

20. Select option 4 for clean configuration and initialize all disks.

```
4
```

21. Answer yes to Zero disks, reset config and install a new file system.

```
y
```

22. 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. After initialization is complete, the storage system reboots. You can continue to node 02 configuration while the disks for node 01 are zeroing.

## Node 2

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. From the Loader-A prompt, enter:

```
printenv
```

3. If the last-OS-booted-ver parameter is not set to 8.2.2, proceed to step 4 to load Data ONTAP 8.2.2 software. If Data ONTAP 8.2.2 is already loaded, proceed to step 16.
4. Allow the system to boot up.

```
boot_ontap
```

5. Press Ctrl-C when Press Ctrl-C for Boot Menu is displayed.

```
Ctrl-C
```

**Note:** If Data ONTAP 8.2.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, then select option 8 and *yes* to reboot the node. Then proceed with step 15.

6. To install new software first select option 7.

```
7
```

7. Answer *yes* to perform a nondisruptive upgrade.

```
y
```

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

```
e0M
```

9. Select *yes* to reboot now.

```
y
```

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

```
<<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>
```

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

**Note:** This Web server must be pingable.

```
<<var_url_boot_software>>
```

12. Press Enter for the user name, indicating no user name.

```
Enter
```

13. Select *yes* to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

14. Select *yes* to reboot the node.

```
y
```

**Note:** When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the LOADER prompt. If these actions occur, the system might deviate from this procedure.

15. Press Ctrl-C to exit autoboot when you see this message:

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

16. From the LOADER-A prompt, enter:

```
printenv
```

**Note:** If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

17. If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18. At the LOADER-A prompt, enter:

```
autoboot
```

19. When you see Press Ctrl-C for Boot Menu, enter:

```
Ctrl - C
```

20. Select option 4 for clean configuration and initialize all disks.

```
4
```

21. Answer yes to Zero disks, reset config and install a new file system.

```
y
```

22. 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.

## 9.5 Cluster Create in Clustered Data ONTAP

Table 15) Cluster Create in Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clustername>>
Clustered Data ONTAP base license	<<var_cluster_base_license_key>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster management netmask	<<var_clustermgmt_mask>>
Cluster management port	<<var_clustermgmt_port>>
Cluster management gateway	<<var_clustermgmt_gateway>>
Cluster Node01 IP address	<<var_node01_mgmt_ip>>
Cluster Node01 netmask	<<var_node01_mgmt_mask>>

Cluster Node01 gateway	<<var_node01_mgmt_gateway>>
------------------------	-----------------------------

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered Node01.

1. During the first node boot, the Cluster Setup wizard starts running on the console.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

**Note:** If a login prompt appears instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings and then enter the `cluster setup` command.

2. Enter the following command to create a new cluster:

```
create
```

3. Answer No to creating a single node cluster.

```
Do you intend for this node to be used as a single node cluster? {yes, no} [no]:
```

4. Answer Yes to reboot now and set storage failover to HA mode.

```
Do Non-HA mode, Reboot node to activate HA
Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no}
[yes]:
```

5. The system defaults are displayed.

```
System Defaults:
Private cluster network ports [e1a,e2a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
Do you want to use these defaults? {yes, no} [yes]:
```

6. NetApp recommends accepting the system defaults. To accept the system defaults, press Enter.

**Note:** Cluster is created; this can take a minute or two.

7. The steps to create a cluster are displayed.

```
Enter the cluster name: <<var_clustername>>
Enter the cluster base license key: <<var_cluster_base_license_key>>
Creating cluster <<var_clustername>>
Enter additional license key[]:
```

**Note:** For this validated architecture we recommend you install license keys for SnapRestore<sup>®</sup>, CIFS, FCP, FlexClone<sup>®</sup>, and SnapManager<sup>®</sup> Suite. After you finish entering the license keys, press Enter.

```
Enter the cluster administrators (username "admin") password: <<var_password>>
Retype the password: <<var_password>>
Enter the cluster management interface port [e0a]: e0a
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway: <<var_clustermgmt_gateway>>
```

8. Enter the DNS domain name.

```
Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>
```

**Note:** If you have more than one name server IP address, separate them with a comma.

9. Set up the node.

```
Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: e0b
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
enter the node management interface netmask:<<var_node01_mgmt_mask>>
Enter the node management interface default gateway:<<var_node01_mgmt_gateway>>
```

**Note:** The node management interface should be in a different subnet than the cluster management interface. The node management interfaces can reside on the out-of-band management network, and the cluster management interface can be on the in-band management network.

10. Press Enter to accept the AutoSupport™ message.

11. Reboot node 01.

```
system node reboot <<var_node01>>
Y
```

12. When you see Press Ctrl-C for Boot Menu, enter:

```
Ctrl - C
```

13. Select 5 to boot into maintenance mode.

```
5
```

14. When prompted Continue with boot?, enter y.

15. To verify the HA status of your environment, run the following command:

```
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.

16. To see how many disks are not owned, enter:

```
disk show -a
```

**Note:** No disks should be owned in this list.

17. Assign disks.

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

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

18. Reboot the controller.

```
halt
```

19. At the LOADER-A prompt, enter:

```
autoboot
```

## 9.6 Cluster Join in Clustered Data ONTAP

Table 16) Cluster Join in Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clustername>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster Node02 IP address	<<var_node02_mgmt_ip>>
Cluster Node02 netmask	<<var_node02_mgmt_mask>>
Cluster Node02 gateway	<<var_node02_mgmt_gateway>>

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered Node01, and the node joining the cluster in this example is Node02.

1. During the node boot, the Cluster Setup wizard starts running on the console.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

**Note:** If a login prompt displays instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings, and then enter the `cluster setup` command.

2. Enter the following command to join a cluster:

```
join
```

3. The system defaults are displayed.

```
System Defaults:
Private cluster network ports [e1a,e2a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
Do you want to use these defaults? {yes, no} [yes]:
```

4. NetApp recommends accepting the system defaults. To accept the system defaults, press Enter.

**Note:** The cluster creation can take a minute or two.

5. The steps to create a cluster are displayed.

```
Enter the name of the cluster you would like to join [<<var_clustername>>]:Enter
```

**Note:** The node should find the cluster name.

6. Set up the node.

```
Enter the node management interface port [e0M]: e0b
Enter the node management interface IP address: <<var_node02_mgmt_ip>>
Enter the node management interface netmask: Enter
Enter the node management interface default gateway: Enter
```

7. The node management interface should be in a subnet different from the cluster management interface. The node management interfaces can reside on the out-of-band



management network, and the cluster management interface can be on the in-band management network.

8. Press Enter to accept the AutoSupport message.
9. Log in to the Cluster Interface with the admin user id and `<<var_password>>`.
10. Reboot node 02.

```
system node reboot <<var_node02>>
Y
```

11. When you see `Press Ctrl-C for Boot Menu`, enter:

```
Ctrl - C
```

12. Select 5 to boot into maintenance mode.

```
5
```

12. At the question, `Continue with boot?` enter:

```
y
```

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

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

```
ha-config show
```

14. To see how many disks are not owned, enter:

```
disk show -a
```

15. Assign disks.

**Note:** This reference architecture allocates half the disks to each controller. Workload design could dictate different percentages, however. Assign all remaining disks to node 02.

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

16. Reboot the controller:

```
halt
```

17. At the `LOADER-A` prompt, enter:

```
autoboot
```

18. Press `Ctrl-C` for boot menu when prompted.

```
Ctrl-C
```

## 9.7 Log in to the Cluster

1. Open an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.

## 9.8 Zero All Spare Disks

1. Zero all spare disks in the cluster.

```
disk zerospares
```

## 9.9 Set Auto-Revert on Cluster Management

1. To set the auto-revert parameter on the cluster management interface, enter:

```
network interface modify -vserver <<var_clustername>> -lif cluster_mgmt -auto-revert true
```

## 9.10 Failover Groups Management in Clustered Data ONTAP

1. Create a management port failover group.

```
network interface failover-groups create -failover-group fg-cluster-mgmt -node <<var_node01>> -port e0a
network interface failover-groups create -failover-group fg-cluster-mgmt -node <<var_node02>> -port e0a
```

## 9.11 Assign Management Failover Group to Cluster Management LIF

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<var_clustername>> -lif cluster_mgmt -failover-group fg-cluster-mgmt
```

## 9.12 Failover Groups Node Management in Clustered Data ONTAP

1. Create a management port failover group.

```
network interface failover-groups create -failover-group fg-node-mgmt-01 -node <<var_node01>> -port e0b
network interface failover-groups create -failover-group fg-node-mgmt-01 -node <<var_node01>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt-02 -node <<var_node02>> -port e0b
network interface failover-groups create -failover-group fg-node-mgmt-02 -node <<var_node02>> -port e0M
```

## 9.13 Assign Node Management Failover Groups to Node Management LIFs

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<var_node01>> -lif mgmt1 -auto-revert true -use-failover-group enabled -failover-group fg-node-mgmt-01
network interface modify -vserver <<var_node02>> -lif mgmt1 -auto-revert true -use-failover-group enabled -failover-group fg-node-mgmt-02
```

## 9.14 Flash Cache in Clustered Data ONTAP

Complete the following steps to enable Flash Cache on each node:

1. Run the following commands from the cluster management interface:

```
system node run -node <<var_node01>> options flexscale.enable on
system node run -node <<var_node01>> options flexscale.lopri_blocks off
system node run -node <<var_node01>> options flexscale.normal_data_blocks on
system node run -node <<var_node02>> options flexscale.enable on
system node run -node <<var_node02>> options flexscale.lopri_blocks off
system node run -node <<var_node02>> options flexscale.normal_data_blocks on
```

**Note:** Data ONTAP 8.1 and later does not require a separate license for Flash Cache.

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

## 9.15 64-Bit Aggregates in Clustered Data ONTAP

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 the number of disks it will contain.

1. Execute the following command to create new aggregates:

```
aggr create -aggregate aggr01_n1 -nodes <<var_node01>> -s <<var_raidsize>> -diskcount <<var_num_disks>>
aggr create -aggregate aggr01_n2 -nodes <<var_node02>> -s <<var_raidsize>> -diskcount <<var_num_disks>>
```

**Note:** Retain 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.

**Note:** Calculate the RAID group size to allow for roughly balanced (same size) RAID groups of from 12 through 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.

**Note:** The aggregate cannot be created until disk zeroing completes. Use the `aggr show` command to display aggregate creation status. Do not proceed until both `aggr01_n1` and `aggr01_n2` are online. NetApp Best Practice suggests not creating an aggregate with fewer than five disks.

2. Disable Snapshot copies for the two data aggregates just created.

```
node run <<var_node01>> aggr options aggr01_n1 nosnap on
node run <<var_node02>> aggr options aggr01_n2 nosnap on
```

3. Delete any existing Snapshot copies for the two data aggregates.

```
node run <<var_node01>> snap delete -A -a -f aggr01_n1
node run <<var_node02>> snap delete -A -a -f aggr01_n2
```

4. Rename the root aggregate on node 01 to match the naming convention for this aggregate on node 02.

```
aggr show
aggr rename -aggregate aggr0 -newname <<var_node01_rootaggrname>>
```

## 9.16 Service Processor

Gather information about the network and the AutoSupport settings before configuring the Service Processor (SP).

Configure the SP using DHCP or static addressing. If the SP uses a static IP address, verify that the following SP prerequisites have been met:

- An available static IP address
- The network netmask
- The network gateway IP
- AutoSupport information

A best practice is to configure the AutoSupport recipients and mail host before configuring the SP. Data ONTAP automatically sends AutoSupport configuration to the SP, allowing the SP to send alerts and notifications through an AutoSupport

message to the system administrative recipients specified in AutoSupport. When configuring the SP, enter the name or the IP address of the AutoSupport mail host, when prompted.

A service processor needs to be set up on each node.

### **Configure the Service Processor on Node 01**

1. From the cluster shell, enter the following command:

```
system node run <<var_node01>> sp setup
```

2. Enter the following to set up the SP:

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node01_sp_ip>>
Please enter the netmask of the SP[]: <<var_node01_sp_mask>>
Please enter the IP address for the SP gateway[]: <<var_node01_sp_gateway>>
```

### **Configure the Service Processor on Node 02**

1. From the cluster shell, enter the following command:

```
system node run <<var_node02>> sp setup
```

2. Enter the following to set up the SP:

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node02_sp_ip>>
Please enter the netmask of the SP[]: <<var_node02_sp_mask>>
Please enter the IP address for the SP gateway[]: <<var_node02_sp_gateway>>
```

## **9.17 Storage Failover in Clustered Data ONTAP**

Run the following commands in a failover pair to enable storage failover.

1. Enable failover on one of the two nodes.

```
storage failover modify -node <<var_node01>> -enabled true
```

**Note:** Enabling failover on one node enables it for both nodes.

2. Enable HA mode for two-node clusters only.

**Note:** Do not run this command for clusters with more than two nodes because it will cause problems with failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

3. Verify that hardware assist is correctly configured and if needed modify the partner IP address.

```
storage failover hwassist show
storage failover modify -hwassist-partner-ip <<var_node02_mgmt_ip>> -node <<var_node01>>
storage failover modify -hwassist-partner-ip <<var_node01_mgmt_ip>> -node <<var_node02>>
```

## **9.18 IFGRP LACP in Clustered Data ONTAP**

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

1. Run the following commands on the command line to create interface groups (ifgrps).

```

ifgrp create -node <<var_node01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e4a
ifgrp create -node <<var_node02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e4a

```

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

**Note:** The interface group name must follow the standard naming convention of a0x.

## 9.19 VLAN in Clustered Data ONTAP

### 1. Create SMB VLANs.

```

network port vlan create -node <<var_node01>> -vlan-name a0a-<<var_smb_vlan_id>>
network port vlan create -node <<var_node02>> -vlan-name a0a-<<var_smb_vlan_id>>

```

## 9.20 Jumbo Frames in Clustered Data ONTAP

### 1. To configure a clustered Data ONTAP network port to use jumbo frames (which usually have an MTU of 9,000 bytes), run the following command from the cluster shell:

```

network port modify -node <<var_node01>> -port a0a -mtu 9000

WARNING: Changing the network port settings will cause a serveral second interruption in
carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0a -mtu 9000

WARNING: Changing the network port settings will cause a serveral second interruption in
carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node01>> -port a0a-<<var_smb_vlan_id>> -mtu 9000

WARNING: Changing the network port settings will cause a serveral second interruption in
carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0a-<<var_smb_vlan_id>> -mtu 9000

WARNING: Changing the network port settings will cause a serveral second interruption in
carrier.
Do you want to continue? {y|n}: y

```

## 9.21 NTP in Clustered Data ONTAP

To configure time synchronization on the cluster, complete the following steps:

### 1. Set the time zone for the cluster.

```

timezone <<var_timezone>>

```

**Note:** For example, in the Eastern United States, the time zone is `America/New_York`.

### 2. Set the date for the cluster.

```

date <<ccyymmddhhmm>>

```

**Note:** The format for the date is `<[Century] [Year] [Month] [Day] [Hour] [Minute]>`; for example, `201208081240`.

### 3. Configure the Network Time Protocol (NTP) for each node in the cluster.

```
system services ntp server create -node <<var_node01>> -server
<<var_global_ntp_server_ip>>
system services ntp server create -node <<var_node02>> -server
<<var_global_ntp_server_ip>>
```

## 9.22 SNMP in Clustered Data ONTAP

1. Configure SNMP basic information, such as the location and contact. When polled, this information is visible as the `sysLocation` and `sysContact` variables in SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

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

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

## 9.23 SNMPv1 in Clustered Data ONTAP

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.

## 9.24 SNMPv3 in Clustered Data ONTAP

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

1. Create a user called `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application snmp
```

2. Select all of the default authoritative entities and select `md5` as the authentication protocol.
3. Enter an eight-character minimum-length password for the authentication protocol, when prompted.
4. Select `des` as the privacy protocol.
5. Enter an eight-character minimum-length password for the privacy protocol, when prompted.

## 9.25 AutoSupport HTTPS in Clustered Data ONTAP

AutoSupport sends support summary information to NetApp through HTTPS.

1. Execute the following commands to configure AutoSupport:

```
system node autosupport modify -node * -state enable -mail-hosts <<var_mailhost>> -
transport https -support enable -noteto <<var_storage_admin_email>>
```

## 9.26 Cisco Discovery Protocol in Clustered Data ONTAP

Enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers by using the following procedure.

**Note:** To be effective, CDP must also be enabled on directly connected networking equipment such as switches and routers.

To enable CDP on the NetApp storage controllers, complete the following step:

1. Enable CDP on Data ONTAP.

```
node run -node <<var_node01>> options cdpd.enable on
node run -node <<var_node02>> options cdpd.enable on
```

## 9.27 Vserver

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

```
vserver setup
```

Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.

You can enter the following commands at any time:  
"help" or "?" if you want to have a question clarified,  
"back" if you want to change your answers to previous questions, and  
"exit" if you want to quit the Vserver Setup Wizard. Any changes you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default or omit a question, do not enter a value.

Step 1. Create a Vserver.  
You can type "back", "exit", or "help" at any question.

2. Enter the Vserver name.

```
Enter the Vserver name:Infra_vs1
```

3. Select the Vserver data protocols to configure.

```
Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi}:cifs, fcp
```

4. Select the Vserver client services to configure.

```
Choose the Vserver client services to configure {ldap, nis, dns}:Enter
```

5. Enter the Vserver's root volume aggregate:

```
Enter the Vserver's root volume aggregate {aggr01_n1, aggr01_n2} [aggr01_n1]:aggr01_n1
```

6. Enter the Vserver language setting. English is the default [C].

```
Enter the Vserver language setting, or "help" to see all languages [C]:Enter
```

7. Enter the Vserver's security style:

```
Enter the Vservers root volume's security style {unix, ntfs, mixed} [unix]:ntfs
```

8. Answer no to Do you want to create a data volume?

```
Do you want to create a data volume? {yes, no} [Yes]: no
```

9. Answer no to Do you want to create a logical interface?

```
Do you want to create a logical interface? {yes, no} [Yes]: no
```

10. Answer no to Do you want to Configure CIFS? {yes, no} [yes]: no.

```
Do you want to Configure CIFS? {yes, no} [yes]: no
```

11. Answer no to Do you want to Configure FCP? {yes, no} [yes]: no.

```
Do you want to Configure FCP? {yes, no} [yes]: no
```

12. Add the two data aggregates to the Infra\_vs1aggregate list for NetApp Virtual Console.

```
vserver modify -vserver Infra_vs1 -aggr-list aggr01_n1, aggr01_n2
```

## 9.28 Create Load Sharing Mirror of Vserver Root Volume in Clustered Data ONTAP

1. Create a volume to be the load sharing mirror of the infrastructure Vserver root volume on each node.

```
volume create -vserver Infra_vs1 -volume root_vol_m01 -aggregate aggr01_n1 -size 20MB -type DP
volume create -vserver Infra_vs1 -volume root_vol_m02 -aggregate aggr01_n2 -size 20MB -type DP
```

2. Create the mirroring relationships.

```
snapmirror create -source-path //Infra_vs1/root_vol -destination-path //Infra_vs1/root_vol_m01 -type LS
snapmirror create -source-path //Infra_vs1/root_vol -destination-path //Infra_vs1/root_vol_m02 -type LS
```

3. Initialize the mirroring relationship.

```
snapmirror initialize-ls-set -source-path //Infra_vs1/root_vol
```

4. Set an hourly (at 5 minutes past the hour) update schedule on each mirroring relationship.

```
snapmirror modify -source-path //Infra_vs1/root_vol -destination-path * -schedule hourly
```

## 9.29 Failover Groups SMB in Clustered Data ONTAP

1. Create a cifs port failover group.

```
network interface failover-groups create -failover-group fg-smb-<<var_smb_vlan_id>> -node <<var_node01>> -port a0a-<<var_smb_vlan_id>>
network interface failover-groups create -failover-group fg-smb-<<var_smb_vlan_id>> -node <<var_node02>> -port a0a-<<var_smb_vlan_id>>
```

## 9.30 NAS LIF in Clustered Data ONTAP

1. Create an SMB logical interface (LIF).

```
network interface create -vserver Infra_vs1 -lif smb_lif01 -role data -data-protocol cifs -home-node <<var_node01>> -home-port a0a-<<var_smb_vlan_id>> -address <<var_node01_smb_lif_ip>> -netmask <<var_node01_smb_lif_mask>> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -use-failover-group enabled -failover-group fg-smb-<<var_smb_vlan_id>>

network interface create -vserver Infra_vs1 -lif smb_lif02 -role data -data-protocol cifs -home-node <<var_node02>> -home-port a0a-<<var_smb_vlan_id>> -address <<var_node02_smb_lif_ip>> -netmask <<var_node02_smb_lif_mask>> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -use-failover-group enabled -failover-group fg-smb-<<var_smb_vlan_id>>
```

## 9.31 FCP LIF in Clustered Data ONTAP

1. Create four FCoE LIFs, two on each node.

```
network interface create -vserver Infra_vs1 -lif fcp_lif01a -role data -data-protocol fcp -home-node <<var_node01>> -home-port 3a
network interface create -vserver Infra_vs1 -lif fcp_lif01b -role data -data-protocol fcp -home-node <<var_node01>> -home-port 4a
network interface create -vserver Infra_vs1 -lif fcp_lif02a -role data -data-protocol fcp -home-node <<var_node02>> -home-port 3a
```



```
network interface create -vserver Infra_vs1 -lif fcp_lif02b -role data -data-protocol fcp
-home-node <<var_node02>> -home-port 4a
```

### 9.32 FC Service in Clustered Data ONTAP

1. Create the FC service on each Vserver. This command also starts the FC service and sets the FC alias to the name of the Vserver.

```
fcp create -vserver Infra_vs1
```

### 9.33 Add Infrastructure Vserver Administrator

1. Add the infrastructure Vserver administrator and Vserver administration logical interface in the in-band management network with the following commands:

```
network interface create -vserver Infra_vs1 -lif vsmgmt -role data -data-protocol none -
home-node <<var_node02>> -home-port e0a -address <<var_vserver_mgmt_ip>> -netmask
<<var_vserver_mgmt_mask>> -status-admin up -failover-policy nextavail -firewall-policy
mgmt -auto-revert true -use-failover-group enabled -failover-group fg-cluster-mgmt

network routing-groups route create -vserver Infra_vs1 -routing-group
d<<var_clustermgmt_ip>>/<<var_clustermgmt_cidr_netmask>> -destination 0.0.0.0/0 -gateway
<<var_clustermgmt_gateway>>

security login password -username vsadmin -vserver Infra_vs1
Please enter a new password: <<var_vsadmin_password>>
Please enter it again: <<var_vsadmin_password>>

security login unlock -username vsadmin -vserver Infra_vs1
```

### 9.34 HTTPS Access in Clustered Data ONTAP

Secure access to the storage controller must be configured.

1. Increase the privilege level to access the certificate commands.

```
set -privilege advanced
Do you want to continue? {y|n}: y
```

2. Generally, a self-signed certificate is already in place. Check it with the following command:

```
security certificate show
```

3. Run the following commands as one-time commands to generate and install self-signed certificates:

**Note:** You can also use the `security certificate delete` command to delete expired certificates

```
security certificate create -vserver Infra_vs1 -common-name
<<var_security_cert_vserver_common_name>> -size 2048 -country <<var_country_code>> -state
<<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email
<<var_storage_admin_email>>

security certificate create -vserver <<var_clustername>> -common-name
<<var_security_cert_cluster_common_name>> -size 2048 -country <<var_country_code>> -state
<<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email
<<var_storage_admin_email>>

security certificate create -vserver <<var_node01>> -common-name
<<var_security_cert_node01_common_name>> -size 2048 -country <<var_country_code>> -state
<<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email
<<var_storage_admin_email>>

security certificate create -vserver <<var_node02>> -common-name
<<var_security_cert_node02_common_name>> -size 2048 -country <<var_country_code>> -state
```

```
<<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email <<var_storage_admin_email>>
```

#### 4. Configure and enable SSL and HTTPS access and disable Telnet access.

```
system services web modify -external true -ssl3-enabled true
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http -action allow
system services firewall policy create -policy mgmt -service http -action deny -ip-list 0.0.0.0/0
system services firewall policy delete -policy mgmt -service telnet -action allow
system services firewall policy create -policy mgmt -service telnet -action deny -ip-list 0.0.0.0/0
security ssl modify -vserver Infra_vs1-certificate <<var_security_cert_vserver_common_name>> -enabled true
Y
security ssl modify -vserver <<var_clustername>> -certificate <<var_security_cert_cluster_common_name>> -enabled true
Y
security ssl modify -vserver <<var_node01>> -certificate <<var_security_cert_node01_common_name>> -enabled true
Y
security ssl modify -vserver <<var_node02>> -certificate <<var_security_cert_node02_common_name>> -enabled true
Y
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled true
vserver services web access create -name spi -role admin -vserver <<var_clustername>>
vserver services web access create -name ontapi -role admin -vserver <<var_clustername>>
```

**Note:** vserver services web access create –name compat –role admin –vserver <<var\_clustername>> It is normal for some of these commands to return an error message stating that the entry does not exist.

### 9.35 DNS Service in Clustered Data ONTAP

1. Create the DNS service on each Vserver. This command also starts the DNS service on the Vserver.

```
dns create -vserver Infra_vs1 -domains <<var_dnsdomain>> -name-servers <<var_ip_dnsserver>> -state enabled
```

### 9.36 SMB in Clustered Data ONTAP

Run all commands to configure SMB on the Vserver.

1. Secure the default rule for the default export policy and create the FlexPod export policy.

```
vserver export-policy rule modify -vserver Infra_vs1 -policyname default -ruleindex 1 -rorule never -rwrule never -superuser never
vserver export-policy create -vserver Infra_vs1 FlexPod
```

2. Create a new rule for the FlexPod export policy.

**Note:** For each Hyper-V host being created, create a rule. Each host will have its own rule index. Your first Hyper-V host will have rule index 1, your second Hyper-V host will have rule index 2, and so on.

```
vserver export-policy rule create -vserver Infra_vs1 -policyname FlexPod -ruleindex 1 -protocol cifs -clientmatch <<var_vmhost_host1_smb_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid false
```

3. Assign the FlexPod export policy to the infrastructure Vserver root volume.

```
volume modify -vserver Infra_vs1 -volume root_vol -policy FlexPod
```

#### 4. Create the CIFS service and add it to Active Directory.

```
vserver cifs create -vserver Infra_vs1 -cifs-server Infra_vs1 -domain <<var_dnsdomain>>
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "FlexPod.com" domain.

Enter the user name: adminXX

Enter the password: XXnetapp!

### 9.37 FlexVol in Clustered Data ONTAP

1. The following information is required to create a FlexVol<sup>®</sup> volume: the volume's name and size, and the aggregate on which it will exist. Create one VHD store volume, a server boot LUN volume, and the System Center SQL Database volumes. Also update the Vserver root volume load sharing mirrors to make the SMB shares accessible.

```
volume create -vserver Infra_vs1 -volume infra_vhd_store_1 -aggregate aggr01_n2 -size 500g -state online -policy FlexPod -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume ucs_boot -aggregate aggr01_n1 -size 1TB -state online -policy default -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume quorum -aggregate aggr01_n1 -size 5GB -state online -policy default -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume sc_sql_db -aggregate aggr01_n1 -size 1TB -state online -policy default -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume sc_sql_log -aggregate aggr01_n1 -size 500GB -state online -policy default -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume scvmm_pool1 -aggregate aggr01_n2 -size 4TB -state online -policy FlexPod -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume witness -aggregate aggr01_n1 -size 100GB -state online -policy default -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_vs1 -volume sc_app_vm -aggregate aggr01_n1 -size 1TB -state online -policy default -space-guarantee none -percent-snapshot-space 0

snapmirror update-ls-set -source-path //Infra_vs1/root_vol
```

### 9.38 Deduplication in Clustered Data ONTAP

1. Enable deduplication on appropriate volumes.

```
volume efficiency on -vserver Infra_vs1 -volume infra_vhd_store_1
volume efficiency on -vserver Infra_vs1 -volume ucs_boot
volume efficiency on -vserver Infra_vs1 -volume scvmm_lib
volume efficiency on -vserver Infra_vs1 -volume scvmm_pool0
volume efficiency on -vserver Infra_vs1 -volume sc_sql_db
volume efficiency on -vserver Infra_vs1 -volume sc_sql_log
volume efficiency on -vserver Infra_vs1 -volume app_vm
```

### 9.39 Create Infrastructure SMB Share

1. Create the SMB share to house the infrastructure Virtual Machines.

```
cifs share create -share-name infra_vhd_store_1 -vserver Infra_vs1 -path /infra_vhd_store_1 -share-properties browsable,continuously-available
```

## 10 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 2.2(3d) is the minimum required UCS firmware version. See the FlexPod for Microsoft Private Cloud v4 Design Guide for details.

### 10.1 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.

## 10.2 Enable FC Switch Mode On the Fabric Interconnects

Switching FC modes requires the Fabric Interconnects to reboot. The reboot will take place automatically. When the Fabric Interconnects complete the reboot process a new management session must be established for to continue with management and configuration.

1. Navigate to the Equipment tab in the left pane and expand the Fabric Interconnects object.
2. Select Fabric Interconnect A in the left pane and click Set FC Switch Mode in the left pane.
3. Wait for the Fabric Interconnects to reboot before proceeding.

## 10.3 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. Log back into USC Manager
2. Select the LAN tab at the top of the left window.
3. Select `Pools > IP Pool ext-mgmt`.
4. Right-click `Management IP Pool`.
5. Select `Create Block of IP Addresses`.
6. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
7. Click `OK` to create the IP block.
8. Click `OK` in the message box.

## 10.4 Synchronize Cisco UCS to NTP

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

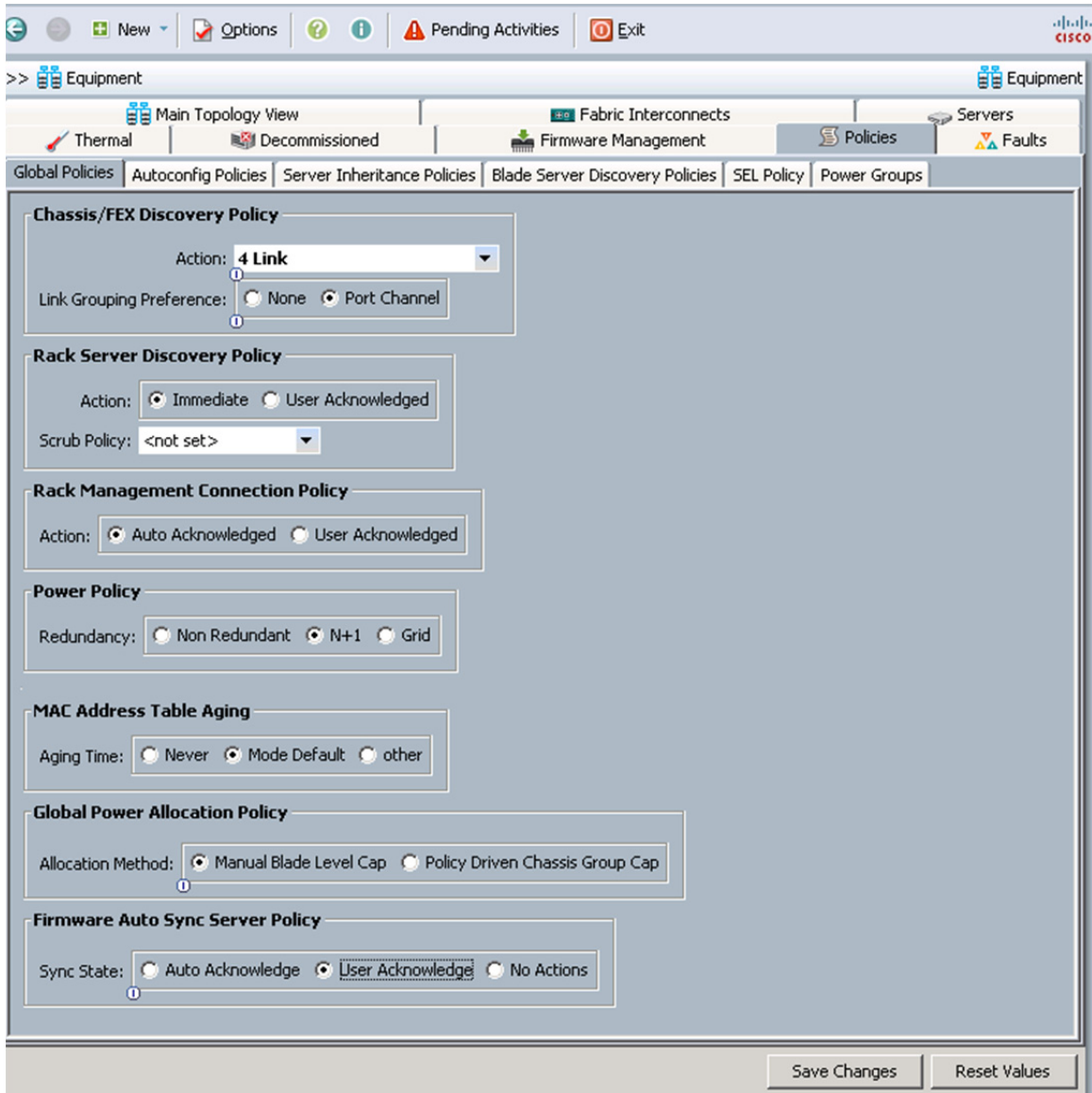
1. Select the `Admin` tab at the top of the left window.

2. Select **All > Timezone Management**.
3. Right-click **Timezone Management**.
4. In the right pane, select the appropriate timezone in the **Timezone** drop-down menu.
5. Click **Add NTP Server**.
6. Input the NTP server IP and click **OK**.
7. Click **Save Changes** and then **OK**.

## 10.5 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.

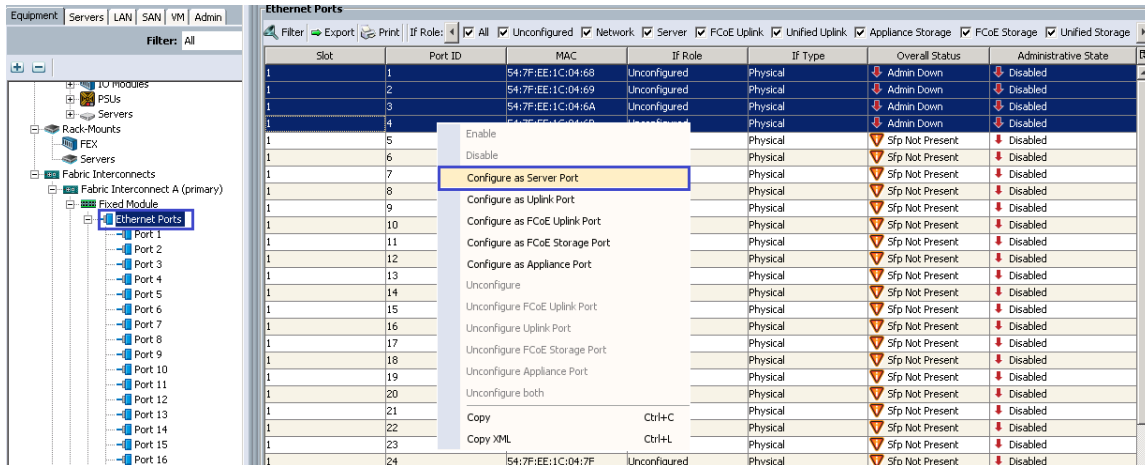
1. Navigate to the **Equipment** tab in the left pane and select the **Equipment** top-node object.
2. In the right pane, click the **Policies** tab.
3. Under **Global Policies**, change the **Chassis Discovery Policy** to **4-link** or set it to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Keep **Link Grouping Preference** set to **Port Channel**
5. Select **Manual Blade Level Cap** for the **Global Power Allocation Policy**
6. Select **User Acknowledge** for the **Firmware Auto Sync Server Policy**
7. Click **Save Changes** in the bottom right corner.



## 10.6 Enable Server, Uplink Ports, and FCoE Storage Ports

These steps provide details for enabling server, uplinks, and FCoE storage 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 27 and 28 that are connected to the Cisco Nexus 9396 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 ports 31 and 32 that are connected to the NetApp FAS 8040 storage array, right-click them, and select Configure as FCoE Storage Port.
11. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
12. At the prompt, click Yes to confirm the uplink ports, and then click OK.
13. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
14. Expand the Ethernet Ports object.
15. 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.
16. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
17. Select ports 27 and 28 that are connected to the Cisco Nexus 9396 switches, right-click them, and select Configure as Uplink Port.
18. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
19. At the prompt, click Yes to confirm the uplink ports, and then click OK.
20. Select ports 31 and 32 that are connected to the NetApp FAS 8040 storage array, right-click them, and select Configure as FCoE Storage Port.
21. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
22. At the prompt, click Yes to confirm the uplink ports, and then click OK.

## 10.7 Create Uplink Port Channels to the Cisco Nexus 9396 Switches

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

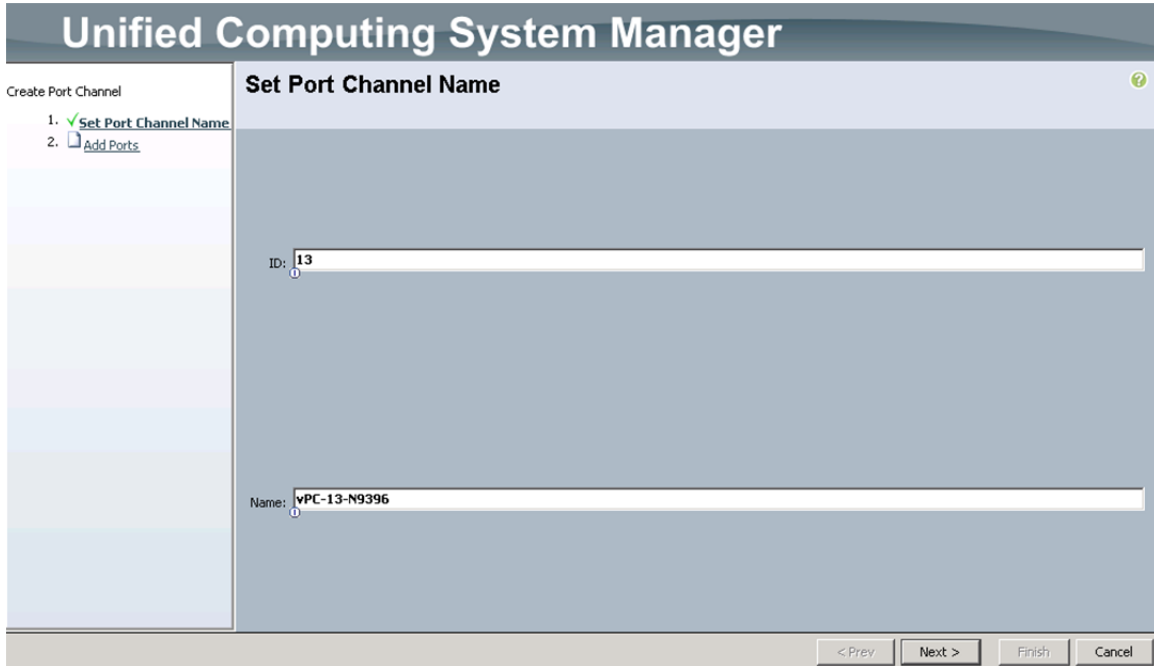
1. Select the LAN tab on the left of the window.

**Note:** Two Port Channels are created, one from fabric A to both Cisco Nexus 9396 switches and one from fabric B to both Cisco Nexus 9396 switches.

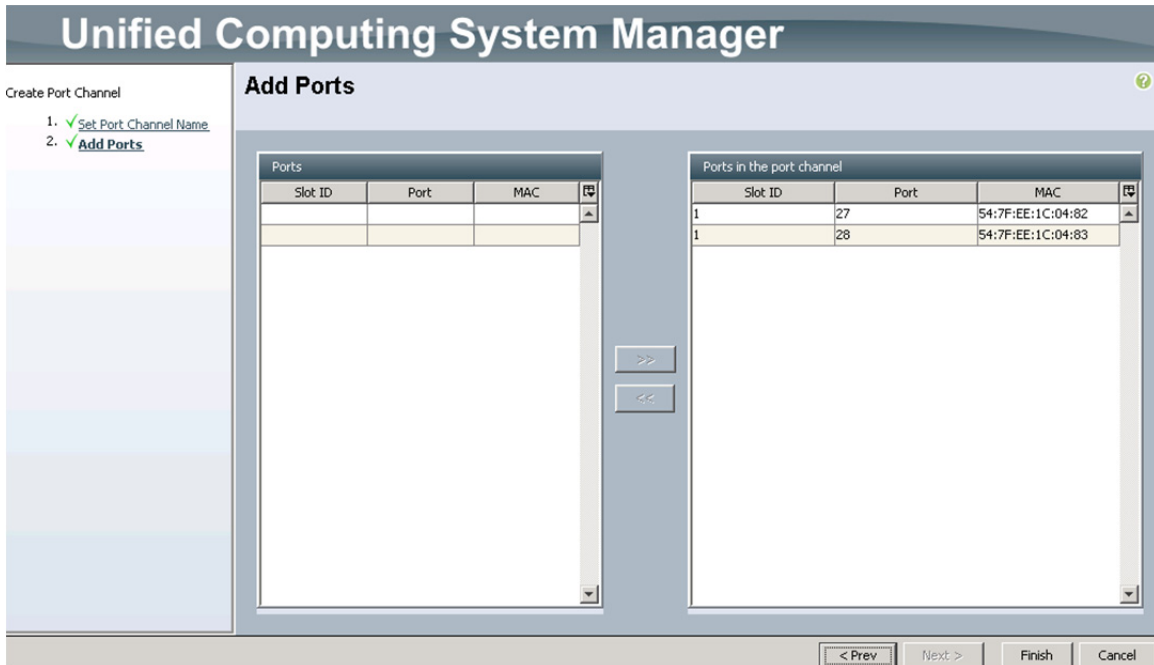
2. Under LAN Cloud, expand the Fabric A tree.



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-N9396 as the name of the Port Channel.
7. Click Next.

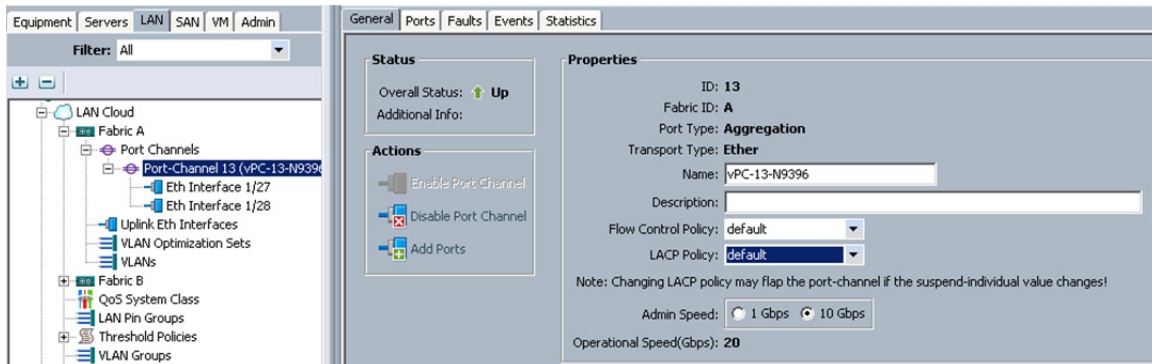


8. Select the port with slot ID: 1 and port: 27 and also the port with slot ID: 1 and port 28 to be added to the Port Channel.
9. Click >> to add the ports to the Port Channel.



10. Click **Finish** to create the Port Channel.

11. Expand the Port Channel node and click on the newly created port channel to view the status.



12. Under LAN Cloud, expand the Fabric B tree.

13. Right-click Port Channels.

14. Select Create Port Channel.

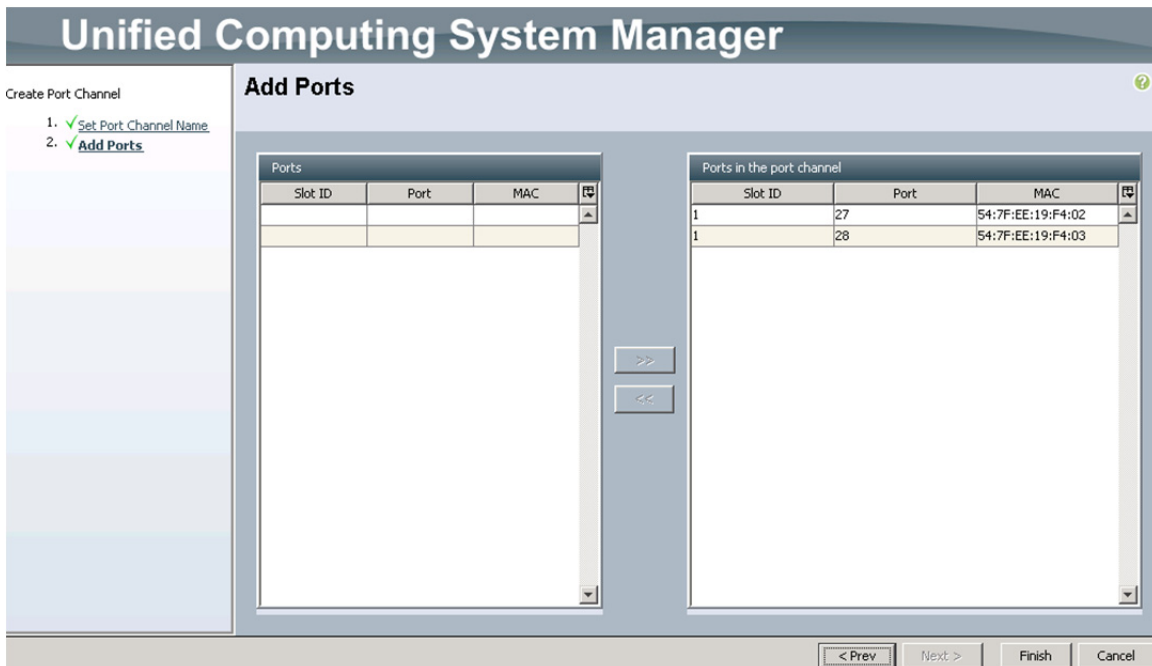
15. Enter 14 as the unique ID of the Port Channel.

16. Enter vPC-14-N9396 as the name of the Port Channel.

17. Click Next.

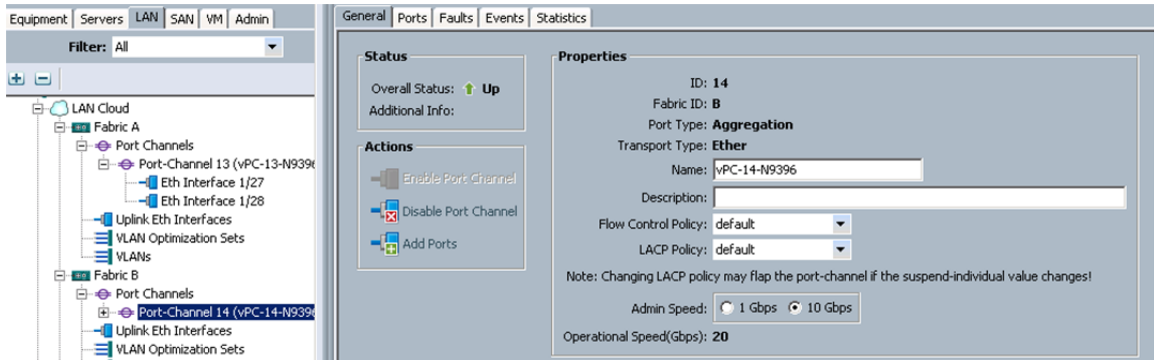
18. Select the port with slot ID: 1 and port: 27 and also the port with slot ID: 1 and port 28 to be added to the Port Channel.

19. Click >> to add the ports to the Port Channel.



20. Click **Finish** to create the Port Channel.

21. Expand the Port Channel node and click on the newly created port channel to view the status.



## 10.8 Create an Organization

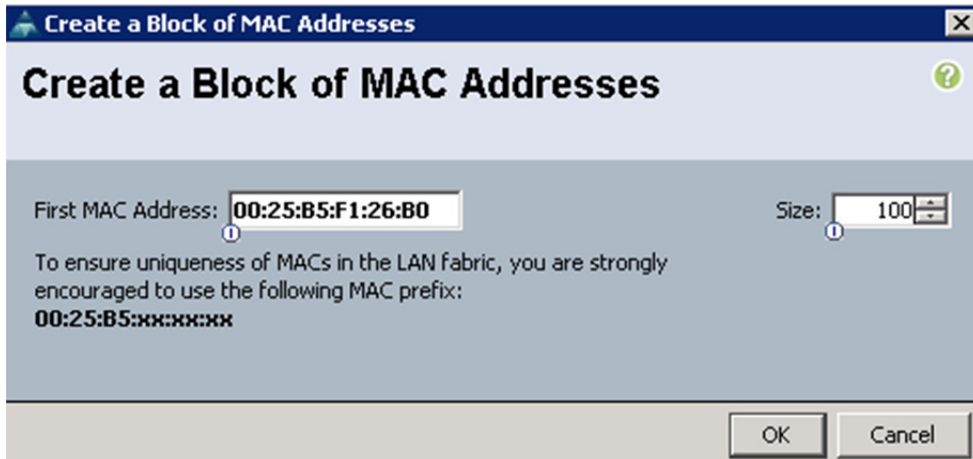
These steps provide details for configuring an organization in the Cisco UCS environment. Organizations are used as a means to organize and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources. This document does not assume the use of Organizations;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

1. Navigate to the Server Tab.
2. Expand Servers and expand Service Profiles
3. Select Service Profiles in the right tree view and click `Create Organization` in the left main view.
4. Enter a name for the organization.
5. Enter a description for the organization (optional).
6. Click `OK`.
7. In the message box that displays, click `OK`.

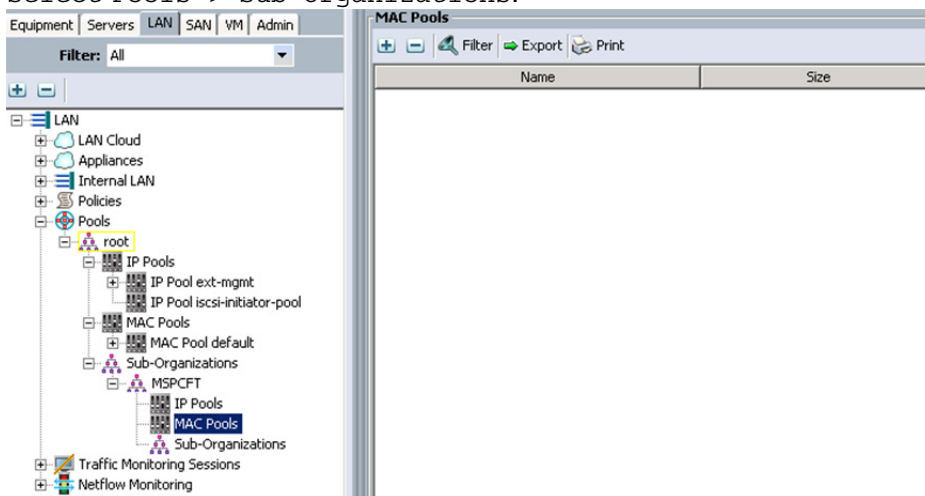
## 10.9 Create a MAC Address Pool

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

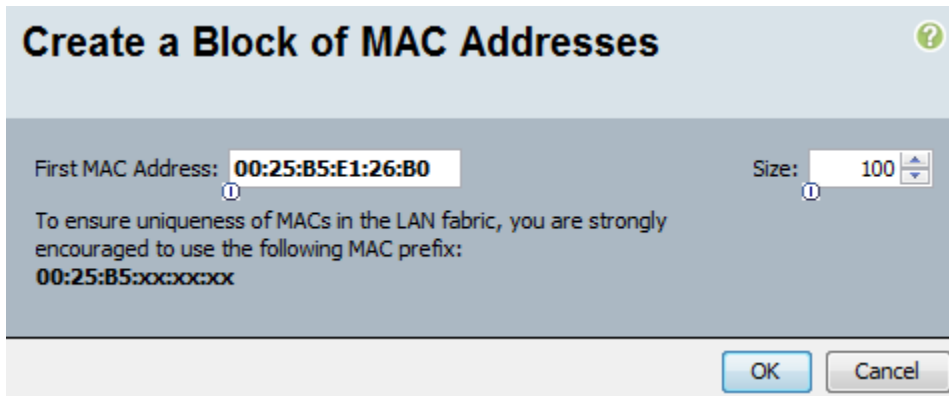
1. Select the `LAN` tab on the left of the window.
2. Select `Pools > root > MAC Pools > MAC Pool default`
3. In the right pane click `Create a Block of MAC Addresses`.
4. Specify a starting MAC address.
5. Specify a size of the MAC address pool sufficient to support the available blade resources.



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 the name of the MAC pool.
10. (Optional) Enter a description of the MAC pool.
11. Select Default assignment order.
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.



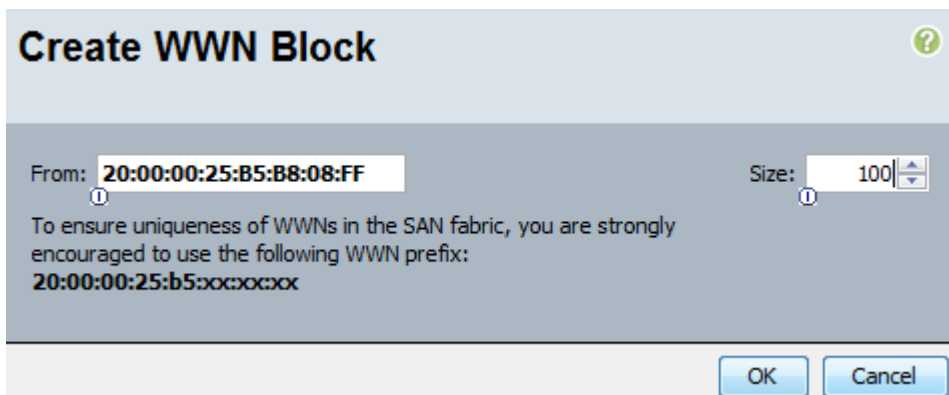
16. Click **OK**.
17. Click **Finish**.
18. In the message box that displays, click **OK**.

## 10.10 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 **WWNN Pool node-default**.
5. Click **Create WWN Block** to add a block of WWNN's.
 

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



7. Click **OK** to proceed.
8. Click **Finish** to proceed.
9. Click **OK** to finish.
10. Select **Pools > root >** and the previously created sub organization.
11. Right click **WWNN** and select **Create WWN Pool**
12. Enter **WWNN\_Pool** as the name of the WWNN pool.
13. (Optional) Add a description for the WWNN pool.

14. Click **Next** to continue.
15. Click **Add** to add a block of WWNN's.
16. Specify a size of the WWPN block sufficient to support the available server resources.

**Create WWN Block**

From:  Size:

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:  
**20:00:00:25:b5:xx:xx:xx**

OK Cancel

17. Click **OK**.
18. Click **Finish** to create the WWPN pool.
19. Click **OK**.

## 10.11 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 node-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.

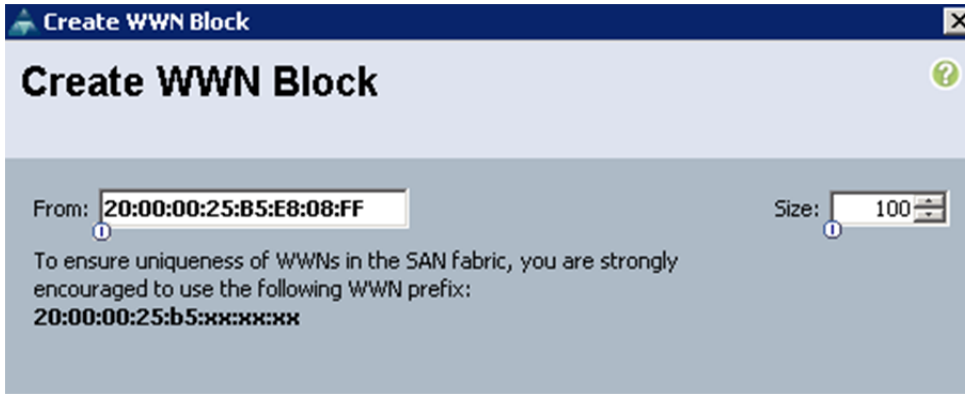
**Create WWN Block**

From:  Size:

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:  
**20:00:00:25:b5:xx:xx:xx**

OK Cancel

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.

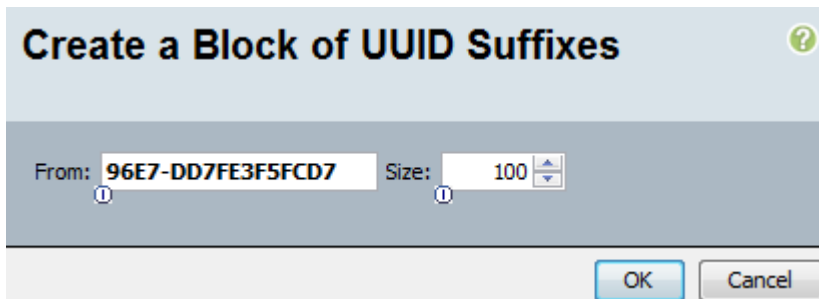


11. Click OK.
12. Click Finish to create the WWPN pool.
13. Click OK.

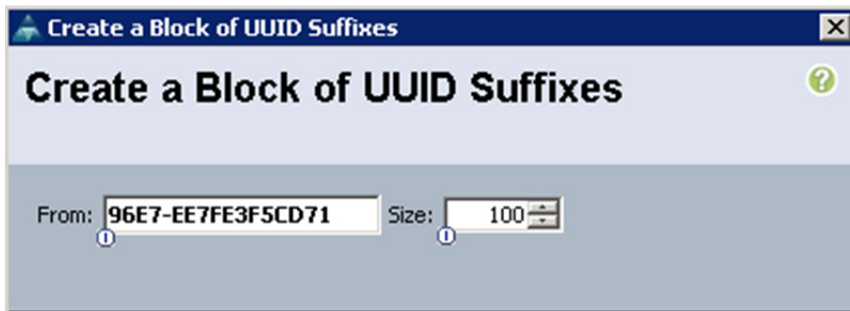
## 10.12 Create UUID Suffix Pools

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. Expand UUID Suffix Pools
4. Right click Pool default and select Create a Block of UUID Suffixes.
5. Specify a size of the UUID block sufficient to support the available blade resources.



6. Click OK.
7. Expand root > Sub-Organizations > previously created organization.
8. Right click UUID Suffix Pools and select Create UUID Suffix Pool
9. Name the UUID suffix pool UUID\_Pool.
10. (Optional) Give the UUID suffix pool a description.
11. Leave the prefix at the derived option.
12. Click Next to continue.
13. Click Add to add a block of UUID's
14. The From field is fine at the default setting.
15. Specify a size of the UUID block sufficient to support the available blade resources.



16. Click **OK**.
17. Click **Finish** to proceed.
18. Click **OK** to finish.

### 10.13 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 >** and the previously created sub organization.
3. Right-click **Server Pools**.
4. Select **Create Server Pool**.
5. Name the server pool **Mgmt\_Pool**.
6. (Optional) Give the server pool a description.
7. Click **Next** to continue to add servers.
8. Select four server to be used for the infrastructure cluster and Click **>>** to add them to the pool.
9. Click **Finish**.
10. Select **OK** to finish.
11. Create another pool, **App\_Pool**, for the application (tenant) servers.

### 10.14 Create VLANs

The following VLANs need to be created:

VLAN Name	VLAN ID
Native	2
Mgmt	10
MF-Public	1001
CS-Database	1002
SMB	1003
CSV	1004
LiveMigration	1005



AF-Public	1007
-----------	------

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.

**Note:** 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**.

The screenshot shows the 'Create VLANs' configuration window. The 'VLAN Name/Prefix' field contains 'Mgmt\_VLAN'. The 'Multicast Policy Name' is set to '<not set>' with a '+ Create Multicast Policy' button. The 'Scope' section has radio buttons for 'Common/Global' (selected), 'Fabric A', 'Fabric B', and 'Both Fabrics Configured Differently'. Below this, a message states: 'You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")'. The 'VLAN IDs' field contains '10'. The 'Sharing Type' section has radio buttons for 'None' (selected), 'Primary', 'Isolated', and 'Community'.

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**.

The screenshot shows the 'Create VLANs' configuration window. The 'VLAN Name/Prefix' field contains 'CSV-VLAN'. The 'Multicast Policy Name' is set to '<not set>' with a '+ Create Multicast Policy' button. The 'Scope' section has radio buttons for 'Common/Global' (selected), 'Fabric A', 'Fabric B', and 'Both Fabrics Configured Differently'. Below this, a message states: 'You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")'. The 'VLAN IDs' field contains '1004'. The 'Sharing Type' section has radio buttons for 'None' (selected), 'Primary', 'Isolated', and 'Community'.

15. Right-click VLANs .
16. Select Create VLANs.
17. Enter SMB-VLAN as the name of the VLAN to be used for the VHD access LAN.
18. Keep the Common/Global option selected for the scope of the VLAN.
19. Enter the VLAN ID for the SMB VLAN.
20. Click OK.

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

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

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

27. Right click VLANs
28. Select Create VLANs.
29. Enter VM-Database-VLAN as the name of the VLAN to be used for the VM data VLAN.
30. Keep the Common/Global option selected for the scope of the VLAN.
31. Enter the VLAN ID for the VM data VLAN.
32. Click OK.

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

33. Right-click VLANs .
34. Select Create VLANs.
35. Enter MF-Public-VLAN as the name of the VLAN to be used for the VM data VLAN.
36. Keep the Common/Global option selected for the scope of the VLAN.
37. Enter the VLAN ID for the Management Fabric Public VLAN.
38. Click OK.

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

39. Right-click VLANs .
40. Select Create VLANs.
41. Enter VM-AF-Public-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 Application Fabric Public VLAN.
44. Click OK.

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

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

VLAN Name/Prefix:

Multicast Policy Name:

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs:

Sharing Type:  None  Primary  Isolated  Community

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

## 10.15 Create VSANs

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 Storage Cloud tree.
3. Right-click VSANs
4. Select Create Storage VSAN.
5. Enter Fabric-A as the VSAN name for fabric A.
6. Set the Enabled option for the FC Zoning Setting
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.

## Create Storage VSAN ?

Name:

**FC Zoning Settings**

FC Zoning:  Disabled  Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.  
Enter the VSAN ID that maps to this VSAN.

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.  
Enter the VLAN ID that maps to this VSAN.

VSAN ID:

FCoE VLAN:

11. Right-click VSANs .
12. Select Create Storage VSAN.
13. Enter Fabric-B as the VSAN name for fabric B.
14. Set the Enabled option for the FC Zoning Settings
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.

## Create Storage VSAN ?

Name:

**FC Zoning Settings**

FC Zoning:  Disabled  Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.  
Enter the VSAN ID that maps to this VSAN.

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.  
Enter the VLAN ID that maps to this VSAN.

VSAN ID:

FCoE VLAN:

## 10.16 Configure the VSAN for the FCoE Storage 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 port 31 that is connected to the NetApp FAS 8040 storage array.
5. In the right pane, click the VSAN dropdown menu and select `Fabric A / vsan Fabric-A (101)`.
6. Click the `Save Changes` button.
7. Select port 32 that is connected to the NetApp FAS 8040 storage array.
8. In the right pane, click the VSAN dropdown menu and select `Fabric A / vsan Fabric-A (101)`.
9. Click the `Save Changes` button.
10. Select `Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module`.
11. Expand the `Ethernet Ports` object.
12. Select port 31 that is connected to the NetApp FAS 8040 storage array.
13. In the right pane, click the VSAN dropdown menu and select `Fabric B / vsan Fabric-B (102)`.
14. Click the `Save Changes` button.
15. Select port 32 that is connected to the NetApp FAS 8040 storage array.
16. In the right pane, click the VSAN dropdown menu and select `Fabric B / vsan Fabric-B (102)`.
17. Click the `Save Changes` button.

## 10.17 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 >` and the previously created sub organization.
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`.

### Create Fibre Channel Adapter Policy

Name:

Description:

**Resources** ▼

**Options** ▲

FCP Error Recovery:  Disabled  Enabled

Flogi Retries:  [0-infinite]

Flogi Timeout (ms):  [1000-255000]

Plugi Retries:  [0-255]

Plugi Timeout (ms):  [1000-255000]

Port Down Timeout (ms):  [0-240000]

Port Down IO Retry:  [0-255]

Link Down Timeout (ms):  [0-240000]

IO Throttle Count:  [256-1024]

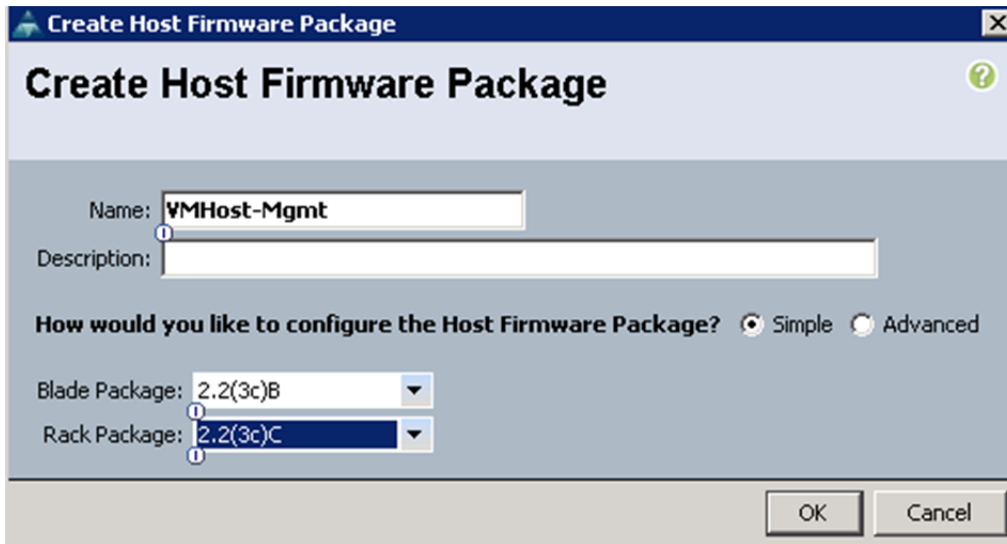
Max LUNs Per Target:  [1-1024]

Interrupt Mode:  MSI X  MSI  IN Tx

## 10.18 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.

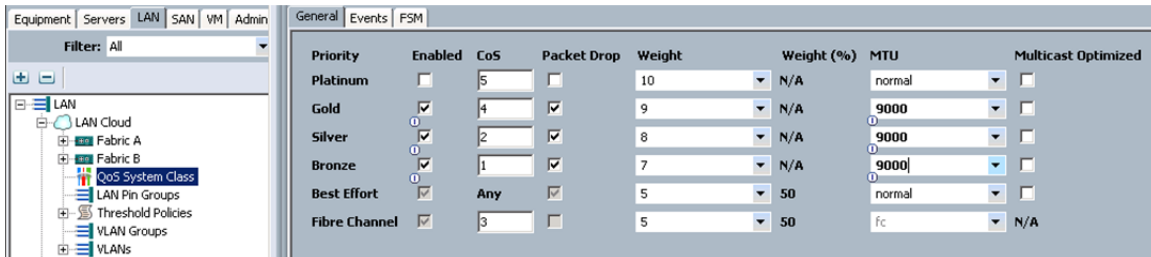
1. Select the `Servers` tab at the top left of the window.
2. Select `Policies > root` or a suborganization.
3. Right Click `Host Firmware Packages`.
4. Select `Create Host Firmware Package`.
5. Enter the name of the host firmware package for the corresponding server configuration and an optional description.
6. Two types of host firmware package are available. The simple option specifies all firmware based on a firmware version bundle. The Advanced 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.



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

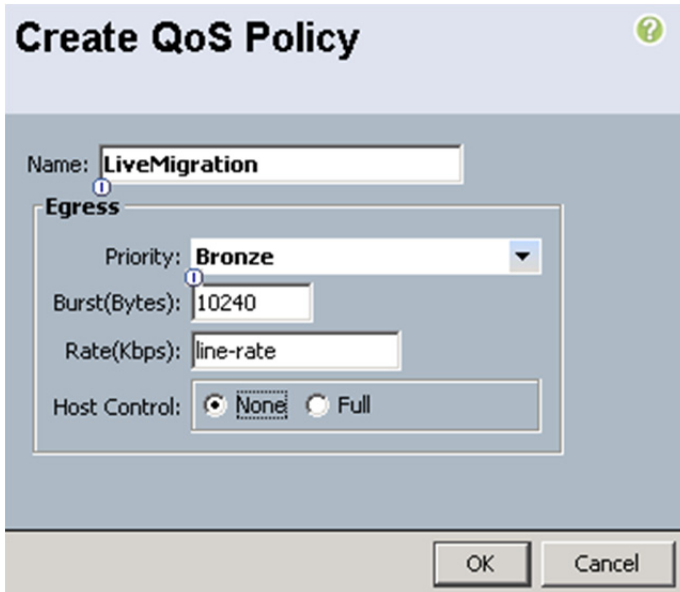
These steps provide details for setting Jumbo frames and enabling the quality of server in the Cisco UCS Fabric.

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 Bronze row, type 9000 in the MTU boxes.
5. Click Save Changes in the bottom right corner.
6. Click OK to continue.

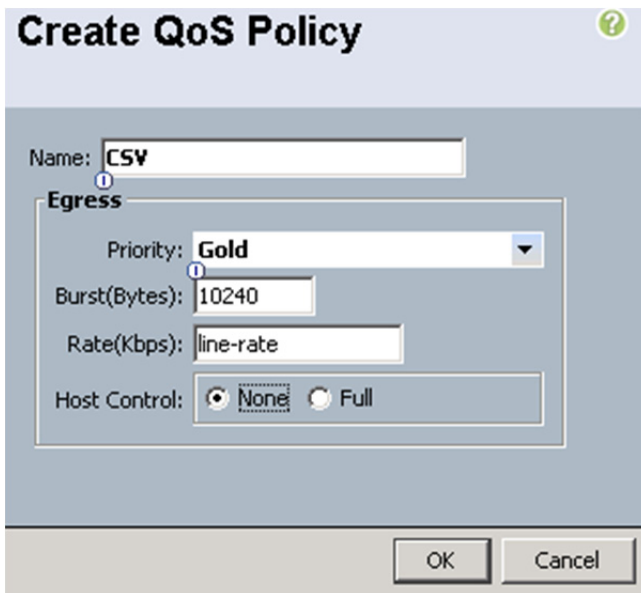


7. Select the LAN tab on the left of the window.
8. Go to LAN > Policies > Root > and the previously created sub organization.
9. In the right pane click root to expand it and expand the previously created suborganization.
10. Right-click previously created suborganization and select Create QoS Policies.
11. Enter LiveMigration as the QoS Policy name.
12. Change the Priority to Bronze. 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.

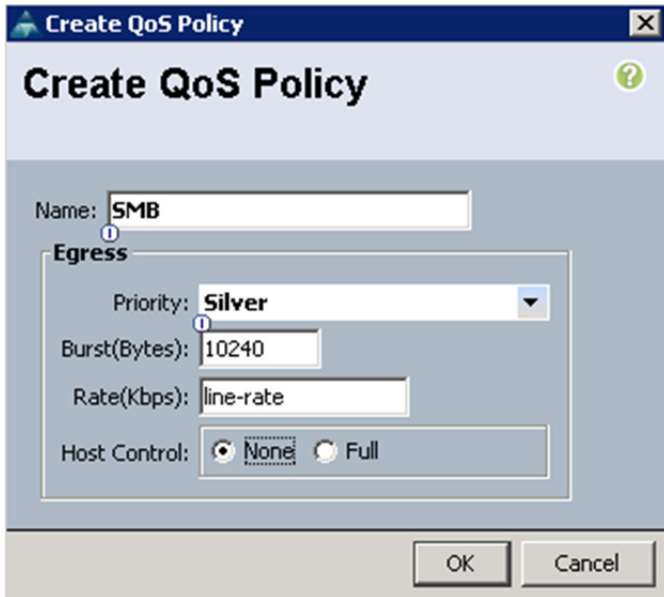




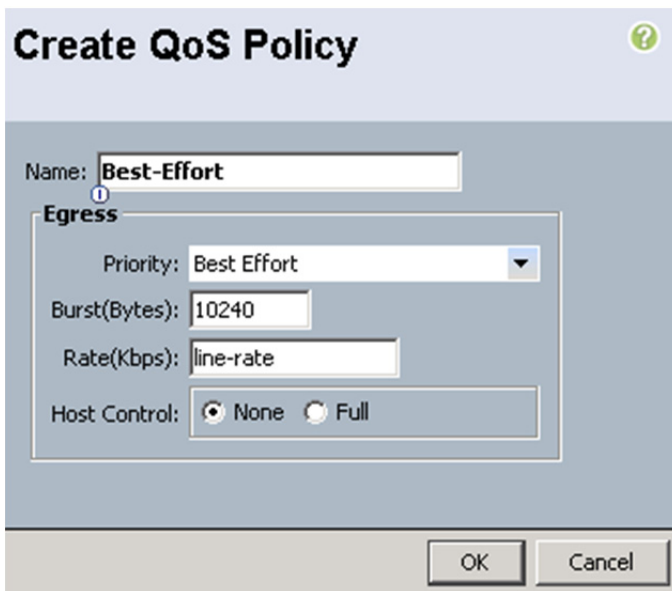
14. Right-click previously created suborganization .
15. Select Create QoS Policy .
16. Enter CSV as the QoS Policy name .
17. Change the Priority to Gold. Leave Burst (Bytes) set to 10240 . Leave Rate (Kbps) set to line-rate. Leave Host Control set to None .
18. Click OK in the bottom right corner .



19. Right-click previously created suborganization .
20. Select Create QoS Policy .
21. Enter SMB 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 .



24. Right-click previously created suborganization.
25. Select Create QoS Policy.
26. Enter Best-Effort as the QoS Policy name.
27. Change the Priority to Best Effort. Leave Burst (Bytes) set to 10240. Leave Rate(Kbps) set to line-rate. Leave Host Control set to None.
28. Click OK in the bottom right corner.

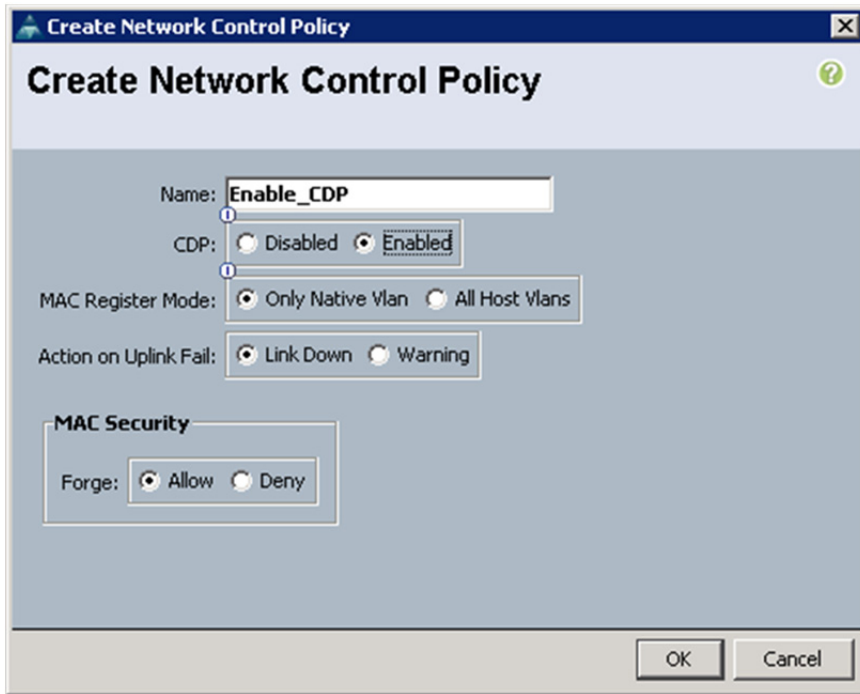


## 10.20 Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.

3. Expand the suborganizations and select the previously created suborganization
4. Select Network Control Policies tab in the right pane.
5. Right click on the previously created suborganization and select Create Network Control Policy.
6. Enter Enable\_CDP as the policy name.
7. For CDP, select the Enabled option.
8. Click OK to create the network control policy.



## 10.21 Create VMQ Connection Policy

VMQ distributes the computational workload associated with virtual machine network traffic across multiple cores in the Hyper-V host. The Cisco VIC supports up to 256 queues per server and a maximum of 128 queues per eNIC. The VMQ queue value should be configured based on the expected number of synthetic NICs in the in all VMs that are bound to the Hyper-V switch that is bound to the adapter, plus 2. The extra 2 queues are for the default queue and a queue for the eNIC itself.

The value configured for the number of VMQ's should be equal to or greater than the number of required queues, but should not exceed the maximum number supported by the Cisco VIC.

The following table lists the VMQ configuration for this deployment.

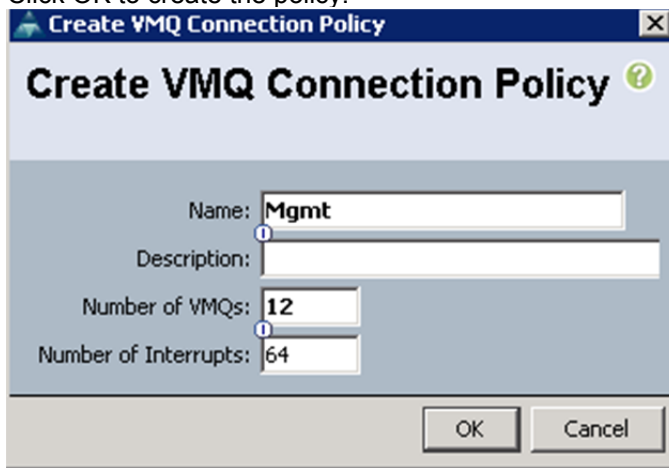
Name	Value
Mgmt	12
Public	50

SC-Database	50
SMB-SQL	10

The number of configured interrupts should be equal to or greater than the number of logical CPU cores in the Hyper-V host.

To create a VMQ Connection policy, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Expand the suborganizations and select the previously created suborganization
4. Select VMQ Connection Policy tab in the right pane.
5. Right click on the previously created suborganization and select Create VMQ Connection Policy.
6. Enter the policy name.
7. Keep the default value 12 for number of VMQs.
8. Keep the default value 64 for Number of Interrupts.
9. Click OK to create the policy.



10. Repeat this procedure to create VMQ Connection Policy for Public, SC-Database, and SMB-SQL eNIC's.

## 10.22 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 > and the previously created sub organization .
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.

**Create Power Control Policy**

Name:

Description:

**Power Capping**

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

No Cap  cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

## 10.23 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 >` and the previously created sub organization .
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`.
7. Click `OK` to complete creating the Local Disk Configuration Policy.

**Create Local Disk Configuration Policy**

Name:

Description:

Mode:

FlexFlash

FlexFlash State:  Disable  Enable

If **FlexFlash State** is disabled, SD cards will become unavailable immediately. Please ensure SD cards are not in use before disabling the FlexFlash State.

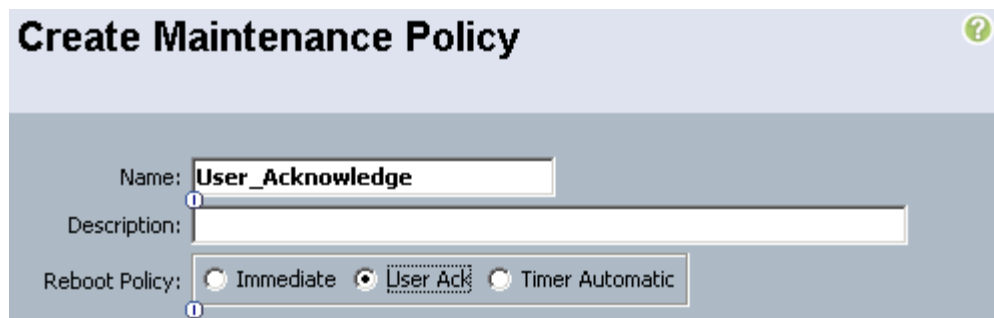
FlexFlash RAID Reporting State:  Disable  Enable

OK Cancel

## 10.24 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.



**Create Maintenance Policy** ?

Name:

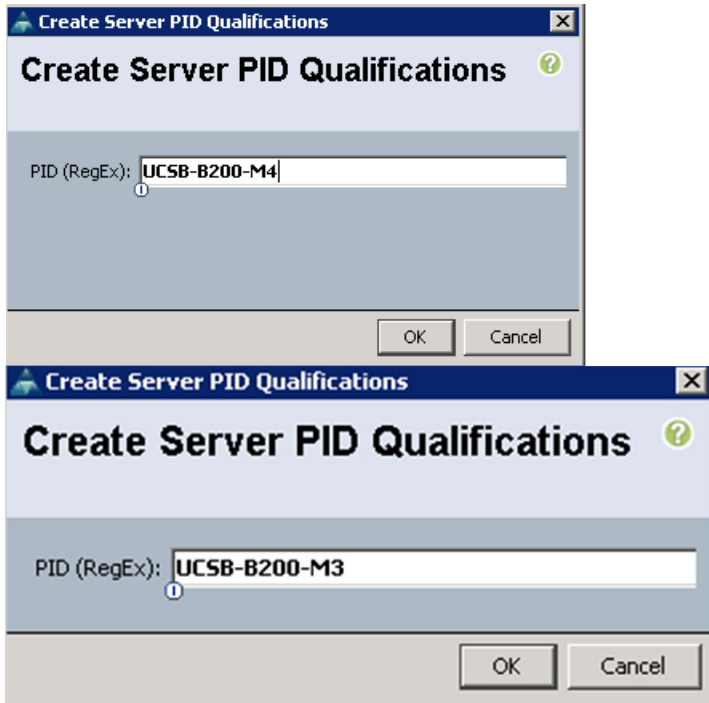
Description:

Reboot Policy:  Immediate  User Ack  Timer Automatic

## 10.25 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 >` and the previously created sub organization .
3. Right-click `Server Pool Qualification Policies`.
4. Select `Create Server Pool Policy Qualification`.
5. Enter the Policy Name.
6. Select `Create Server PID Qualifications`.
7. Enter `UCSB-B200-M4` or `UCSC-C220-M4S` as the `Model (RegEx)` .
8. Click `OK` to complete creating the `Server Pool Qualification Policy`.
9. Click `OK`.



## 10.26 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 >` and the previously created sub organization .
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 optimize Hyper-V support:

Property	Setting
Quiet Boot	Disabled
Virtual Technology (VT)	Enabled
Processor C State	Disabled
CPU Performance	Enterprise
VT For Direct IO	Enabled
Interrupt Remap	Enabled
Coherency Support	Disabled
ATS Support	Enabled
Pass Through DMA Support	Enabled

## Main



Name:

Reboot on BIOS Settings Change:

Quiet Boot:  disabled  enabled  Platform Default

Post Error Pause:  disabled  enabled  Platform Default

Resume Ac On Power Loss:  stay-off  last-state  reset  Platform Default

Front Panel Lockout:  disabled  enabled  Platform Default

## Processor



Turbo Boost:  disabled  enabled  Platform Default

Enhanced Intel Speedstep:  disabled  enabled  Platform Default

Hyper Threading:  disabled  enabled  Platform Default

Core Multi Processing: Platform Default

Execute Disabled Bit:  disabled  enabled  Platform Default

Virtualization Technology (VT):  disabled  enabled  Platform Default

Direct Cache Access:  disabled  enabled  Platform Default

Processor C State:  disabled  enabled  Platform Default

Processor C1E:  disabled  enabled  Platform Default

Processor C3 Report:  disabled  acpi-c2  acpi-c3  Platform Default

Processor C6 Report:  disabled  enabled  Platform Default

Processor C7 Report:  disabled  enabled  Platform Default

CPU Performance:  enterprise  high-throughput  hpc  Platform Default

Max Variable MTRR Setting:  auto-max  8  Platform Default



## Intel Directed IO

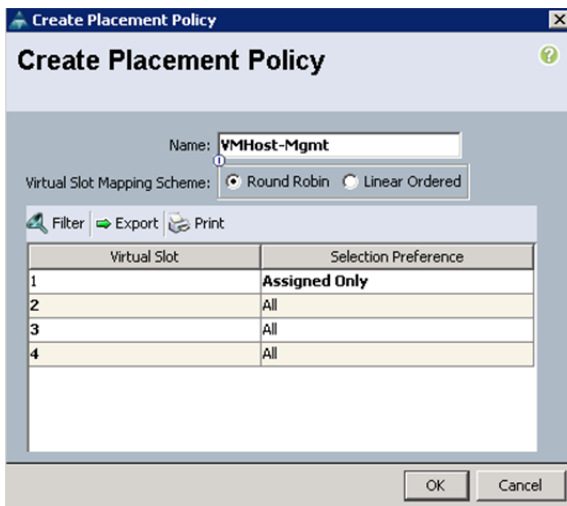


VT For Directed IO:	<input type="radio"/> disabled	<input checked="" type="radio"/> enabled	<input type="radio"/> Platform Default
Interrupt Remap:	<input type="radio"/> disabled	<input checked="" type="radio"/> enabled	<input type="radio"/> Platform Default
Coherency Support:	<input checked="" type="radio"/> disabled	<input type="radio"/> enabled	<input type="radio"/> Platform Default
ATS Support:	<input type="radio"/> disabled	<input checked="" type="radio"/> enabled	<input type="radio"/> Platform Default
Pass Through DMA Support:	<input type="radio"/> disabled	<input checked="" type="radio"/> enabled	<input type="radio"/> Platform Default

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

## 10.27 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-Infra**.
3. Click **1** and select **Assign Only**.
4. Click **OK**.



**Create Placement Policy**

Name:

Virtual Slot Mapping Scheme:  Round Robin  Linear Ordered

Filter Export Print

Virtual Slot	Selection Preference
1	<b>Assigned Only</b>
2	All
3	All
4	All

OK Cancel

## 10.28 Create a vNIC Template

The following table shows the vNICs that must be created and their properties.

Name	Mgmt	MF-Public	SC-Database	SMB	SMB-SQL	CSV	Live Migration	AF-Public
Fabric	A	B	B	B	A	A	B	A
Failover	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Target	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter
Template Type	Updating	Updating	Updating	Updating	Updating	Updating	Updating	Updating
VLAN ID	Mgmt	MF-Public	CS-Database	SMB	SMB	CSV	Live Migration	AF-Public
Native VLAN	Yes	No	No	Yes	No	Yes	Yes	No
MTU	1500	1500	1500	9000	9000	9000	9000	1500
MAC Pool	MSPCFT	MSPCFT	MSPCFT	MSPCFT	MSPCFT	MSPCFT	MSPCFT	MSPCFT
QOS Policy	Best Effort	Best Effort	Best Effort	SMB	SMB	CSV	Live Migration	Best Effort
Network Control Policy	Enable CDP	Enable CDP	Enable CDP	Enable CDP	Enable CDP	Enable CDP	Enable CDP	Enable CDP
Connection Policies	VMQ	VMQ	VMQ	Dynamic vNIC	VMQ	Dynamic vNIC	Dynamic vNIC	VMQ
VMQ Connection Policy	Mgmt	Public	SC-Database		SMB-SQL			Public

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 > and the previously created sub organization .
3. Right-click vNIC Templates .
4. Select Create vNIC Template .
5. Enter CSV as the vNIC template name.
6. Configure options:
  - a. Leave Fabric A checked.
  - b. Check the Enable Failover box.
  - c. Under target, unselect the VM box.
  - d. Select Updating Template as the Template Type .
  - e. Under VLANs , select CSV VLAN and set as Native VLAN .

- f. For MTU, enter 9000.
  - g. For MAC Pool, select the MAC pool created earlier.
  - h. For QoS Policy, select CSV.
  - i. For Network Control Policy, select Enable\_CDP.
7. Click OK to complete creating the vNIC template.
  8. Click OK.

### Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter  
 VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	AF-Public	<input type="radio"/>
<input checked="" type="checkbox"/>	CSV-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt VLAN	<input type="radio"/>

**Create VLAN**

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy:

9. Select the LAN tab on the left of the window.
10. Go to Policies > root > and the previously created sub organization .
11. Right-click vNIC Templates .
12. Select Create vNIC Template .
13. Enter LiveMigration as the vNIC template name.
14. Configure options:
  - a. Check Fabric B.
  - b. Check the Enable Failover box.

- c. Under target, unselect the VM box.
- d. Select Updating Template as the Template Type.
- e. Under VLANs, select Live-Migration-VLAN and set as Native VLAN.
- f. For MTU, enter 9000.
- g. For MAC Pool: select the MAC pool created earlier.
- h. For QoS Policy, select Live-Migration.
- i. For Network Control Policy, select Enable\_CDP.

15. Click OK to complete creating the vNIC template.

16. Click OK.

### Create vNIC Template ?

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter

VM

**Warning**

If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	AF-Public	<input type="radio"/>
<input type="checkbox"/>	CSV-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	LiveMigration-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt VLAN	<input type="radio"/>

MTU:

**Warning**

Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy:

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. Configure options:
  - a. Check Fabric A.
  - b. Check the Enable Failover box.
  - c. Under target, unselect the VM box.
  - d. Select Updating Template as the Template Type.
  - e. Under VLANs, select MGMT-VLAN. Set as Native VLAN.
  - f. Under MAC Pool: select the MAC pool created earlier.
  - g. For QOS Policy, select Best-Effort.
  - h. For Network Control Policy, select Enable\_CDP.
  - i. For Connection Policies, Select VMQ.
  - j. For VMQ Connection Policy, select Mgmt.

## Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter  
 VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	Infra-VLAN	<input type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Mgmt_VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	Native	<input type="radio"/>
<input type="checkbox"/>	SC-Database-VLAN	<input type="radio"/>

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy:

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> and the previously created sub organization.
27. Right-click vNIC Templates.
28. Select Create vNIC Template.
29. Enter MF-Public as the vNIC template name.
30. Configure options:
  - a. Check Fabric B.
  - b. Check the Enable Failover box.
  - c. Under target, unselect the VM box.

- d. Select Updating Template as the Template Type.
- e. Under VLANs, select VM-MF-Public. Do not set a Native VLAN.
- f. For MAC Pool, select the MAC pool created earlier.
- g. For QoS Policy, select Best-Effort.
- h. For Network Control Policy, select Enable\_CDP.
- i. For Connection Policies, Select VMQ.
- j. For VMQ Connection Policy, select Public.

### Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

Target

Adapter  
 VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	Infra-VLAN	<input type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt_VLAN	<input type="radio"/>
<input type="checkbox"/>	Native	<input type="radio"/>
<input type="checkbox"/>	SC-Database-VLAN	<input type="radio"/>

+ Create VLAN

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy:

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 SC-Database as the vNIC template name.
38. Configure options:
  - a. Check Fabric B.
  - b. Check the Enable Failover box.
  - c. Under target, unselect the VM box.
  - d. Select Updating Template as the Template Type.
  - e. Under VLANs, select VM-Database. Do not set as Native VLAN.
  - f. Under MAC Pool, select the MAC pool created earlier.
  - g. For QOS Policy, select Best-Effort.
  - h. For Network Control Policy, select Enable\_CDP.
  - i. For Connection Policies, Select VMQ.
  - j. For VMQ Connection Policy, select SC-Database.



## Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter  
 VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	MIF-PUBLIC-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt_VLAN	<input type="radio"/>
<input type="checkbox"/>	Native	<input type="radio"/>
<input checked="" type="checkbox"/>	SC-Database-VLAN	<input type="radio"/>
<input type="checkbox"/>	SMB-VLAN	<input type="radio"/>
<input type="checkbox"/>	iSCSI-B-VLAN	<input type="radio"/>

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy:

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 > and the previously created sub organization .
43. Right-click vNIC Templates.
44. Select Create vNIC Template.
45. Enter SMB as the vNIC template name.
46. Configure options:
  - a. Check Fabric B.
  - b. Check the Enable Failover box. Under target,
  - c. Select Adapter box.

- d. Select Updating Template as the Template Type.
- e. Under VLANs, select SMB-VLAN and set as Native VLAN.
- f. For MTU, enter 9000.
- g. For MAC Pool, select the MAC pool created earlier.
- h. For QoS Policy, select SMB.
- i. For Network Control Policy, select Enable\_CDP.

47. Click OK to complete creating the vNIC template.

48. Click OK.

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

Target:  Adapter  VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt_VLAN	<input type="radio"/>
<input type="checkbox"/>	Native	<input type="radio"/>
<input type="checkbox"/>	SC-Database-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	SMB-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	ISCSI-B-VLAN	<input type="radio"/>

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy:

49. Select the LAN tab on the left of the window.

50. Go to Policies > root > and the previously created sub organization .

51. Right-click vNIC Templates .

52. Select Create vNIC Template .

53. Enter SMB-SQL as the vNIC template name.

54. Configure options:

- a. Check Fabric A.
- b. Check the Enable Failover box.
- c. Under target, select Adapter box.
- d. Select Updating Template as the Template Type.
- e. Under VLANs, select SMB-VLAN and set as Native VLAN.
- f. For MTU, enter 9000.
- g. For MAC Pool, select the MAC pool created earlier.
- h. For QoS Policy, select SMB.
- i. For Network Control Policy, select Enable\_CDP.
- j. For Connection Policies, Select VMQ.
- k. For VMQ Connection Policy, select SMB-SQL.

## Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter  
 VM

**Warning**  
If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN	
<input type="checkbox"/>	MF-PUBLIC-VLAN	<input type="radio"/>	
<input type="checkbox"/>	Mgmt_VLAN	<input type="radio"/>	
<input type="checkbox"/>	Native	<input type="radio"/>	
<input type="checkbox"/>	SC-Database-VLAN	<input type="radio"/>	
<input checked="" type="checkbox"/>	SMB-VLAN	<input type="radio"/>	
<input type="checkbox"/>	iSCSI-A-VLAN	<input type="radio"/>	

+ Create VLAN

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy:

55. Click OK to complete creating the vNIC template.
56. Click OK.
57. Select the LAN tab on the left of the window.
58. Go to Policies > root > and the previously created sub organization .
59. Right-click vNIC Templates .
60. Select Create vNIC Template .
61. Enter SMB as the vNIC template name.
62. Configure options:
  - a. Check Fabric B .
  - b. Check the Enable Failover box.
  - c. Under target, unselect the VM box.

- d. Select Updating Template as the Template Type.
- e. Under VLANs, select VM-AF-Public. Do not set a Native VLAN.
- f. For MAC Pool, select the MAC pool created earlier.
- g. For QoS Policy, select Best-Effort.
- h. For Network Control Policy, select Enable\_CDP.
- i. For Connection Policies, Select VMQ.
- j. For VMQ Connection Policy, select Public.

### Create vNIC Template

Name:

Description:

Fabric ID:  Fabric A  Fabric B  Enable Failover

**Target**

Adapter  
 VM

**Warning**  
If VM is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type:  Initial Template  Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	AF-Public	<input type="radio"/>
<input type="checkbox"/>	CSV-VLAN	<input type="radio"/>
<input type="checkbox"/>	Infra-VLAN	<input type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input type="checkbox"/>	MF-Public-VLAN	<input type="radio"/>

**Create VLAN**

MTU:

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy:

63. Click OK to complete creating the vNIC template.

## 10.29 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 SAN tab on the left of the window.
2. Go to Policies > root > and the previously created sub organization .
3. Right-click vHBA Templates .
4. Select Create vHBA 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.

**Create vHBA Template**

Name:

Description:

Fabric ID:  A  B

Select VSAN:

Template Type:  Initial Template  Updating Template

Max Data Field Size:

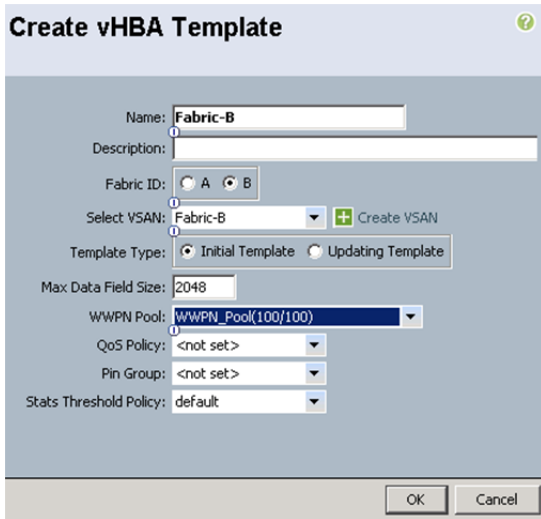
WWPN Pool:

QoS Policy:

Pin Group:

Stats Threshold Policy:

9. Select the VSAN tab on the left of the window.
10. Go to Policies > root > and the previously created sub organization .
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 Fabric-B. Under WWN Pool, select the previously created WWN pool.
15. Click OK to complete creating the vHBA template.
16. Click OK.



### 10.30 Create Boot Policies

These steps provide details for creating boot policies for the Cisco UCS environment. These directions apply to an environment in which the volume that stores the boot LUNs is owned by storage array node-1. The Physical ports 3a on each storage node are connected to fabric A and the physical ports 4a on each storage node fabric B. The boot policy configures the primary target to be node-1 port 3a (lif01a) and 4a (lif01b) and the secondary target is node will be node-2 port 3a (lif02a) and 4a (lif02b).

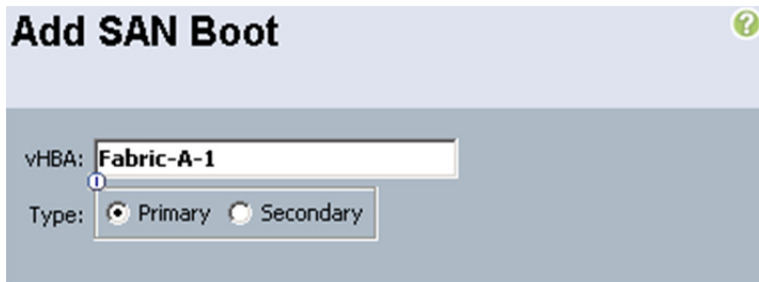
**Note:** To obtain the WWPN information for the FAS cluster lifs, log in to the FAS cluster and run the fcp portname show command.

Vserver	Logical Interface	WWPN
Infra_vs1	fcp_lif01a	A - 20:00:00:a0:98:54:f0:bc
Infra_vs1	fcp_lif01b	20:01:00:a0:98:54:f0:bc
Infra_vs1	fcp_lif02a	A- 20:02:00:a0:98:54:f0:bc
Infra_vs1	fcp_lif02b	20:03:00:a0:98:54:f0:bc

4 entries were displayed.

1. Select the Servers tab at the top left of the window.
2. Go to Policies > root > and the previously created sub organization .
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Name the boot policy Infra\_vs1.
6. (Optional) Give the boot policy a description.
7. Leave Reboot on Boot Order Change unchecked.
8. Leave Enforce vNIC/HBA/iSCSI Name checked.
9. Expand the Local Devices drop-down menu and select Add Remote CD-ROM.
10. Expand the vHBAs drop-down menu and select Add SAN Boot.
11. Enter Fabric-A-1 in the vHBA field in the Add SAN Boot window that displays.
12. Make sure that Primary is selected as the type.

13. Click **OK** to add the SAN boot initiator.



**Add SAN Boot** ?

vHBA:

Type:  Primary  Secondary

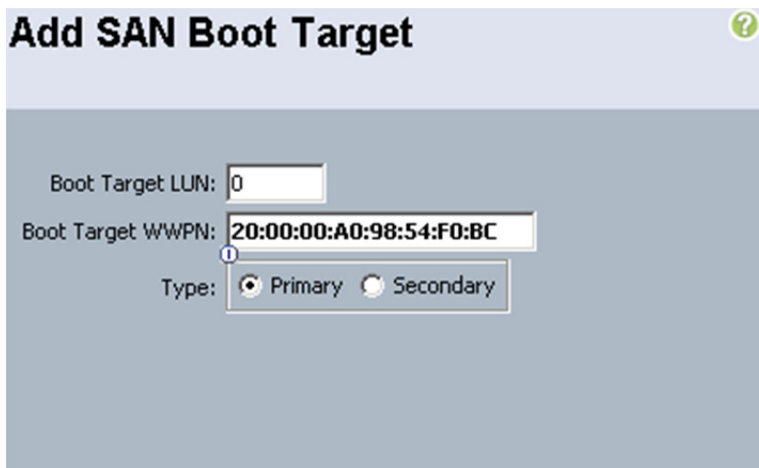
14. Under the vHBA drop-down menu, select **Add SAN Boot Target**. Keep the value for **Boot Target LUN** as 0.

15. Enter the WWPN for the primary FCoE adapter interface `lif01a` of node-1. To obtain this information, log in to the FAS cluster and run the `fcportname show` command.

16. Be sure to use the FC portname for `lif01a` and not the FC node name.

17. Keep the type as **Primary**.

18. Click **OK** to add the SAN boot target.



**Add SAN Boot Target** ?

Boot Target LUN:

Boot Target WWPN:

Type:  Primary  Secondary

19. Under the vHBA drop-down menu, select **Add SAN Boot Target**. Keep the value for **Boot Target LUN** as 0.

20. Enter the WWPN for the primary FCoE adapter interface `lif02a` of node-2. To obtain this information, log in to the FAS cluster and run the `fcportname show` command.

21. Be sure to use the FC portname for port `lif02a` and not the FC node name.

22. Click **OK** to add the SAN boot target.



**Add SAN Boot Target** ?

Boot Target LUN:

Boot Target WWPN:

Type:  Primary  Secondary

23. Select `Add SAN Boot` under the vHBA drop-down menu.
24. Enter `Fabric-B-1` in the vHBA field in the Add SAN Boot window that displays.
25. The type should automatically be set to `Secondary` and it should be grayed out. This is fine.
26. Click `OK` to add the SAN boot target.

**Add SAN Boot** ?

vHBA:

Type:  Primary  Secondary

27. Select `Add SAN Boot Target` under the vHBA drop-down menu.
28. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as `0`.
29. Enter the WWPN for the primary FCoE adapter interface `lif01b` of the node-1. To obtain this information, log in to FAS cluster and run the `fcportname show` command.
30. Be sure to use the FC portname for `portli01b` and not the FC node name.
31. Keep the type as `Primary`.
32. Click `OK` to add the SAN boot target.

**Add SAN Boot Target** ?

Boot Target LUN:

Boot Target WWPN:

Type:  Primary  Secondary

33. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as `0`.
34. Enter the WWPN for the primary FCoE adapter interface `lif02b` of node-2. To obtain this information, log in to controller A and run the `fcport show adapters` command.

35. Be sure to use the FC portname for port lif01b and not the FC node name.
36. Click OK to add the SAN boot target.

**Add SAN Boot Target** ?

Boot Target LUN:

Boot Target WWPN:  1

Type:  Primary  Secondary

37. Click Save Changes .

### 10.31 Create the Storage Connection Policy

1. Select the SAN tab at the top left of the window.
2. Go to Policies > root > and the previously created sub organization .
3. Right-click Storage Connection Policies.
4. Select Create Storage Connection Policy.
5. Enter Storage Connection Policy name.
6. Select the Zoning Type Single Initiator Multiple Targets.

**Create Storage Connection Policy** ?

Name:  1

Description:

Zoning Type:  None  Single Initiator Single Target  Single Initiator Multiple Targets

**FC Target Endpoints** 1

Filter | Export | Print

WWPN	Path	VSAN

+  
trash  
refresh

OK Cancel

7. Click the plus icon to add the FC Target Endpoint
8. Enter the WWPN for fcp\_lif01a.
9. Select Path A
10. Select VSAN Fabric-A

**Create FC Target Endpoint**

WWPN: 20:00:00:A0:98:54:F0:BC

Description:

Path:  A  B

Select VSAN: VSAN Fabric-A (101) + Create VSAN

OK Cancel

11. Click OK to create the FC Target Endpoint
12. Click the plus icon to add the FC Target Endpoint
13. Enter the WWPN for fcp\_lif02a.
14. Select Path A
15. Select VSAN Fabric-A
16. Click OK to create the FC Target Endpoint

**Create FC Target Endpoint**

WWPN: 20:02:00:A0:98:54:F0:BC

Description:

Path:  A  B

Select VSAN: VSAN Fabric-A (101) + Create VSAN

OK Cancel

17. Click OK to create the FC Target Endpoint.

## Create Storage Connection Policy



Name:

Description:

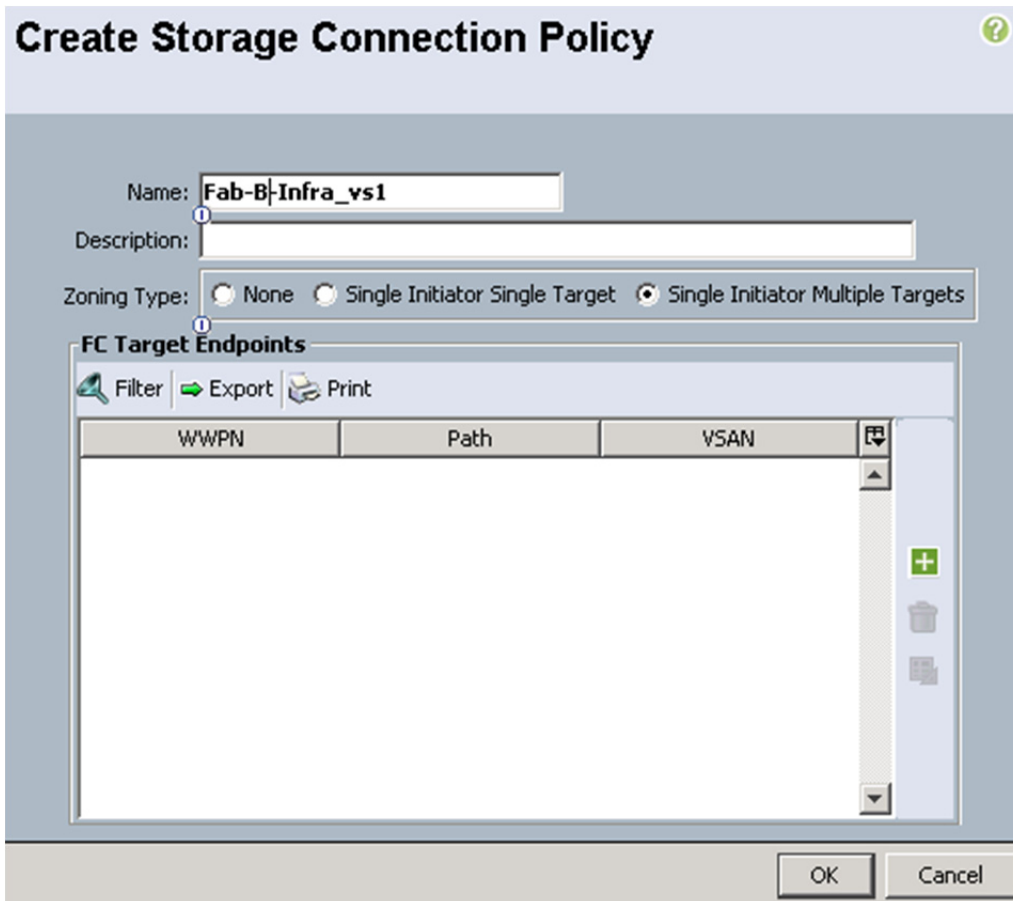
Zoning Type:  None  Single Initiator Single Target  Single Initiator Multiple Targets

**FC Target Endpoints**

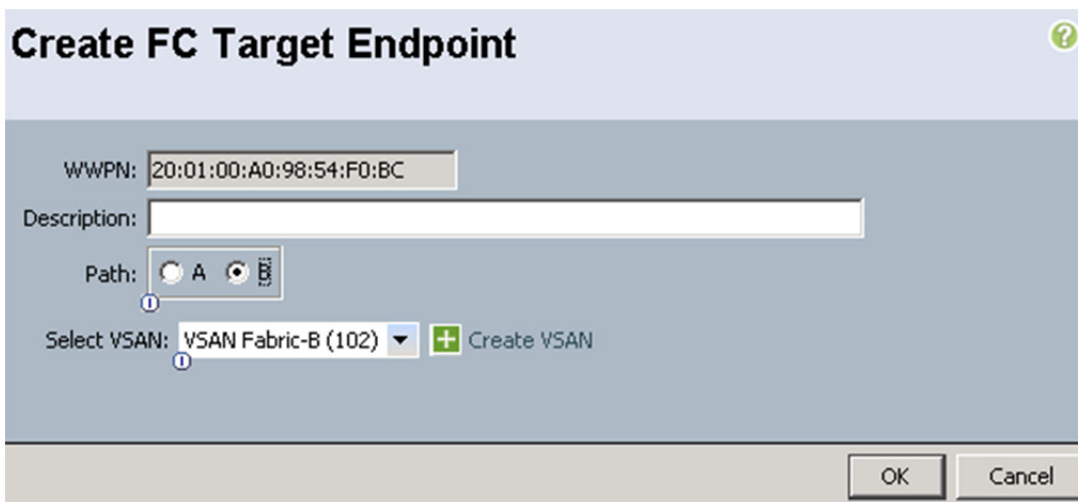
Filter Export Print

WWPN	Path	VSAN	
20:02:00:A0:98:54:F0:BC	A	Fabric-A	
20:00:00:A0:98:54:F0:BC	A	Fabric-A	

18. Click OK to create the Storage Connection Policy.
19. Enter Storage Connection Policy name.
20. Select the Zoning Type Single Initiator Multiple Targets.



21. Click the plus icon to add the FC Target Endpoint.
22. Enter the WWPN for fcp\_lif01b.
23. Select Path A.
24. Select VSAN Fabric-B.



25. Click OK to create the FC Target EndPoint.
26. Click the plus icon to add the FC Target Endpoint.
27. Enter the WWPN for fcp\_lif02b.

28. Select Path A.
29. Select VSAN Fabric-B.
30. Click OK to create the FC Target EndPoint.

### Create FC Target Endpoint ?

WWPN:

Description:

Path:  A  B

Select VSAN:

31. Click OK to create the FC Target Endpoint.

### Create Storage Connection Policy ?

Name:

Description:

Zoning Type:  None  Single Initiator Single Target  Single Initiator Multiple Targets

**FC Target Endpoints**

WWPN	Path	VSAN
20:03:00:A0:98:54:F0:BC	B	Fabric-B
20:01:00:A0:98:54:F0:BC	B	Fabric-B

32. Click OK to create the storage Connection Policy.

## 10.32 Create Service Profile Templates

This section details the creation of a service profile templates.

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 (expert)`.
5. The `Create Service Profile Template` window displays.
6. Name the service profile template `VMHost-Mgmt`.
7. Select `Updating Template`.
8. In the `UUID` section, select `UUID_Pool` previously create as the `UUID` pool.
9. Click `Next` to continue to the next section.

### Identify Service Profile Template ?

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name:

The template will be created in the following organization. Its name must be unique within this organization.  
Where: **org-root/org-MSPCFT**

The template will be created in the following organization. Its name must be unique within this organization.

Type:  Initial Template  Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.

**UUID**

UUID Assignment:

The UUID will be assigned from the selected pool.  
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

### Networking Section

Leave the `Dynamic vNIC Connection Policy` field at the default.

1. Select `Expert` for the `How would you like to configure LAN connectivity?` option.

## Networking

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy:  + Create Dynamic vNIC Connection Policy

---

**How would you like to configure LAN connectivity?**  Simple  **Expert**  No vNICs  Use Connectivity Policy

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Fabric ID	Native VLAN	

Delete + Add Modify

**iSCSI vNICs**

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

## Create vNIC

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

8. Click **Add** to add a vNIC to the template.
9. The **Create vNIC** window displays. Name the vNIC **LiveMigration**.
10. Check the **Use LAN Connectivity Template** checkbox.



11. Select `LiveMigration` for the vNIC Template field.
12. Select `Windows` in the Adapter Policy field.
13. Click `OK` to add the vNIC to the template.

**Create vNIC** ?

Name:  ⓘ

Use vNIC Template:  ⓘ  
+ Create vNIC Template

vNIC Template:  ⓘ

**Adapter Performance Profile**

Adapter Policy:  ⓘ + Create Ethernet Adapter Policy

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

**Create vNIC** ?

Name:  ⓘ

Use vNIC Template:  ⓘ  
+ Create vNIC Template

vNIC Template:  ⓘ

**Adapter Performance Profile**

Adapter Policy:  ⓘ + Create Ethernet Adapter Policy

20. Click `Add` to add a vNIC to the template.

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

**Create vNIC** ?

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

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

## Create vNIC ?

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

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

## Create vNIC ?

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

39. Click Add to add a vNIC to the template.
40. The Create vNIC window displays. Name the vNIC SMB-SQL

41. Check the Use LAN Connectivity Template checkbox.
42. Select SMB for the vNIC Template field.
43. Select Windows in the Adapter Policy field.
44. Click OK to add the vNIC to the template.

**Create vNIC** ?

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

45. Click Add to add a vNIC to the template.
46. The Create vNIC window displays. Name the vNIC AF-Public
47. Check the Use LAN Connectivity Template checkbox.
48. Select SMB for the vNIC Template field.
49. Select Windows in the Adapter Policy field.
50. Click OK to add the vNIC to the template.

**Create vNIC** ?

Name:

Use vNIC Template:

+ Create vNIC Template

vNIC Template:

**Adapter Performance Profile**

Adapter Policy:  + Create Ethernet Adapter Policy

## Storage Section

1. Select SAN-Boot for the local disk configuration policy.

2. Select the `Expert` option for the `How would you like to configure SAN connectivity` field.
3. In the `WWNN Assignment` field, select `WWNN_Pool`.
4. Click the `Add` button at the bottom of the window to add vHBAs to the template.
5. The `Create vHBA` window displays. Name the vHBA `Fabric-A-1`.
6. Check the box for `Use vHBA Template`.
7. Select `Fabric-A` in the `vHBA Template` field.
8. Select `Windows-NetApp` in the `Adapter Policy` field.
9. Click `OK` to add the vHBA to the template.

**Create vHBA**

Name:

Use vHBA Template:

[+ Create vHBA Template](#)

vHBA Template:

**Adapter Performance Profile**

Adapter Policy:  [+ Create Fibre Channel Adapter Policy](#)

10. Click the `Add` button at the bottom of the window to add vHBAs to the template.
11. The `Create vHBA` window displays. Name the vHBA `Fabric-B-1`.
12. Check the box for `Use vHBA Template`.
13. Select `Fabric-B` in the `vHBA Template` field.
14. Select `Windows-NetApp` in the `Adapter Policy` field.
15. Click `OK` to add the vHBA to the template.

## Create vHBA

Name:

Use vHBA Template:

[+ Create vHBA Template](#)

vHBA Template:

**Adapter Performance Profile**

Adapter Policy:  [+ Create Fibre Channel Adapter Policy](#)

16. Verify – Review the table to make sure that all four vHBAs were created.

**World Wide Node Name**

WWNN Assignment:

The WWNN will be assigned from the selected pool.  
The available/total WWNNs are displayed after the pool name.

Name	WWPN
vHBA Fabric-A-1	Derived
vHBA If	
vHBA Fabric-B-1	Derived
vHBA If	

[Delete](#) [+ Add](#) [Modify](#)

17. Click **Next** to continue to the next section.

## Zoning Section

1. Click the **Add** button in the **Select vHBA Initiator Group** field.
2. Enter the vHBA Initiator Group Name.
3. Select the Storage Connection Policy previously created for fabric A and the SVM `Infra_vs1`.

### Create vHBA Initiator Group

**vHBA Initiator Group**

Name:

Description:

Storage Connection Policy:  + Create Storage Connection Policy

**Global Storage Connection Policy**

Global storage connection policy **defined under org** is assigned to this vHBA initiator group.

**Properties**

Storage Connection Policy: **Fab-A-Infra\_vs1**  
 Description:  
 Zoning Type: **Single Initiator Multiple Targets**

**FC Target Endpoints**

Filter Export Print

WWPN	Path	VSAN
20:00:00:A0:98:54:F0:BC	A	Fabric-A
20:02:00:A0:98:54:F0:BC	A	Fabric-A

OK Cancel

4. Click OK to create the vHBA Initiator Group.
5. Click the Add button in the Select vHBA Initiator Group field.
6. Enter the vHBA Initiator Group Name.
7. Select the Storage Connection Policy previously created for fabric B and the SVM Infra\_vs1.

### Create vHBA Initiator Group

**vHBA Initiator Group**

Name:

Description:

Storage Connection Policy:  + Create Storage Connection Policy

**Global Storage Connection Policy**

Global storage connection policy **defined under org** is assigned to this vHBA initiator group.

**Properties**

Storage Connection Policy: **Fab-B-Infra\_vs1**  
 Description:  
 Zoning Type: **Single Initiator Multiple Targets**

**FC Target Endpoints**

Filter Export Print

WWPN	Path	VSAN
20:01:00:A0:98:54:F0:BC	B	Fabric-B
20:03:00:A0:98:54:F0:BC	B	Fabric-B

OK Cancel

8. Click OK to create the vHBA Initiator Group.
9. Select the Fabric-A-1 in the vHBA Initiator box.

10. Select Host-A-Infra\_vs1 in the Select vHBA Initiators Group box.

11. Click >>Add To >> button to add the selected initiator to the selected Initiator Group.

**Zoning**  
Specify zoning information

Zoning configuration involves the following **steps**:

1. **Select** vHBA Initiator(s) (vHBAs are created on storage page)
2. **Select** vHBA Initiator Group(s)
3. **Add** selected Initiator(s) to selected Initiator Group(s)

**Select vHBA Initiators**

Name
Fabric-A-1
Fabric-B-1

>> Add To >>

**Select vHBA Initiator Groups**

Name	Storage Connection Policy Name
Hast-B-Infra_vs1	Fab-B-Infra_vs1
Host-A-Infra_vs1	Fab-A-Infra_vs1

Delete Add Modify

< Prev Next > Finish Cancel

12. Select the Fabric-B-1 in the vHBA Initiator box.

13. Select Host-B-Infra\_vs1 in the Select vHBA Initiators Group box.

14. Click >>Add To >> button to add the selected initiator to the selected Initiator Group.

**Zoning**  
Specify zoning information

Zoning configuration involves the following **steps**:

1. **Select** vHBA Initiator(s) (vHBAs are created on storage page)
2. **Select** vHBA Initiator Group(s)
3. **Add** selected Initiator(s) to selected Initiator Group(s)

**Select vHBA Initiators**

Name
Fabric-A-1
Fabric-B-1

>> Add To >>

**Select vHBA Initiator Groups**

Name	Storage Connection Policy Name
Hast-B-Infra_vs1	Fab-B-Infra_vs1
Host-A-Infra_vs1	Fab-A-Infra_vs1
Storage Initiator Fabric-A-1	

Delete Add Modify

< Prev Next > Finish Cancel

15. Click Next to continue the next section.

## vNIC/vHBA Placement Section

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



**Modify vNIC/vHBA Placement**

Specify how vNICs and vHBAs are placed on physical network adapters

vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement: **VMIHost-Mgmt** + Create Placement Policy

Virtual Network Interface connection provides a mechanism of placing vNICs and vHBAs on physical network adapters. vNICs and vHBAs are assigned to one of Virtual Network Interface connection specified below. This assignment can be performed explicitly by selecting which Virtual Network Interface connection is used by vNIC or vHBA or it can be done automatically by selecting "any". vNIC/vHBA placement on physical network interface is controlled by placement preferences.

Please select one Virtual Network Interface and one or more vNICs or vHBAs

Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
vCon 1		Assigned Only
vCon 2		All
vCon 3		All
vCon 4		All

**vNIC/vHBA Placement**

Specify how vNICs and vHBAs are placed on physical network adapters

vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement: **VMIHost-Mgmt** + Create Placement Policy

Virtual Network Interface connection provides a mechanism of placing vNICs and vHBAs on physical network adapters. vNICs and vHBAs are assigned to one of Virtual Network Interface connection specified below. This assignment can be performed explicitly by selecting which Virtual Network Interface connection is used by vNIC or vHBA or it can be done automatically by selecting "any". vNIC/vHBA placement on physical network interface is controlled by placement preferences.

Please select one Virtual Network Interface and one or more vNICs or vHBAs

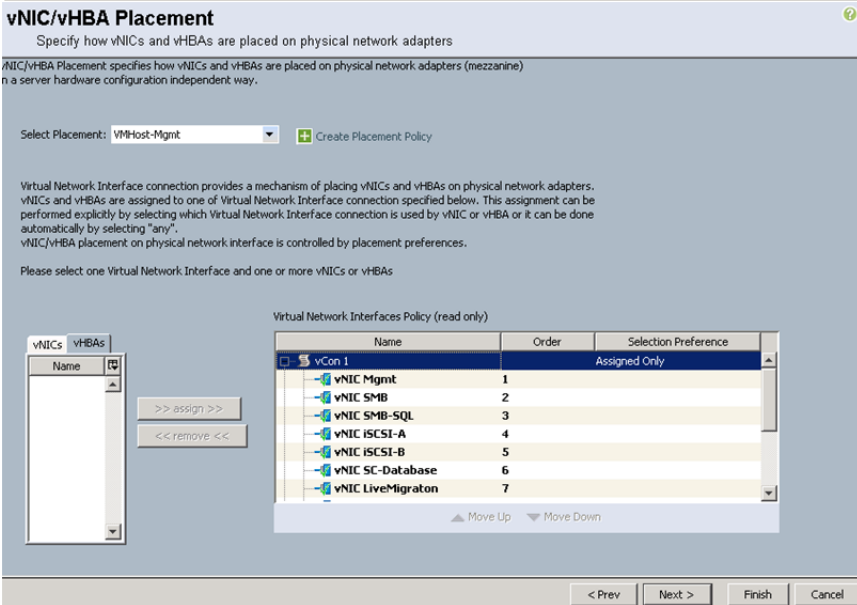
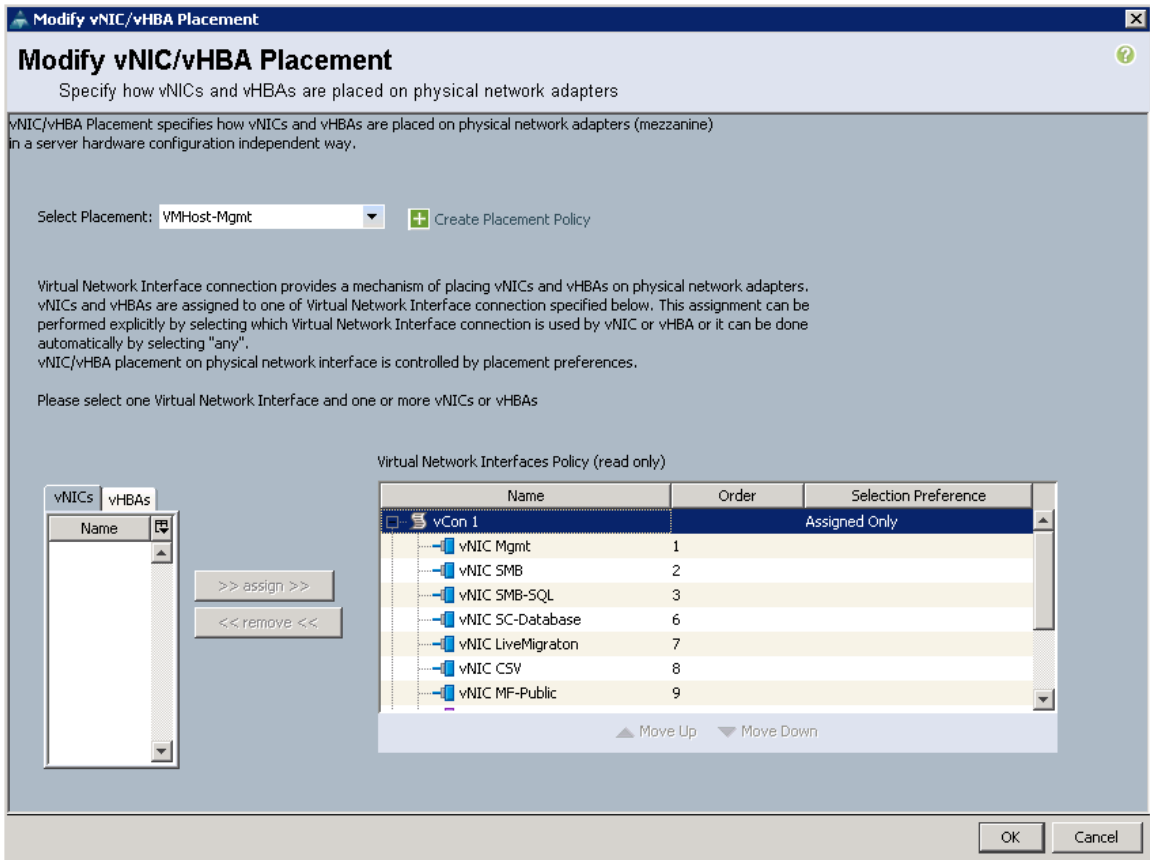
Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
vCon 1		Assigned Only
vCon 2		All
vCon 3		All
vCon 4		All

Name
CSV
LiveMigrat...
MF-Public
Mgmt
SC-Databa...
SMB
SMB-SQL
iSCSI-A
iSCSI-B

2. Select vCon1 assign the vNICs in the following order:
  - Mgmt
  - SMB
  - SMB-SQL
  - SC-Database
  - LiveMigration
  - CSV
  - MF-Public
  - AF-Public
3. Click the vHBA tab and add the vHBAs in the following order:
  - Fabric-A-1
  - Fabric-B-1

- Verify: Review the table to make sure that all of the vHBAs and vNICs were created.



- Click **Next** to continue to the next section.

## vMedia Policy Selection

**Note:** vMedia Policy configuration can be skipped.

1. Click **Next**.

## Server Boot Order Section

1. Select `Infra_vs1` 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.

### Server Boot Order ?

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: Infra\_vs1 + Create Boot Policy

Name: **Infra\_vs1**  
 Description:  
 Reboot on Boot Order Change: **No**  
 Enforce vNIC/vHBA/iSCSI Name: **Yes**  
 Boot Mode: **Legacy**

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

Boot Order

Filter Export Print

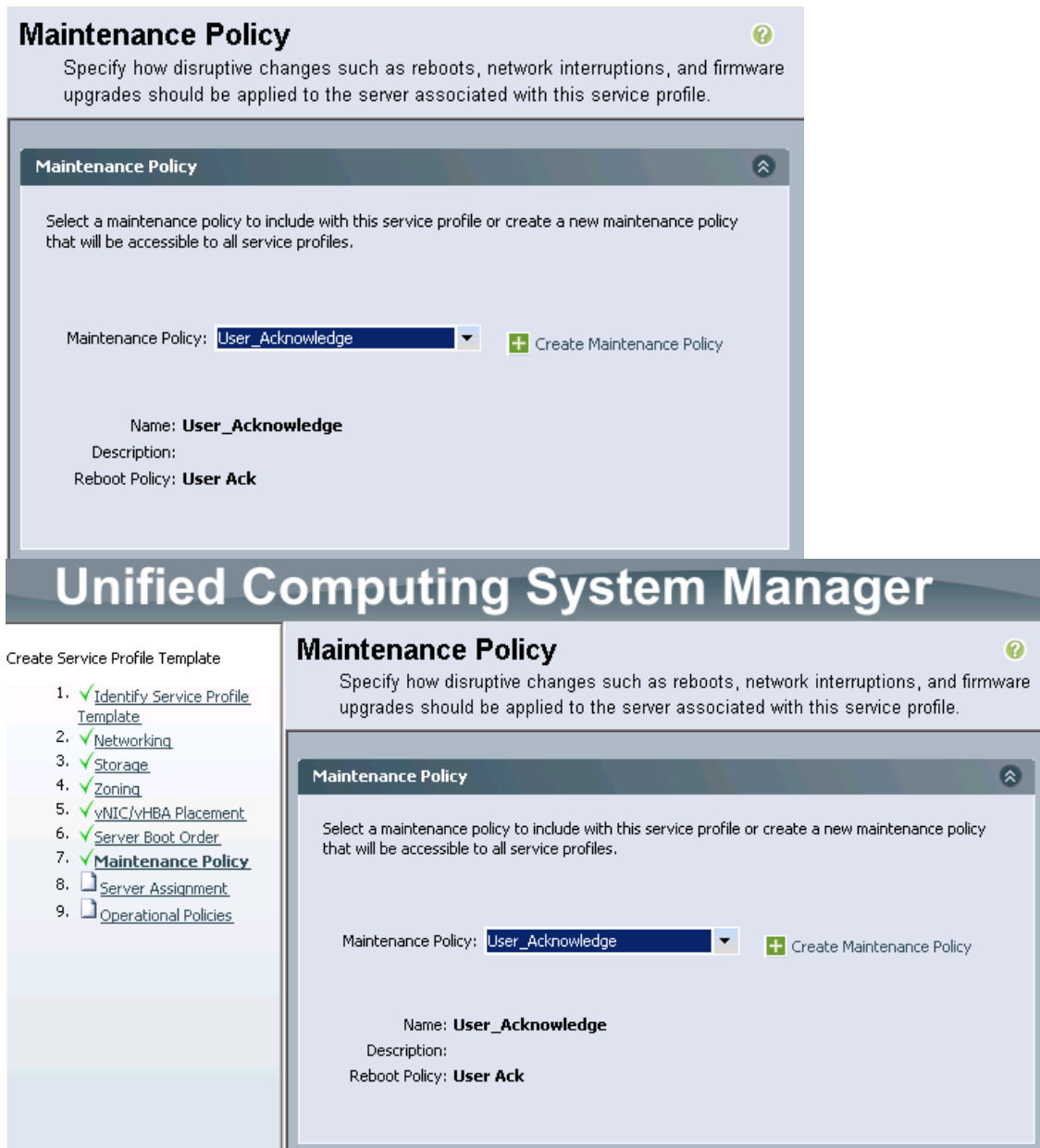
Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN	
Remote CD/DVD	1					
San	2					
SAN primary		Fabric-A-1	Primary			
SAN Target primary			Primary	0	20:00:00:A0:98:54:F0:BC	
SAN Target secondary			Secondary	0	20:02:00:A0:98:54:F0:BC	
SAN secondary		Fabric-B-1	Secondary			
SAN Target primary			Primary	0	20:01:00:A0:98:54:F0:BC	
SAN Target secondary			Secondary	0	20:03:00:A0:98:54:F0:BC	

Create iSCSI vNIC
Set iSCSI Boot Parameters

< Prev
Next >
Finish
Cancel

## 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 `Mgmt_Pool` in the `Pool Assignment` field.
2. Select `VMHost-Infra` 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.

## Server Assignment

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment:  + Create Server Pool

Select the power state to be applied when this profile is associated with the server.

Up  Down

The service profile template will be associated with one of the servers in the selected pool.  
If desired, you can specify an additional server pool policy qualification that the selected server must meet.  
To do so, select the qualification from the list.

Server Pool Qualification:

Restrict Migration:

---

### Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with.  
Otherwise the system uses the firmware already installed on the associated server.

Host Firmware:  + Create Host Firmware Package

< Prev    Next >    Finish    Cancel

## 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.

## Operational Policies



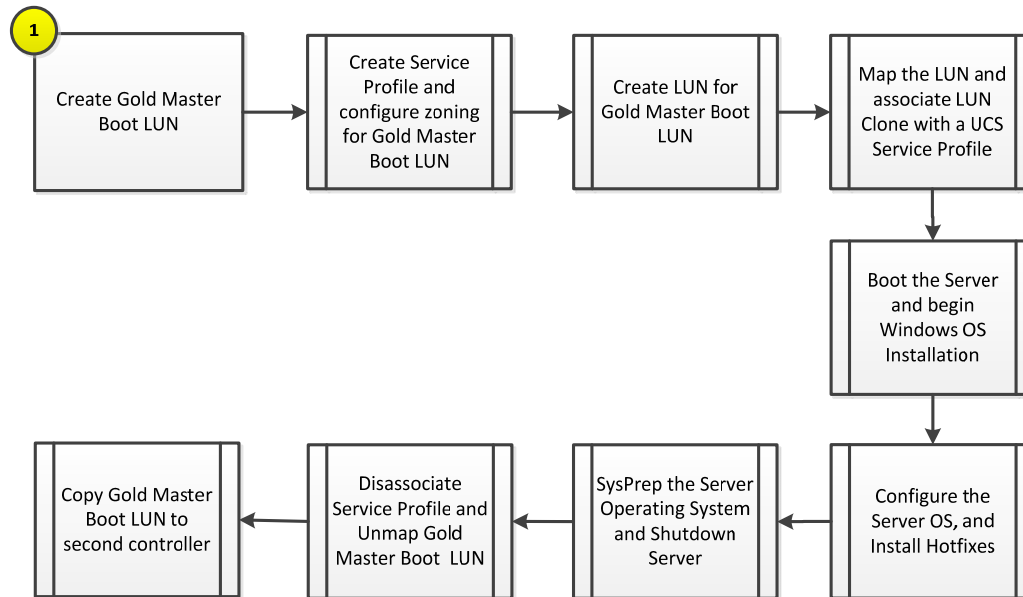
Optionally specify information that affects how the system operates.

<b>BIOS Configuration</b>
If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile BIOS Policy: <input type="text" value="VMHost-Mgmt"/> Create BIOS Policy
<b>External IPMI Management Configuration</b>
<b>Management IP Address</b>
<b>Monitoring Configuration (Thresholds)</b>
<b>Power Control Policy Configuration</b>
Power control policy determines power allocation for a server in a given power group. Power Control Policy: <input type="text" value="No-Power-Cap"/> Create Power Control Policy
<b>Scrub Policy</b>
<b>KVM Management Policy</b>

< Prev   Next >   Finish   Cancel

## Create Gold Master Boot LUN

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



## 11 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.

### 11.1 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 3.0 or higher installed on an administrative host

**Note:** NetApp Power Tools can be downloaded from NetApp Communities site. <http://nt-ap.com/PoshToolkit>.

- Access to Windows 2012 R2 installation ISO image
- Access to Cisco UCS FCoE driver installation ISO image
- Access to Cisco UCS Ethernet driver installation ISO image



## 11.2 Create Gold Master Service Profile

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

1. Open the UCS Manager and select the Servers tab at the top left of the window.
2. Select and expand the Service Profile Templates > root > sub –organization object.
3. Right-click VMHost-Mgmt and select the action “Create Service Profiles From Template”.
4. Enter GoldMaster for the service profile Name Prefix.
5. Enter the Name Suffix Starting Number.
6. Enter 1 for the number of instances to create.
7. Select GoldMaster for the Service Profile Template field. It should be under Organizations > root > sub-organization.
8. Click OK to create the service profile, and OK again to acknowledge the creation.
9. Select the newly created service profile, from the left hand management pane expand vHBA Fabric-A-1 and write down the WWPN.

## 11.3 Create the GoldMaster Boot LUN

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

1. Log into the NetApp Cluster by opening an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Create a new Qtree to hold the boot LUN.

```
qtree create -volume ucs_boot -Qtree goldmaster
```

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

```
lun create /vol/ucs_boot/goldmaster/boot.lun -Size 200gb -OsType windows_2008 -space-reserve disabled -vserver infra_svm
```

4. Create the NetApp igroup for the Gold Master Boot LUN and the WWPN from the <<vHBA\_A>> vHBA in the Goldmaster service profile to the Gold Master Boot LUN igroup.

```
igroup create -igroup goldmaster -protocol fcp -ostype hyper_v -initiator <vHBA_A WWPN> -vserver infra_svm
```

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

```
lun map -path /vol/ucs_boot/goldmaster/boot.lun -igroup goldmaster -lun-id 0 -vserver infra_svm
```

## 11.4 Prepare to Install Windows Server 2012

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

1. Right-click the GoldMaster 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*.

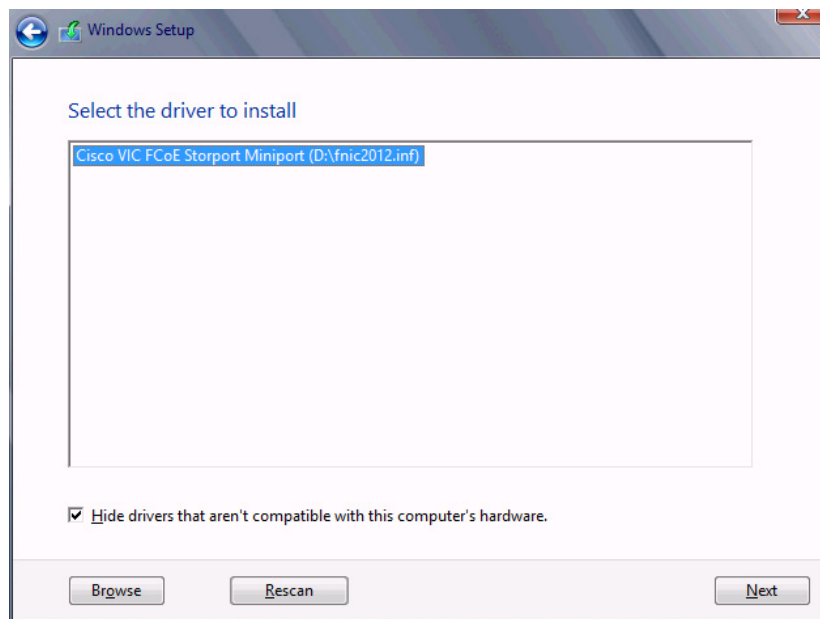
## 11.5 Install Windows Server 2012

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. Change 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 auto detect, Click Next.

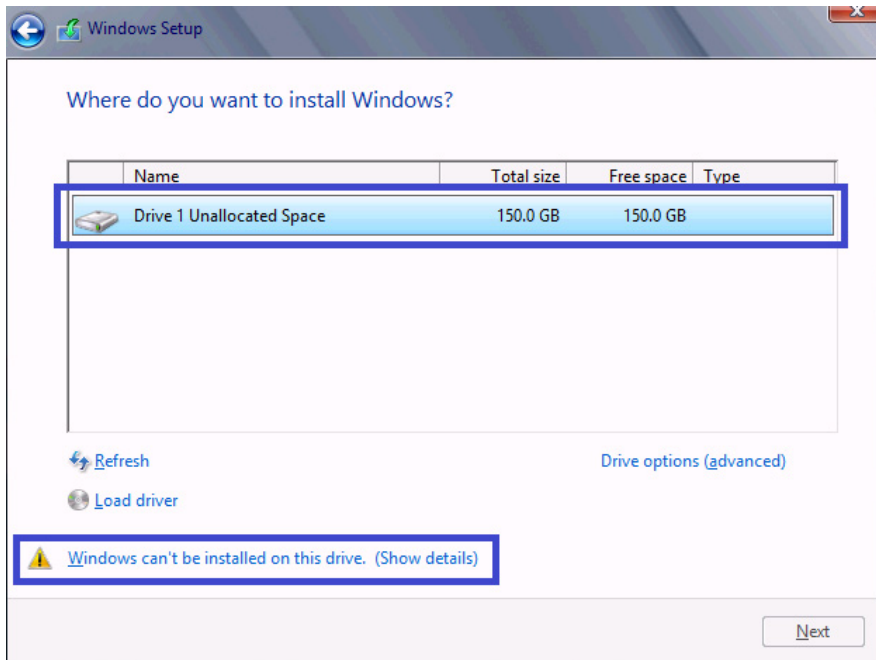


14. You should see a LUN listed in the drive selection screen.

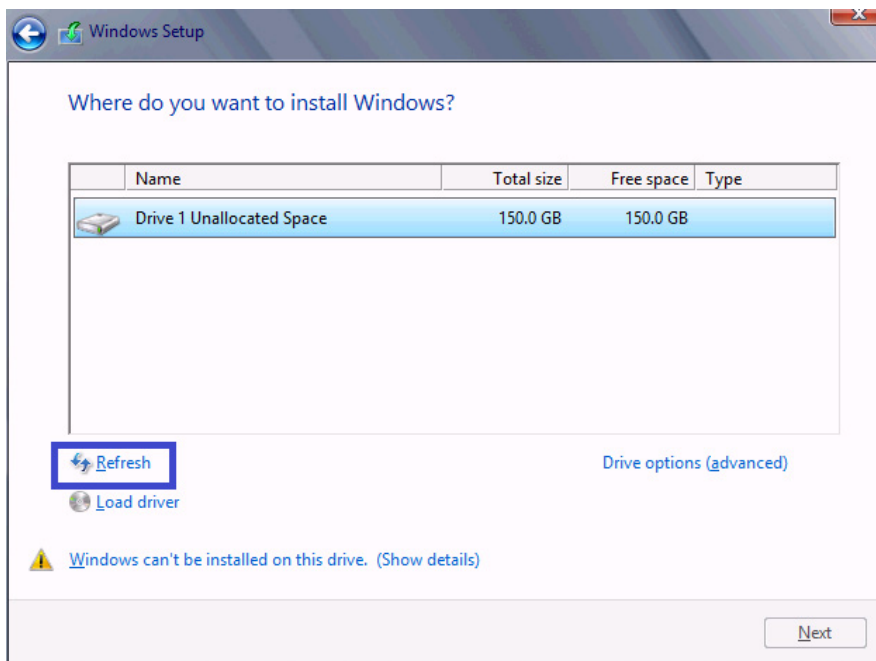
**Note:** Only a single LUN instance should be displayed. Multiple instance of the same LUN indicated that there are multiple paths to the installation LUN. Verify that the SAN zoning is correct and restart the installation.

**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.

## 11.6 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
```

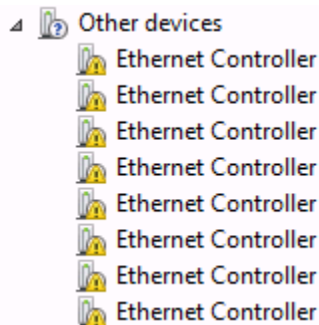
5. Add MPIO by entering the following command:

```
Add-WindowsFeature Multipath-IO -IncludeManagementTools -Restart
```

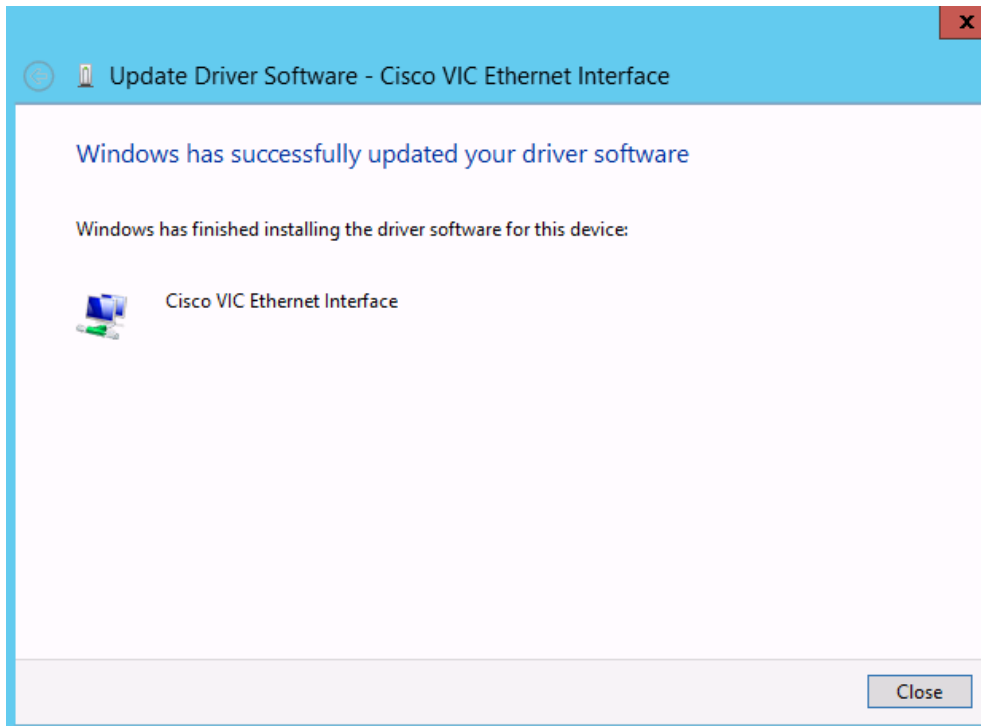
## 11.7 Install Windows eNIC Drivers

The following steps describe how to install all required network drivers if it was not installed at the same time as the storage driver.

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.



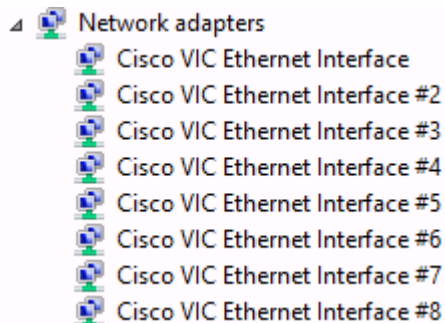
7. Right-click one of the Ethernet Controller, and select Update Driver Software.
8. Click Browse my computer for driver software.
9. Click Browse, and select the CDROM drive, click OK.
10. Click Next >Close.



11. Right-click 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.

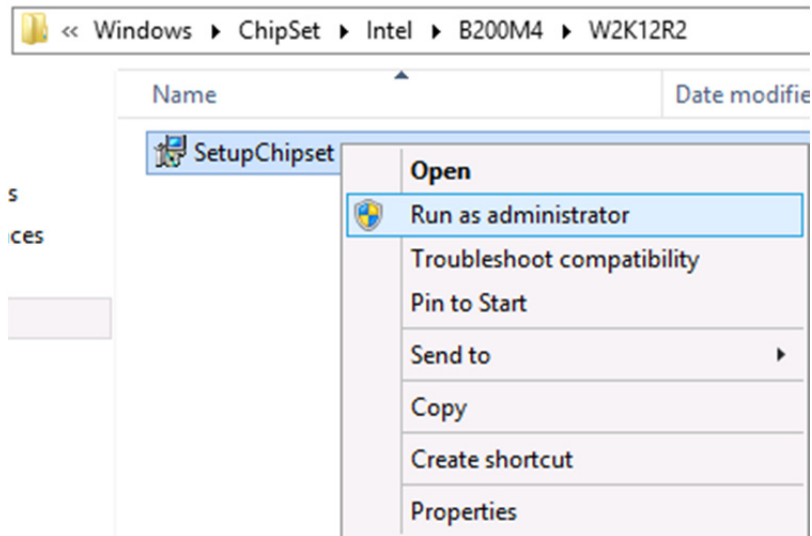


16. Configure the TCP/IP settings on the appropriate NIC to provide network access for installing the additional software components.

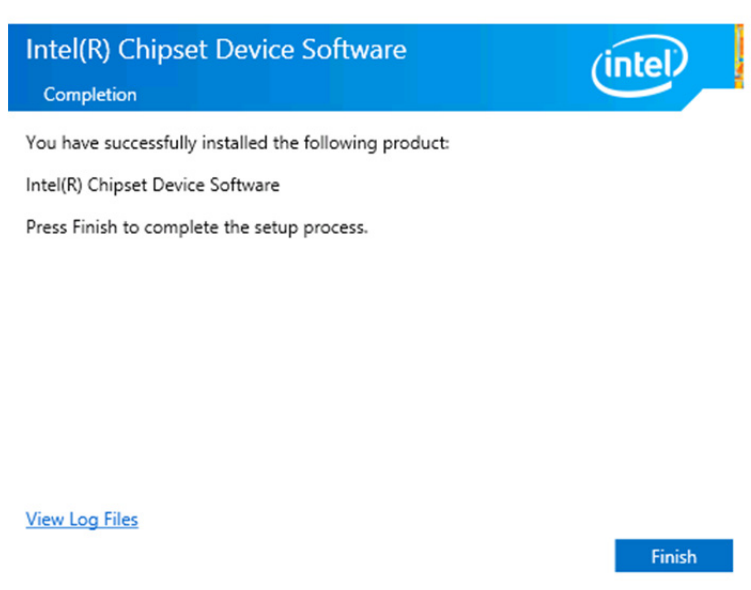
## 11.8 Install Intel Chipset Device Software for Xeon E5-2600v2 and E5-2600v3 Processors

1. Using the same Cisco drivers ISO image file navigate to the chipset directory (Windows->ChipSet->B200M4->W2K12R2. Right click SetupChipSet.exe and select Run as Administrator.

**Note:** SetupChipSet.exe in the B200M4 directory can be selected for B200 M3 servers also.



2. Click Next in the Welcome screen.
3. Review the license agreement and click Accept to continue.
4. Click Install in the Readme File Information screen to begin the installation process.



6. Click Finish to Exit the installation wizard.

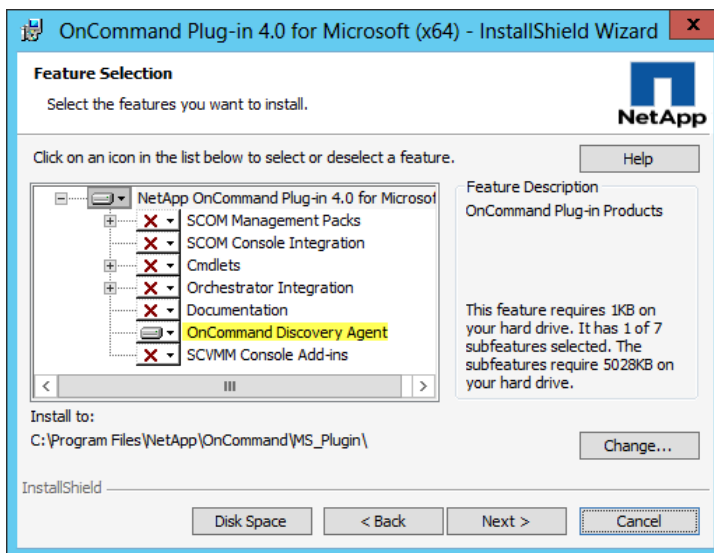
## 11.9 Install the Data ONTAP PowerShell Toolkit

The following step describes how 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](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.

## 11.10 Install NetApp OnCommand Discovery Agent

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



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

## 11.11 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 USCM. Select and expand the Service Profile Templates > root object.
3. Right-click Goldmaster and select Disassociate Service Profile.
4. Log in to the administrative host that has the Data ONTAP PowerShell Toolkit module.
5. Unmap the goldmaster igroup from the Gold Master Boot LUN.

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

## 12 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.

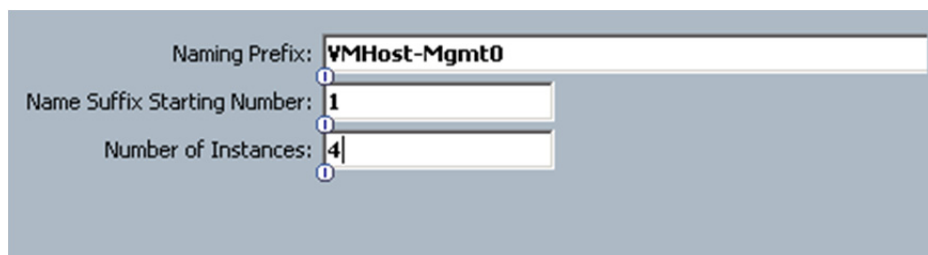
This section provides high-level walkthrough on how to deploy Hyper-V hosts for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- Fully configured Cisco UCS Service Profile Templates
- A Gold Master Boot LUN running Windows Server 2012 R2 (x64) has been created

### 12.1 Create Service Profiles

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

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



Naming Prefix:

Name Suffix Starting Number:

Number of Instances:

8. Click `OK` in the message box.

### 12.2 Gather the 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 17) vHBA WWPNs for Fabric A and Fabric B**

Cisco UCS Service Profile Name	Fabric-A-1 WWPN	Fabric-B-1 WWPN
VMHost-Mgmt01		
VMHost-Mgmt02		
VMHost-Mgmt03		
VMHost-Mgmt04		

**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.

### 12.3 FlexClone Boot LUN

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

1. Log into the NetApp Cluster by opening an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Create a new Qtree to hold the boot LUN.

```
qtree create -volume ucs_boot -Qtree VMHost-Mgmt01
qtree create -volume ucs_boot -Qtree VMHost-Mgmt02
qtree create -volume ucs_boot -Qtree VMHost-Mgmt03
qtree create -volume ucs_boot -Qtree VMHost-Mgmt04
```

3. Using the information from above table Create igroups.

```
igroup create -igroup VMHost-Mgmt01 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vserver infra_svm

igroup create -igroup VMHost-Mgmt02 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vserver infra_svm

igroup create -igroup VMHost-Mgmt03 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vserver infra_svm

igroup create -igroup VMHost-Mgmt04 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vserver infra_svm
```

4. Clone the boot LUN from the goldmaster boot LUN.

```
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-Mgmt01/boot.lun -vserver infra_svm
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-Mgmt02/boot.lun -vserver infra_svm
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-Mgmt03/boot.lun -vserver infra_svm
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-Mgmt04/boot.lun -vserver infra_svm
```

5. Map the boot LUN to the new iGroup.

```
lun map -Path /vol/ucs_boot/VMHost-Mgmt01/boot.lun -InitiatorGroup VMHost-Mgmt01 -lun-id
0 -vserver infra_svm
```

```

lun map -Path /vol/ucs_boot/VMHost-Mgmt02/boot.lun -InitiatorGroup VMHost-Mgmt02 -lun-id
0 -vserver infra_svm

lun map -Path /vol/ucs_boot/VMHost-Mgmt03/boot.lun -InitiatorGroup VMHost-Mgmt03 -lun-id
0 -vserver infra_svm

lun map -Path /vol/ucs_boot/VMHost-Mgmt04/boot.lun -InitiatorGroup VMHost-Mgmt04 -lun-id
0 -vserver infra_svm

```

## 12.4 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 Mgmt\_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 Mgmt\_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. Repeat for each service profile.

## 12.5 Configure Windows Networking for FlexPod

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

### All Hosts

1. Open a PowerShell window and issue the command Get-NetAdapter
2. Note the MAC address for each adapter.

```

PS C:\> Get-NetAdapter

```

Name	InterfaceDescription	ifIndex	Status	MacAddress
Ethernet 8	Cisco VIC Ethernet Interface #8	20	Up	00-25-B5-E1-26-F8
Ethernet 7	Cisco VIC Ethernet Interface #7	19	Up	00-25-B5-E1-26-E8
Ethernet 3	Cisco VIC Ethernet Interface #3	15	Up	00-25-B5-E1-26-D9
Ethernet 2	Cisco VIC Ethernet Interface #2	14	Up	00-25-B5-E1-26-D8
Ethernet 4	Cisco VIC Ethernet Interface #4	16	Up	00-25-B5-E1-26-C9
Ethernet 5	Cisco VIC Ethernet Interface #5	17	Up	00-25-B5-E1-26-C8
Ethernet	Cisco VIC Ethernet Interface	13	Up	00-25-B5-E1-26-B9
Ethernet 6	Cisco VIC Ethernet Interface #6	18	Up	00-25-B5-E1-27-09

3. In UCS Manager select the service profile of the server and click on the Network tab. Locate the vNIC.

Name	MAC Address	Actual Order
vNIC AF-Public	00:25:B5:E1:27:09	9
vNIC CSV	00:25:B5:E1:26:D8	7
vNIC LiveMigraton	00:25:B5:E1:26:D9	6
vNIC MF-Public	00:25:B5:E1:26:B9	8
vNIC Mgmt	00:25:B5:E1:26:E8	1
vNIC SC-Database	00:25:B5:E1:26:C9	4
vNIC SMB	00:25:B5:E1:26:C8	2
vNIC SMB-SQL	00:25:B5:E1:26:F8	3

- Identify the vNIC with the MAC Address noted in step 2.
- Using PowerShell rename the LAN adapter and assign the appropriate IP configuration to reflect the network it is associated with. For example, the following command renames adapter Ethernet 7 to Mgmt and configures the IPV4 address and DNS and registers the name in DNS.

```

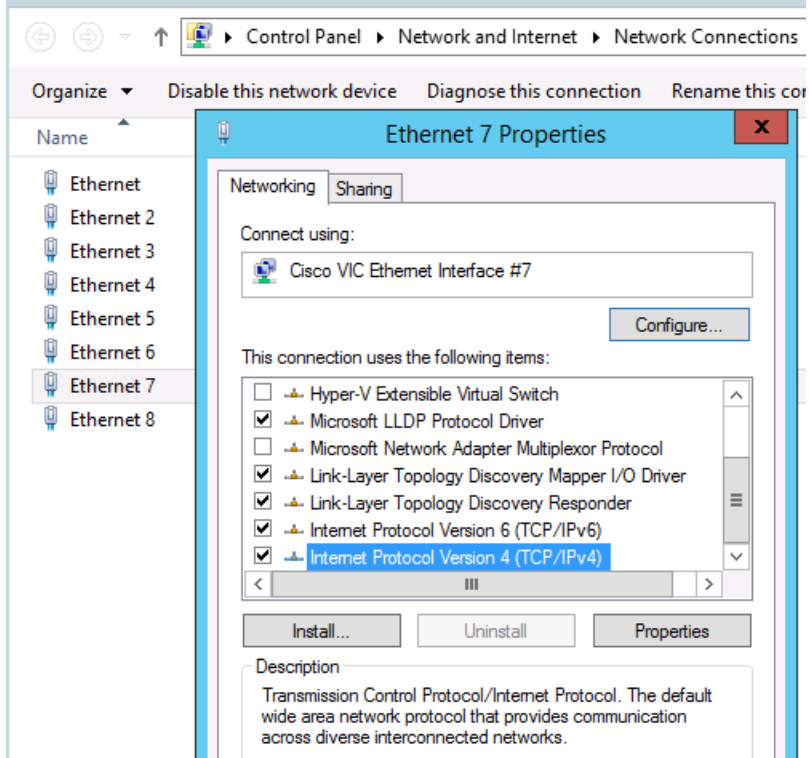
Rename-NetAdapter -Name "Ethernet 7" -NewName "Mgmt"
New-NetIPAddress -InterfaceIndex 19 -IPAddress 10.10.0.61 -PrefixLength 24 -
DefaultGateway 10.10.0.1
Set-DnsClientServerAddress -InterfaceIndex 19 -ServerAddresses ("10.0.4.61","10.0.4.62")
Set-DnsClient -InterfaceIndex 19 -RegisterThisConnectionsAddress $true

```

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

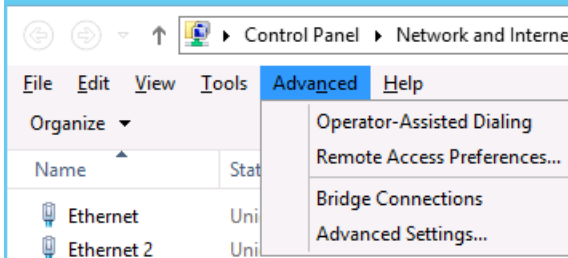
**Note:** Default gateway and DNS entries should be configured for the Mgmt NIC only.

**Note:** The settings can also be set via the GUI.



- Repeat for each eNIC in windows.

- In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings.

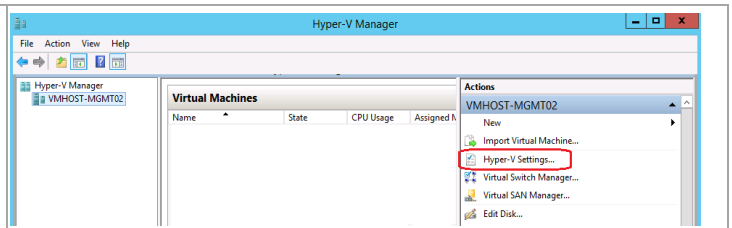


- Select the adapter and use the arrows to move it up or down in binding order.
- The recommended binding order is:
  - Mgmt
  - SMB
  - LiveMigration
  - CSV
  - SC-Database
  - MF-Public
  - AF-Public
  - SMB-SQL

## 12.6 Enable Enhanced Session Mode

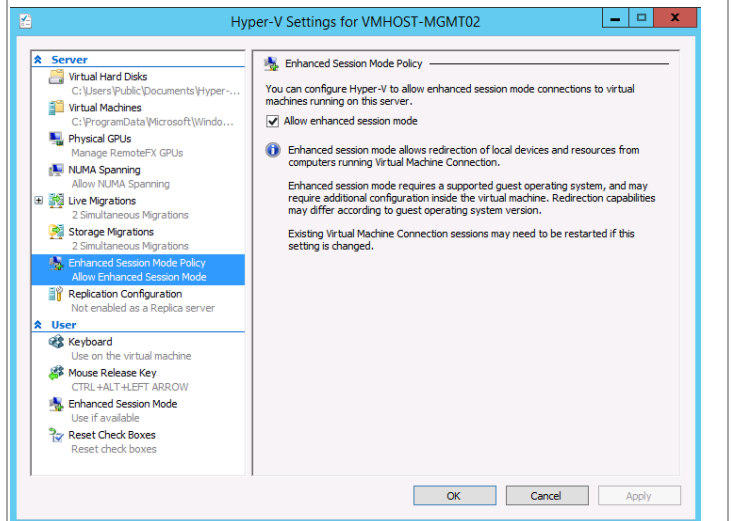
### All Hosts

In the **Hyper-V Manager** console, select **Hyper-V Settings...** under **Actions**.



In the **Hyper-V Settings** page select **Enhanced Session Mode Policy**. Check the box by **Allow enhanced session mode** and click **OK** to accept the change.

Repeat for all Hyper-V Servers.



## 12.7 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
SC-Database	External	No	SC-Database	No
SMB-SQL	External	No	SMB-SQL	No

3. Create virtual switch Mgmt.

```
New-VMSwitch -Name Mgmt -NetAdapterName Mgmt -AllowManagementOS $true
```

4. Create virtual switch SC-Database.

```
New-VMSwitch -Name SC-Database -NetAdapterName SC-Database -AllowManagementOS $false
```

5. Create virtual switch SMB-SQL.

```
New-VMSwitch -Name SMB-SQL -NetAdapterName SMB-SQL -AllowManagementOS $false
```

## 12.8 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. The optional domain controllers can be omitted from the configuration in this case or used as a resource domain. The domain controller virtual machines will not be clustered because redundancy is provided by deploying multiple domain controllers running in virtual machines on different servers. Since these virtual machines reside on Hyper-V hosts that run Windows Failover cluster, but are not clustered themselves, Hyper-V Manager should be used to manage them instead of Virtual Machine Manager.

See Appendix B: Build of Materials if an active directory domain controller needs to be created.

## 12.9 Prepare Nodes for Clustering

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

### All Hosts

1. Add Failover Clustering feature.

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

2. Rename the Host.

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

### 3. Add the host to Active Directory.

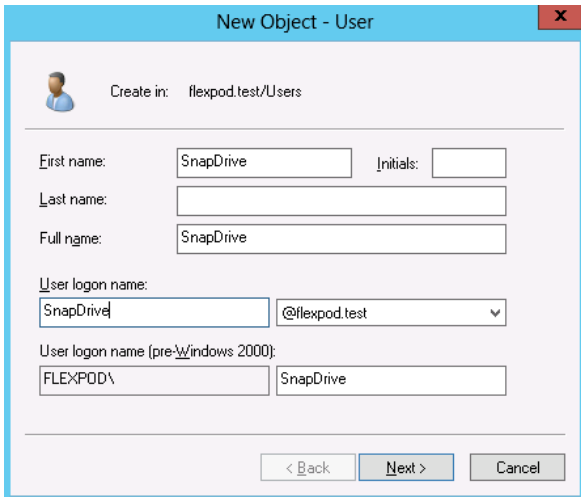
```
Add-Computer -DomainName <domain_name> -Restart
```

## 12.10 Install NetApp SnapDrive

The following section describes how to install the NetApp SnapDrive for 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.



New Object - User

Create in: flexpod.test/Users

First name: SnapDrive Initials:

Last name:

Full name: SnapDrive

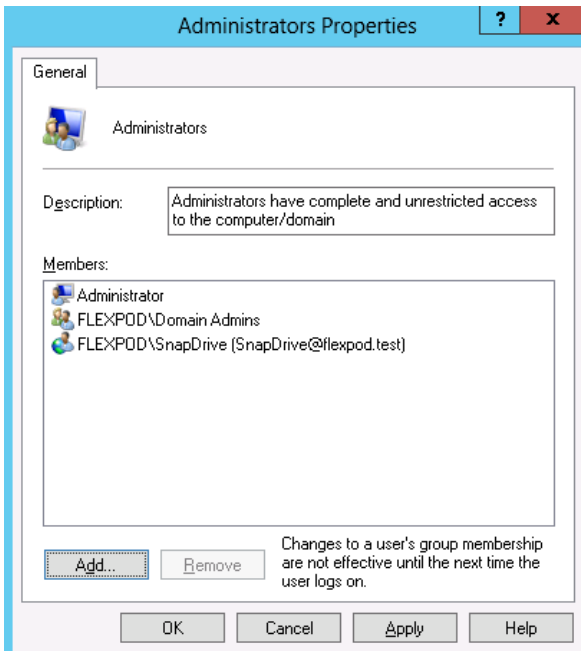
User logon name: SnapDrive @flexpod.test

User logon name (pre-Windows 2000): FLEXP0D\SnapDrive

< Back Next > Cancel

### All Hosts

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



Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

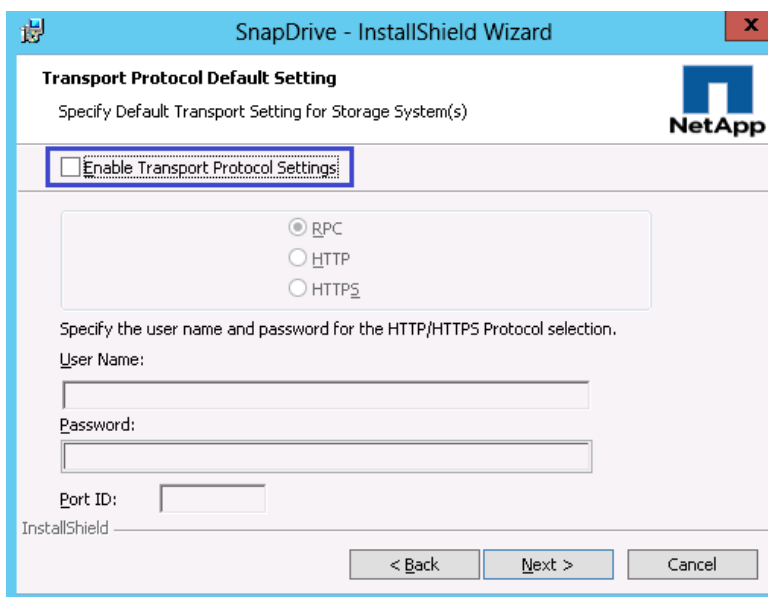
- Administrator
- FLEXP0D\Domain Admins
- FLEXP0D\SnapDrive (SnapDrive@flexpod.test)

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK Cancel Apply Help

2. Launch the SnapDrive installer - SnapDrive7.0.3\_x64.exe.
3. Launch the Installer, 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 Enable Preferred storage system IP Address, and Click Next.
11. Uncheck the Enable Transport Protocol Settings, and click Next



12. Leave Enable dataset protection integration Unchecked, and click Next.
13. Click Install.
14. 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.

15. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_vserver_mgmt>> -IP << var_vserver_mgmt_ip>>
```

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

```
Set-SdStorageConnectionSetting -StorageSystem <<var_vserver_mgmt>> -protocol https -credential vsadmin
```

## 12.11 Install NetApp SnapManager for Hyper-V

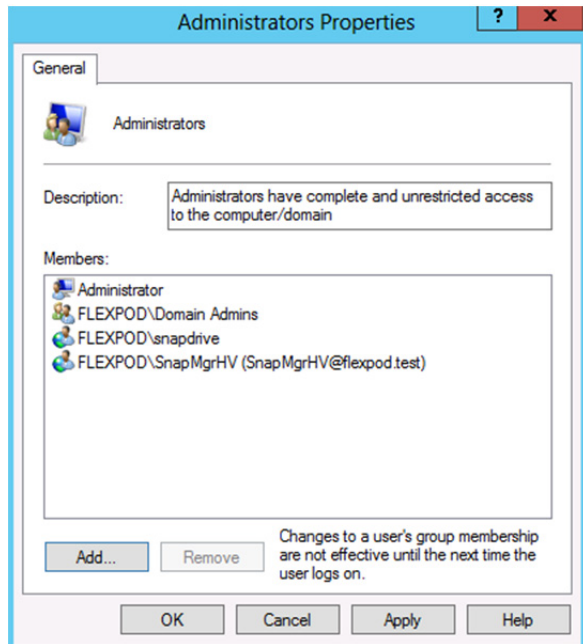
The following section describes how to installation of the NetApp SnapManager for Hyper-V. For detailed information regarding the installation see the Administration and Installation Guide.

## Service Account preparation

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

## All Hosts

1. Add the SMHV service account to the local Administrators group in Windows.



## All Hosts

1. Download the SnapManager for Hyper-V installer from [http://support.netapp.com/NOW/download/software/snapmanager\\_hyperv\\_win/2.0/SMHV2.0\\_x64.exe](http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/2.0/SMHV2.0_x64.exe)
2. Launch the Installer, click **Next**.
3. Select the Storage based Licensing method and click **Next**.
4. Validate the installation path and click **Next**.
5. Enter the Account information for the SMHV service account and click **Next**.
6. Accept the default TCP/IP port for the Web Service.
7. Click **Install**.
8. Click **Finish**.

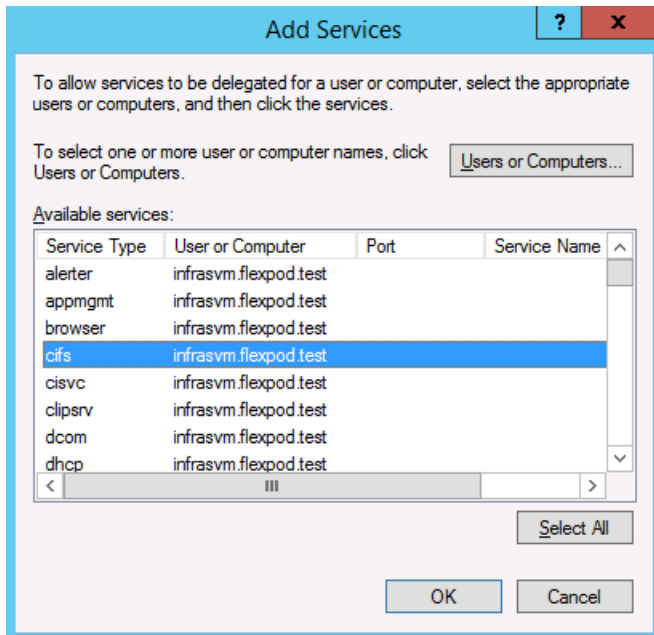
## 12.12 Configure Constrained Delegation for Hyper-V Hosts

While the hosts themselves already have the required permissions to access the SMB share, you will encounter access denied errors when trying to perform remote management functions that access the SMB share. To avoid these issues, configure constrained delegation for the Hyper-V hosts by following these steps.

1. Start Active Directory Users and Computers. Browse to the Computer objects for the Hyper-V hosts.
2. Right-click on a Hyper-V host and select Properties.



3. Select the Delegation tab.
  - a. Select Trust this computer for delegation to the specified services only
  - b. Select Use Kerberos only
  - c. Click Add
4. Click the Users or Computers... button on the top of the Add Services popup.
5. Enter the Name of the Infrastructure Storage Virtual Machine, and click OK.
6. Select cifs and click OK.



7. Click OK
8. Repeat for each Hyper-V host

## 12.13 Create a Cluster

### One Host Node 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 = 'LiveMigration' }
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Mgmt' }
Get-ClusterNetworkInterface | ? Name -like *SMB* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'SMB' }
```

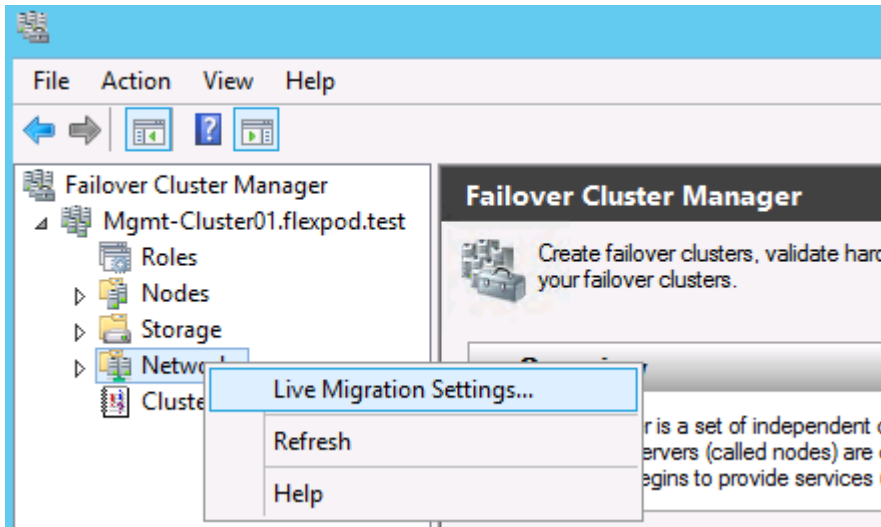
4. Designate the CSV network.

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

## 12.14 Configure Live Migration Network

### One Host Node Only

1. Open Failover Cluster Manager from Server Manager select Tools -> Failover Cluster Manager.
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.

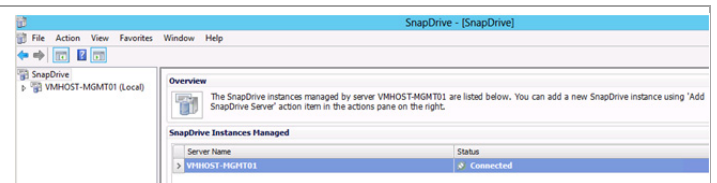
## 12.15 Create Quorum Witness and Cluster Shared Volume LUNs

### One Host Node Only

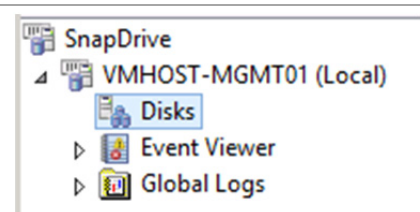
1. Open a PowerShell prompt and move the Available Storage cluster group by running.

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

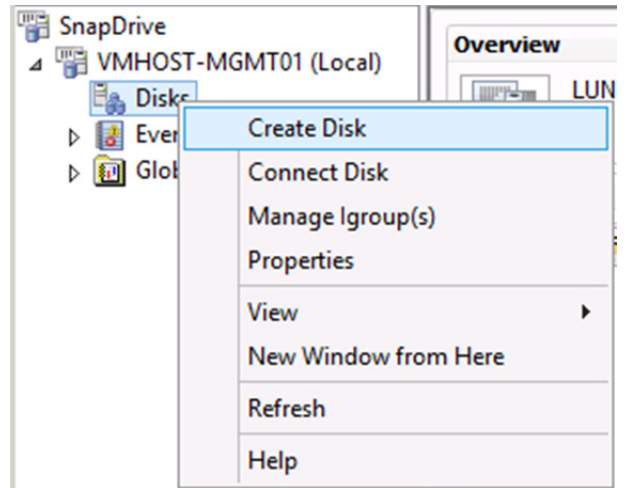
Open SnapDrive from the start screen to configure cluster storage.



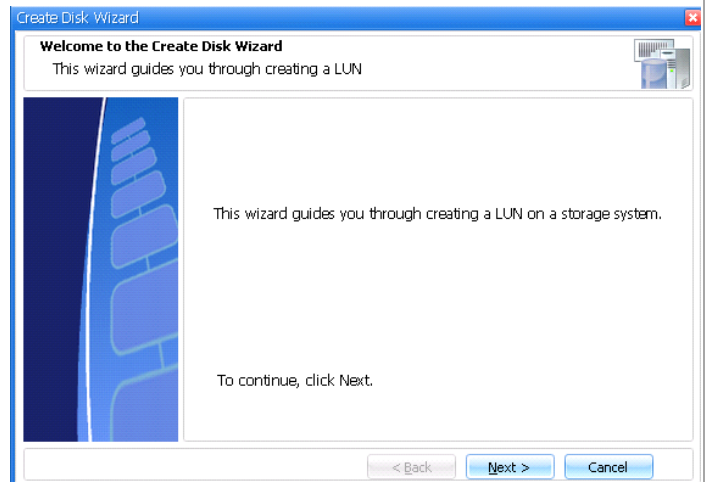
Expand server name object in the left tree view, and select the disk object.



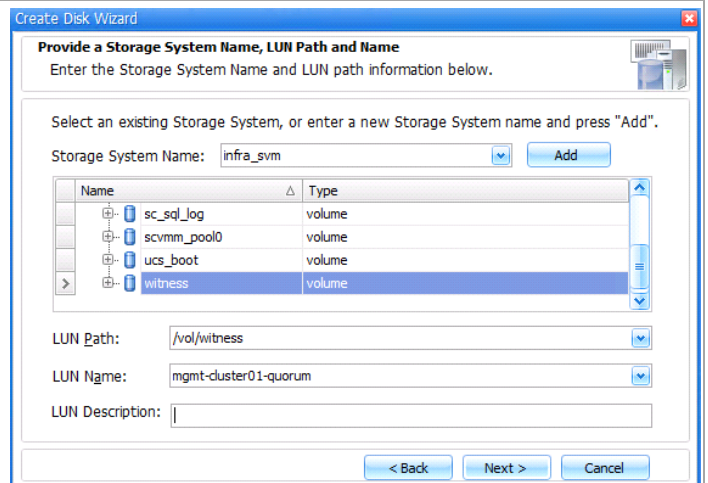
Right-click the Disks icon and choose to **Create Disk**.



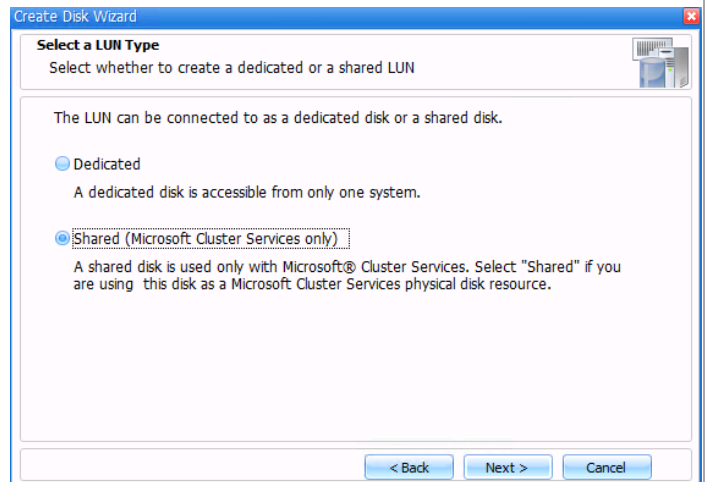
Click **Next** on the welcome screen.



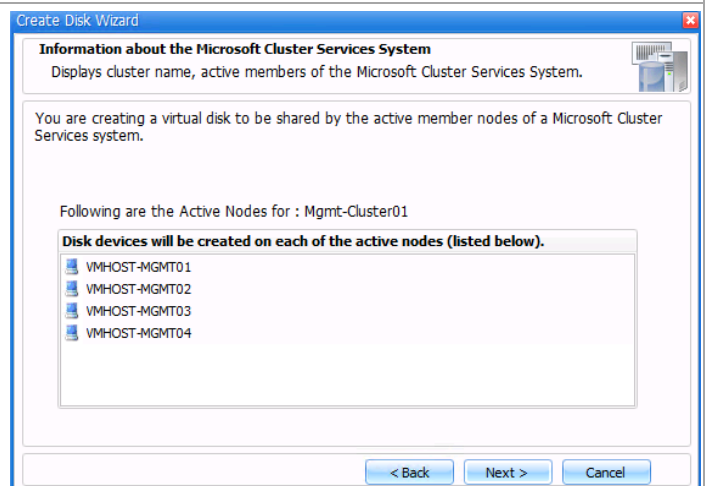
Enter in the IP Address or host name of the infrastructure Virtual Storage Machine in the Storage System Name field and click **Add**. Select the volume from the volume list. Enter the LUN name and click **Next**.



Select Shared (Microsoft Cluster Service) click **Next**.



Review the list of cluster nodes and click **Next**.



Select the following parameters:

**Driver Parameters**

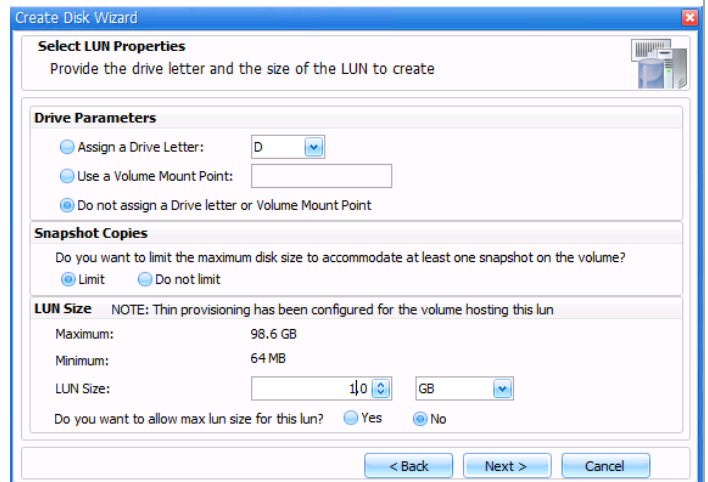
Do not assign a drive letter or Volume Mount Point

**Snapshot Copies**

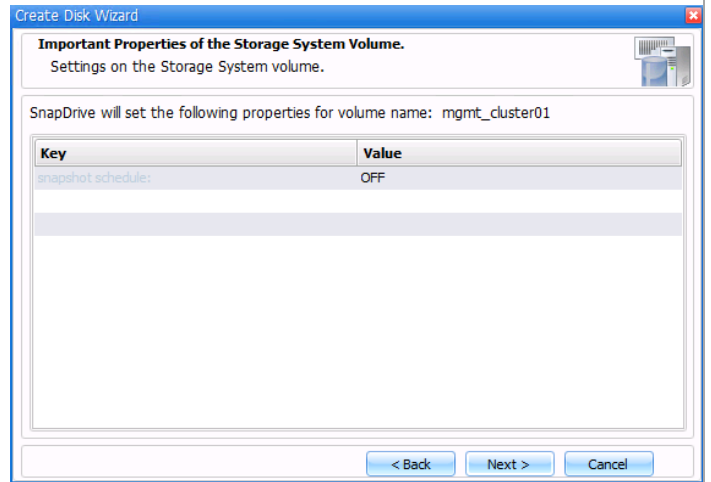
Limit

**LUN Size:**

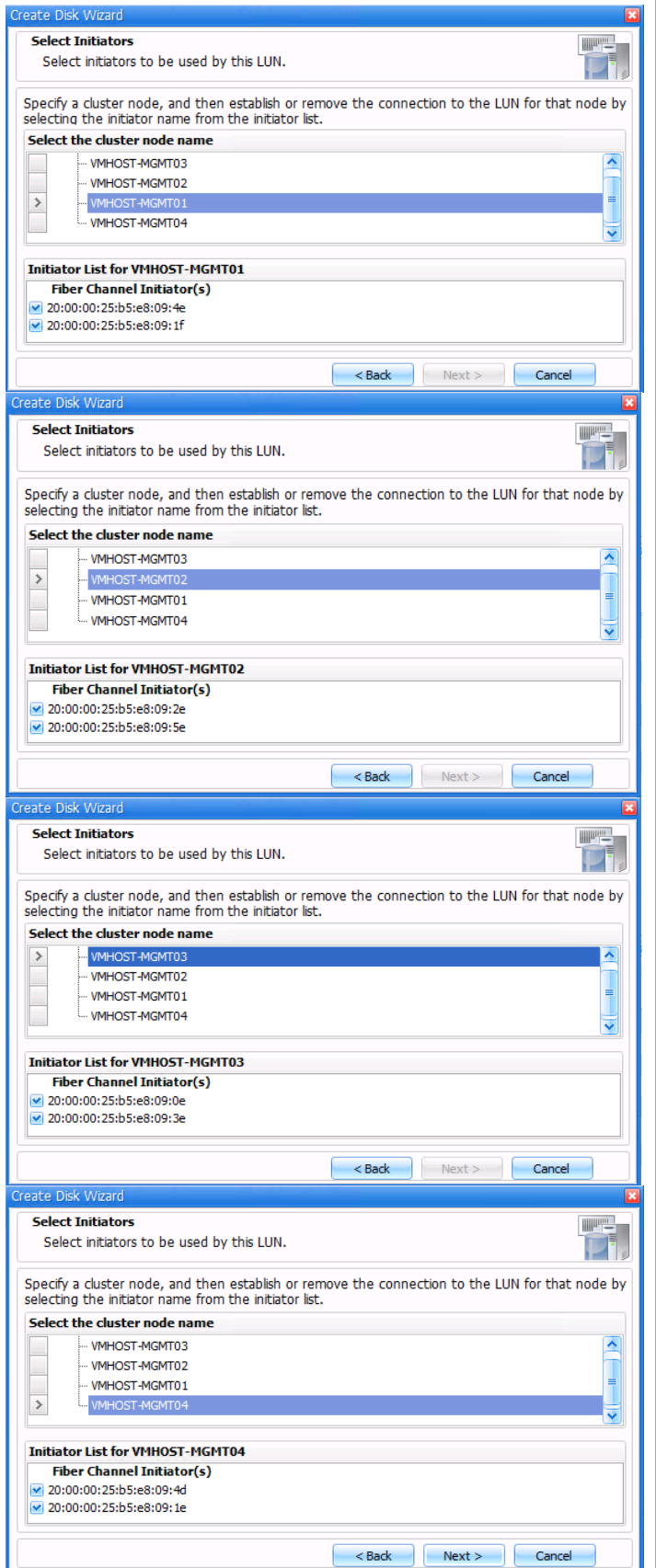
1GB



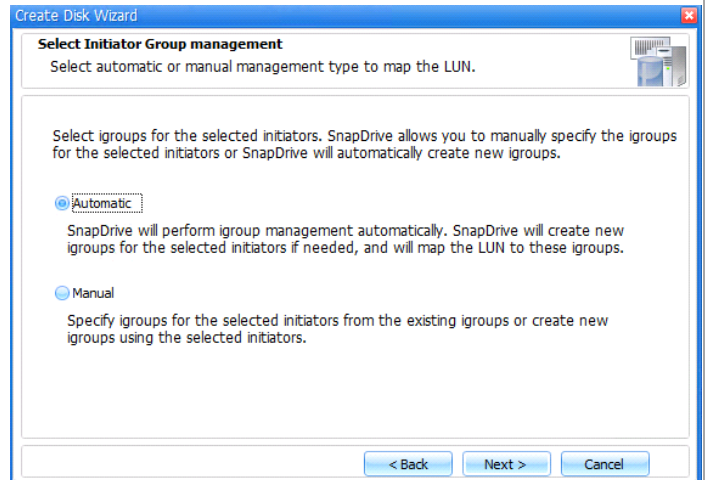
Review the automatic snapshot setting for the target volume and click **Next**.



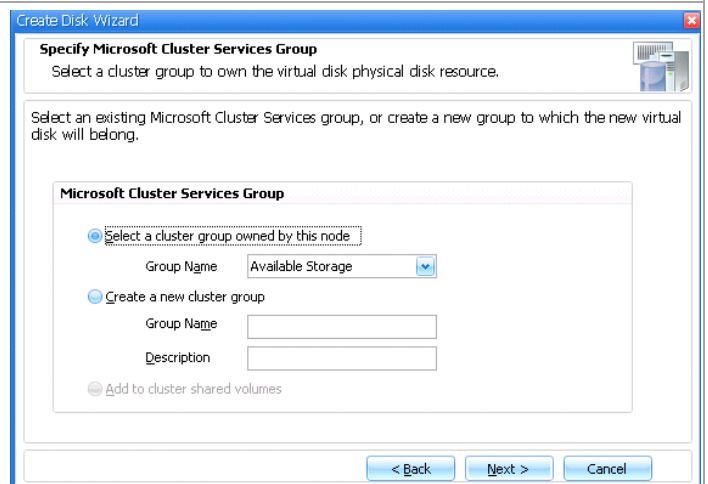
In the Select Initiators screen, select each cluster node and WWPNs for HBAs Fabric-A-1 and Fabric-B-1.



Select Automatic igroup management and click **Next**.

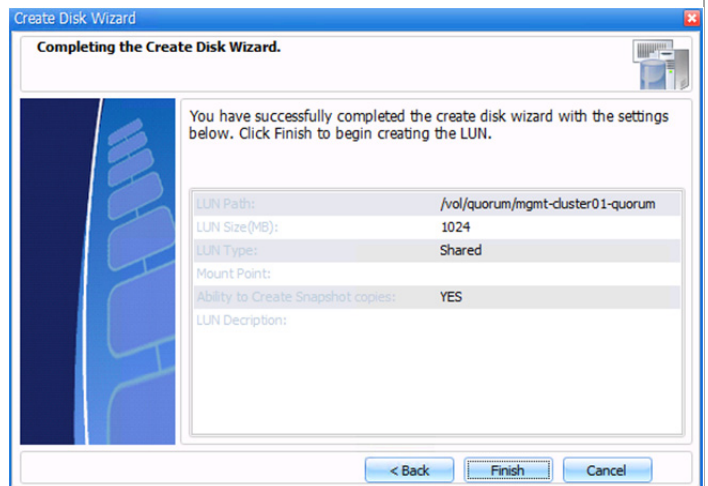


Select the cluster group owned by this node and select the **Available Storage** group.



Review the parameters and click **Finish**. Repeat this process to create a 300 GB volume to be used as a Cluster Shared Volume. This second volume will be used to store the database and log files for an instance of SQL Server Analysis Services. Repeat this process to create a 300 GB volume to be used as a Cluster Shared Volume. This third volume will be used to store the virtual hard disks for the SQL virtual machines.

**Note:** When a VM has a virtual hard disk for storage stored on CSV, such as the storage for SQL Server Analysis Services, SnapDrive for Hyper-V requires that the VM's system drive also be stored on CSV.

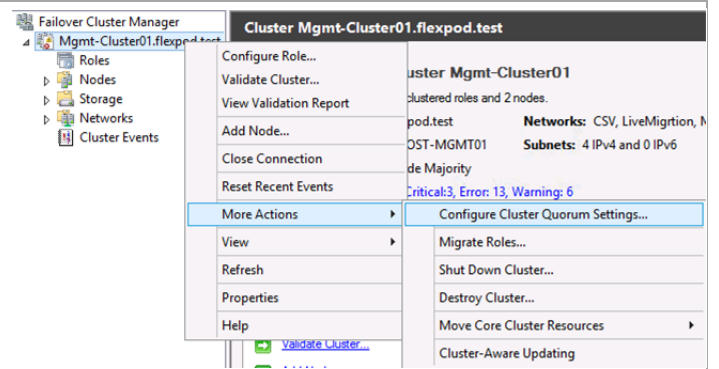


## Change the Management Cluster to Use a Quorum Disk

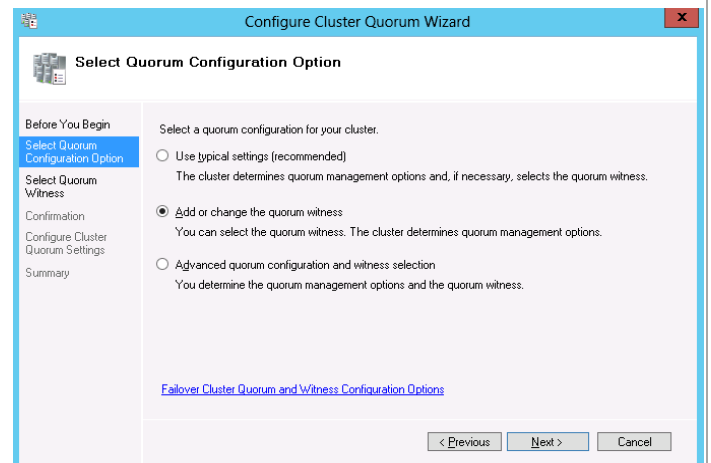
In failover cluster manager, select **More Actions** in the action pane and click **Configure Cluster Quorum Settings..**

The following cmdlet can be used to assign the quorum disk as an alternative to using Failover Cluster Manager.

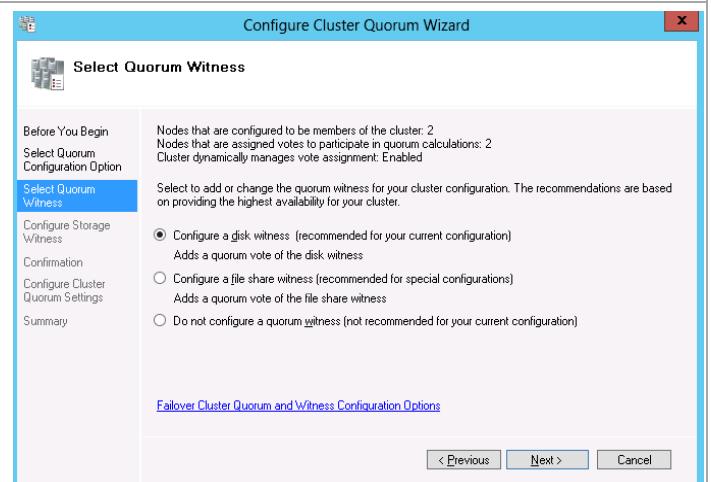
```
Set-ClusterQuorum -
NodeAndDiskMajority
<ClusterQuorumDisk>
```



Select **Add or Change the quorum witness**, and click **Next**.

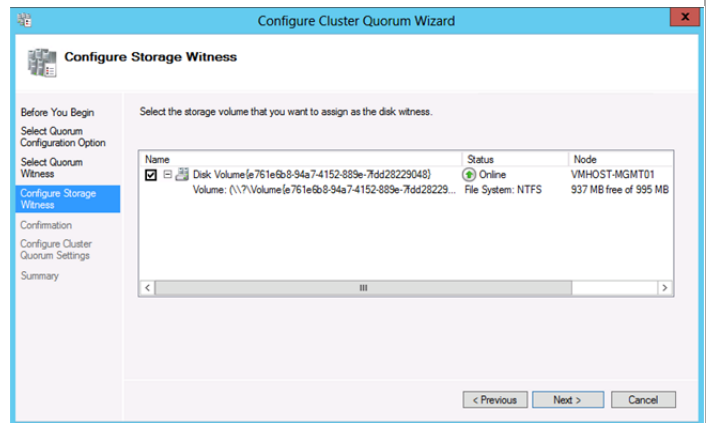


Select **Configure a disk witness** and click **Next**.

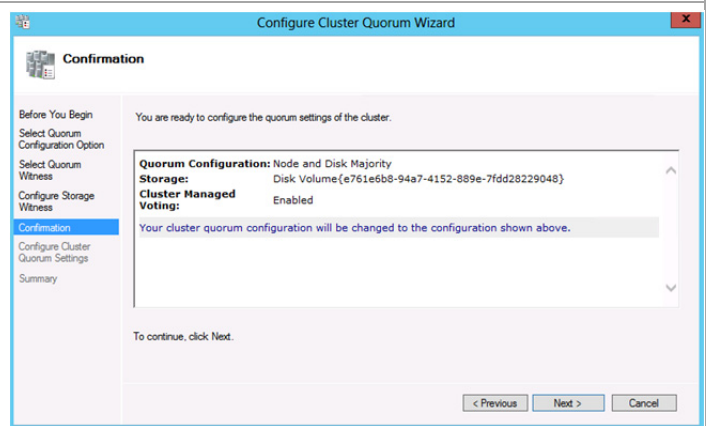




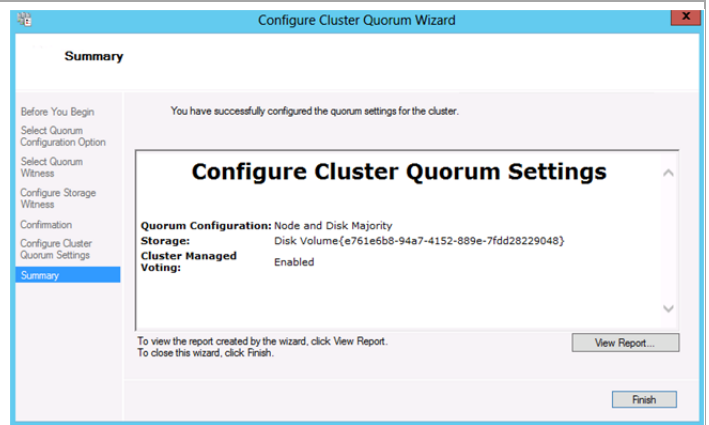
Select the LUN without a drive letter that was previously created to be the quorum LUN. Click **Next**.



Confirm the settings and click **Next**.



Review the results and click **Finish** to close the wizard screen.



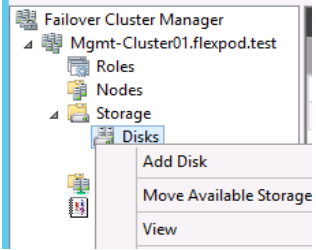
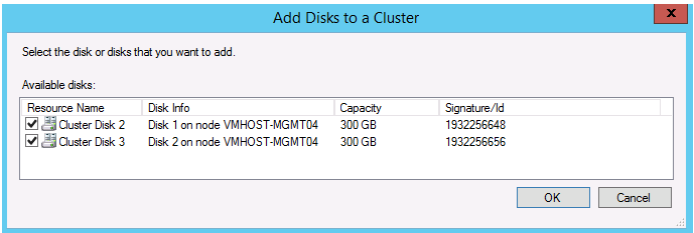
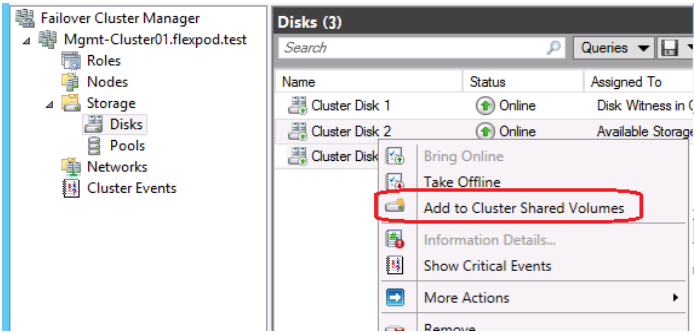
## Create Cluster Shared Volume LUNs with SnapDrive

Two Cluster Shared Volumes (CSV) are needed. Whereas all other SQL Server databases are stored on SMB shares, SQL Server Analysis Services does not support placing its databases onto a SMB share. A CSV is created for storing the SSAS database. NetApp SnapManager for Hyper-V requires that VMs using a CSV resident virtual hard disk, such the above SSAS requirement, be configured with all virtual hard disks on CSV. A CSV is created to store the system drives and configuration files for the four SQL Server VMs.

Repeat the SnapDrive LUN creation procedure above to create the CSV and SSAS LUNs with the following parameters:

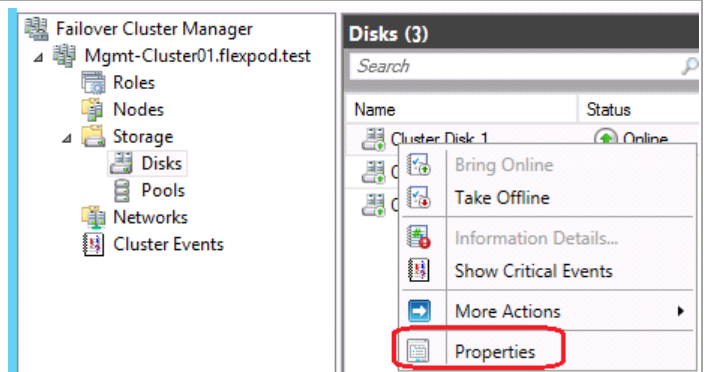
LUN Name	Purpose	Size	Mapped Cluster Nodes
CSV01	SQL Server Virtual Machines	300GB	All Mgmt Cluster Nodes
SSAS	SQL Server Analysis Server Databases	300GB	All Mgmt Cluster Nodes

### Create Cluster Shared Volume in Failover Cluster Manager

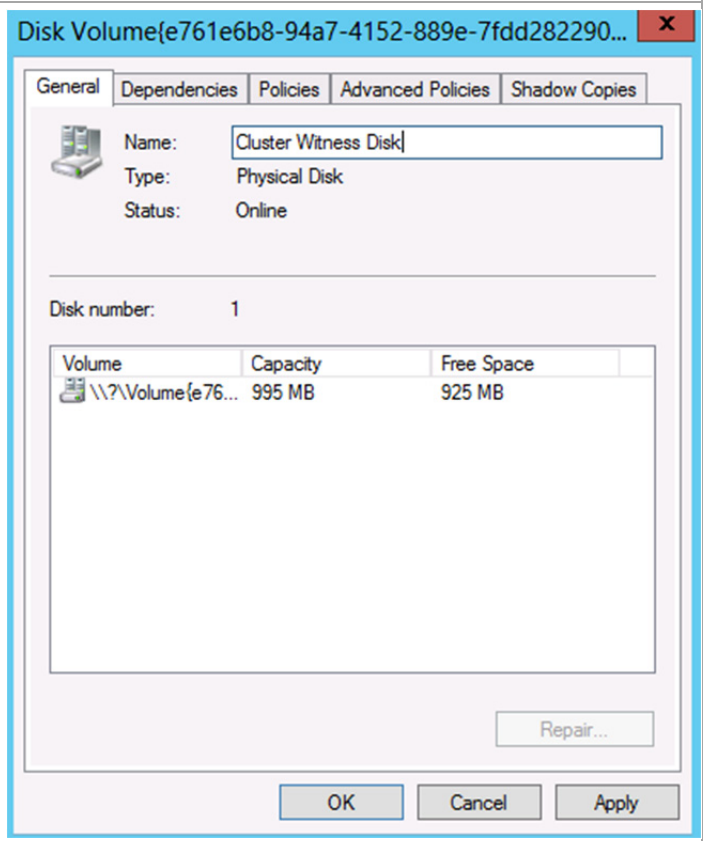
<p>In the Failover Cluster Management console right-click <b>Disks</b> and select <b>Add Disk</b>.</p>													
<p>In the <b>Add Disks to a Cluster</b> window, select the other volumes created earlier. Click <b>OK</b> to continue.</p>	 <table border="1" data-bbox="862 961 1511 1045"> <thead> <tr> <th>Resource Name</th> <th>Disk Info</th> <th>Capacity</th> <th>Signature/Id</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Cluster Disk 2</td> <td>Disk 1 on node VMHOST-MGMT04</td> <td>300 GB</td> <td>1932256648</td> </tr> <tr> <td><input checked="" type="checkbox"/> Cluster Disk 3</td> <td>Disk 2 on node VMHOST-MGMT04</td> <td>300 GB</td> <td>1932256656</td> </tr> </tbody> </table>	Resource Name	Disk Info	Capacity	Signature/Id	<input checked="" type="checkbox"/> Cluster Disk 2	Disk 1 on node VMHOST-MGMT04	300 GB	1932256648	<input checked="" type="checkbox"/> Cluster Disk 3	Disk 2 on node VMHOST-MGMT04	300 GB	1932256656
Resource Name	Disk Info	Capacity	Signature/Id										
<input checked="" type="checkbox"/> Cluster Disk 2	Disk 1 on node VMHOST-MGMT04	300 GB	1932256648										
<input checked="" type="checkbox"/> Cluster Disk 3	Disk 2 on node VMHOST-MGMT04	300 GB	1932256656										
<p>Right-click on each newly added disk and select <b>Add to Cluster Shared Volumes</b>.</p>													

## Assign Management Cluster Disk Names

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

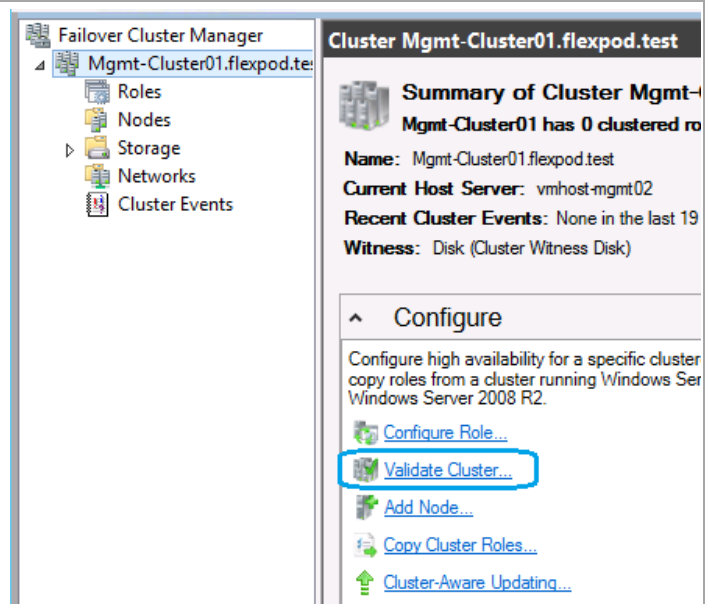


In the Name field, enter a name that reflects the LUN role.  
Repeat for the second and third disks.

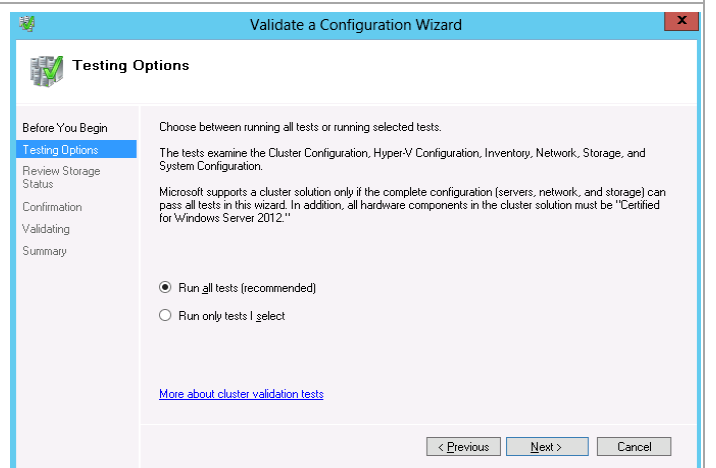


## 12.16 Validate the Management Cluster

Select the Mgmt-Cluster01 cluster in the left tree view and click **Validate Cluster**.

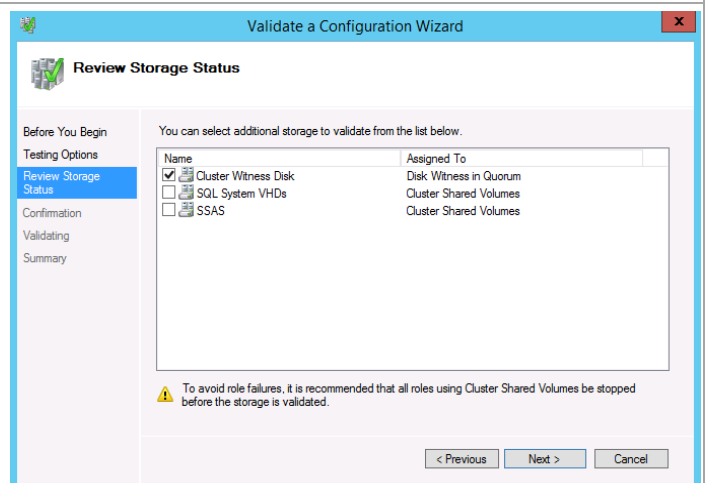


Select **Run all tests** and click **Next**.

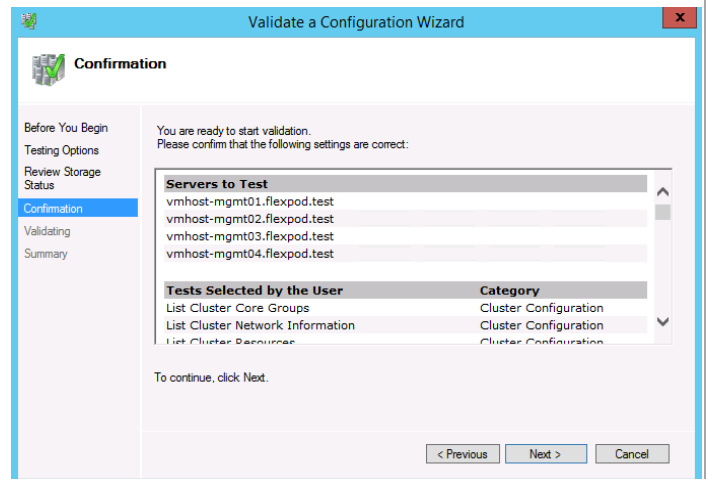


Select the Cluster Witness Disk on the cluster and click **Next**.

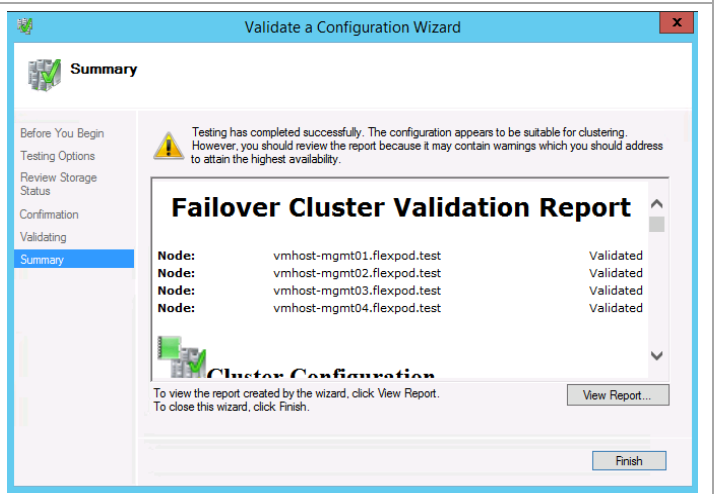
**Note:** Selecting all the disks causes the validation to run longer as each disk needs to be failed over to each node. Since all disks are coming from the same storage array, selecting a single disk proves the proper storage configuration.



Confirm the selected options and click **Next**.



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



**Note:** Because the CSV, LiveMigration, and SMB networks are non-routed networks, they will not be able to reach other networks defined on the cluster. Therefore you may receive a number of warning messages like the following for each node. These warnings are expected to be reported by the validation wizard and can safely be disregarded.

*Node vmhost-mgmt02.flexpod.test is reachable from node vmhost-mgmt01.flexpod.test by multiple communication paths, but one or more of these paths experienced more than 10% packet loss.*

## 13 Create Gold Master Template VM

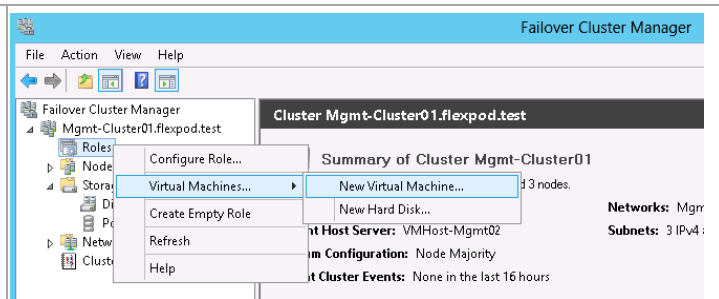
Instead of using Windows Deployment Services to automate the provisioning Hyper-V virtual machines, the deployment process of Virtual Machines takes advantage of the built-in cloning capabilities of the NetApp storage.

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 3.0 or higher installed on Hyper-V cluster nodes
- Access to Windows 2012 R2 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.**

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

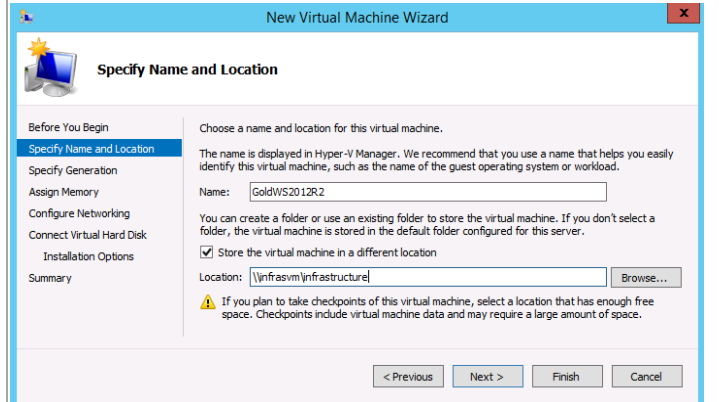


The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:

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

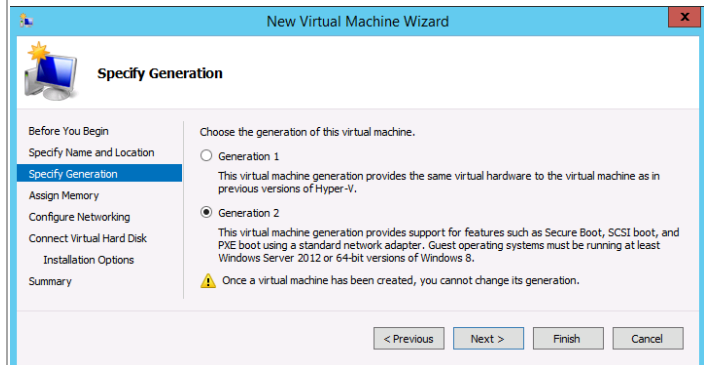
Select the **Store the virtual machine in a different location** check box. In the **Location** text box, specify the location of the VHD SMB share on your storage cluster vserver.

Click **Next** to continue.



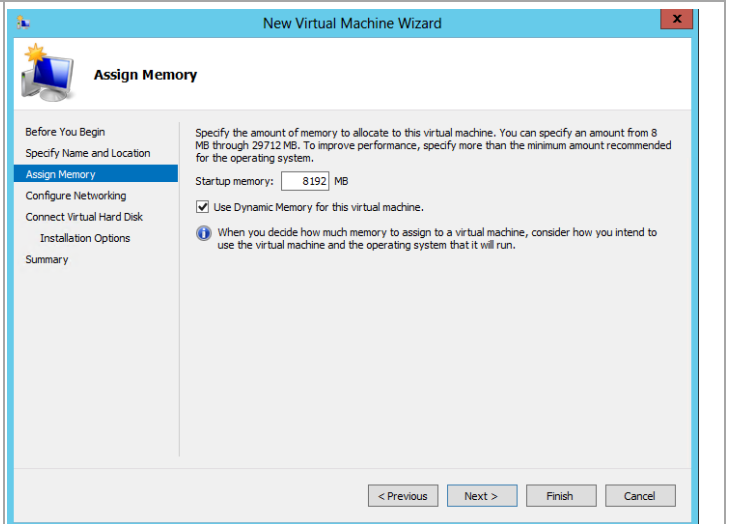
On the **Specify Generation** window select the radio button by **Generation 2**.

Click **Next** to continue.



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

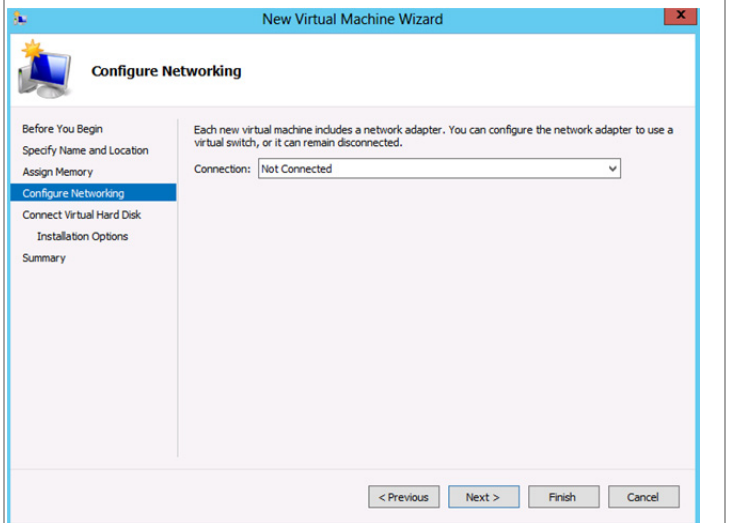
**Memory** – specify the amount of memory in megabytes (MB) required for each virtual machine. Identify this value in the configuration table above.



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

**Connection** – specify the Not Connected connection in the drop-down menu.

Click **Next** to continue.



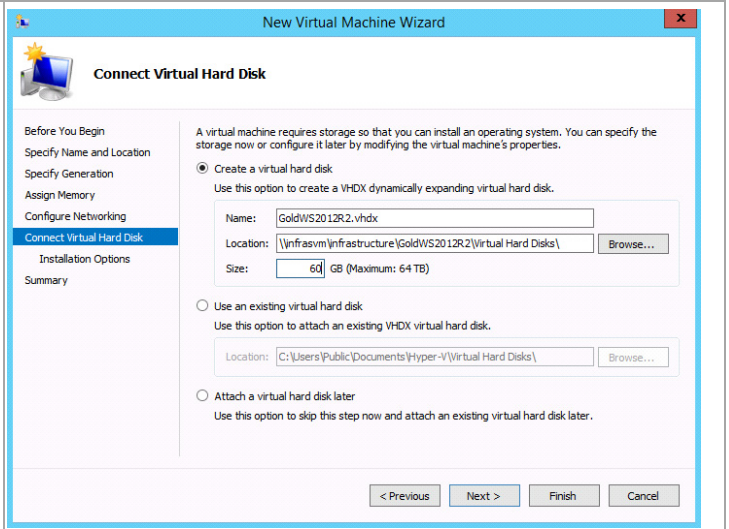
In the **Connect Virtual Hard Disk** dialog, select the **Create a virtual hard disk** option and provide the following values:

**Name** – specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.

**Location** – accept the default location of the VHD share on your storage cluster vservers combined with the virtual machine name.

**Size** – specify the size of the VHD (for operating system partitions this should be 60 GB).

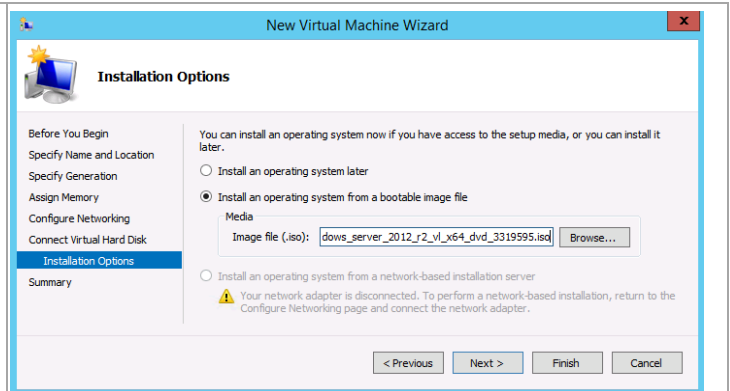
Click **Next** to continue.



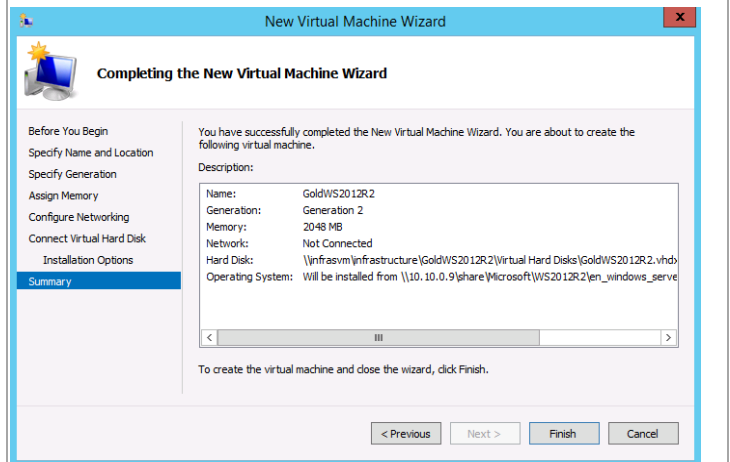
In the **Installation Options** dialog, select the **Install an operating system from a boot CD/DVD-ROM** option and

- **Image file (.iso)**: Specify the path to the Windows Server 2012 R2 iso.

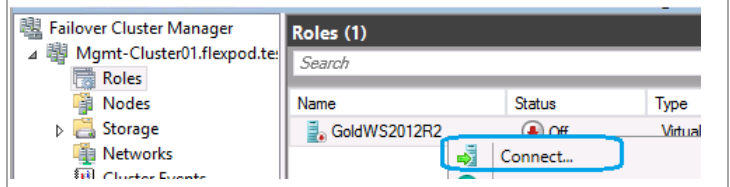
Click **Next** to continue.



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



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



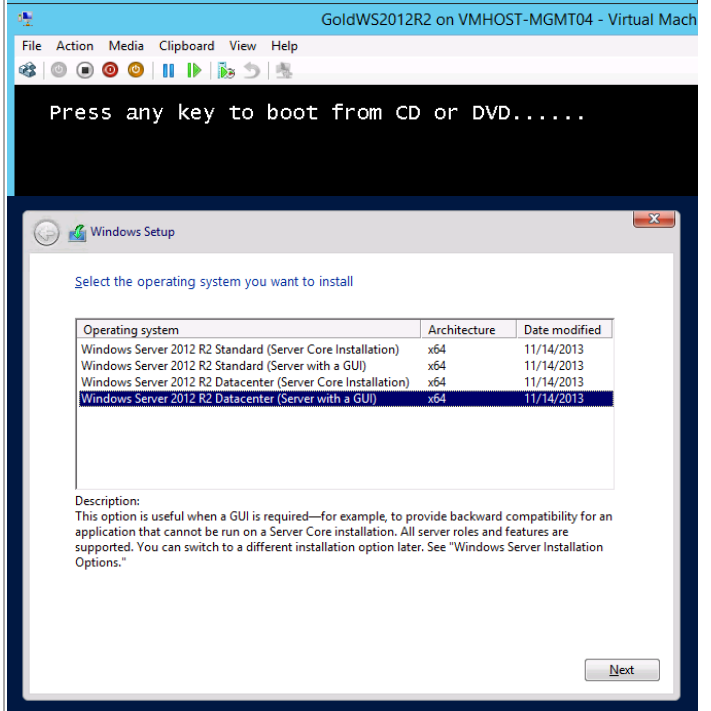
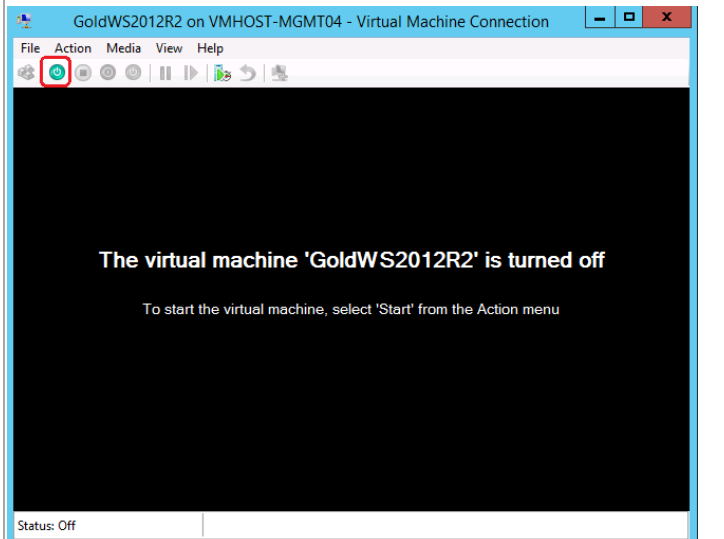


Click the **PowerON** Button to power on the VM and boot into the Windows Server 2012 Installer.

1. Be prepared for the **Press any key to boot from CD or DVD ...** message. If you fail to press a key, the boot will fail. Simply stop the VM and start it again.
2. After the installer is finished loading, Enter the relevant region information and click **Next**.
3. Click **Install now**.
4. Depending on the media used, you may have to enter the Product Key and click **Next**.
5. Select **Windows Server 2012 R2 Datacenter (Server with a GUI)** and click **Next**.

**Note:** You may optionally remove the GUI after the Hyper-V cluster is operational.

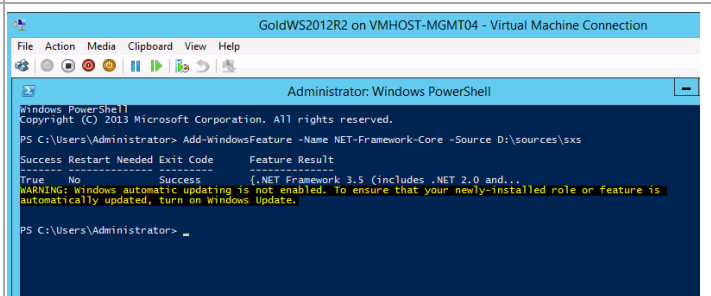
6. After reviewing the EULA, Check the I accept the license terms, and click **Next**.
7. Select Custom: Install Windows only (advanced).
8. Select the Drive 0 as the installation location for Windows. Press click **Next** to continue with the install.
9. When Windows is finished installing enter an Administrator password on the settings page and click Finish.



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

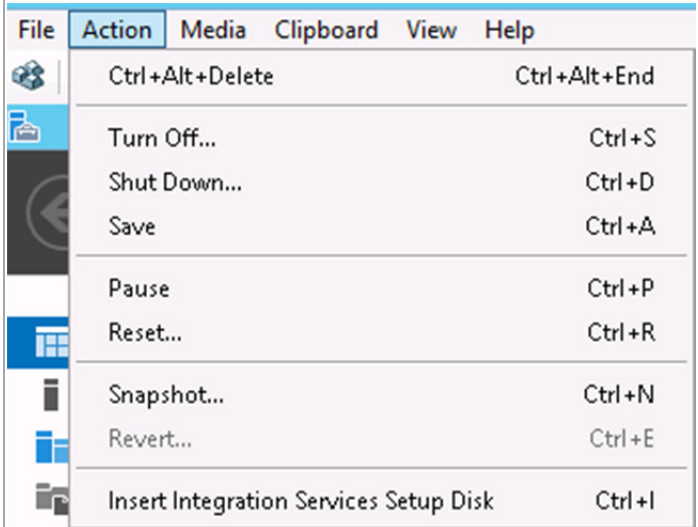
```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```

Eject the DVD drive after completing this operation.



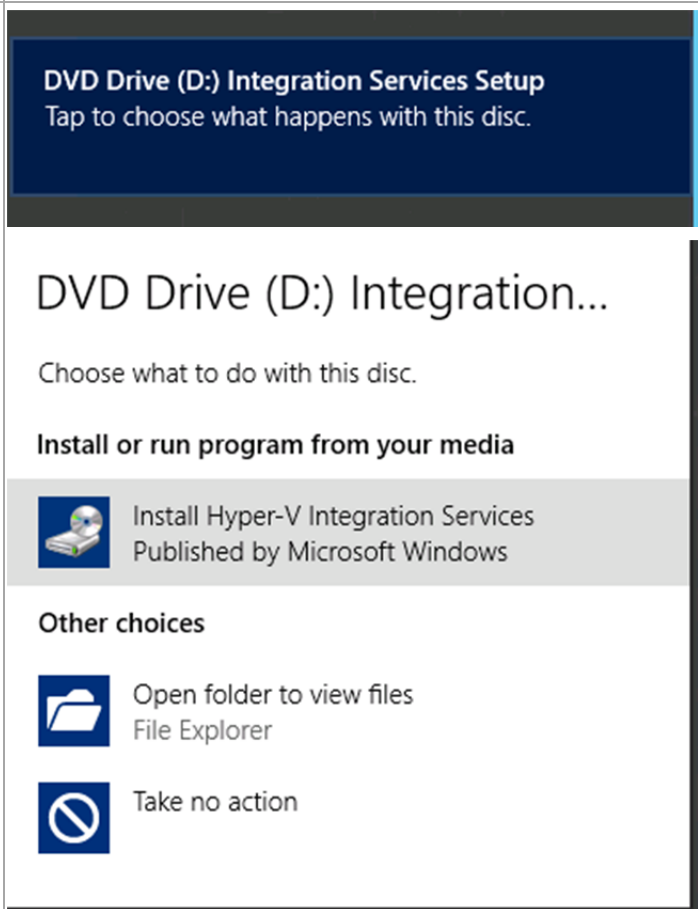
Install important and recommended Windows Updates and reboot. It might take several checks to updates to get all updates applied. Also set the Remote Desktop option to Enabled so the machine can be connected to remotely.

Login to Windows with the administrator account. Click Action and select Insert **Integration Services Setup Disk**.



After a few seconds, the option to run the Integration Services Setup appears on the desktop. Select this option.

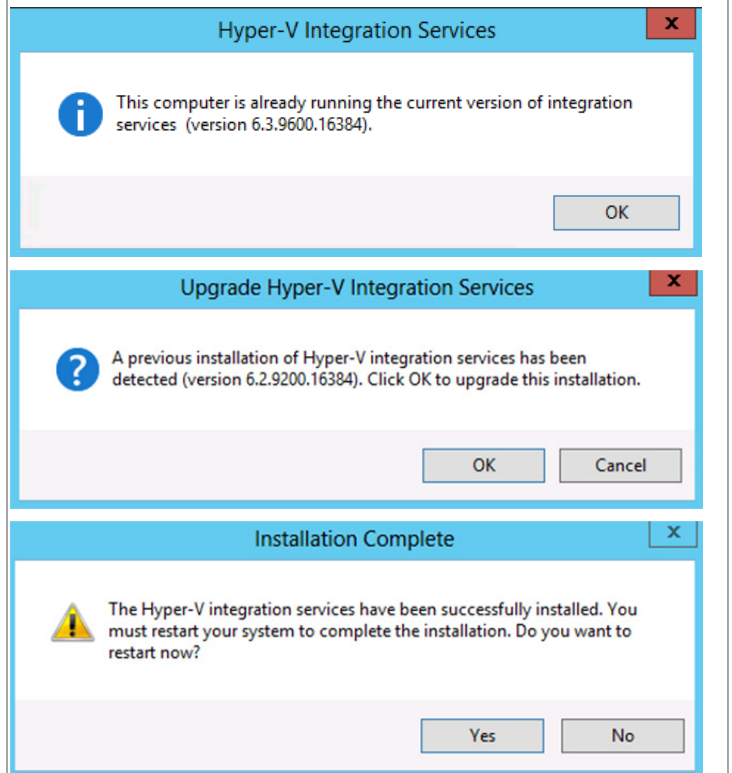
Select Install Hyper-V Integration Services Published by Microsoft Windows.



Most likely the latest version of the integration services will be installed and you will see the first message. But if the version is dated, you need to update them.

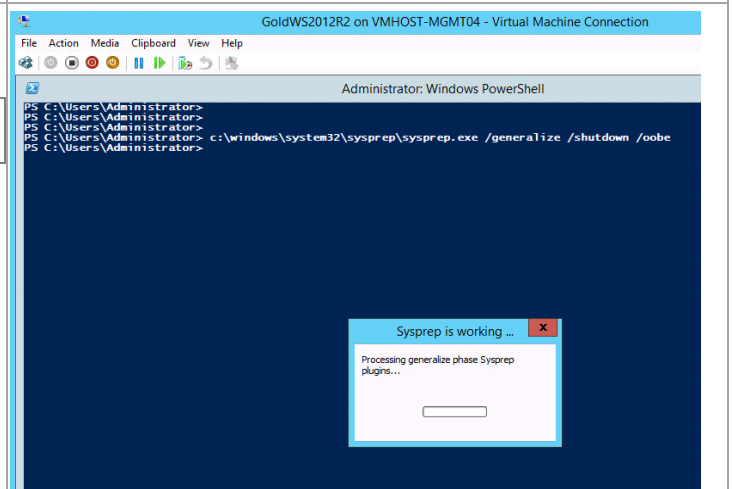
Click **OK** to update the Hyper-V integration services version.

Click **Yes** to restart your system and complete the installation.



After the system reboots, login into Windows and open the PowerShell prompt. Run the following command to sysprep the operating system.

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



**Note:** You will need to use a process similar to the process above to create a Windows Server 2008 R2 virtual machines to be used for the Service Manager Portal. Instead of running sysprep on it, it will simply be deployed to be configured for the portal function.

## 14 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 four-node Hyper-V failover cluster. These virtual machines serve as the basis for fabric management operations. The following table summarizes the fabric management virtual machine requirements by the System Center component that supports the product or operating system role.

Component Roles	VM Name	vCPU	RAM (GB)	VHD (GB)	vNICs	Preferred Hosts
SQL Server Cluster Node 1	SQL01	16	32	60	SC-Database SMB-SQL	Node1 Node2
SQL Server Cluster Node 2	SQL02	16	32	60	SC-Database SMB-SQL	Node2 Node3
SQL Server Cluster Node 3	SQL03	16	32	60	SC-Database SMB-SQL	Node3 Node4
SQL Server Cluster Node 4	SQL04	16	32	60	SC-Database SMB-SQL	Node4 Node1
Virtual Machine Manager	SCVMM01	4	8	60	MF-Public SC-Database	Node1 Node2
Virtual Machine Manager	SCVMM02	4	8	60	MF-Public SC-Database	Node3 Node4
App Controller	SCAC01	4	8	60	MF-Public SC-Database	Node1 Node3
Operations Manager Management Server	SCOM01	8	16	60	MF-Public SC-Database	Node1 Node2
Operations Manager Management Server	SCOM02	8	16	60	MF-Public SC-Database	Node3 Node4
Operations Manager Reporting Server	SCOM03	8	16	60	MF-Public SC-Database	Node2 Node4
Orchestrator Runbook/Deployment Server	SCO01	4	8	60	MF-Public SC-Database	Node1 Node2
Orchestrator supplemental Runbook Server	SCO02	4	8	60	MF-Public SC-Database	Node3 Node4
Service Provider Foundation Server	SCSPF01	2	4	60	MF-Public SC-Database	Node3 Node1
Service Provider Foundation Server	SCSPF02	2	4	60	MF-Public SC-Database	Node4 Node2
Service Management Automation Server	SCSMA01	2	4	60	MF-Public SC-Database	Node3 Node1
Service Management Automation Server	SCSMA02	2	4	60	MF-Public SC-Database	Node4 Node2
Service Manager Management Server	SCSM01	4	16	60	MF-Public SC-Database	Node1 Node2
Service Manager Data Warehouse	SCSM02	8	16	60	MF-Public SC-Database	Node3 Node4
Service Manager Portal	SCSM03	8	16	60	MF-Public SC-Database	Node2 Node4
Server Reporting Server	SCRS01	4	16	60	MF-Public SC-Database	Node4 Node1
WAP management portal for Tenants	WAP01	2	4	60	MF-Public SC-Database	Node1 Node3
WAP management portal for Tenants	WAP01b	2	4	60	MF-Public SC-Database	Node2 Node4
WAP Tenant Authentication	WAP02	2	4	60	MF-Public SC-Database	Node1 Node3
WAP Tenant Authentication	WAP02b	2	4	60	MF-Public SC-Database	Node2 Node4
WAP Tenant public API	WAP03	2	4	60	MF-Public SC-Database	Node1 Node3

<b>WAP Tenant public API</b>	WAP03b	2	4	60	MF-Public SC-Database	Node2 Node4
<b>WAP Tenant API</b>	WAP04	2	4	60	MF-Public SC-Database	Node1 Node3
<b>WAP Tenant API</b>	WAP04b	2	4	60	MF-Public SC-Database	Node2 Node4
<b>WAP Admin API</b>	WAP05	2	4	60	MF-Public SC-Database	Node1 Node3
<b>WAP Admin API</b>	WAP05b	2	4	60	MF-Public SC-Database	Node2 Node4
<b>WAP management portal for Admins</b>	WAP06	2	4	60	MF-Public SC-Database	Node3 Node1
<b>WAP Admin Authentication</b>	WAP07	2	4	60	MF-Public SC-Database	Node4 Node2
<b>Infrastructure (SMI-S Agent)</b>	SCInfra01	2	4	60	MF-Public	Node2 Node4
<b>Hyper-V Network Virtualization Gateway</b>	HNVGW01	2	8	60	MF-Public	Node3 Node4
<b>Hyper-V Network Virtualization Gateway</b>	HNVGW02	2	8	60	MF-Public	Node4 Node1
<b>Cisco Nexus 1000V VSM 1</b>	N1KV-VSM01	1	4	4	Mgmt	Node2 Node3
<b>Cisco Nexus 1000V VSM 2</b>	N1KV-VSM02	1	4	4	Mgmt	Node4 Node1
<b>Totals</b>		<b>172</b>	<b>372 GB</b>	<b>2108 GB</b>		

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

## 14.1 Automated Creation and Configuration

The following PowerShell script will create the VM's for the Fabric Management cluster using the assumptions of this Deployment Guide. Copy this script into Notepad or the PowerShell ISE and edit to reflect the customer environment. When edited, run from an elevated PowerShell prompt with an account that is administrator on the storage controller. It copies the VHDX file from the previously created sysprepped Gold Master template VM.

**Note:** The automated process does not build the Windows Server 2008 R2 based VM used for the Service Management Portal server. That must be built by hand.

**Note:** The automated process builds the SQL Server VMs onto CSV. Make sure the proper CSV location is defined in this script.

```
<#
Build the VM definitions for the Private Cloud VMs

W A R N I N G
W A R N I N G
W A R N I N G

This script MUST be run from an elevated PowerShell environment.

The variables in this script should be modified to reflect the customer environment.

The VMs are built onto the cluster, so even though all are built
on one host, they will be available to other nodes after the Failover Cluster
refreshes.
Input values for each VM include:
- Name / name of VM; also used to construction the VM's directory tree
- Memory / amount of memory to allocate to VM
- vCPUs / number of virtual CPUs to allocate to VM
- vNIC1 / first virtual NIC to assign to VM
- vLANtag1 / VLAN to associate with vNIC1
- vNIC2 / second virtual NIC to assign to VM
- vLANtag2 / VLAN to associate with vNIC2
- VMhostName1 / initial host to which the VM is deployed. First of two preferred
owners.
- VMhostName2 / Second preferred owner

There are some special values associated with vNIC and vLANtag entries.
$vNICnull -- Do not assign a vNIC
$vLANnull -- do not assign a VLAN tag to the vNIC
$vNoSwitch -- used in place of the vLANtag entry to mean to create the vNIC but do not
assign to a virtual switch

#>

# Variables to be edited for the customer environment

# Virtual Switch Names and VLAN IDs

$vNIC1 = "MF-Public"
$vNIC2 = "SC-Database"
$vNIC3 = "SMB-SQL"
$vNICnull = $null
$vLAN1 = "1001"
$vLAN2 = "1002"
$vLAN3 = "1003"
$vLANnull = $null
$vNoSwitch = "NoSwitch" # Create vNIC but do not assign to vSwitch
```

```

$smb = \\infrasm\infrastructure
$csvg = "C:\ClusterStorage\Volume2\"
$templateSource = "\\infrasm\infrastructure\GoldWS2012R2\Virtual Hard
Disks\GoldWS2012R2.vhdx"
$VHD = "\Virtual Hard Disks\"

$vmHost1 = "VMHost-Mgmt01"
$vmHost2 = "VMHost-Mgmt02"
$vmHost3 = "VMHost-Mgmt03"
$vmHost4 = "VMHost-Mgmt04"
$vmCluster = "Mgmt-Cluster01"

# Since good practice would have the sysprepped disk read-only,
# this variable is used to reset the file after copying.

New-Variable -Name read_only -Value 1 -Option readonly

# Virtual Machine information
# Name, Memory, vCPUs, vNIC1, vLANtag1, vNIC2, vLANtag2, VMhostName1, VMhostName2)

$VMArray = @()
# Guest Clustering
$VMArray +=, ("SQL01", 32768MB, 16, $vNIC2, $vLAN2, $vNIC3, $vLAN3, $vmHost1, $vmHost2,
$csvg)
$VMArray +=, ("SQL02", 32768MB, 16, $vNIC2, $vLAN2, $vNIC3, $vLAN3, $vmHost2, $vmHost3,
$csvg)
$VMArray +=, ("SQL03", 32768MB, 16, $vNIC2, $vLAN2, $vNIC3, $vLAN3, $vmHost3, $vmHost4,
$csvg)
$VMArray +=, ("SQL04", 32768MB, 16, $vNIC2, $vLAN2, $vNIC3, $vLAN3, $vmHost4, $vmHost1,
$csvg)
$VMArray +=, ("SCVMM01", 8192MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1,
$vmHost2, $smb)
$VMArray +=, ("SCVMM02", 8192MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3,
$vmHost4, $smb)
$VMArray +=, ("HNVGW01", 8096MB, 2, $vNIC1, $vNoSwitch, $vNICnull, $vLANnull, $vmHost2,
$vmHost3, $smb)
$VMArray +=, ("HNVGW02", 8096MB, 2, $vNIC1, $vNoSwitch, $vNICnull, $vLANnull, $vmHost4,
$vmHost1, $smb)
# Native Application HA
$VMArray +=, ("SCOM01", 16384MB, 8, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1,
$vmHost2, $smb)
$VMArray +=, ("SCOM02", 16384MB, 8, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3,
$vmHost4, $smb)
$VMArray +=, ("SCO01", 8192MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost2,
$smb)
$VMArray +=, ("SCO02", 8192MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3, $vmHost4,
$smb)
#Load Balanced
$VMArray +=, ("WAP01", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost3,
$smb)
$VMArray +=, ("WAP01b", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)
$VMArray +=, ("WAP02", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost3,
$smb)
$VMArray +=, ("WAP02b", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)
$VMArray +=, ("WAP03", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost3,
$smb)
$VMArray +=, ("WAP03b", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)
$VMArray +=, ("WAP04", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost3,
$smb)
$VMArray +=, ("WAP04b", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)
$VMArray +=, ("WAP05", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1, $vmHost3,
$smb)
$VMArray +=, ("WAP05b", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)

```

```

$VMArray +=, ("SCSPF01", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3,
$vmHost1, $smb)
$VMArray +=, ("SCSPF02", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost4,
$vmHost2, $smb)
$VMArray +=, ("SCSMA01", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3,
$vmHost1, $smb)
$VMArray +=, ("SCSMA02", 4096MB, 2, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost4,
$vmHost2, $smb)
# Host Clustering
$VMArray +=, ("SCAC01", 8192MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1,
$vmHost3, $smb)
$VMArray +=, ("SCOM03", 16384MB, 8, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost2,
$vmHost4, $smb)
$VMArray +=, ("SCRS01", 16384MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost4,
$vmHost1, $smb)
$VMArray +=, ("SCSM01", 16384MB, 4, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost1,
$vmHost2, $smb)
$VMArray +=, ("SCSM02", 16384MB, 8, $vNIC1, $vNoSwitch, $vNIC2, $vLAN2, $vmHost3,
$vmHost4, $smb)
$VMArray +=, ("WAP06", 4096MB, 2, $vNIC1, $vNoSwitch, $vNICnull, $vLANnull, $vmHost3,
$vmHost1, $smb)
$VMArray +=, ("WAP07", 4096MB, 2, $vNIC1, $vNoSwitch, $vNICnull, $vLANnull, $vmHost4,
$vmHost2, $smb)
$VMArray +=, ("SCInfra01", 4096MB, 2, $vNIC1, $vNoSwitch, $vNICnull, $vLANnull, $vmHost1,
$vmHost3, $smb)

#Import required modules

if ((Get-Module | Where {$_.Name -like "FailoverClusters"}).Name -ine
"FailoverClusters")
{
    Write-Host "Loading Module: FailoverClusters"
    Import-Module FailoverClusters
}

if ((Get-Module | Where {$_.Name -like "ServerManager"}).Name -ine "ServerManager")
{
    Write-Host "Loading Module: ServerManager"
    Import-Module ServerManager
}

if ((Get-Module | Where {$_.Name -like "Hyper-V"}).Name -ine "Hyper-V")
{
    Write-Host "Loading Module: Hyper-V"
    Import-Module Hyper-V
}

#####
# Process all VMs in array
#####

For ($i = 0; $i -lt $VMArray.length; $i++)
{
    $element = $VMArray[$i]
    $vmName = $element[0]
    $vmMem = $element[1]
    $vmCpu = $element[2]
    $vmVnic1 = $element[3]
    $vmVlan1 = $element[4]
    $vmVnic2 = $element[5]
    $vmVlan2 = $element[6]
    $vmHostOwner1 = $element[7]
    $vmHostOwner2 = $element[8]
    $vmPath = $element[9]

    $vmHost1VMs = Get-VM -Computer $vmHost1
    $vmHost2VMs = Get-VM -Computer $vmHost2
    $vmHost3VMs = Get-VM -Computer $vmHost3
    $vmHost4VMs = Get-VM -Computer $vmHost4

```



```

#####
# Check for existing VM already running on a host
#####

Foreach ($vm in $vmHost1VMs)
{
    If ($vm.Name -eq $vmName)
    {
        Write-Host "Duplicate VM Name - $vmName. Skipping creation"
        Break
    }
}
Foreach ($vm in $vmHost2VMs)
{
    If ($vm.Name -eq $vmName)
    {
        Write-Host "Duplicate VM Name - $vmName. Skipping creation"
        Break
    }
}
Foreach ($vm in $vmHost3VMs)
{
    If ($vm.Name -eq $vmName)
    {
        Write-Host "Duplicate VM Name - $vmName. Skipping creation"
        Break
    }
}
Foreach ($vm in $vmHost4VMs)
{
    If ($vm.Name -eq $vmName)
    {
        Write-Host "Duplicate VM Name - $vmName. Skipping creation"
        Break
    }
}

Write-Host "`n*****`n* Creating:" $vmName "at" (Get-Date) "`n*****"

$vhDir = $vmPath + $vmName + $VHD
$dest = $vhDir + $vmName + ".vhdx"

$vmInfo = New-VM -Name $vmName -Path $vmPath -MemoryStartupBytes $vmMem -NoVhd -
Generation 2 -ComputerName $vmHostOwner1
$trash = New-Item -Path $vhDir -ItemType Directory
copy $templateSource $dest
Get-ChildItem -Path $dest | Where-Object { $_.attributes -match 'readonly' } |
    ForEach-Object { $_.attributes = $_.attributes -Bxor $read_only }
$vmInfo | Add-VMHardDiskDrive -ControllerType SCSI -ControllerNumber 0 -Path $dest
$vmInfo | Remove-VMNetworkAdapter -Name "Network Adapter"
$vmInfo | Set-VM -ProcessorCount $vmCpu -AutomaticStopAction Shutdown
$vmInfo | Set-VMProcessor -CompatibilityForMigrationEnabled $true
$vmInfo | Add-ClusterVirtualMachineRole -Cluster $vmCluster
$vmInfo | Enable-VMIntegrationService -Name 'Guest Service Interface'
Get-ClusterGroup $vmName | Set-ClusterOwnerNode -Owners $vmHostOwner1,$vmHostOwner2
(Get-ClusterGroup $vmName).AutoFailbackType = 1
If ($vmVlan1 -eq "NoSwitch")
{
    $vmInfo | Add-VMNetworkAdapter -Name $vmVnic1
}
Else
{
    $vmInfo | Add-VMNetworkAdapter -Name $vmVnic1 -SwitchName $vmVnic1
    If ($vmVlan1 -ne $null)
    {
        $vmInfo | Set-VMNetworkAdapterVlan -Access -VlanId $vmVlan1 -
VMNetworkAdapterName $vmVnic1
    }
}
}

```

```

If ($vmVlan2 -eq "NoSwitch")
{
    $vmInfo | Add-VMNetworkAdapter -Name $vmVnic2
}
Else
{
    If ($vmVnic2 -ne $null)
    {
        $vmInfo | Add-VMNetworkAdapter -Name $vmVnic2 -SwitchName $vmVnic2
        If ($vmVlan2 -ne $null)
        {
            $vmInfo | Set-VMNetworkAdapterVlan -Access -VlanId $vmVlan2 -
VMNetworkAdapterName $vmVnic2
        }
    }
}
}

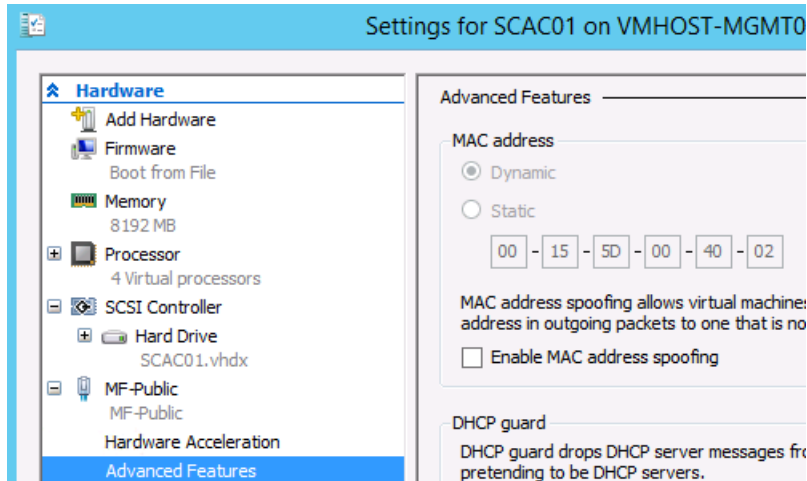
Write-Host "Completed at:" (Get-Date)

```

## Complete Sysprep Build

Using the automated process from a sysprepped gold master image creates images that require a few steps to complete the build of the VM. Basically this amounts to the following steps:

- Start each VM to complete the mini-setup process
- Rename the NICs from their default names
  - In the settings of the VM, expand each NIC and obtain the MAC address from the Advanced Features



- From a PowerShell window issue the Get-NetAdapter cmdlet

```

PS C:\Users\Administrator> Get-NetAdapter

```

Name	InterfaceDescription	ifIndex	Status	MacAddress
Ethernet 2	Microsoft Hyper-V Network Adapter #2	13	Up	00-15-5D-00-40-03
Ethernet	Microsoft Hyper-V Network Adapter	12	Up	00-15-5D-00-40-02

- Match MAC addresses to assign proper name and use the Rename-NetAdapter PowerShell cmdlet to rename the NIC appropriately

```

PS C:\Users\Administrator> Rename-NetAdapter -Name "Ethernet" -NewName "MF-Public"

```

- Assign the proper IP addresses
  - Assign DNS Servers
  - Register to DNS only on primary interface

- Set NIC binding order so primary interface is first
- Rename the VM
- Join the Active Directory domain.

Now they can be configured for their expressed purposes.

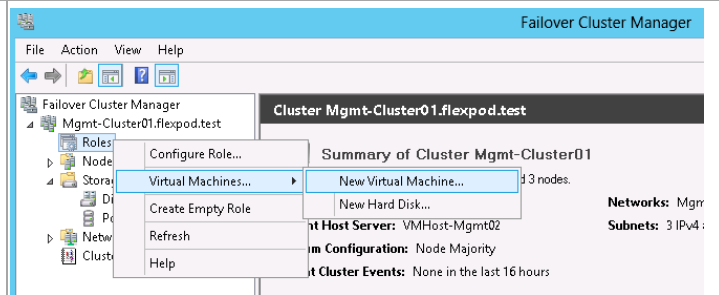
## 14.2 Manual Creation and Configuration

### Create Fabric Management Virtual Guests

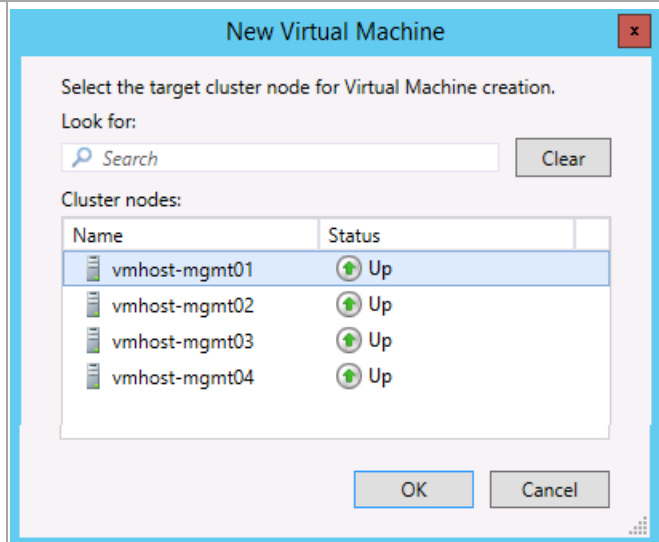
Windows Failover Cluster Manager is used to create the fabric management virtual machines. The installation of the required Windows operating systems can utilize existing customer automated deployment Solutions or a manual build of each virtual machine.

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

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.



Select the appropriate host on which the VM is to be build. Click **OK** to continue.  
On the **Before You Begin** window, click **Next** to continue.

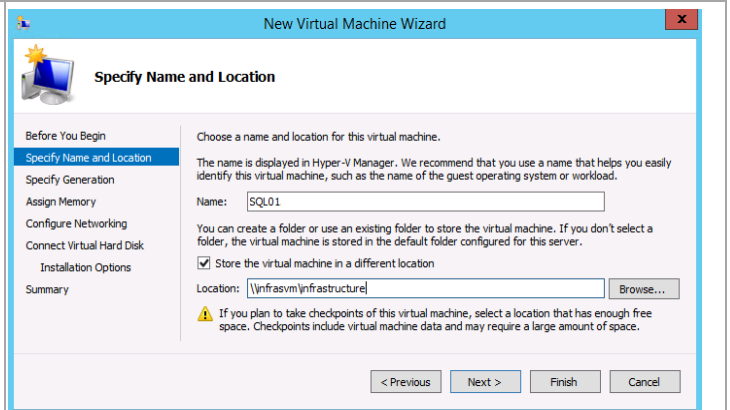


The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:

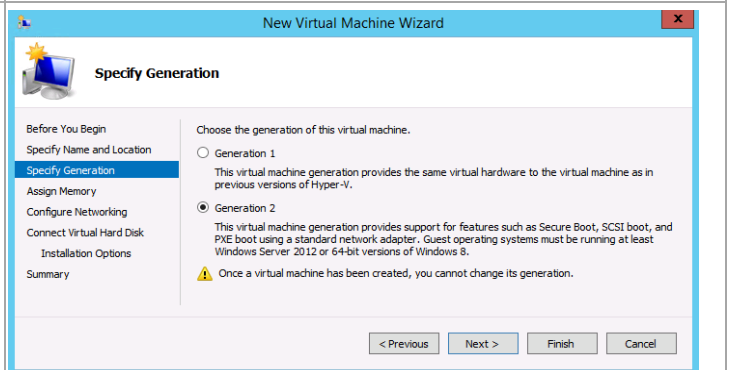
**Name** – specify the name of the virtual machine based on the naming conventions of your organization.

Select the **Store the virtual machine in a different location** check box. In the **Location** text box, specify the location of the VHD share of the storage array vServer.

Click **Next** to continue.



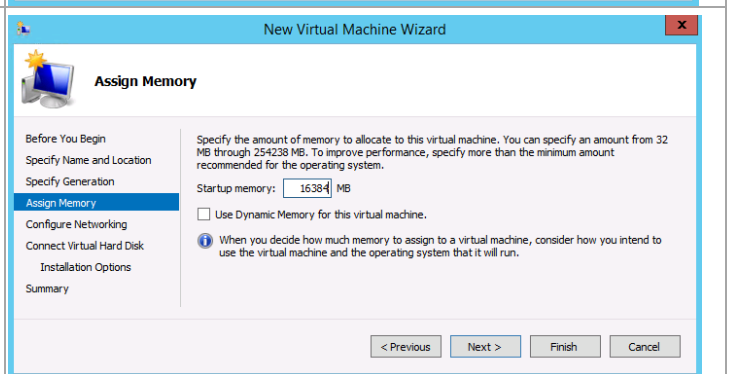
On the **Specify Generation** window, select the radio button by **Generation 2** and click **Next** to continue.



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

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

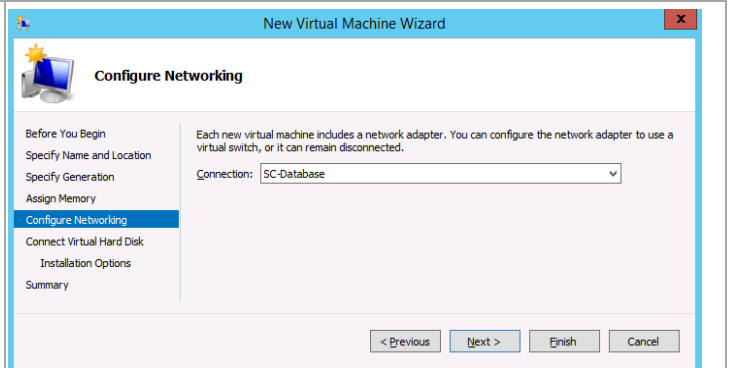
Click **Next** to continue.



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

**Connection** – specify the SC-Database Virtual Switch network connection in the drop-down menu.

Click **Next** to continue.



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

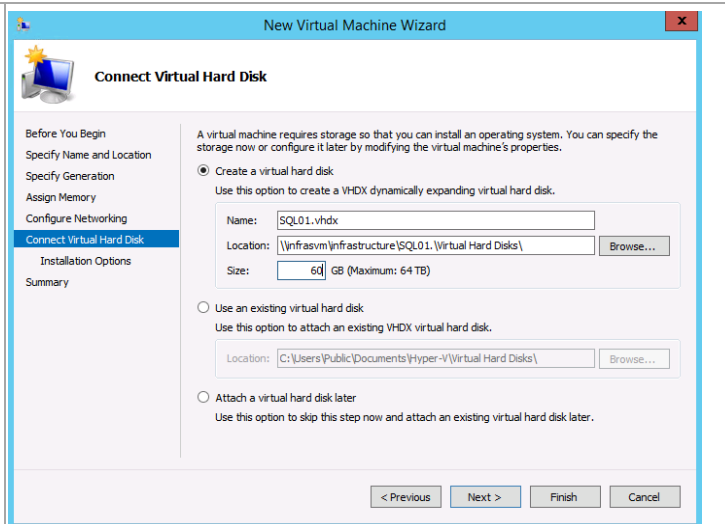
**Name** – specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.

**Location** – accept the default location of the CSV on your fabric management host cluster combined with the virtual machine name.

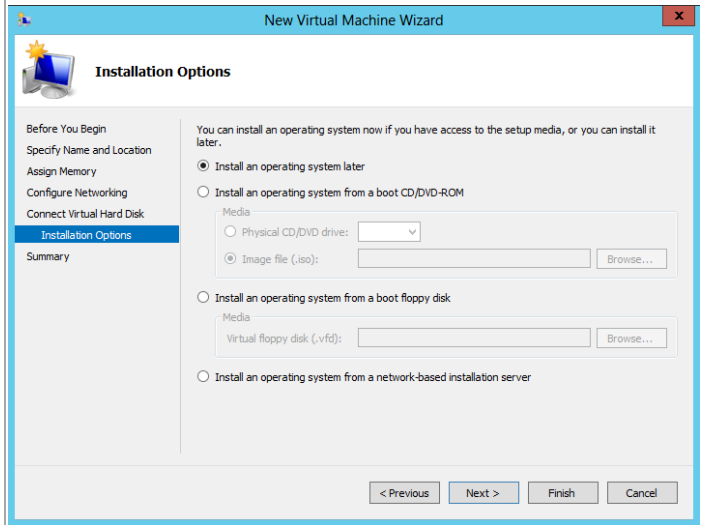
**Size** – specify the size of the VHD (for operating system partitions this should be 60 GB).

Click **Next** to continue.

**Note:** Absent any automated imaging process for the new VMs, a VHD (with Windows Server 2008 R2 or Windows Server 2012 R2 installed and then sysprepped) can be leveraged in place of the new VHD created in this step. This will greatly speed up the provisioning process for the management virtual machines.

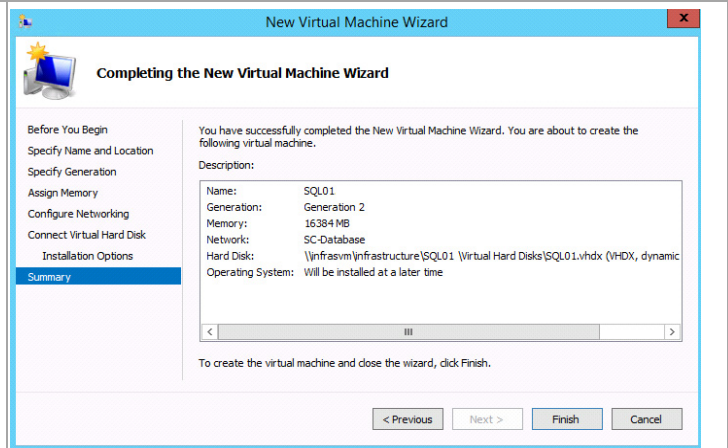


In the **Installation Options** dialog, select the **Install an operating system later** option and click **Next** to continue.

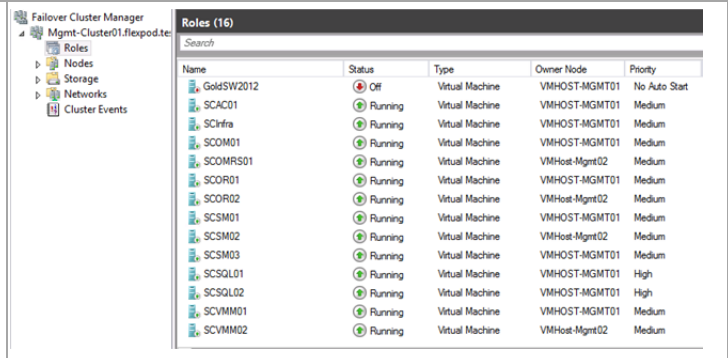


The **Completing the New Virtual Machine Wizard** dialog will display the selections made during the wizard. Click **Finish** to create the virtual machine based on the options selected.

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



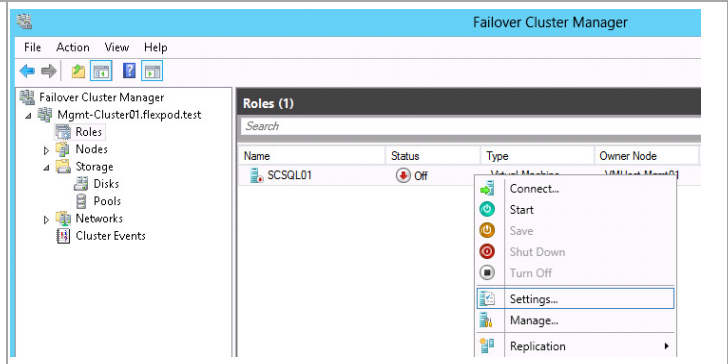
After completion, the virtual machines will be available for management in the **Roles** node of the **Failover Cluster Manager**.



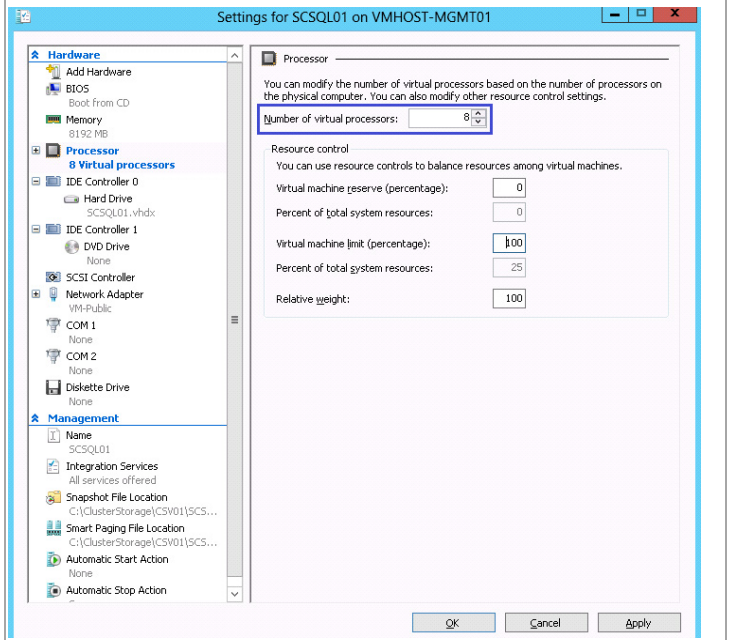
### Modify the Virtual Machine Settings

If you used the manual process to create the virtual machines, 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.

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

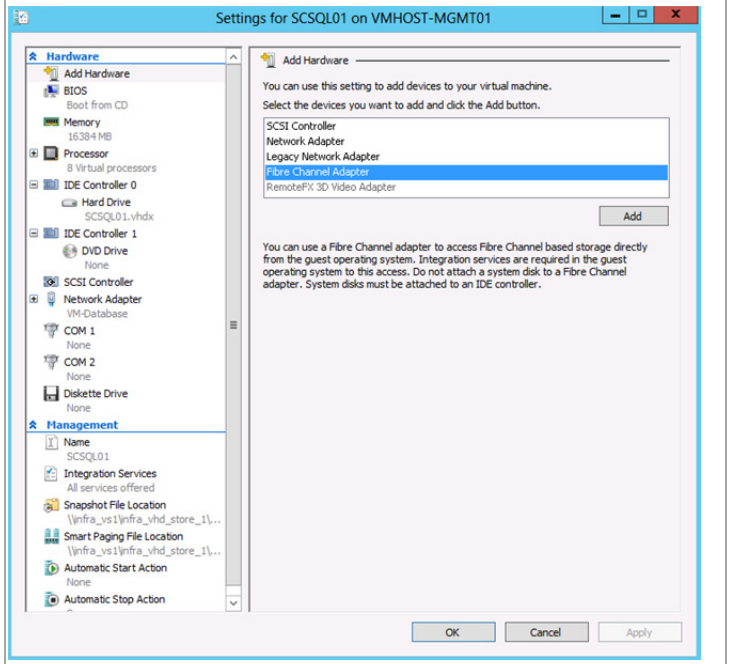


Select **Processor** in the hardware list and set the appropriate number of processors for the specific virtual machine role.

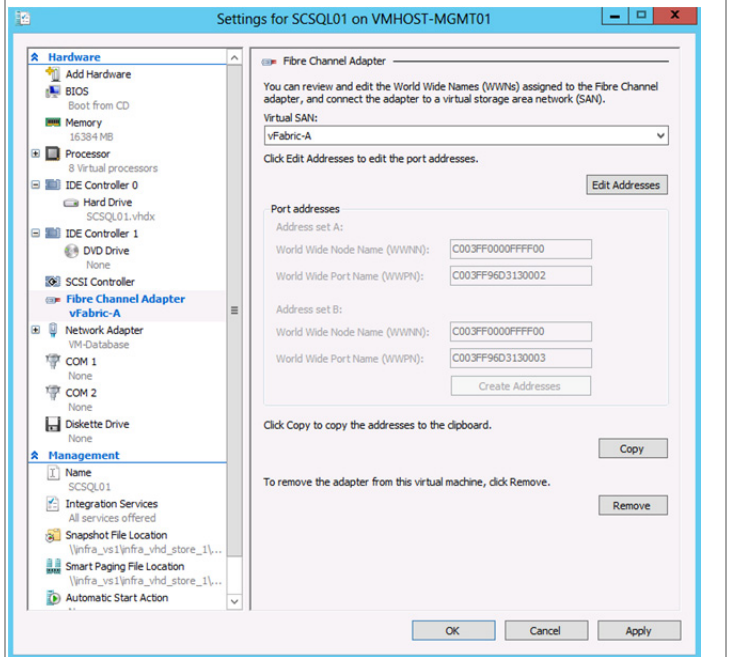


For the SQL Server virtual machines, select **Add Hardware** in the hardware list. Select **Fibre Channel Adapter** in the Add Hardware list and click **Add**.

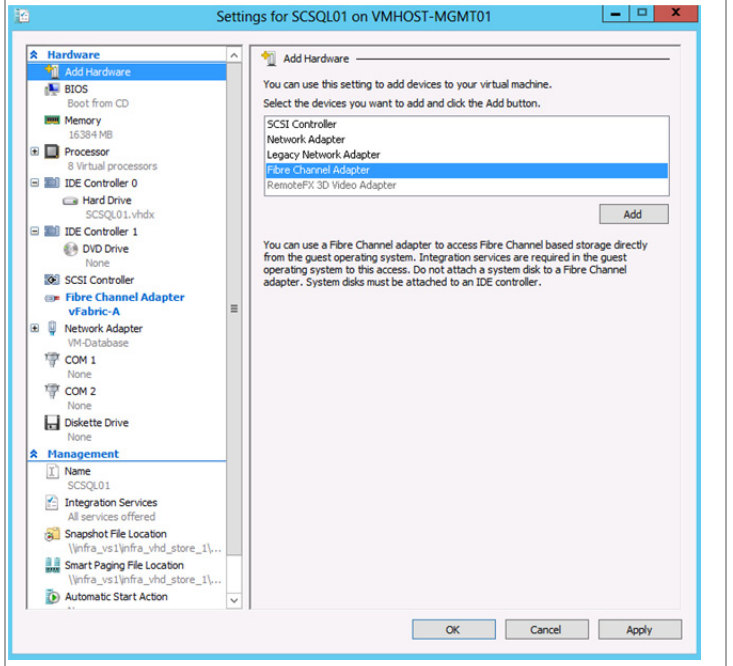
**Note:** These additional adapters must be added to the SQL Server virtual machines for use as Fibre Channel initiators.



Select **vFabric-A** in the virtual SAN dropdown box.

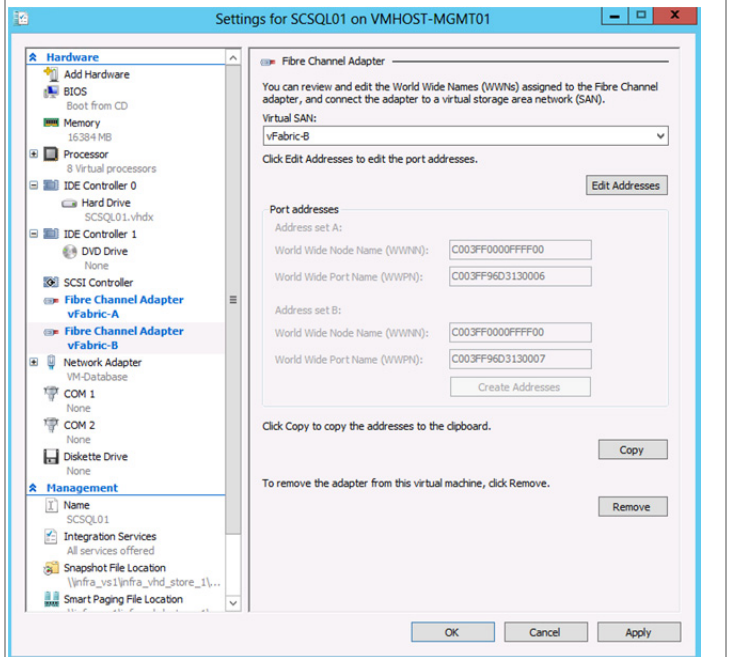


Select **Add Hardware** in the hardware list again. Select **Fibre Channel Adapter** in the Add Hardware list and click **Add**.

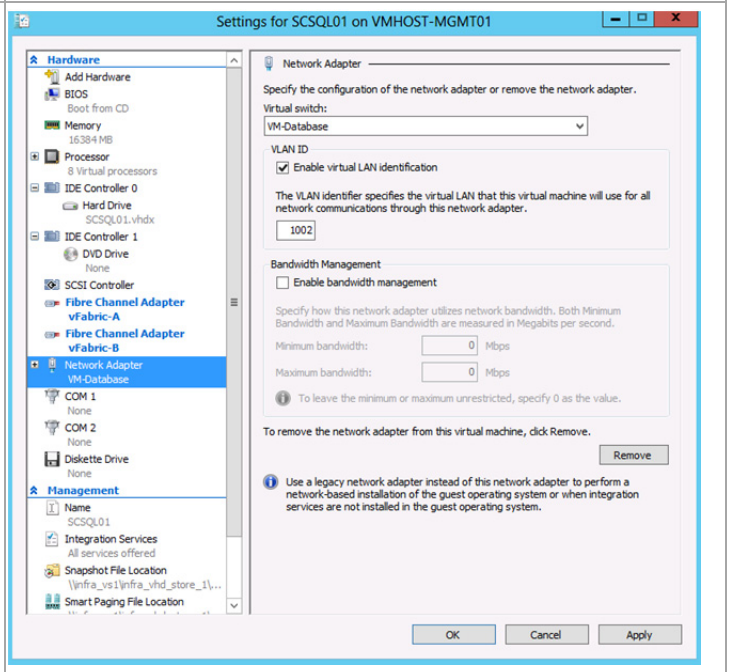




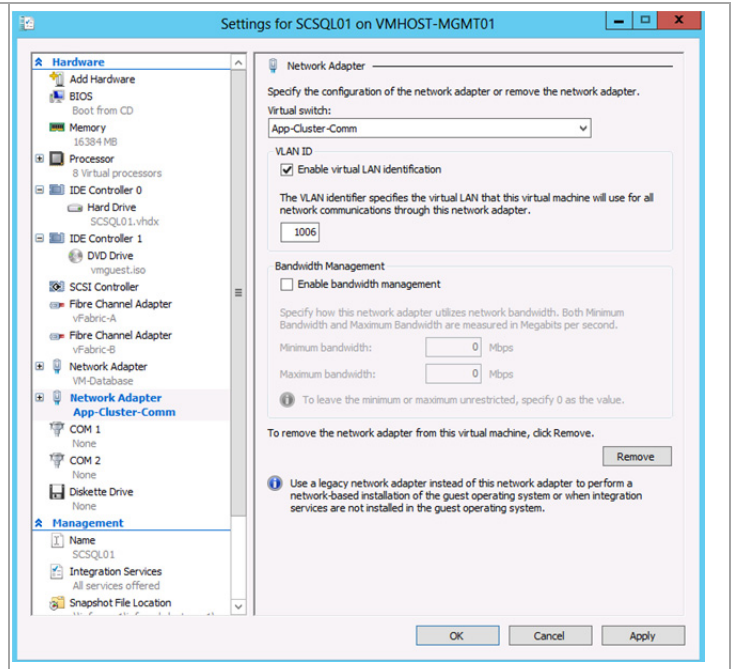
Select **vFabric-B** in the virtual SAN dropdown box.



Select **VM-Database** in the hardware list on the left. Check the **Enable Virtual LAN identification** checkbox. Set the VLAN ID for this network. Click **OK** to complete close the window.



Select **App-Cluster-Comm** in the in the hardware list on the left. **Check the Enable Virtual LAN identification** checkbox. Set the VLAN ID for this network. Click **OK** to complete close the window.



### Install Windows Server in 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. Windows does not need to be installed in each virtual machine if a sysprepped VHDX was used for each virtual machine.

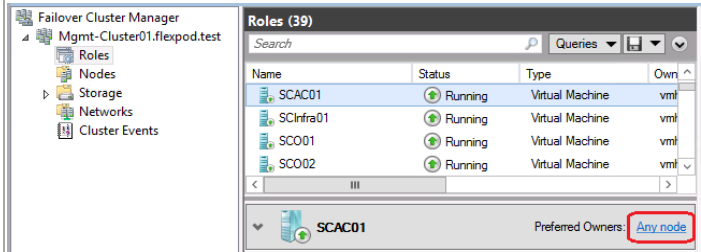
Each Windows instance running in a virtual machine must be renamed after installation. IP addresses must be manually assigned to the NICs if static IP addresses are used instead of DHCP. Each Windows server must be joined to the active directory domain after network connectivity is established.

### 14.3 Define Preferred Owners

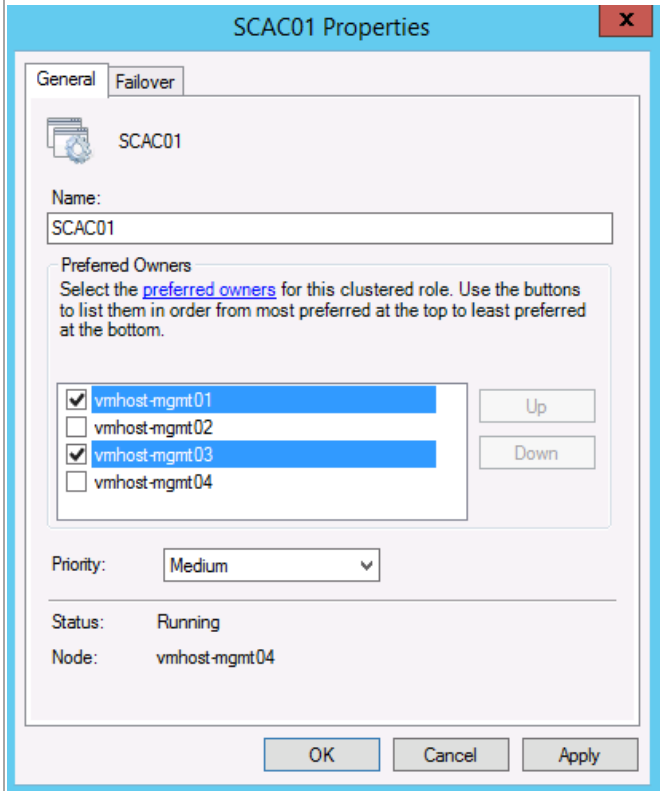
In order to make sure a balanced workload across the four cluster nodes, you should assign preferred owners to each VM. If you used the sample PowerShell script to build your VMs, preferred ownership has already been established for those machines that were created. (The Service Manager Portal and Cisco Nexus 1000V VMs are not created by the sample PowerShell script).

The following steps detail a manual process of assigning preferred ownership. The table at the beginning of this section provides a list of suggested owners for each VM.

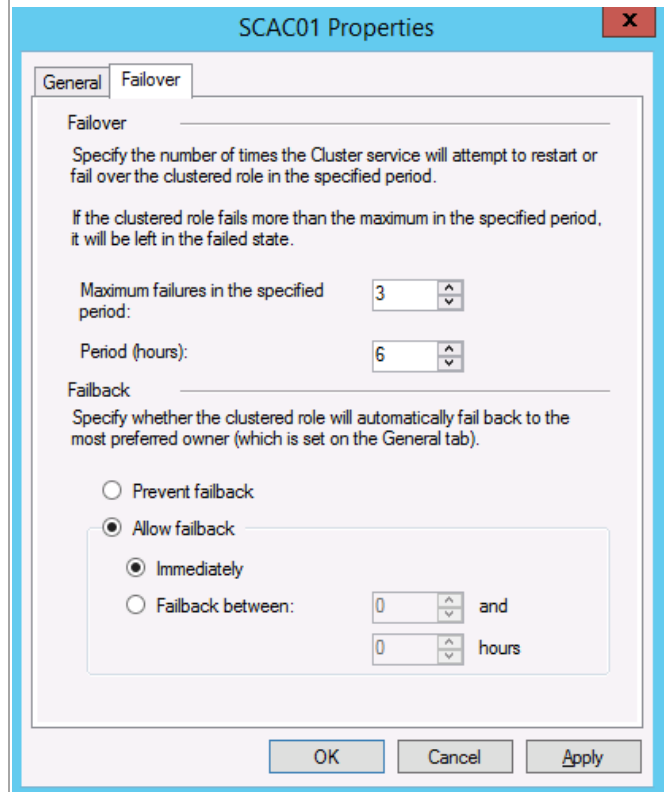
Using Failover Cluster Manager, select a virtual machine. For the **Preferred Owners** you will see **Any Node**. Click on **Any Node**.



The Properties window for the VM will open. On the **General** tab select the hosts you wish to designate as preferred owners.

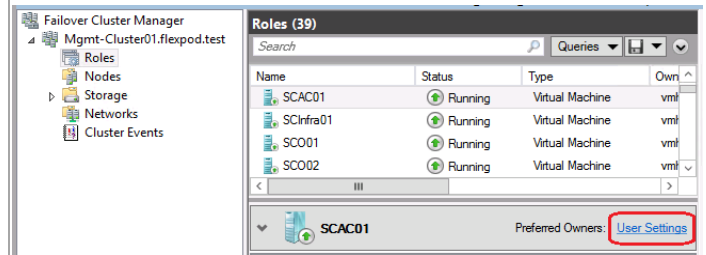


Select the **Failover** tab. In the **Failback** section select the radio button by **Allow failback**. Click **OK** to accept the changes.



In Failover Cluster Manager you will see the Preferred Owners showing as **User Settings**. Repeat for all VMs.

**Note:** Be sure to apply settings to any other VMs created after this point.



## 14.4 Define AntiAffinity

Several of the created VMs are part of highly available configurations for the function they perform. For example, the two VMs created for SCVMM will be clustered to create a highly available environment for SCVMM. If these two VMs were to end up running on the same host, and that host went down, the VMs would failover to other hosts, but while they were restarting on the other hosts, the services of SCVMM would not be available. Antiaffinity classes can be configured on individual VMs to ensure VMs with the same class are not allowed to run on the same host, ensuring that the loss of a host does not take down a service.

The following sample PowerShell script shows how to configure an antiaffinity class for the two SCVMM VMs to ensure both VMs will not end up on the same host. These commands need to be run from any node of the cluster.

```

$aa = New-Object System.Collections.Specialized.StringCollection #Create string object
$tmp = $aa.Add("VMM") #Define value for anti-affinity class
$vm = Get-ClusterGroup -Name SCVMM01 #Get first VM
$vm.AntiAffinityClassNames = $aa #Set anti-affinity class
$vm = Get-ClusterGroup -Name SCVMM02 #Get second VM
$vm.AntiAffinityClassNames = $aa #Set anti-affinity class

```

Similar anti-affinity classes should be defined for the following VMs.

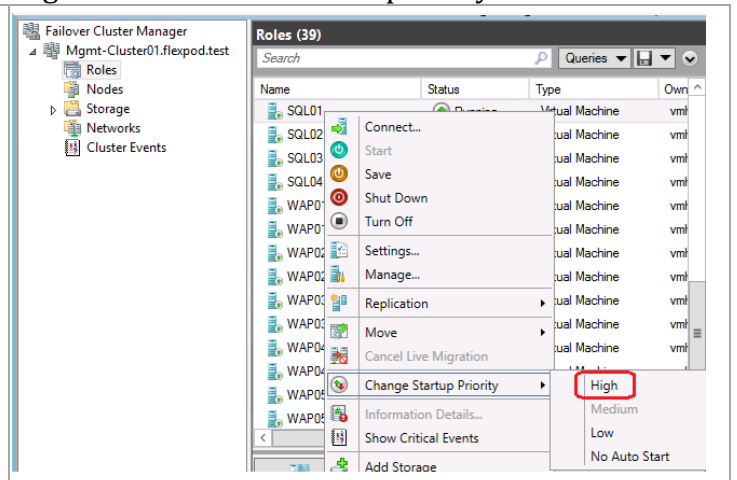
- SCO01, SC02
- SCOM01, SCOM02
- SCSM01, SCSM02
- SCSMA01, SCSMA02
- SCSPF01, SCSPF02
- HNVGW01, HNVGW02
- WAP01, WAP01a
- WAP02, WAP02a
- WAP03, WAP03a
- WAP04, WAP04a
- WAP05, WAP05a
- N1KV-VSM01, N1KV-VSM02 (when these are created later)

## 14.5 Change Startup Priority of VMs

By default, all VMs are configured to try to start as soon as they can when a server is started. This can cause some thrashing to occur as different machines start, maybe expecting another service from another machine to already be started. A prime example of this is that all the System Center components attempt to connect to the SQL Server cluster for their database. If those VMs are starting at the same time as the SQL Server VMs are starting, the System Center VMs are likely to have an initial failure.

Failover clustering allow for the setting of startup priorities for all VMs. Though not required, it is recommended to configure the SQL Server VMs as the highest priority, followed by the System Center VMs, and setting all other VMs to lowest priority.

Within the **Failover Cluster Manager** console right-click on a VM. From the drop-down menu, hover on **Change Startup Priority** and select the desired priority.



## 15 Create Required System Center User Accounts and Security Groups

While each System Center 2012 R2 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 R2 installation:

Component	User account	Suggested name	Description
<b>System Center</b>	Component installation account	FT-SCInstall	This optional account is used to install all System Center 2012 components.
<b>SQL Server</b>	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.
<b>Operations Manager</b>	Management server action account	FT-SCOM-Action	This account is used to carry out actions on monitored computers across a network connection.
<b>Operations Manager</b>	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.
<b>Operations Manager</b>	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.
<b>Operations Manager</b>	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.
<b>Virtual Machine Manager</b>	Virtual Machine Manager service account	FT-SCVMM-SVC	This account is used to run the Virtual Machine Manager service.
<b>Service Manager</b>	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

Component	User account	Suggested name	Description
			database and that this account is a member of the Builtin\Administrators group.
<b>Service Manager</b>	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.
<b>Service Manager</b>	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.
<b>Service Manager</b>	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.
<b>Service Manager</b>	Operations Manager alert connector	FT-SCSM-OMAlert	This account is used for Service Manager Operations Manager Alert connector operations.
<b>Service Manager</b>	Operations Manager CI connector	FT-SCSM-OMCI	This account is used for Service Manager Operations Manager continuous integration (CI) connector operations.
<b>Service Manager</b>	Active Directory connector	FT-SCSM-ADCI	This account is used for Service Manager Active Domain connector operations.
<b>Service Manager</b>	Virtual Machine Manager CI connector	FT-SCSM-VMMCI	This account is used for Service Manager Virtual Machine manager connector operations.
<b>Service Manager</b>	Orchestrator CI Connector	FT-SCSM-OCI	This account is used for System Center Orchestrator connector operations.
<b>Orchestrator</b>	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.
<b>App Controller</b>	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:

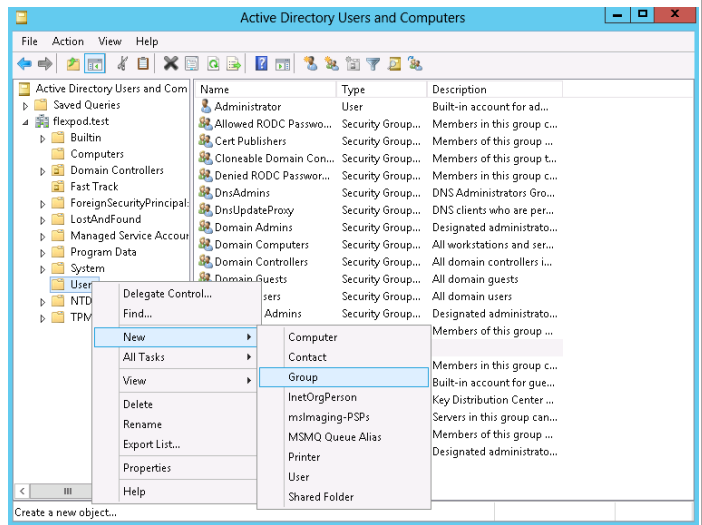
Component	Group	Name	Group notes
<b>System Center 2012</b>	System Center Administrators	FT-SC-Admins	This group's members are full Admins on all System Center components.
<b>SQL Server</b>	SQL Server Administrators	FT-SQL-Admins	This group's members are sysadmins on all SQL Server instances and local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

Component	Group	Name	Group notes
<b>Operations Manager</b>	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.
<b>Virtual Machine Manager</b>	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.
<b>Virtual Machine Manager</b>	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.
<b>Virtual Machine Manager</b>	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.
<b>Virtual Machine Manager</b>	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.
<b>Virtual Machine Manager</b>	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.
<b>Orchestrator</b>	Orchestrator Administrators	FT-SCO-Admins	This group's members are administrators for the Orchestrator installation.
<b>Orchestrator</b>	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.
<b>Service Manager</b>	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.

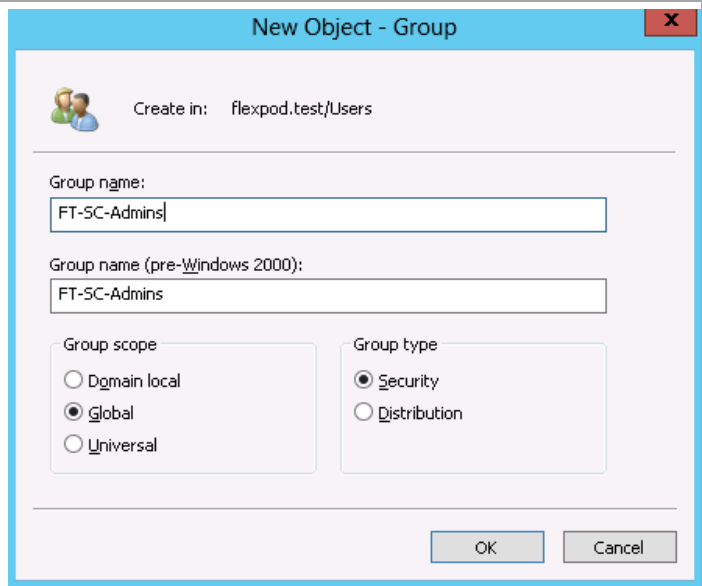


In Active Directory Users and Computers, select the users object in the left tree view. Right-click the Users object, select New and Group.



Enter the user group name in the Group name fields. Accept the default group scope options. Click **OK** to create the group.

Repeat this procedure for all groups in the table above.



Enter the password and password confirmation.  
Click **next**.

New Object - User

Create in: flexpod.test/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back   Next >   Cancel

Click Finish to create the user account.

New Object - User

Create in: flexpod.test/Users

When you click Finish, the following object will be created:

Full name: FT-SQL-Service

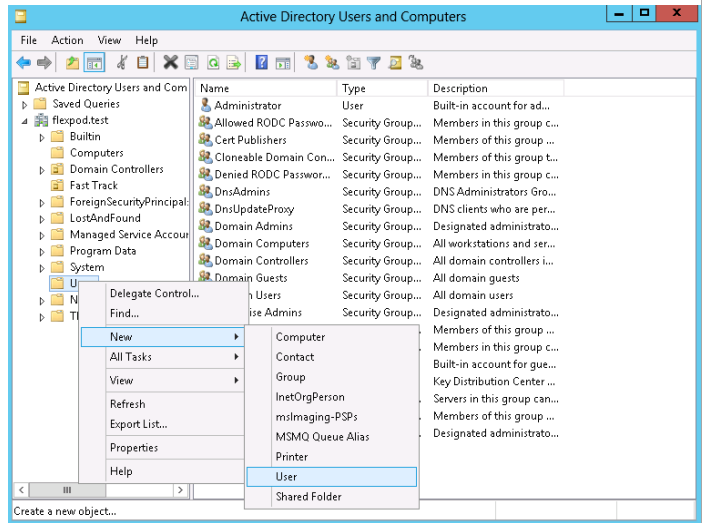
User logon name: FT-SQL-Service@flexpod.test

The password never expires.

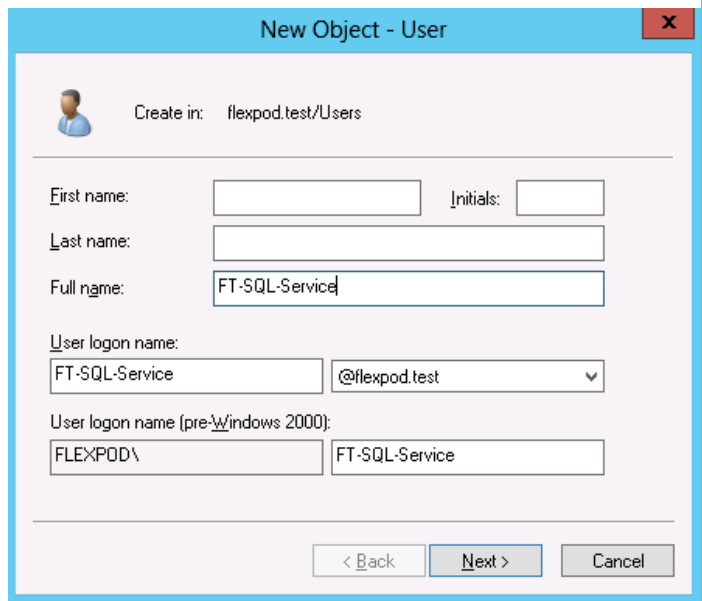
< Back   Finish   Cancel

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

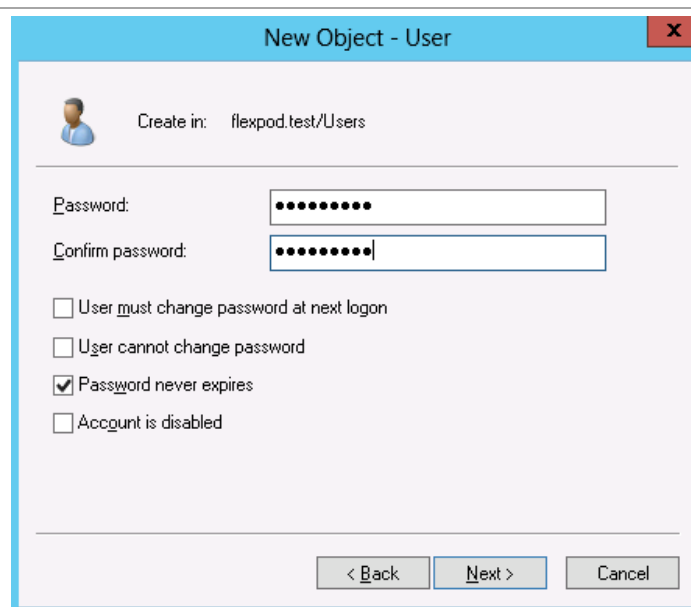
Open Active Directory Users and Computers. Select the users object in the left tree view. Right click the Users object, select New and User.



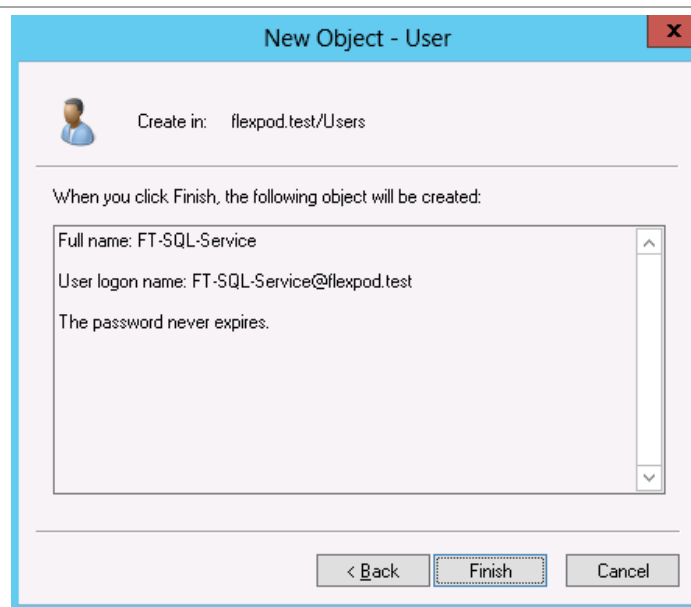
Enter the user account name in the Full Name and User logon name fields. Click Next.



Enter the password and password policy. Click next.



Click Finish to create the user account.



## 15.1 PowerShell to Add Users and Groups

The following sample PowerShell script will add the required accounts and groups to Active Directory. The script reads an XML file that contains the users and groups and details the group memberships. The XML file follows the script file. Modify the XML file if you wish to use a different naming convention.

### FTUsersGroups.ps1

```
<#  
  
FTUsersGroups.ps1 Version=0.1  
4-September-2013
```

Created by Tim Cerling  
tcerling@cisco.com

Execution string: .\FTUsersGroups.ps1 -path <path> -validateOnly -  
toConsole  
    <path> - location of input file FTUsersGroups.xml  
    -validateOnly - only validate contents of FTUsersGroups.xml. Does  
not update AD  
    -toConsole - output log file to console instead of log file

/#>

```
Param
(
    [Parameter(Mandatory=$false,Position=0)]
    [String]$path = (Get-Location),

    [Parameter(Mandatory=$false)]
    [Switch]$validateOnly = $false,

    [Parameter(Mandatory=$false)]
    [Switch]$toConsole = $false
)
```

```
#
# Function Definitions
#
# -----# Function to write log information to either log file or
console
Function Write-Log ($content, $type)
{
    $n = (get-pscallstack).Length - 2
    $lineNum = ((get-pscallstack)[$n].Location -split " line ")[1]

    switch ($type)
    {
        Normal
        {
            If ($ToConsole)
            {
                Write-Host -ForegroundColor Green "$lineNum $(Get-Date
-Format "HH:mm:ss") - $content"
            }
            Else
            {
                Add-Content -Path $logFilePath -Value "$lineNum -
$(Get-Date -Format g): $content"
            }
        }
        Error
        {
            If ($ToConsole)
            {
```

```

        Write-Host -ForegroundColor Red -BackgroundColor Black
"ERROR at line $lineNum `n$content"
    }
    Else
    {
        Add-Content -Path $logFilePath -Value "ERROR at line
$lineNum - $(Get-Date -Format g): $content"
    }
}
}
}

#
# Definition of constants
#
# -----
-----
$startTime = Get-Date
$originalPath = Get-Location
$serrTag = $False
$logFile = "FTUsersGroups.log"
$domain = "DC=FlexPod,DC=test"

#####
#####
#####
#####
#
# Start of Code
#
# -----
-----

# Change to path entered on command line
If (Test-Path $path -PathType Container)
{
    Set-Location $path
}
Else
{
    $serrTag = $True
    Write-Host "Invalid path" -ForegroundColor Red
}

# Read input file
If (Test-Path "$path\FTUsersGroups.xml")
{
    try {$FTUsersGroups = [XML] (Get-Content "$path\FTUsersGroups.xml")}
}
catch {$serrTag = $True; Write-Host "Invalid FTUsersGroups.xml" -
ForegroundColor Red}
}
Else
{
    $serrTag = $True
    Write-Host "Missing FTUsersGroups.xml" -ForegroundColor Red
}

```

```

    }
# Create a log file in the same directory from which the script is
running
If (!$errTag)
{
    If (!$toConsole)
    {
        $localPath = Split-Path (Resolve-Path
$MyInvocation.MyCommand.Path)
        $logFilePath = Join-Path $localPath $logFile
        If (Test-Path($logFilePath))
        {
            Write-Host "Deleting existing log file"
            Remove-Item $logFilePath
        }
        Write-Host "Creating new log file $logfilePath"
        $trash = New-Item -Path $localPath -Name $logFile -ItemType
"file"
    }
}

# Import required modules
if ((Get-Module |where {$_.Name -ilike "ActiveDirectory"}).Name -ine
"ActiveDirectory")
{
    Write-Host "Loading Module: Microsoft Active Directory Module"
    Import-Module ActiveDirectory
}

# Test whether to continue processing
If ($errTag)
{
    Set-Location $originalPath
    $endTime = Get-Date
    $elapsedTime = New-TimeSpan $startTime $endTime
    Write-Host -ForegroundColor Yellow -BackgroundColor Black "`n`n----
-----`n"
    Write-Log "Elapsed time:
$(($elapsedTime.Hours):$(($elapsedTime.Minutes):$(($elapsedTime.Seconds))
"Normal"
    Write-Log "End of processing.`n" "Normal"
    Exit
}
#Process the Organizational Unit (if present)
$xOrgUnit = $FTUsersGroups.FastTrack4.OrgUnit.trim()
If ($xOrgUnit -eq $null) {$xOrgUnit = "Users"}
$sou = "OU=$xOrgUnit,"
$souPath = $sou + $domain

Write-Log "OrgUnit: $xOrgUnit Path: $domain" "Normal"
New-ADOrganizationalUnit -Name $xOrgUnit -Path $domain -
ProtectedFromAccidentalDeletion $true

# Process Users
$FTUsersGroups.FastTrack4.Users | ForEach-Object {$_.Var} | ForEach-
Object {

```

```

    $xUserName = $_.Name.trim()
    $xUserPwd = $_.Pwd.trim()
    $xUserDescr = $_.Descr.trim()
    $secureStringPwd = ConvertTo-SecureString $xUserPwd -AsPlainText -
Force
    $userID = "CN=" + $xUserName + "," + $ouPath
    Write-Log "Name: $xUserName Descr: $xUserDescr Path: $ouPath"
"Normal"
    If (-$validateonly) {
        New-ADUser -Name $xUserName -Description $xUserDescr -Path
$ouPath -Type "user"
        Set-ADUser -Identity $xUserName -DisplayName $xUserName -
GivenName $xUserName -SamAccountName $xUserName
        $secureStringPwd = ConvertTo-SecureString $xUserPwd -
AsPlainText -Force
        Set-ADAccountPassword -Identity $userID -NewPassword
$secureStringPwd
        Enable-ADAccount -Identity $userID
        Set-ADAccountControl -Identity $userID -PasswordNeverExpires
$true
    }
}
Write-Log "-----" "Normal"
# Process Groups
$FTUsersGroups.FastTrack4 | ForEach-Object {$_.Group} | ForEach-Object
{
    $xGrpName = $_.Name.trim()
    $xGrpDescr = $_.Descr.trim()

    If ($xGrpName.Contains("/"))
    {
        $tmpOU = $xGrpName -split '/', 2
        $grpID = "CN=" + $tmpOU[1] + ",OU=" + $tmpOU[0] + "," + $domain
        Write-Log "NOT adding group ... $grpID" "Normal"
    }
    Else
    {
        $grpID = "CN=" + $xGrpName + "," + $ouPath
        If (-$validateOnly) {
            New-ADGroup -Name $xgrpName -Path $ouPath -GroupCategory
"Security" -GroupScope "Global" -SamAccountName $xGrpName -Description
$xGrpDescr
        }
        Write-Log "adding group ... $grpID" "Normal"
    }

    Write-Log "Group: $xGrpName Descr: $xGrpDescr ID: $grpID"
"Normal"

# Add members to group
    $tmp100 = $_.Members
    If ($tmp100 -ne $null)
    {
        $tmp100 | ForEach-Object {$_.Var} | ForEach-Object {

```



```

        $xMemberName = $_.Name.trim()
        $xMemberType = $_.Type.trim()
        $memberID = "CN=" + $xMemberName + "," + $ouPath
        If ($xMemberType -ne "Computer")
        {
            If (-$validateOnly) {
                Add-ADPrincipalGroupMembership -Identity $memberID
-Memberof $grpID
            }
            Write-Log " Member: $xMemberName Type: $xMemberType
memID: $memberID Grp: $grpID" "Normal"
        }
    }
}

Set-Location $originalPath
$endTime = Get-Date
$elapsedTime = New-TimeSpan $startTime $endTime
If ($stoconsole)
{
    Write-Host -ForegroundColor Yellow -BackgroundColor Black "`n`n----
-----`n"

    Write-Host "Elapsed time:
$(($elapsedTime.Hours):$(($elapsedTime.Minutes):$(($elapsedTime.Seconds))"
    Write-Host "End of processing."
}
Else
{
    Write-Log "Elapsed time:
$(($elapsedTime.Hours):$(($elapsedTime.Minutes):$(($elapsedTime.Seconds))"
"Normal"
    Write-Log "End of processing." "Normal"
}
}

```

## FTUsersGroup.xml

```

<?xml version="1.0" encoding="utf-8"?>
<!--
  FTUsersGroups Version=0.1
  18-September-2013
  Created by Tim Cerling
  tcerling@cisco.com
-->

<FastTrack4>
  <OrgUnit>FlexPod</OrgUnit>

  <!-- Users -->
  <Users>
    <Var Name='FT-SCInstall' Pwd='1FlexPod1' Descr='Optional for SC
2012 install' />
  </Users>
</FastTrack4>

```

```

    <Var Name='FT-SQL-SVC' Pwd='1FlexPod1' Descr='SQL service account'
  />
    <Var Name='FT-SCOM-Action' Pwd='1FlexPod1' Descr='OM monitoring' />
    <Var Name='FT-SCOM-SVC' Pwd='1FlexPod1' Descr='OM service account'
  />
    <Var Name='FT-SCOM-DW' Pwd='1FlexPod1' Descr='OM Data warehouse' />
    <Var Name='FT-SCOM-DR' Pwd='1FlexPod1' Descr='OM data reader for
SQL SRS' />
    <Var Name='FT-SCVMM-SVC' Pwd='1FlexPod1' Descr='VMM service
account' />
    <Var Name='FT-SCSM-SVC' Pwd='1FlexPod1' Descr='SM service account'
  />
    <Var Name='FT-SCSM-WF' Pwd='1FlexPod1' Descr='SM workflows' />
    <Var Name='FT-SCSM-SSRS' Pwd='1FlexPod1' Descr='SM SQL SRS for
datamart' />
    <Var Name='FT-SCSM-OLAP' Pwd='1FlexPod1' Descr='SM SQL Analysis
Services' />
    <Var Name='FT-SCSM-OMAlert' Pwd='1FlexPod1' Descr='SM-OM alert
connector' />
    <Var Name='FT-SCSM-OMCI' Pwd='1FlexPod1' Descr='SM-OM connector' />
    <Var Name='FT-SCSM-ADCI' Pwd='1FlexPod1' Descr='SM-AD connector' />
    <Var Name='FT-SCSM-VMMCI' Pwd='1FlexPod1' Descr='SM-VMM connector'
  />
    <Var Name='FT-SCSM-OCI' Pwd='1FlexPod1' Descr='SM-Orchestrator
connector' />
    <Var Name='FT-SCSM-Users' Pwd='1FlexPod1' Descr='SM users' />
    <Var Name='FT-SCO-SVC' Pwd='1FlexPod1' Descr='Orchestrator service
account' />
    <Var Name='FT-SCAC-SVC' Pwd='1FlexPod1' Descr='AppController
service account' />
    <Var Name='FT-SMA-SVC' Pwd='1FlexPod1' Descr='Service Manager
Automation Service Account' />
    <Var Name='FT-SPF-SVC' Pwd='1FlexPod1' Descr='Service Provider
Foundation Service Account' />
  </Users>

<!-- Group Memberships -->
  <Group Name='FT-SC-Admins' Descr='System Center Administrators'>
  </Group>
  <Group Name='FT-SCAC-Admins' Descr='AppCenter Administrators'>
    <Members>
      <Var Name='FT-SCAC-SVC' Type='User' />
      <Var Name='FT-SCVMM-Admins' Type='Group' />
    </Members>
  </Group>
  <Group Name='FT-SQL-Admins' Descr='SQL Server Administrators'>
    <Members>
      <Var Name='FT-SQL-SVC' Type='User' />
      <Var Name='FT-SCSM-OLAP' Type='User' />
      <Var Name='FT-SCSM-SSRS' Type='User' />
    </Members>
  </Group>
  <Group Name='FT-SCOM-Admins' Descr='Operations Manager
Administrators'>
    <Members>
      <Var Name='FT-SCOM-Action' Type='User' />

```

```

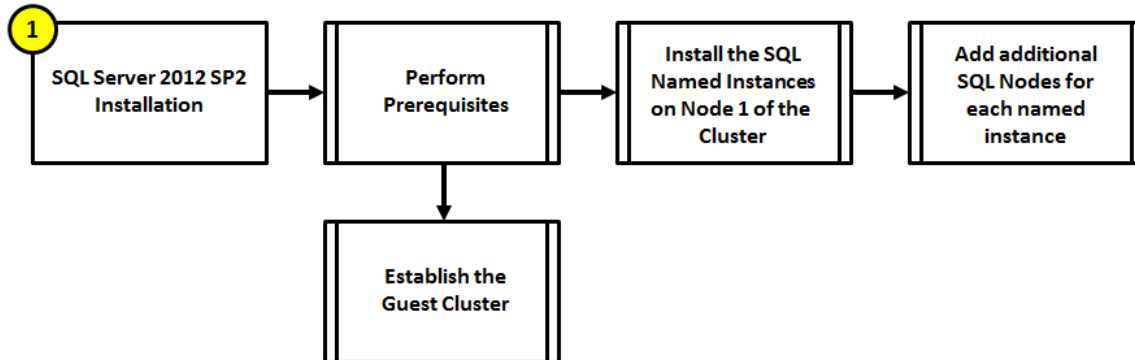
    <Var Name='FT-SCOM-SVC' Type='User' />
    <Var Name='FT-SCOM-DR' Type='User' />
    <Var Name='FT-SCOM-DW' Type='User' />
    <Var Name='FT-SCVMM-SVC' Type='User' />
    <Var Name='OM01' Type='Computer' />
    <Var Name='OM02' Type='Computer' />
  </Members>
</Group>
<Group Name='FT-SCOM-Operators' Descr='Operations Manager Operators'>
  <Members>
    <Var Name='FT-SCSM-OMCI' Type='user' />
  </Members>
</Group>
<Group Name='FT-SCOM-AdvOperators' Descr='Operations Manager Advanced
Operators'>
</Group>
<Group Name='FT-SCVMM-Admins' Descr='Virtual Machine Manager
Administrators'>
  <Members>
    <Var Name='FT-SCVMM-SVC' Type='User' />
    <Var Name='FT-SCSM-VMMCI' Type='User' />
    <Var Name='FT-SCO-SVC' Type='User' />
    <Var Name='FT-SCAC-SVC' Type='User' />
  </Members>
</Group>
<Group Name='FT-SCVMM-FabricAdmins' Descr='VMM Fabric
Administrators'>
</Group>
<Group Name='FT-SCVMM-ROAdmins' Descr='VMM Read-only Administrators'>
</Group>
<Group Name='FT-SCVMM-TenantAdmins' Descr='VMM Tenant
Administrators'>
</Group>
<Group Name='FT-SCVMM-AppAdmins' Descr='VMM Application
Administrators'>
</Group>
<Group Name='FT-SCO-Admins' Descr='Orchestrator Administrators'>
  <Members>
    <Var Name='FT-SCO-SVC' Type='User' />
  </Members>
</Group>
<Group Name='FT-SCO-Operators' Descr='Orchestrator Operators'>
  <Members>
    <Var Name='FT-SCSM-OCI' Type='User' />
  </Members>
</Group>
<Group Name='FT-SCSM-Admins' Descr='Service Manager Administrators'>
  <Members>
    <Var Name='FT-SCSM-OMAlert' Type='User' />
    <Var Name='FT-SCSM-OMCI' Type='User' />
    <Var Name='FT-SCSM-SSRS' Type='User' />
    <Var Name='FT-SCSM-SVC' Type='User' />
    <Var Name='FT-SCSM-WF' Type='User' />
  </Members>
</Group>
<Group Name='Builtin/Distributed COM Users' Descr=' '>

```

```
<Members>
  <Var Name='FT-SCO-Admins' Type='group' />
</Members>
</Group>
<Group Name='FT-SPF-Admins' Descr='Service Provider Foundation
Administrators'>
  <Members>
    <Var Name='FT-SPF-SVC' Type='User' />
  </Members>
</Group>
<Group Name='FT-SPF-Provider' Descr='SPF Provider Web Service
access'>
  <Members>
    <Var Name='FT-SPF-SVC' Type='User' />
  </Members>
</Group>
<Group Name='FT-SPF-VMM' Descr='SPF VMM Web Service access'>
  <Members>
    <Var Name='FT-SPF-SVC' Type='User' />
  </Members>
</Group>
<Group Name='FT-SPF-Usage' Descr='SPF Usage Web Service'>
  <Members>
    <Var Name='FT-SPF-SVC' Type='User' />
  </Members>
</Group>
</FastTrack4>
```

## 16 SQL Server 2012 Failover Cluster Installation

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



### 16.1 Overview

The subsequent sections of this document contain guidance for deploying a four-node SQL Server cluster.

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

1. Four base virtual machines running Windows Server 2012 R2 have been provisioned for SQL Server.
2. Constrained delegation has been configured for each of the SQL Server VMs to access the SMB share where the databases and log files will be stored.
3. One LUN has been configured on the Fabric Management host cluster for use as a Cluster Shared Volume. This LUN is used to store that database and log files for a SQL Server Analysis Server instance as SQL Server Analysis Server does not yet support SMB storage.

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

## Database Instances and Requirements

Fabric Management Component	Instance Name (Suggested)	Components	Collation <sup>1</sup>	Storage Requirements <sup>2</sup>
Virtual Machine Manager	SCVMMDB	Database Engine	Latin1_General_100_CI_AS	2 LUNs
Windows Server Update Services (optional)	SCVMMDB	Database Engine	Latin1_General_100_CI_AS	N/A – Shared instance with Virtual Machine Manager
Operations Manager	SCOMDB	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs
Operations Manager Data Warehouse	SCOMDW	Database Engine, Full-Text Search	Latin1_General_100_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	Latin1_General_100_CI_AS	N/A – Shared instance with Orchestrator and App Controller
Orchestrator	SCDB	Database Engine	Latin1_General_100_CI_AS	2 LUNs
App Controller	SCDB	Database Engine	Latin1_General_100_CI_AS	N/A – Shared instance with Orchestrator and Service Manager Portal

## 16.2 Prerequisites

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

### 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

<sup>1</sup> 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).

<sup>2</sup> Note that additional LUNs may be required for TempDB management in larger scale configurations

User name	Purpose	Permissions
		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.

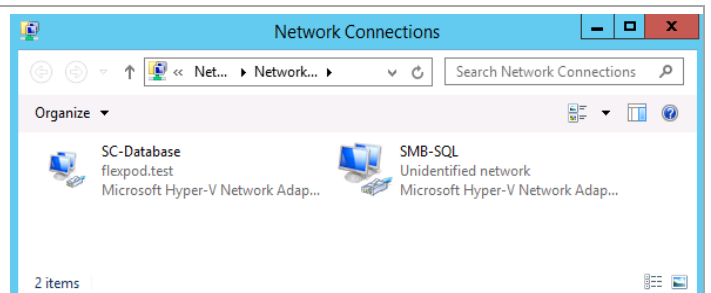
## Groups

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.

## Configure the Network Interfaces the SQL Server Virtual Machine

Login to the SQL Server and open the Network Connections windows. Rename the LAN adapters to reflect the network it is associated with.



Set the appropriate IP settings for each adapter. Use static IP address, subnet mask, gateway, and DNS servers for the database network if these setting need to be manually configured.

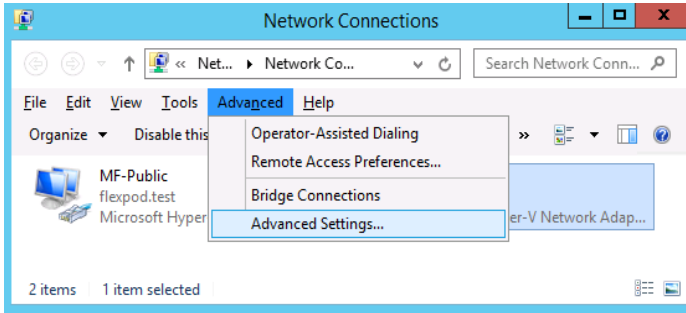
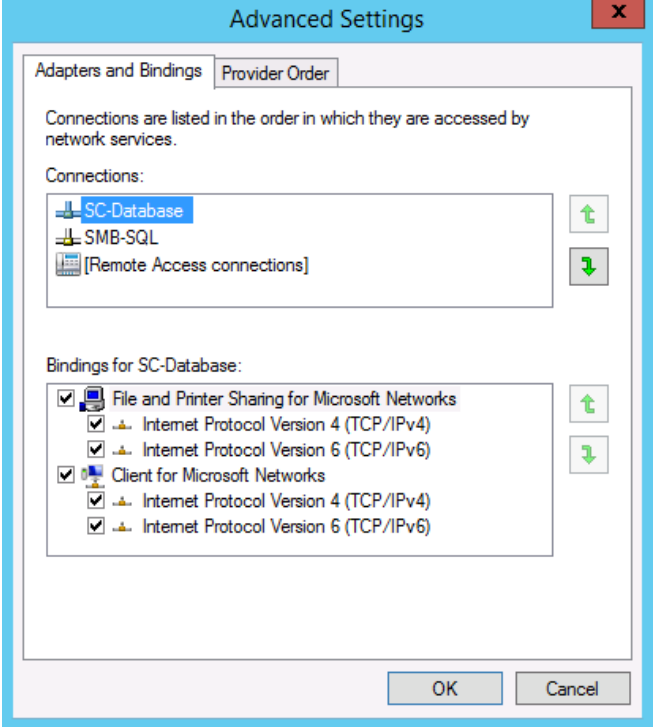
The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the 'SC-Database' network adapter. The 'General' tab is selected. The dialog contains the following settings:

- Obtain an IP address automatically
- Use the following IP address:
  - IP address: 192 . 168 . 2 . 21
  - Subnet mask: 255 . 255 . 255 . 0
  - Default gateway: 192 . 168 . 2 . 1
- Obtain DNS server address automatically
- Use the following DNS server addresses:
  - Preferred DNS server: 10 . 10 . 4 . 61
  - Alternate DNS server: 10 . 10 . 4 . 62
- Validate settings upon exit
- Advanced... button
- OK and Cancel buttons at the bottom.

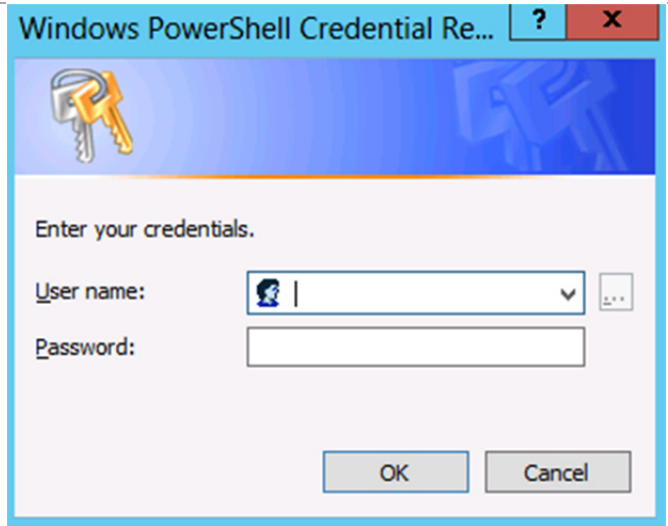
The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the 'SMB-SQL' network adapter. The 'General' tab is selected. The dialog contains the following settings:

- Obtain an IP address automatically
- Use the following IP address:
  - IP address: 192 . 168 . 3 . 24
  - Subnet mask: 255 . 255 . 255 . 0
  - Default gateway: . . .
- Obtain DNS server address automatically
- Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .
- Validate settings upon exit
- Advanced... button
- OK and Cancel buttons at the bottom.



<p>In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -&gt; Advanced Settings</p>	
<p>Select the adapter and use the arrows to move it up or down in binding order. The recommended binding order is:</p> <ul style="list-style-type: none"> <li>• SC-Database</li> <li>• MF-Public</li> <li>• SMB-SQL</li> </ul>	
<p>Open a PowerShell window and rename the computer.</p>	<pre>Rename-Computer -NewName SQL01 -Restart</pre>
<p>After the computer reboots, login again, open a PowerShell window and join the active directory domain.</p>	<pre>Add-Computer -DomainName flexpod.test -Restart</pre>

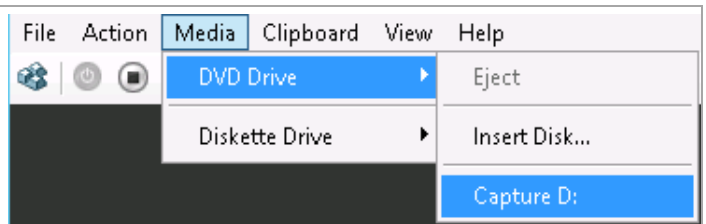
Enter the account and password with privileges to add a computer to the domain.



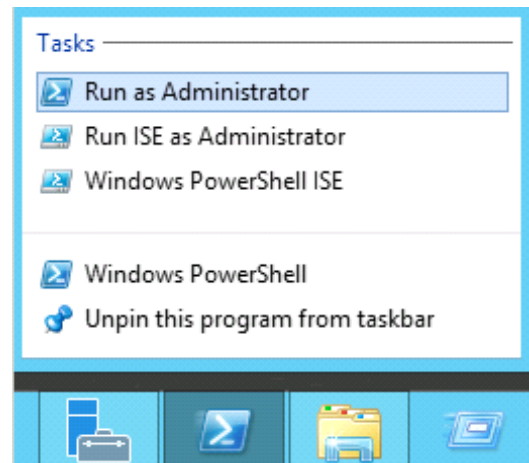
### Install Windows Features in the SQL Server Virtual Machine

Perform this procedure on both SQL Server Virtual Machines.

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

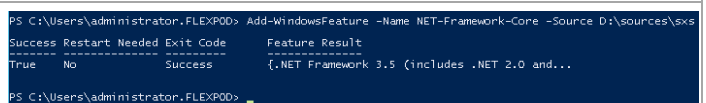


Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.



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

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



Eject the DVD media after the operation is complete.

Add Failover Cluster and Management Tools by entering the following command:

```
Install-WindowsFeature Failover-Clustering -  
IncludeManagementTools
```

```
PS C:\> Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools  
Success Restart Needed Exit Code Feature Result  
-----  
True No Success {Failover Clustering, Remote Server Admini...  
PS C:\>
```

## Establish the SQL Server Guest Cluster

This section assumes SMB shares will 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. Therefore, a LUN on the host cluster was created and set up as a Cluster Shared Volume. Shared VHDX files are created on the CSV for the database and logs files used by SQL Server Analysis Services.

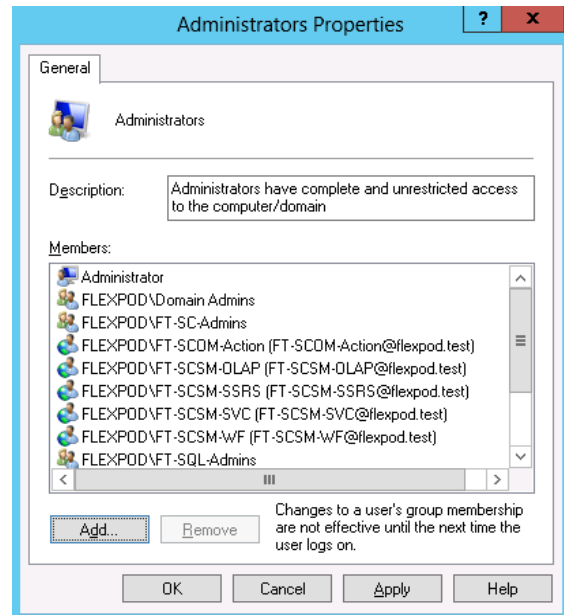
Before creating the guest cluster of the SQL Server VMs, follow the procedure documented earlier to configure Constrained Delegation for each of the SQL Server VMs.

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

Log on to the first node in the SQL Server cluster as a user with local admin rights.

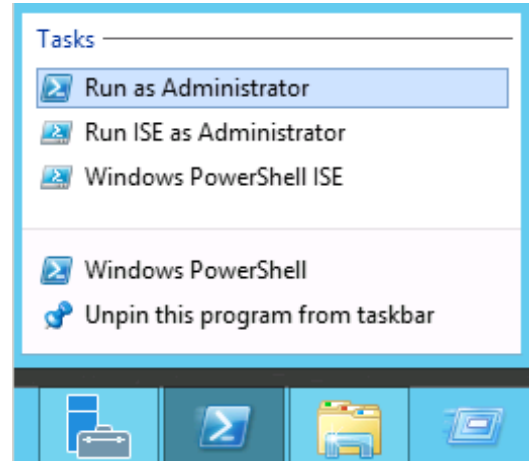
Verify that the following accounts and/or groups are members of the Local Administrators group on each SQL Server node:

1. Fast Track SQL Server service account.
2. Fast Track SQL Server Admins group.
3. Virtual Machine Manager computer accounts.
4. Fast Track Service Manager OLAP account.
5. Fast Track Service Manager SSRS account.
6. Fast Track Service Manager workflow account.
7. Fast Track Service Manager service account.
8. Fast Track Operations Manager action account.
9. Fast Track Virtual Machine Manager service account.



Create a the Windows Failover Cluster using the four SQL Server virtual machines provisioned in the earlier step. Perform the following procedure on one of the SQL Server virtual machines.

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



Create a new cluster by executing the following command

```
New-Cluster -Name <cluster_name> -Node
<Node1>, <Node2>, <node3>, <node4> -NoStorage -
StaticAddress <cluster_ip_address>
```

```
PS C:\> New-Cluster -Name SQL-Cluster01 -Node SQL01,SQL02,SQL03,SQL04 -NoStorage -StaticAddress 192.168.1.10
Report File Location: C:\Windows\cluster\Reports\Create Cluster Wizard SQL-Cluster01 on 2014.10.15 AT 09:28:34.mht
Name
----
SQL-Cluster01
PS C:\>
```

Rename the cluster networks to match their function.

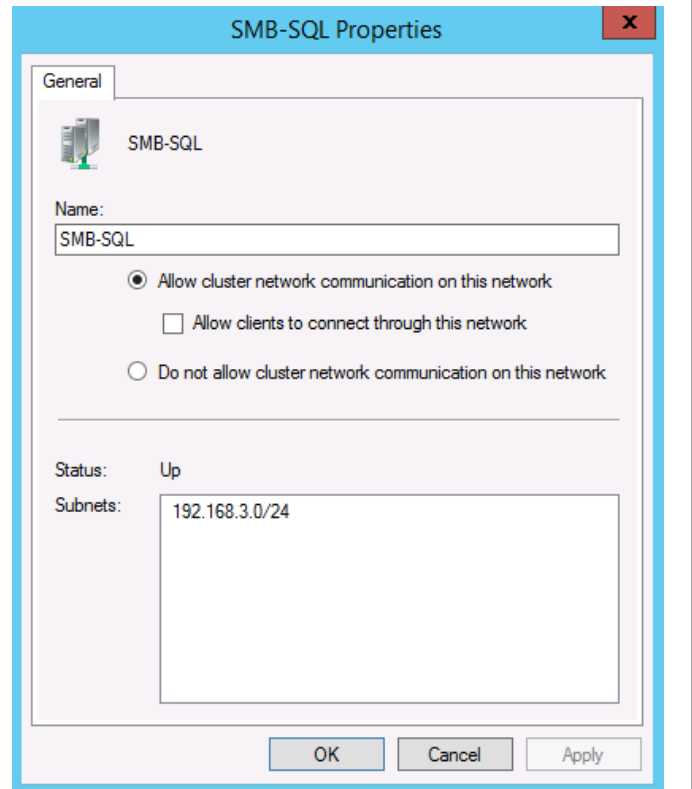
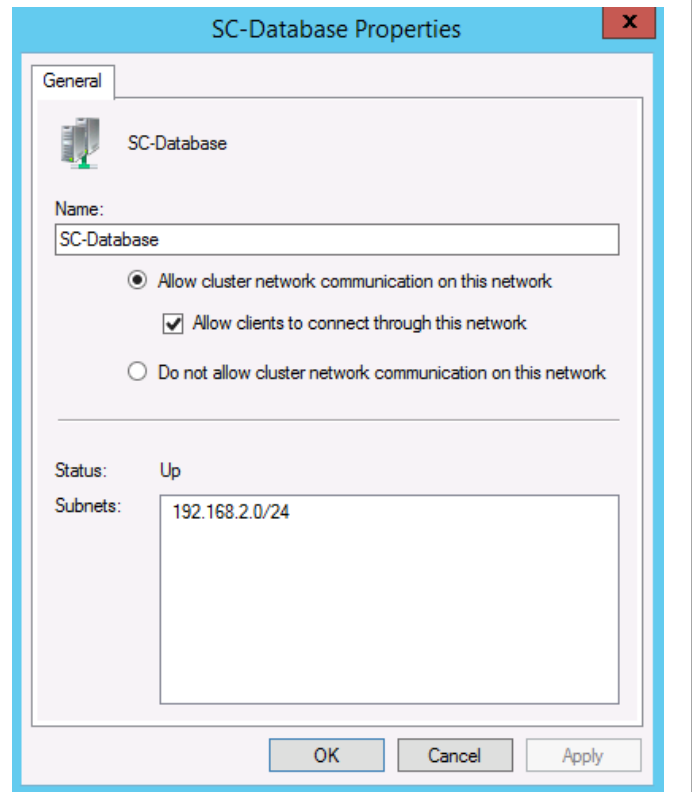
```
Get-ClusterNetworkInterface | ? Name -like
*SMB* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'SMB-SQL'}
```

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

Using Failover Cluster Manager, expand the Networks object in the left tree view. Right click each network and select properties.

**Check** Allow clients to connect through this network for the SC-Database network.

**Uncheck** Allow clients to connect through this network for the SMB-SQL network.



## Create and Map Storage for SQL Server

Most storage will be placed on SMB shares. The exception is for SQL Server Analysis Services. It does not yet support storing its database and logs on SMB shares. In the creation of the Fabric Management host cluster, a Cluster Shared Volume was created. Shared virtual hard disks will be created on the CSV to be used by the SQL Server Analysis Services instance.

### SQL Server Database and Quorum SMB Shares and Drive Letters

Component(s)	Instance Name	Purpose	Size	SMB Share or Drive Letter
Service Manager Management	SCSMDB	Instance Database and Logs	145 GB/70 GB	Database \\infrasm\scsmdb Logs \\infrasm\scsmdblog
Service Manager Data Warehouse	SCSMDW	Instance Database and Logs	1 TB/ 500 GB	Database \\infrasm\scsmdw Logs \\infrasm\scsmdwlog
Service Manager Analysis Service	SCSMAS	Instance Database and Logs	8 GB/4 GB	Database E: Logs F:
Service Manager SharePoint Farm Orchestrator App Controller	SCDB	Instance Database and Logs	10 GB/5 GB	Database \\infrasm\scdb Logs \\infrasm\scdblog
Virtual Machine Manager Windows Server Update Services	SCVMMDB	Instance Database and Logs	6 GB/3 GB	Database \\infrasm\scvmmdb Logs \\infrasm\scvmmdblog
Operations Manager	SCOMDB	Instance Database and Logs	130 GB/65 GB	Database \\infrasm\scomdb Logs \\infrasm\scomdblog
Operations Manager Data Warehouse	SCOMDW	Instance Database and Logs	1 TB/ 500 GB	Database \\infrasm\scomdw Logs \\infrasm\scomdwlog
Windows Azure Pack	WAPDB	Instance Database and Logs	200GB / 100GB	Database \\infrasm\wapdb Logs \\infrasm\wapdblog
N/A	N/A	SQL Server Failover Cluster Quorum	1 GB	\\infrasm\sql-witness

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

These steps provide details for SQL Server database SMB Shares.

1. Log into the NetApp Cluster by opening an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

2. Create a new Qtree to hold the SQL Server databases.

```
qtree create -volume sc_sql_db -Qtree scsmdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scsmdblog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scsmdw -security-style ntfs -vserver infra_svm
```

```

qtree create -volume sc_sql_db -Qtree scsmdwlog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scsmas -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scsmaslog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scdblog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scvmmdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scvmmdblog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scomdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scomdblog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scomdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree scomdblog -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree wapdb -security-style ntfs -vserver infra_svm
qtree create -volume sc_sql_db -Qtree wapdblog -security-style ntfs -vserver infra_svm

```

### 3. Create the qtree quota policy for each qtree.

```

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
145g -target scsmdb -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
70g -target scsmdblog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
1TB -target scsmdw -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
500g -target scsmdwlog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit 8g
-target scsmas -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit 4g
-target scsmaslog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
10- -target scdb -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit 5g
-target scdblog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
100g -target scvmmdb -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
50g -target scvmmdblog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
200g -target scomdb -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
100g -target scomdblog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
500g -target scomdw -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
250g -target scomdwlog -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
200g--target wapdb -vserver infra_svm

quota policy rule create -policy-name default -volume sc_sql-db -type tree -disk-limit
100g -target wapdblog -vserver infra_svm

```

### 4. Create SMB Shares.

```

share create -share-name scsmdb -path /sc-sql_db/scsmdb -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scsmdblog -path /sc-sq_db/scsmdblog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scsmdw -path /sc-sql_db/scsmdw -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scsmdwlog -path /sc-sq_db/scsmdwlog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scsmas -path /sc-sql_db/scsmas -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scsmaslog -path /sc-sq_db/scsmaslog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scdb -path /-c_sql_db/scdb -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scdblog -path /sc_-ql_db/scdblog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm
-
share create -share-name scvmmdb -path /sc_-ql_db/scvmmdb -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scvmmlg -path /sc_sq_log/scvmmlg -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scomdb -path /sc-sql_db/scomdb -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name scomlog -path /sc_s-l_log/scomlog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm
-
share create -share-name scomdw -path /sc_sql_db/scomdw -share-properties
browsable,continuously-available, oplocks -vserver infra_svm
-
share create -share-name scomdwlog -path /sc_sql-log/scomdwlog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name wapdb -path /sc_sql_db/wapdb -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

share create -share-name wapdblog -path /sc_sq_log/wapdblog -share-properties
browsable,continuously-available, oplocks -vserver infra_svm

```

## 5. Remove the Everyone permission from the shares.

```

share access-control delete -share scsmdb -user-or-group Everyone -vserver infra_svm
share access-control delete -share scsmdblog -user-or-group Everyone -vserver infra_svm
share access-control delete -share scsmdw -user-or-group Everyone -vserver infra_svm
share access-control delete -share scsmdwlog -user-or-group Everyone -vserver infra_svm
share access-control delete -share scdb -user-or-group Everyone -vserver infra_svm
share access-control delete -share scdblog -user-or-group Everyone -vserver infra_svm
share access-control delete -share scvmmdb -user-or-group Everyone -vserver infra_svm
share access-control delete -share scvmmdblog -user-or-group Everyone -vserver infra_svm
share access-control delete -share scomdb -user-or-group Everyone -vserver infra_svm
share access-control delete -share scomdblog -user-or-group Everyone -vserver infra_svm
share access-control delete -share scomdw -user-or-group Everyone -vserver infra_svm
share access-control delete -share scomdwlog -user-or-group Everyone -vserver infra_svm
share access-control delete -share wapdb -user-or-group Everyone -vserver infra_svm
share access-control delete -share wapdblog -user-or-group Everyone -vserver infra_svm

```

## 6. Add Permissions to the following accounts with NTFS full control for the shares.



```

share access-control create -share scsmdb -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scsmdblog -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scsmdw -user-or-group NET-PP\SQL-Admins -permission
full_control -vserver infra_svm

share access-control create -share scsmdwlog -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scdb -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scdblog -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scvmmdb -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scvmmdblog -user-or-group NET-PP\SQL-Admins -
permission full_Control -vserver infra_svm

share access-control create -share scomdb -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scomdblog -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scomdw -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share scomdwlog -user-or-group NET-PP\SQL-Admins -permission
full_control -vserver infra_svm

share access-control create -share wapdb -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

share access-control create -share wapdblog -user-or-group NET-PP\SQL-Admins -permission
full_Control -vserver infra_svm

```

## Configure Shared VHDX Files

Two shared virtual hard disks (VHDX) files will be created to provide storage to be used by SQL Server Analysis Services. Log into one of the Fabric Management host nodes and issue the following PowerShell cmdlets to create the database and log VHDX files for use by the SCSMAS virtual machine.

```

New-VHD -Path C:\ClusterStorage\Volume1\SCSMASDB.VHDX -Fixed -SizeBytes 8GB
New-VHD -Path C:\ClusterStorage\Volume1\SCSMASDBLOG.VHDX -Fixed -SizeBytes 4GB

```

## Configure the SQL Cluster to Use a File Share Witness

To change the management cluster to use the quorum disk, complete the following steps on one server only:

1. Open an SSH connection to NetApp cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Create a qtree in the SCVMM pool to house the infrastructure virtual machines (VMs).

```

qtree create -volume witness -qtree sql-witness -security-style ntfs -vserver infra_svm

```

3. Create the qtree quota policy for the infrastructure VM share.

```
quota policy rule create -policy-name default -volume witness -type tree -disk-limit 5g -target sql-witness -vserver infra_svm
```

4. Create the SMB share to house the infrastructure VMs–

```
share create -share-name sql-witness -path /witness/sql-witness -share-properties browsable, oplocks -vserver infra_svm
```

5. Remove the Everyone permission from the Witness share.

```
cifs share access-control delete -share sql-witness -user-or-group Everyone -vserver infra_svm
```

6. Add Permissions the following accounts with NTFS full control permissions over the Share:

- SQL Node 1
- SQL Node 2
- SQL Node 3
- SQL Node 4
- SQL Cluster Name Object (CNO)

```
share access-control create -share sql-witness -user-or-group NETAPP\SQL01$ -permission full_Control -vserver infra_svm  
  
share access-control create -share sql-witness -user-or-group NETAPP\SQL02$ -permission full_Control -vserver infra_svm  
  
share access-control create -share sql-witness -user-or-group NETAPP\SQL03$ -permission full_Control -vserver infra_svm  
  
share access-control create -share sql-witness -user-or-group NETAPP\SQL04$ -permission full_Control -vserver infra_svm  
  
share access-control create -share sql-witness -user-or-group NETAPP\SQL-Cluster01$ -permission full_Control -vserver infra_svm
```

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

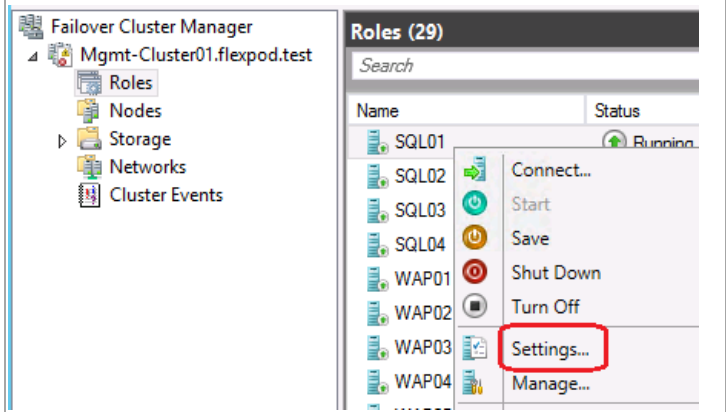
8. Set the Cluster to use the SMB share created earlier.

```
Set-ClusterQuorum -FileShareWitness \\infrasm\sql-witness
```

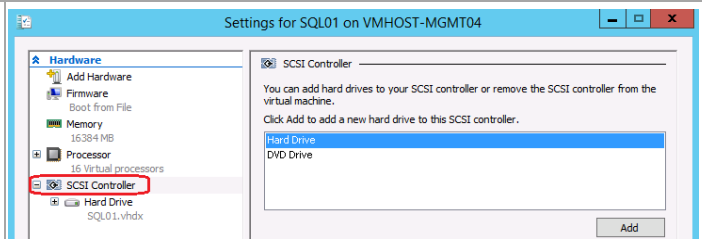
## Add a Shared VHDX to Cluster

Previously, two VHDX files were created to be used by the SQL Server Analysis Services instance that will be installed on this cluster. The disks need to be added to each node of the SQL cluster. Use the following steps on each node of the SQL cluster to add the shared VHDX.

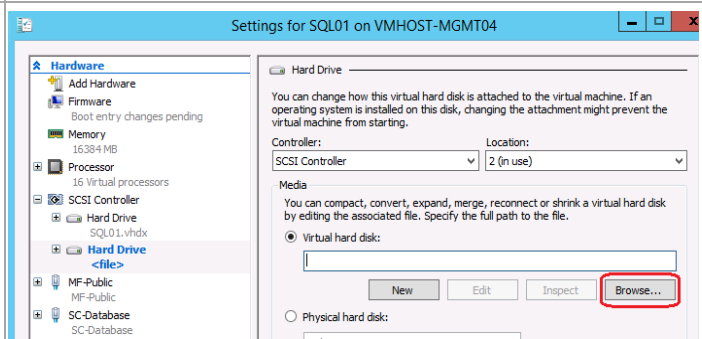
From the Failover Cluster Manager on the Fabric Management cluster, expand **Roles** and right-click on a node of the SQL cluster. Select **Settings...**



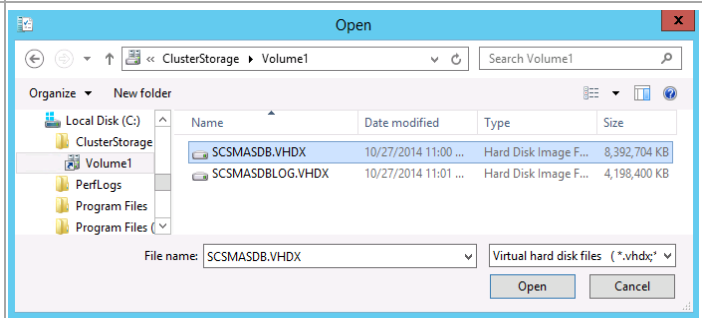
In the **Settings** window, select the **SCSI Controller**. Then select **Hard Drive** and click **Add**.



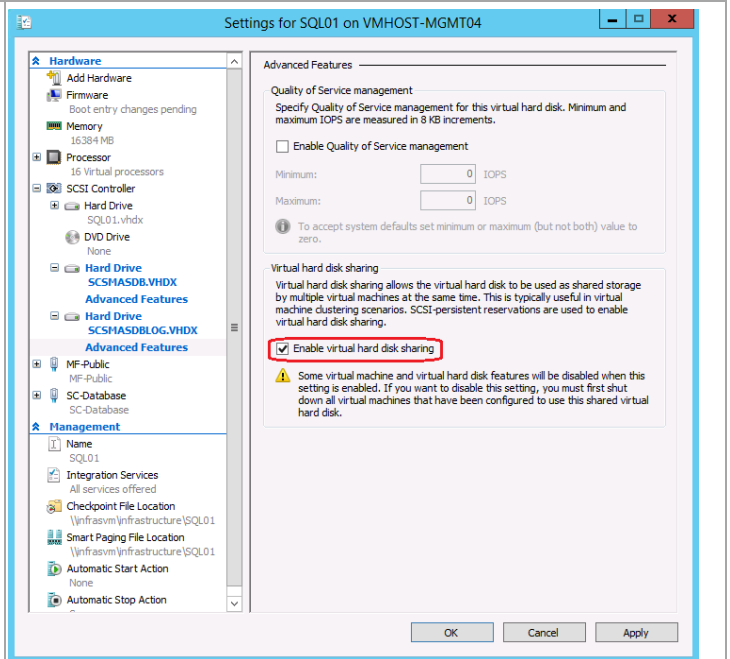
Select the **Browse...** button under **Hard Drive** to browse to the location of the shared VHDX files.



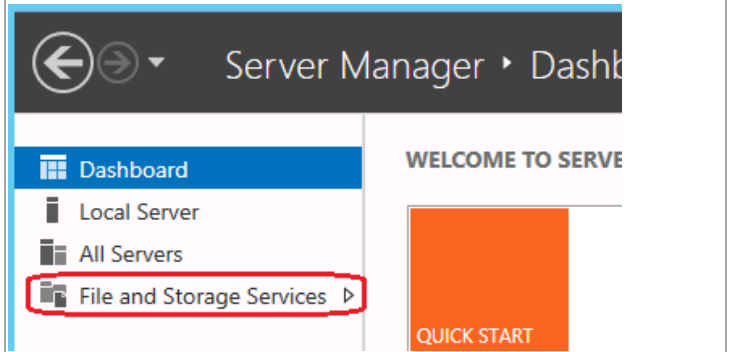
In the Windows Explorer window that opens, browse to **C:\ClusterStorage\Volume1**. Select the database VHDX file and click **Open**.



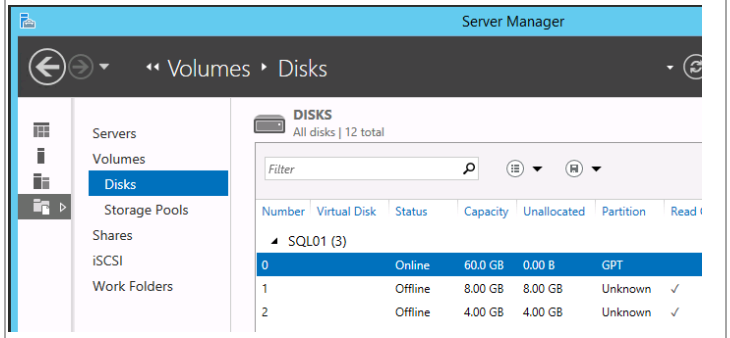
Back in the **Settings** window, expand the **Hard Drive** and click on **Advanced Features**. Repeat the previous three steps, starting with selection **SCSI Controller**, to add the VHDX for the database log VHDX file. Click **OK** to continue. Repeat for each node of the SQL cluster.



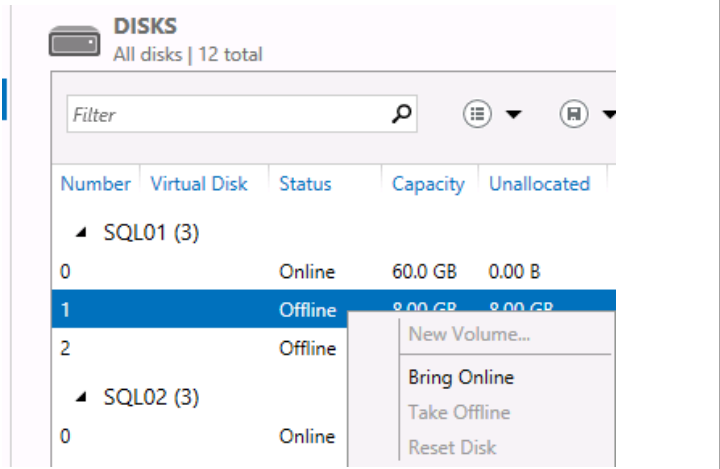
Log into the first node of the SQL Cluster. In Server Manager, select **File and Storage Services**.



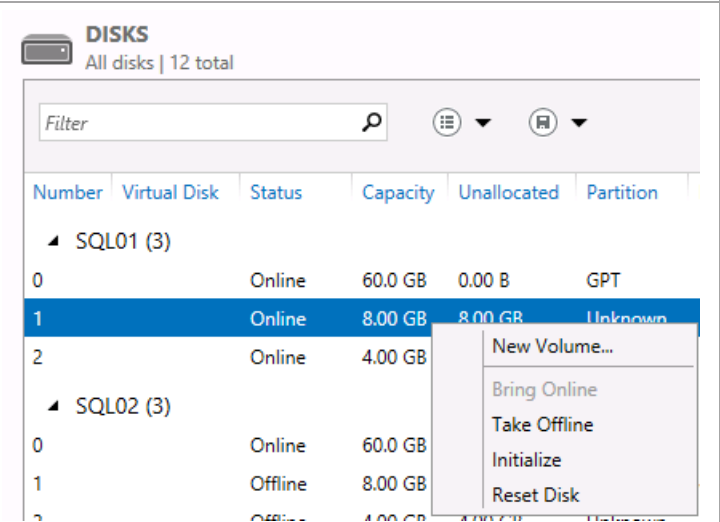
Select **Disks** to see the disks available to the system.



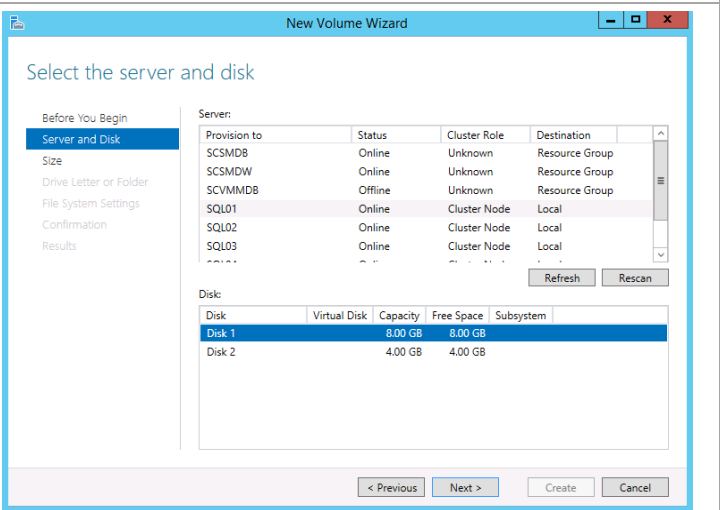
Right-click on the first **Offline** disk and select **Bring Online**. Ignore the warning about the disk already being online on another system. Repeat for the second Offline disk.



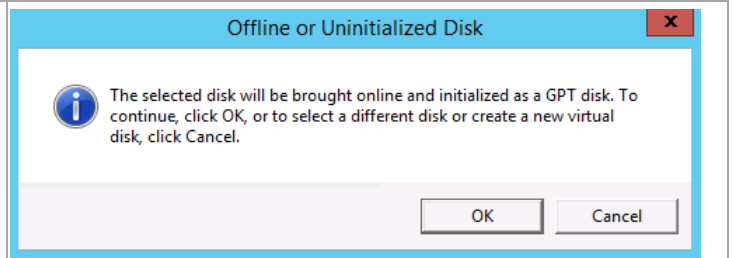
Right-click the 8GB disk and select **New Volume...**



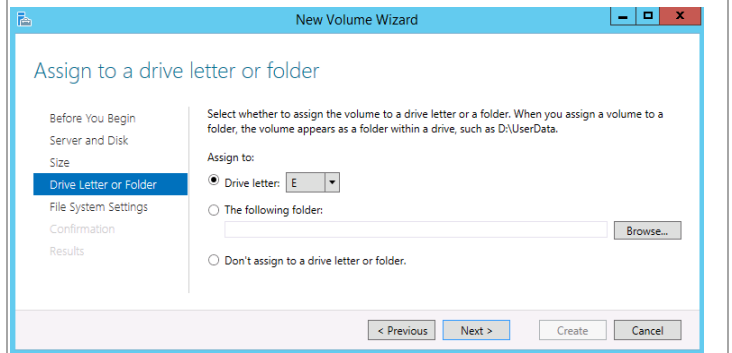
Click **Next** on the introductory screen for the New Volume Wizard. On the **Select the server and disk** window, select **Disk 1**. Click **Next** to continue.



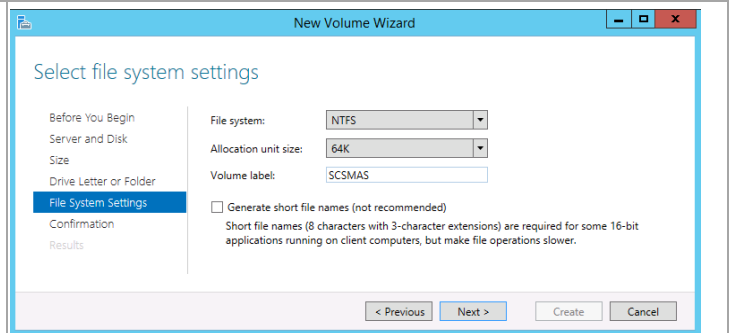
On the **Offline or Uninitialized Disk** window, click **OK**.  
Click **OK** on the following window to specify the default size of the volume.



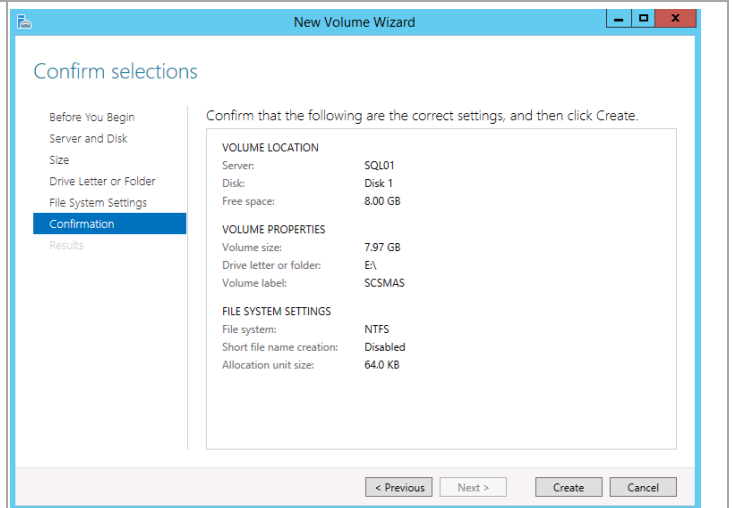
Assign the drive letter **E:** to the database VHDX. When you repeat this step for the database log VHDX, assign the drive letter **F:**.  
Click **Next** to continue.



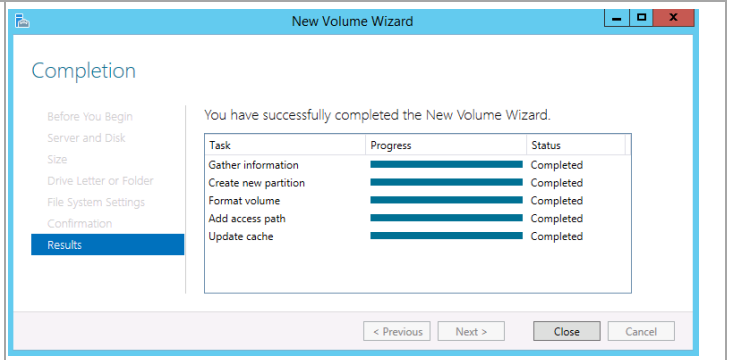
On the **Select file system Settings** windows, ensure the **NTFS** file system is selected. For the database VHDX, specify **64K** for the Allocation unit size. Leave it at the Default for the database log VHDX. Enter an appropriate **Volume label**.  
Click **Next** to continue.



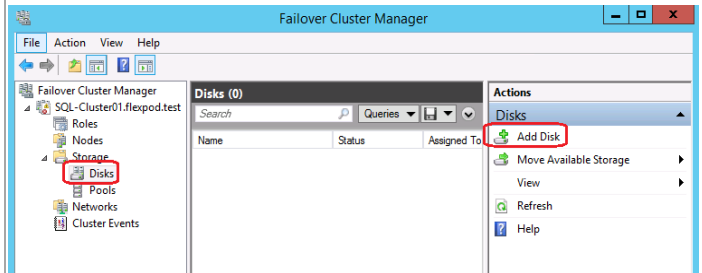
Confirm your settings and click **Create** to create the new volume.



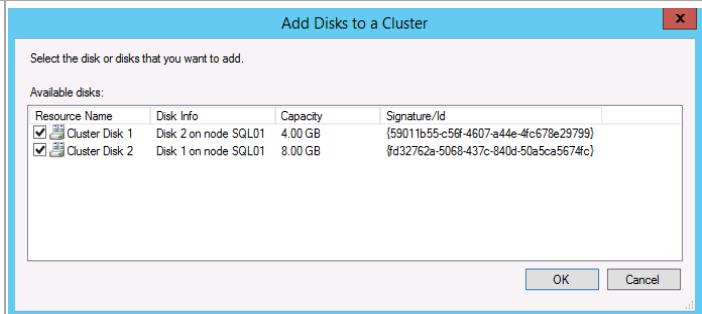
On the Completion window, click **Close**.  
 Repeat for the database log VHDX.  
 These steps have to be performed on **only one** of the cluster nodes.



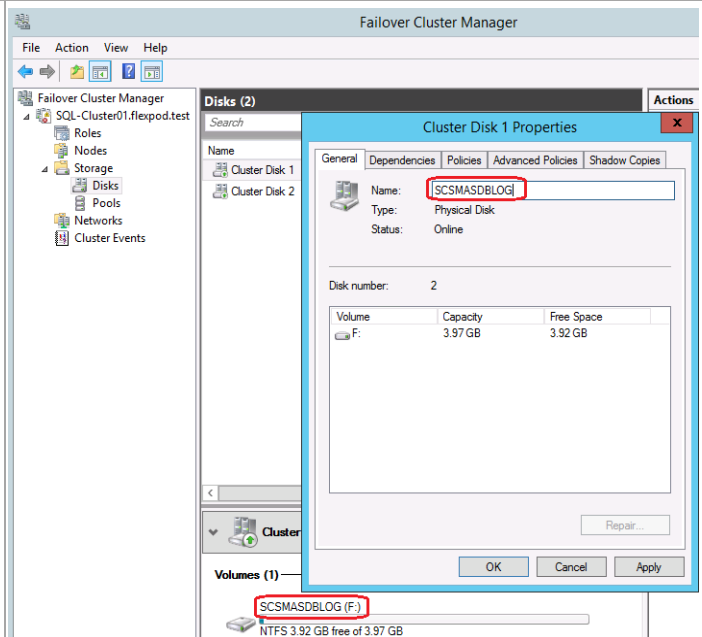
In the Failover Cluster Manager console, expand **Storage** and click on **Disks**. From the **Actions** menu, select **Add Disk**.



Ensure both disks are select and click **OK**.

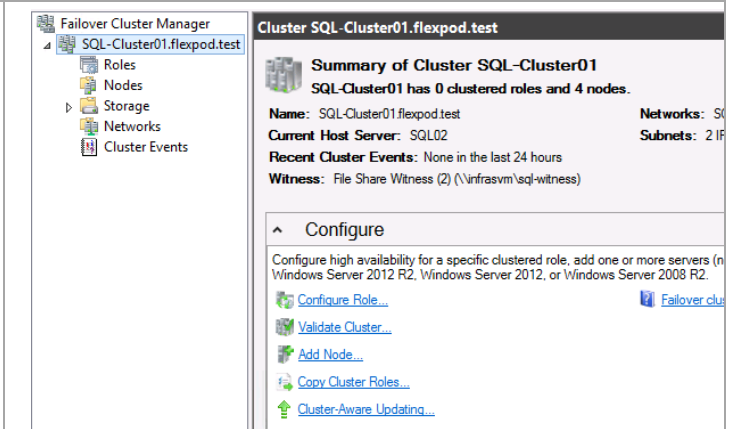


Right-click the first disk and select **Properties**.  
 Note the name of the disk in the window at the bottom and rename the disk properties name to match. Click **OK** to accept the name change.  
 Repeat for the other disk.

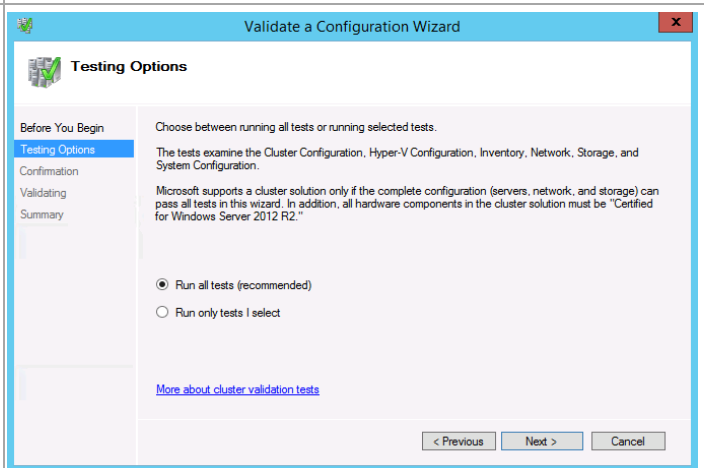


## Validate the SQL Server Cluster

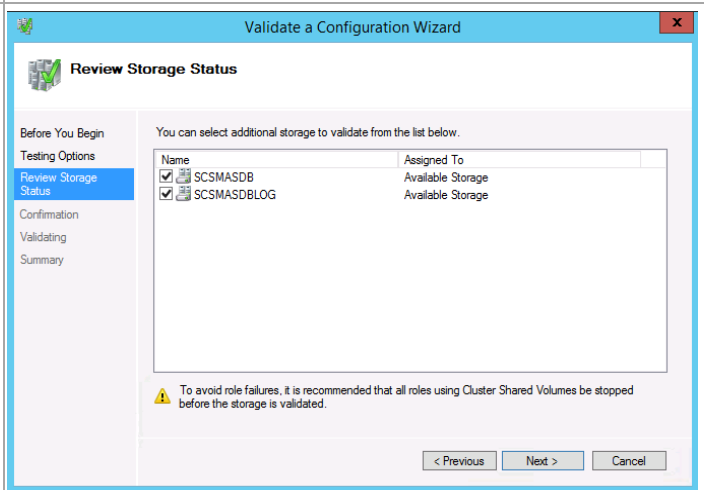
Select the SQL Server cluster in the left tree view and click Validate Cluster.



Select **Run all tests** and click Next.

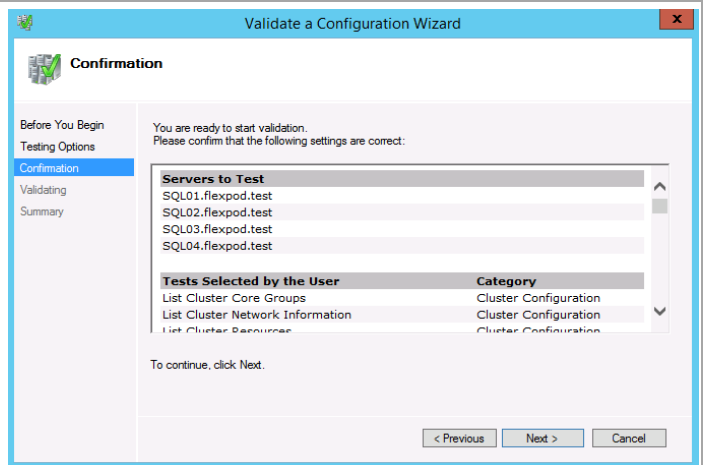


Select all disks on the cluster and click **Next**.





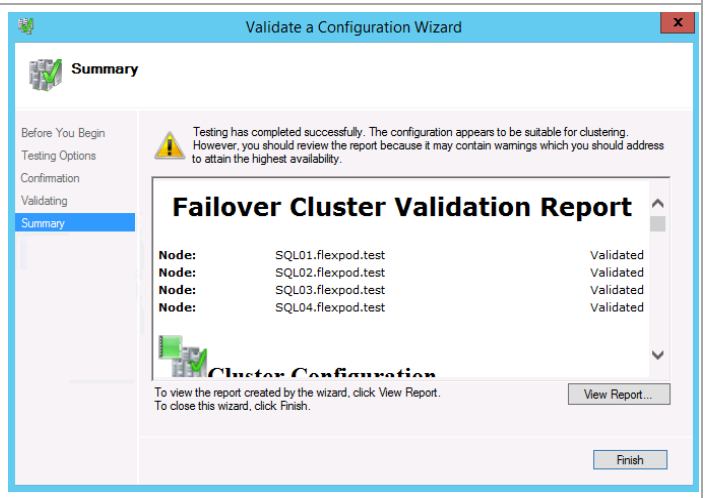
Confirm the selected options and click **Next**.



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

Because the second network is non-routed, it will not be able to reach other networks defined on the cluster. Therefore you will receive a number of warning messages like the following for each node. These warnings are expected to be reported by the validation wizard and can safely be disregarded.

*Node SQL02.flexpod.test is reachable from node SQL01.flexpod.test by multiple communication paths, but one or more of these paths experienced more than 10% packet loss.*



## 16.3 Install SQL Server 2012 SP2

### 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
<b>SQL Server Instance Name</b>	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
<b>SQL Server Instance Failover Cluster Network Name</b>	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
<b>SQL Server Instance DATA Storage</b>	\\Infrasvm \SCSMDB	\\Infrasvm \SCSMDW	Cluster Disk 1 Drive E:	\\Infrasvm \SCDB	\\Infrasvm \SCVMMDB	\\Infrasvm \SCOMDB	\\Infrasvm \SCOMDW

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
<b>SQL Server Instance LOG Storage</b>	\\Infrasvm\SCSMDBLOG	\\Infrasvm\SCSMDWLOG	Cluster Disk 2 Drive F:	\\Infrasvm\SCDBLOG	\\Infrasvm\SCVMMDBLOG	\\Infrasvm\SCOMDBLOG	\\Infrasvm\SCOMDWLOG
<b>Cluster Service Name</b>	SQL Server (SCSMDB)	SQL Server (SCSMDW)	SQL Server (SCSMAS)	SQL Server (SCDB)	SQL Server (SCVMMDB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)
<b>Clustered SQL Server Instance IP Address</b>	192.168.2.71	192.168.2.72	192.168.2.73	192.168.2.74	192.168.2.75	192.168.2.76	192.168.2.77
<b>Host Cluster Public Network Interface Subnet Mask</b>	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
<b>Host Cluster Public Network Interface Name</b>	SC-Database	SC-Database	SC-Database	SC-Database	SC-Database	SC-Database	SC-Database
<b>SQL Server Instance Listening TCP/IP Port</b>	10471	10472	10473	10474	10475	10476	10477
<b>SQL Server Instance Preferred Owners</b>	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.

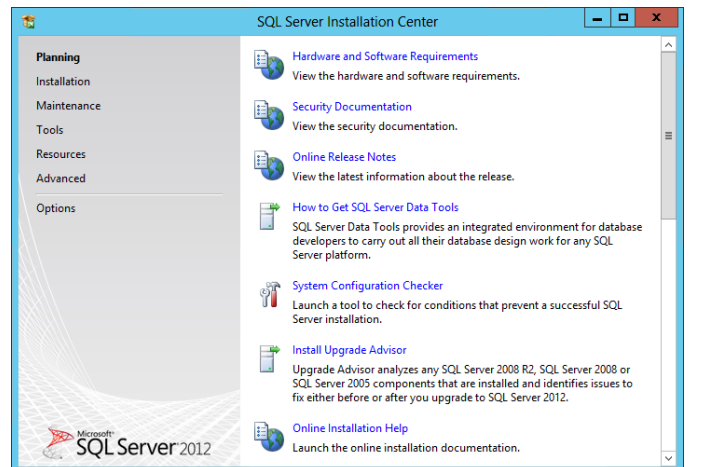
Perform the following steps on the **first fabric management SQL Server node** virtual machine with an account that has both local Administrator rights and permissions in AD DS to create the SQL Server CNOs.

As outlined before, Fast Track requires separate instances for each System Center product. The instances associated with these products are:

1. SCSMDB (Service Manager database instance).
2. SCSMDW (Service Manager Data Warehouse instance).
3. SCSMAS (Service Manager SQL Analysis Services instance).
4. SCDB (Shared App Controller, Orchestrator, Service Manager self-service portal Microsoft SharePoint® Foundation 2010 services and WSUS database instance).
5. SCVMMDB (Virtual Machine Manager database instance and optional WSUS database instance).
6. SCOMDB (Operations Manager database instance).
7. SCOMDW (Operations Manager Data Warehouse instance).

For multi-instance failover clusters, installation of SQL Server 2012 must be performed once for each instance. As such, these steps must be performed for each instance sequentially.

From the SQL Server 2012 SP2 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear. Select the **Installation** menu option.



From the **SQL Server Installation Center**, click the **New SQL Server failover cluster installation** link.



**New SQL Server failover cluster installation**  
Launch a wizard to install a single-node SQL Server 2012 failover cluster.

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.

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 8. Failed 0. Warning 0. Skipped 0.

Hide details << Re-run

[View detailed report](#)

Rule	Status
Setup administrator	Passed
Setup account privileges	Passed
Restart computer	Passed
Windows Management Instrumentation (WMI) service	Passed
Consistency validation for SQL Server registry keys	Passed
Long path names to files on SQL Server installation media	Passed
SQL Server Setup Product Incompatibility	Passed
.NET 2.0 and .NET 3.5 Service Pack 1 update for Windows 2008 ...	Passed

OK Cancel

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

Microsoft SQL Server 2012 Service Pack 1 - System Configuration Check Report

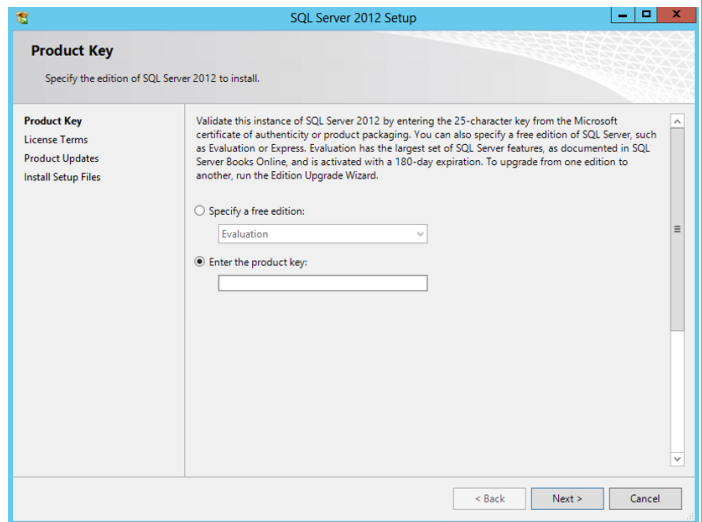
Computer Name(s): SRVSQLN01  
Report Date/Time: 2/1/2013 10:06 PM  
Saved to Directory: C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap\Log\20130201\_220625\SystemConfigurationCheck\_Report.htm

Rule Name	Rule Description	Result	Message/Corrective Action
<b>GlobalRules: SQL Server 2012 Setup configuration checks for rules group 'GlobalRules'</b>			
NotRebootPackageDownLevel	This rule determines whether the computer has the required update package for .NET Framework 2.0 or .NET Framework 3.5 SP1 that is needed for a successful installation of Visual Studio components that are included in SQL Server.	Not applicable	This rule does not apply to your system configuration.
ServerCore48BitCheck	Checks if this version of SQL Server is 64-bit.	Not applicable	This rule does not apply to your system configuration.
ServerCorePlatformCheck	Checks if this version of SQL is supported on the currently running Windows Server Core OS.	Not applicable	This rule does not apply to your system configuration.
AcPermissionsFacet	Checks if the SQL Server registry keys are consistent.	Passed	SQL Server registry keys are consistent and can support SQL Server installation or upgrade.
HasSecurityBackupAndDebugPrivilegesCheck	Checks whether the account that is running SQL Server Setup has the right to back up files and directories, the right to manage auditing and the security log and the right to debug programs.	Passed	The account that is running SQL Server Setup has the right to back up files and directories, the right to manage auditing and security log and the right to debug programs.
MediaPathLength	Checks whether the SQL Server installation media is too long.	Passed	The SQL Server installation media is not too long.
NotRebootPackage	This rule determines whether the computer has the required update package for .NET Framework 2.0 or .NET Framework 3.5 SP1 that is needed for a successful installation of Visual Studio components that are included in SQL Server.	Passed	This computer has the required update package.
RebootRequiredCheck	Checks if a pending computer restart is required. A pending restart can cause Setup to fail.	Passed	The computer does not require a restart.
SetupCompatibilityCheck	Checks whether the current version of SQL Server is compatible with a later installed version.	Passed	Setup has not detected any incompatibilities.
ThreadHasAdminPrivilegeCheck	Checks whether the account running SQL Server Setup has administrator rights on the computer.	Passed	The account running SQL Server Setup has administrator rights on the computer.
WmiServiceStateCheck	Checks whether the WMI service is started and running on the computer.	Passed	The Windows Management Instrumentation (WMI) service is running.

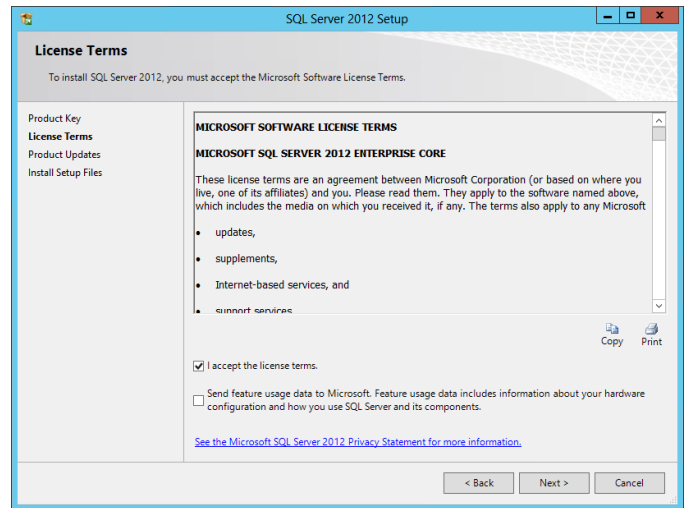
Rules Documentation: <http://go.microsoft.com/fwlink/?linkid=194954>  
Community: <http://go.microsoft.com/fwlink/?linkid=194952>  
Setup Help File: <http://go.microsoft.com/fwlink/?linkid=193183>

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

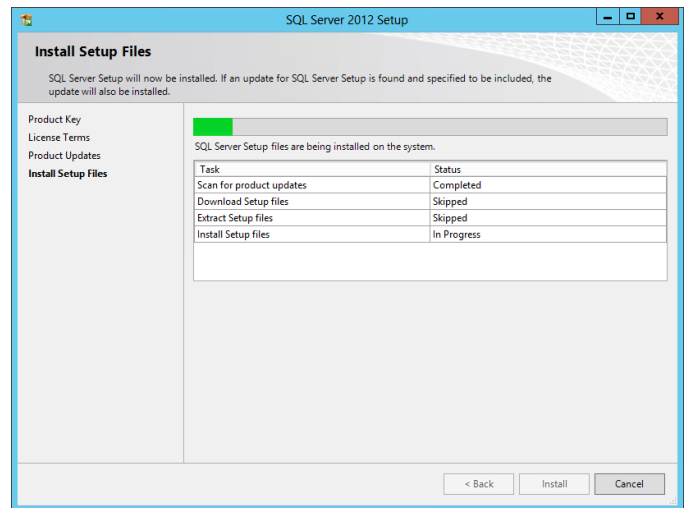
**Note:** if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



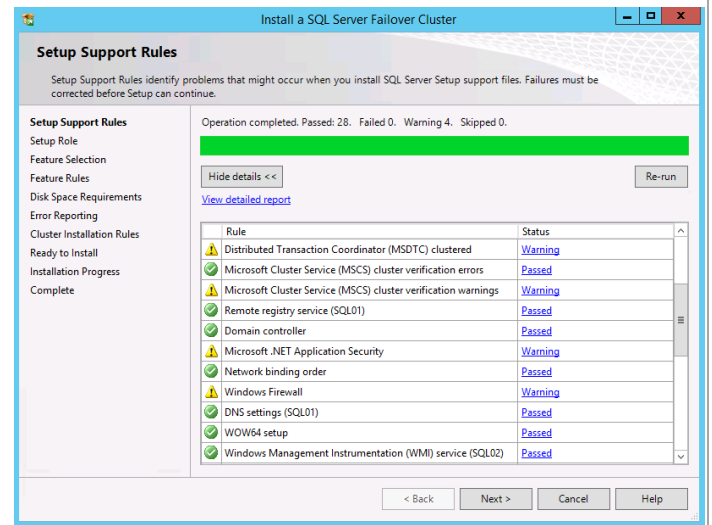
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization’s policies and click **Next** to continue.



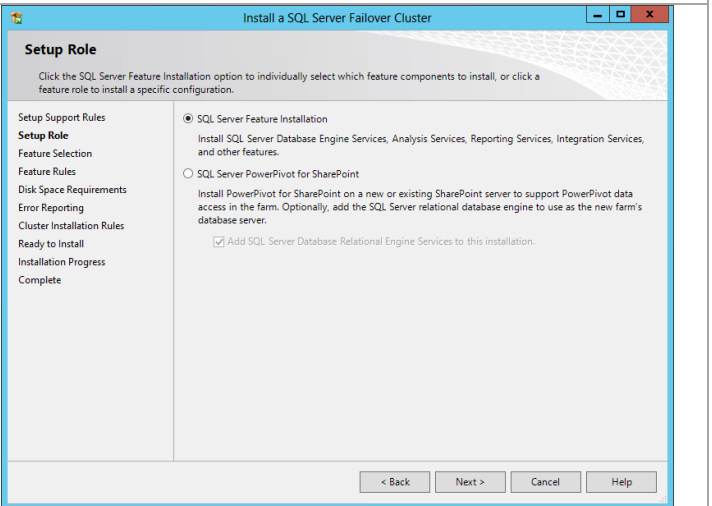
The **Install Setup Files** process runs automatically.



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, which are acceptable. Note that the use of MSDTC is not required for the System Center 2012 SP2 environment. Click **Next** to continue.



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

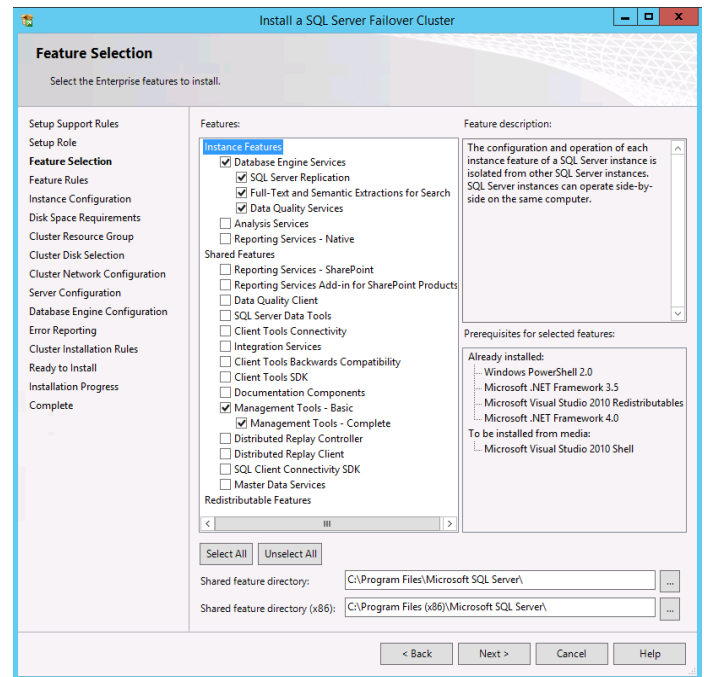


In the **Feature Selection** dialog, features for the various instances will be selected. Note that not all features are supported for failover cluster installations, so the features for Fast Track are limited to the features as listed below. SQL Server with failover clusters requires the selection of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

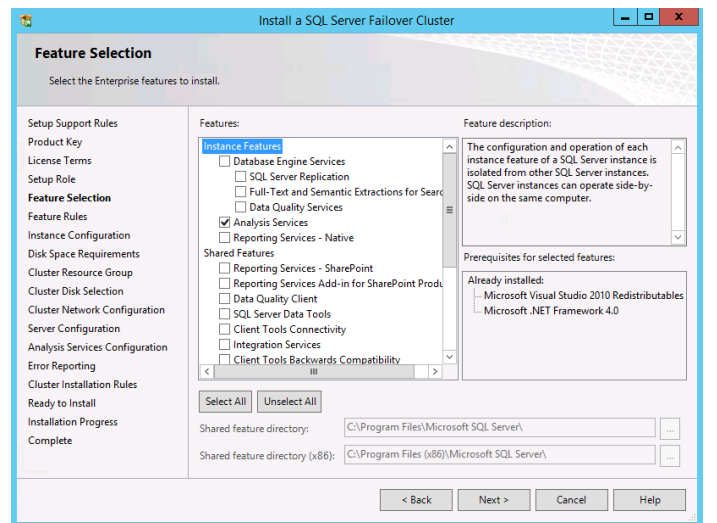
- SCDB
  - Database Engine Services
- SCOMDB
  - Database Engine Services
- SCOMDW
  - Database Engine Services
- SCSMAS
  - Analysis Services
- SCSMDB
  - Database Engine Services
- SCSMDW
  - Database Engine Services
- SCVMMDB
  - Database Engine Services

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

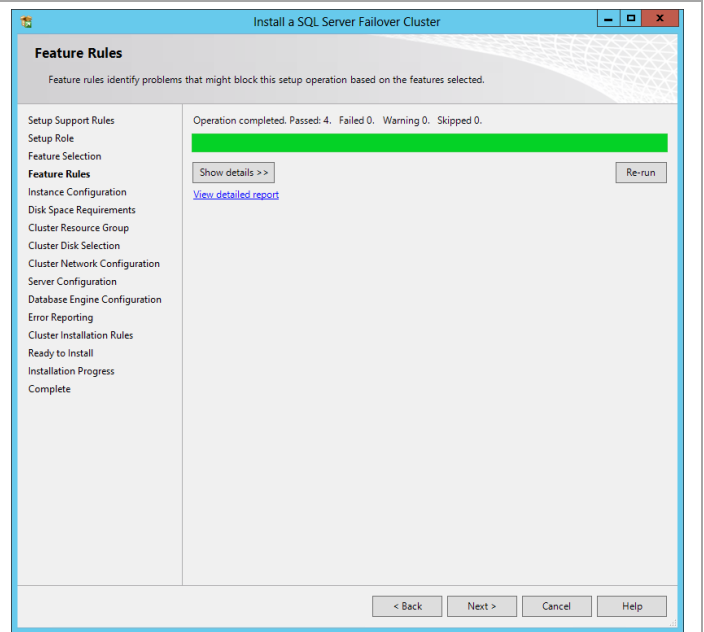
## Database Engine Services (all instances except SCSMAS):



## Analysis Services (SCSMAS instance only):



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



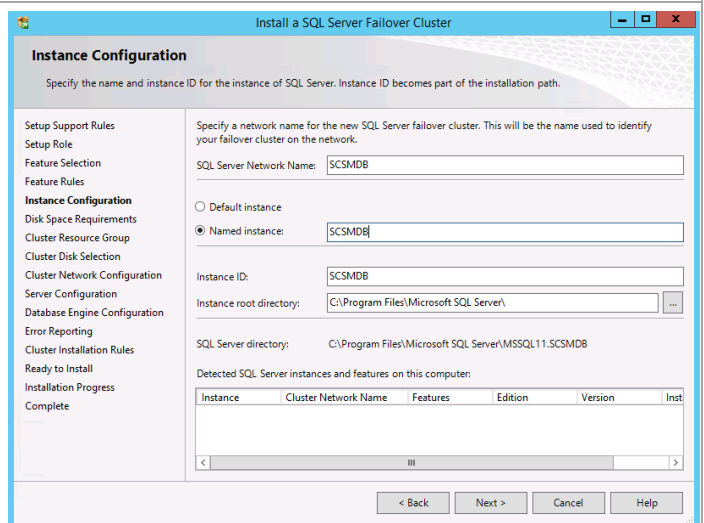
In the **Instance Configuration** dialog, make the following selections (refer to the worksheet created earlier):

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

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

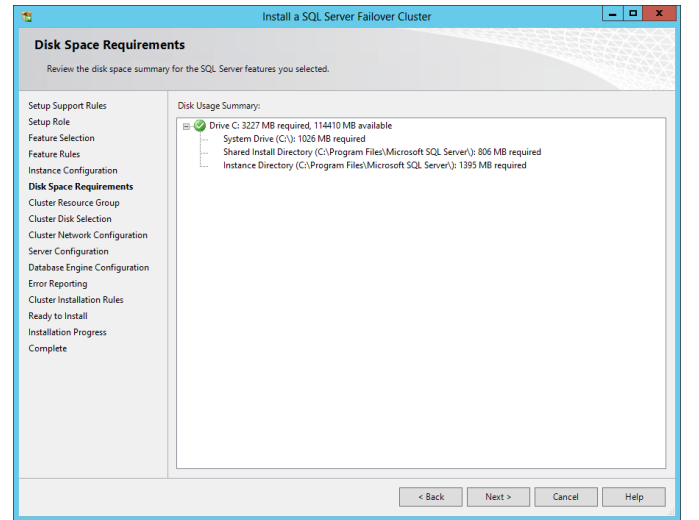
- **Instance ID** – specify the instance name being installed. Verify that it matches the **Named instance** value.
- **Instance root directory** – accept the default location of `%ProgramFiles%\Microsoft SQL Server`.

Click **Next** to continue.

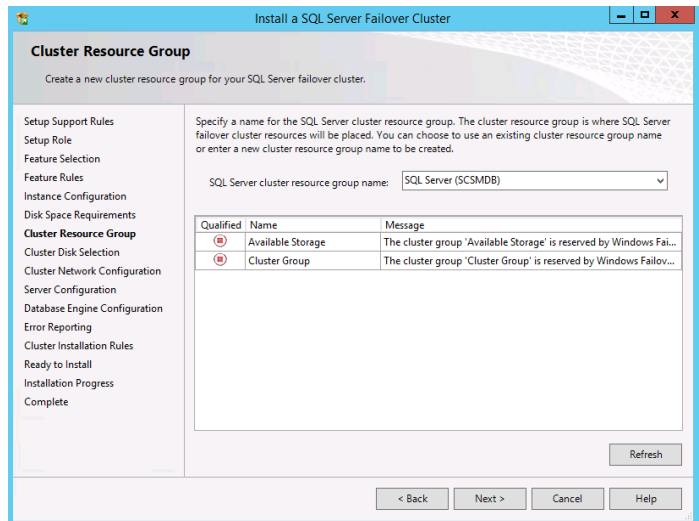




In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.

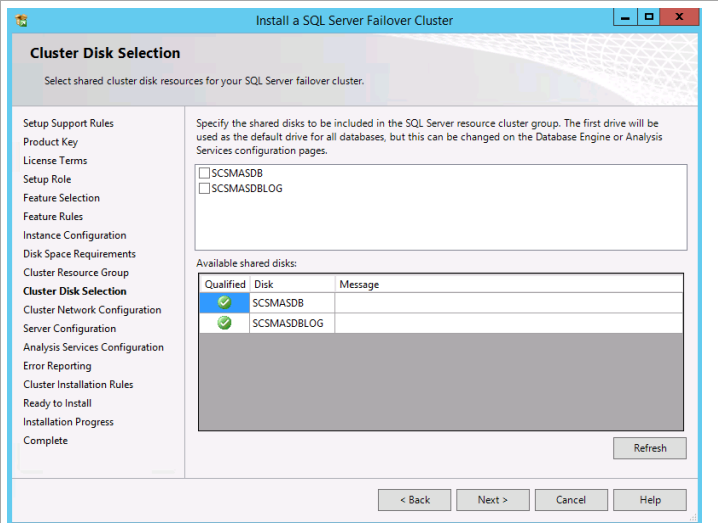


In the **Cluster Resource Group** dialog, in the **SQL Server cluster resource group name** drop-down menu, accept the default value of **SQL Server (<InstanceName>)**. Click **Next** to continue.

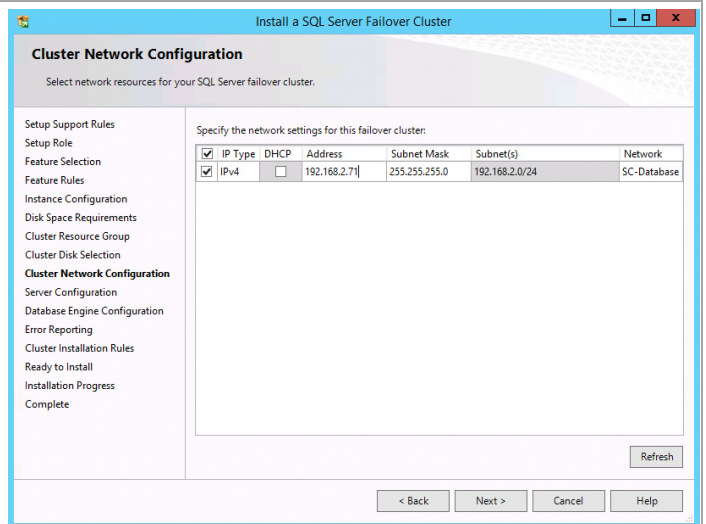


Depending on what and when you are installing, the **Cluster Disk Selection** window will show things differently. If you have not yet installed the Analysis Services instance the two disks provisioned for SQL Server Analysis Services will show as available. Ensure that the check boxes are cleared for any instance installation except the Analysis Services installation. **ONLY** for the Analysis Services installation should both disks be selected.

After you have installed the Analysis Services instance, the disks will no longer show in the top part of the window and the bottom part will reflect that fact that the disks have already been assigned.

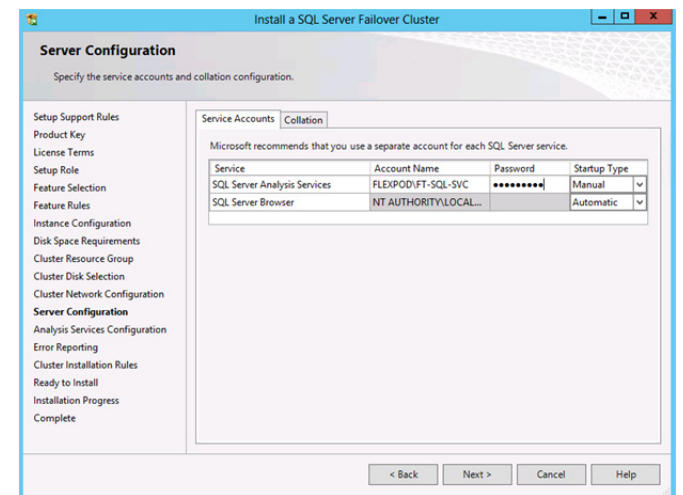
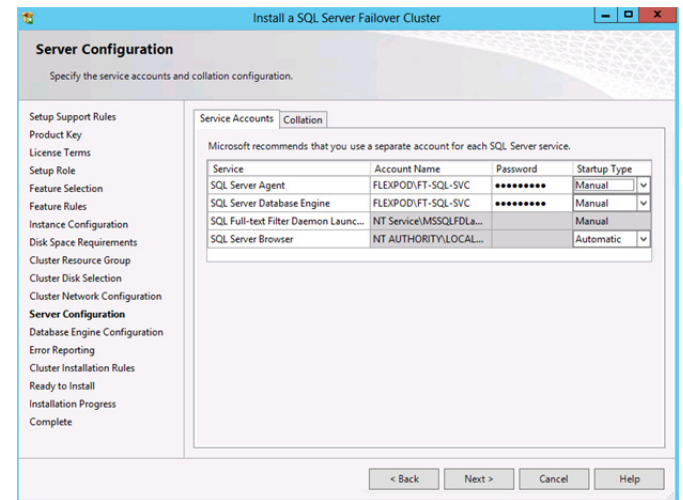


In the **Cluster Network Configuration** dialog, refer to the worksheet created earlier to assign the correct IP for each instance. Clear the **DHCP** check box if you are using static addressing and enter the IP address in the **Address** field text box. When complete, click **Next** to continue.

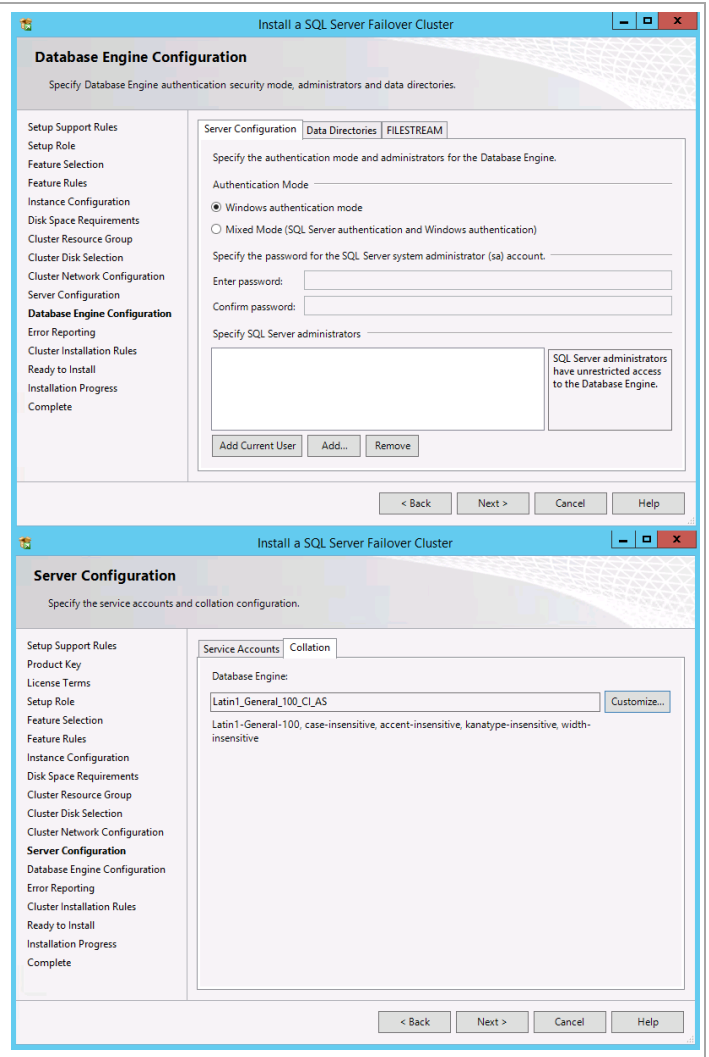


In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services.

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



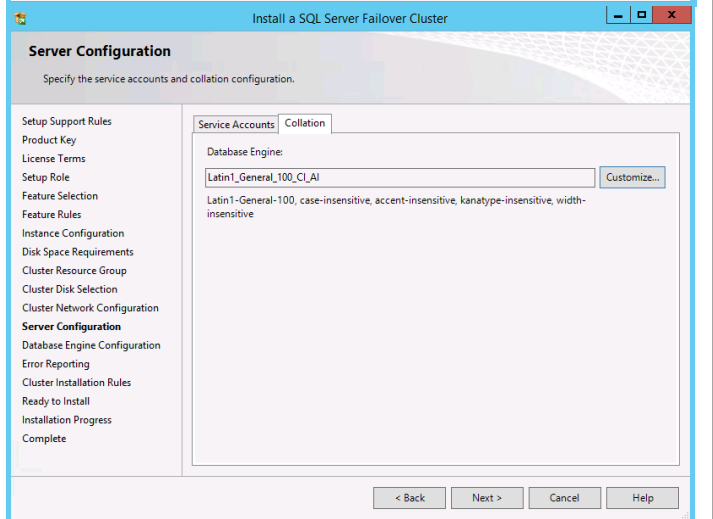
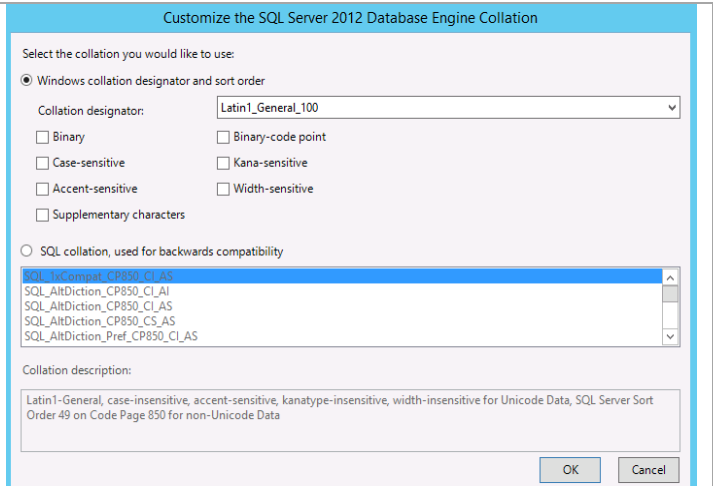
In the same **Server Configuration** dialog, select the **Collation** tab. Accept the default collation in the **Database Engine** field (unless multiple language support is required in Service Manager<sup>3</sup>) and click **Next** to continue.



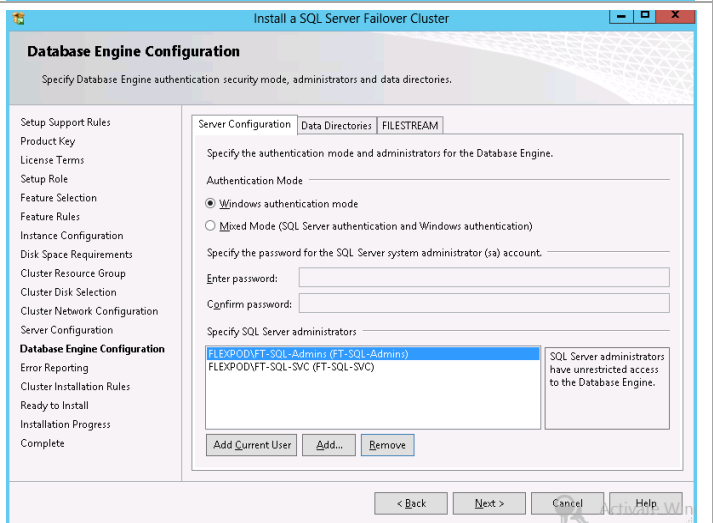
<sup>3</sup> <http://social.technet.microsoft.com/wiki/contents/articles/7784.collation-in-system-center-2012-service-manager.aspx>.

**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.

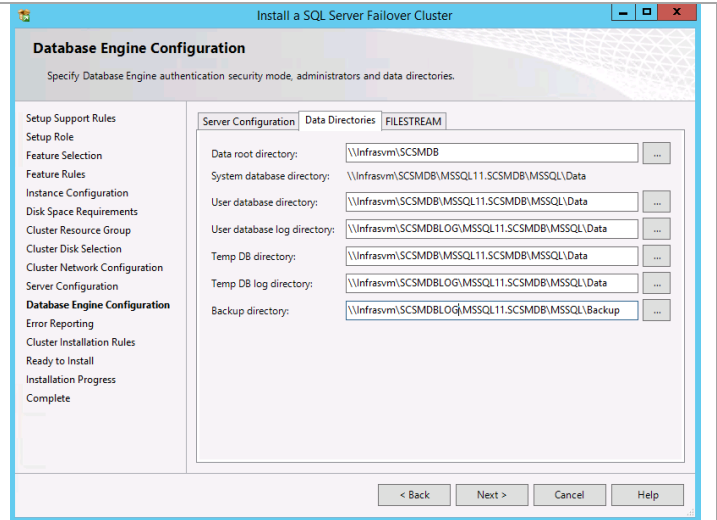


In the **Database Engine Configuration** dialog, select the **Account Provisioning** tab. In the **Authentication Mode** section, select the **Windows authentication mode** option. In the **Specify SQL Server administrators** section, click the **Add Current User** button to add the current installation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

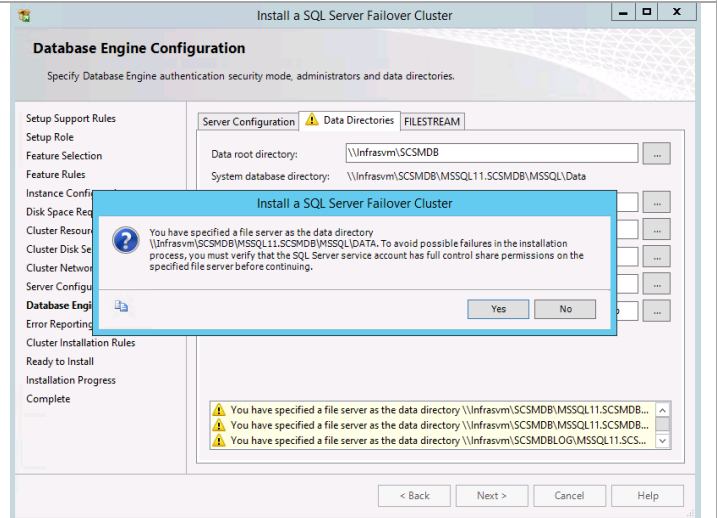


In the same **Database Engine Configuration** dialog, select the **Data Directories** tab. The proper SMB share associated with the SQL Server database and log locations must be specified. To redirect log files by default to their SMB resource, change the SMB share in the **User database log directory** and **Temp DB log directory** text boxes. It is also recommended to change the Backup Directory to a separate location such as the log share. 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 SMB share if performance is not adequate using the two primary SMB shares.



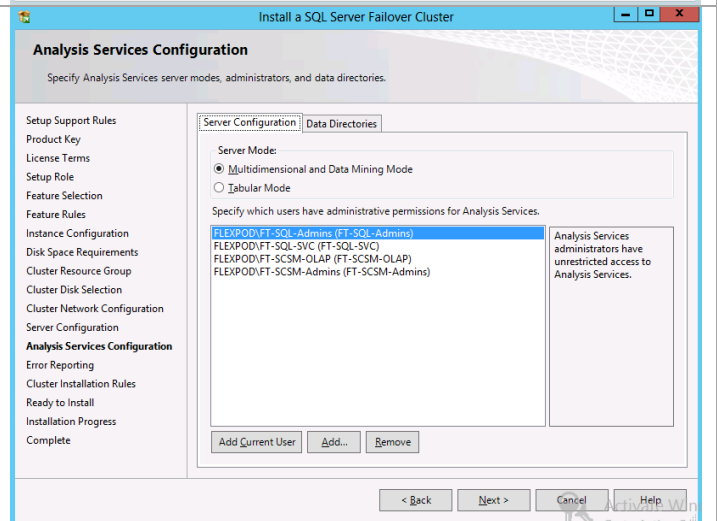
When you click Next to continue you will receive a warning telling you to ensure you have included the SQL service account with full permissions on the share. Since this completed during the creation of the shares, you can click **Yes** to continue.



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

Service Manager instance:

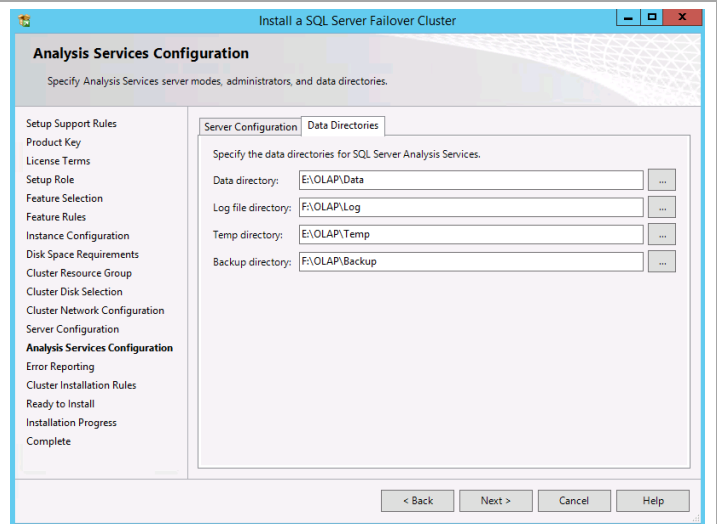
- Fast Track SQL Server Admins group
- Fast Track SQL Server Service account
- Fast Track SM Admins group
- Fast Track SM OLAP account



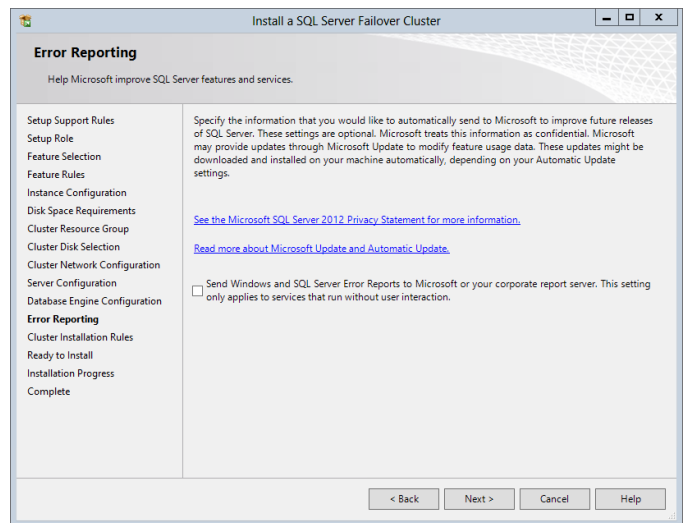
For instances with Analysis Services, use the following configuration:

On the **Data Directories** tab, set the Data directory, and Temp directory to the cluster disk configured for the database files. Set the Log file directory and the Backup directory to the cluster disk configured for the log files. Do not change the folder structure unless your organization has specific standards for this.

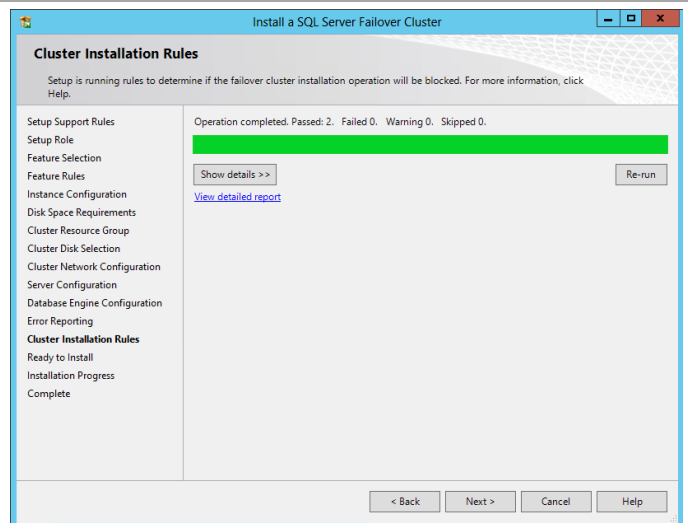
When complete, click **Next** to continue.



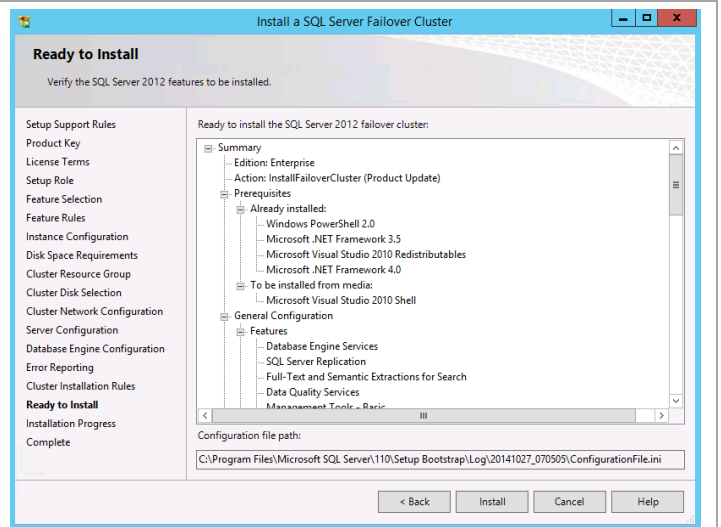
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



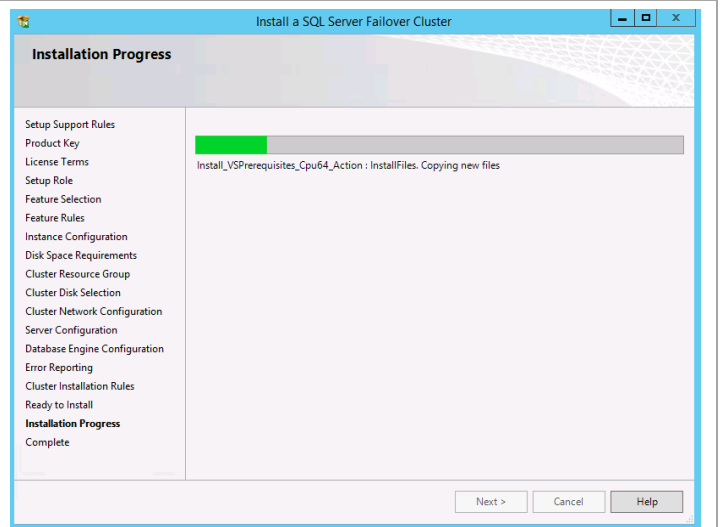
In the **Cluster Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



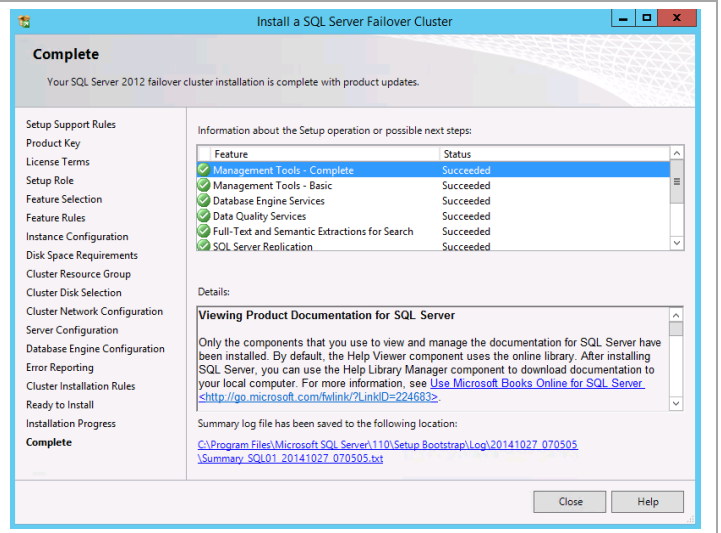
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



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

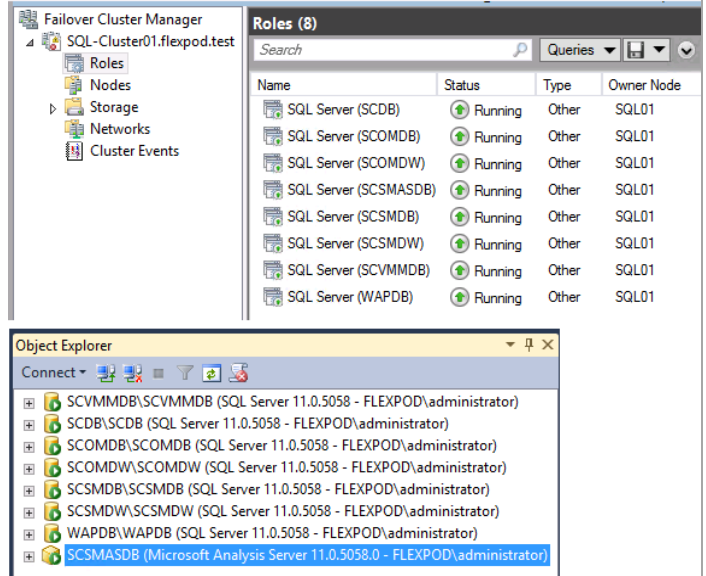


When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



Repeat these steps for each associated SQL Server instance required for Fast Track installation (eight instances total).

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



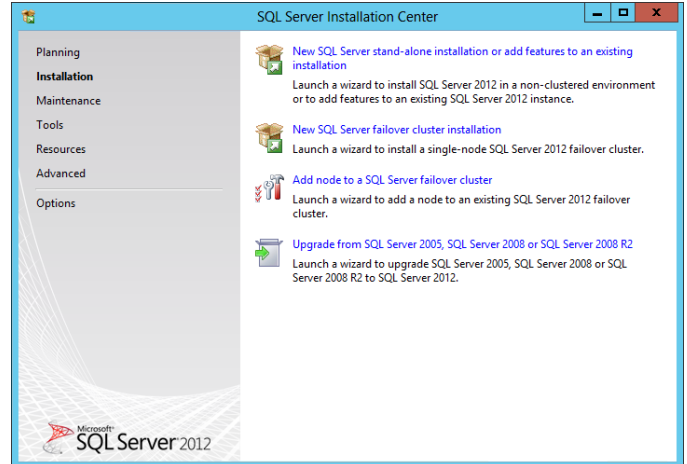


## Install the SQL Server Named Instances on Other Guest Cluster Nodes

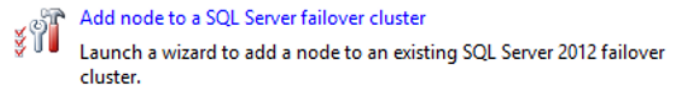
When the creation of all required SQL Server instances on Node 1 is complete, the other nodes can be added to each instance of the cluster. Follow the steps below to begin the installation of additional nodes of the cluster.

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

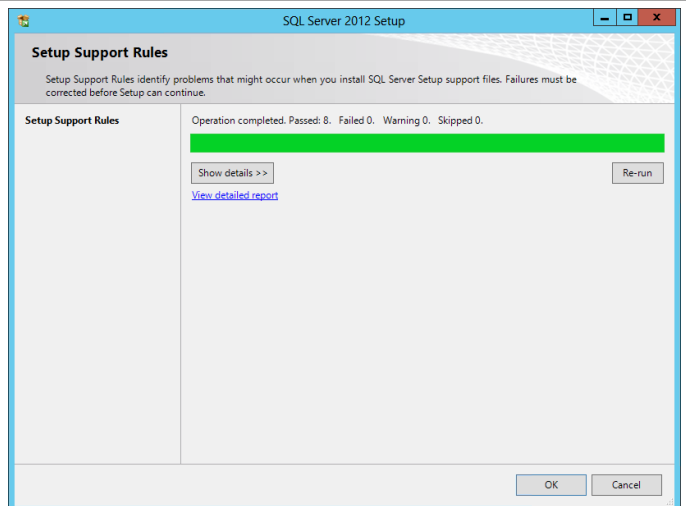
From the SQL Server 2012 SP2 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear.



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

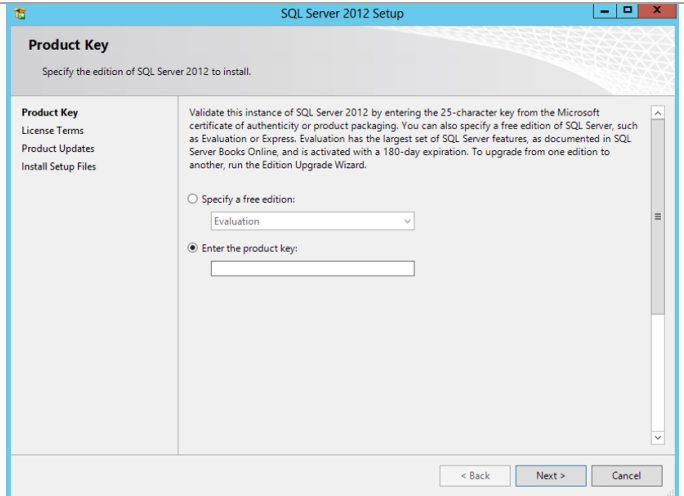


The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

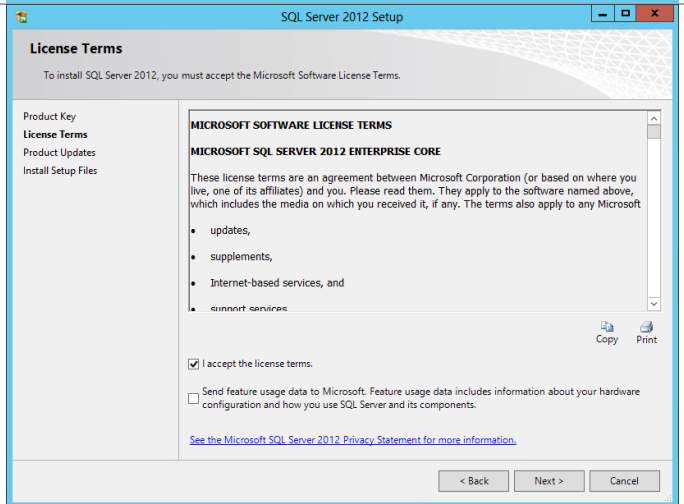


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

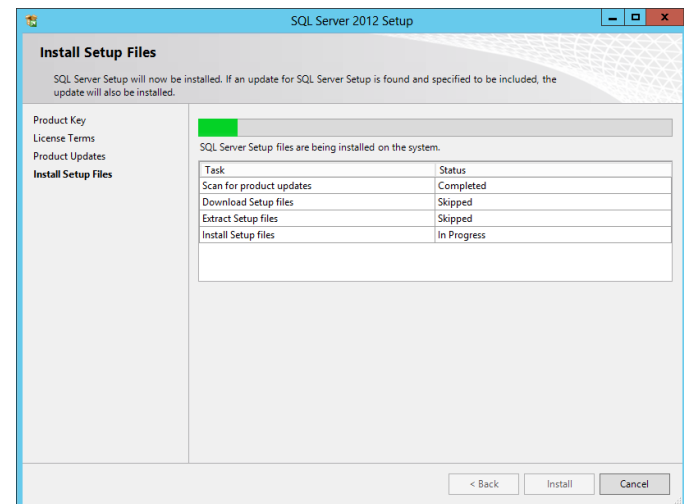
**Note:** If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



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

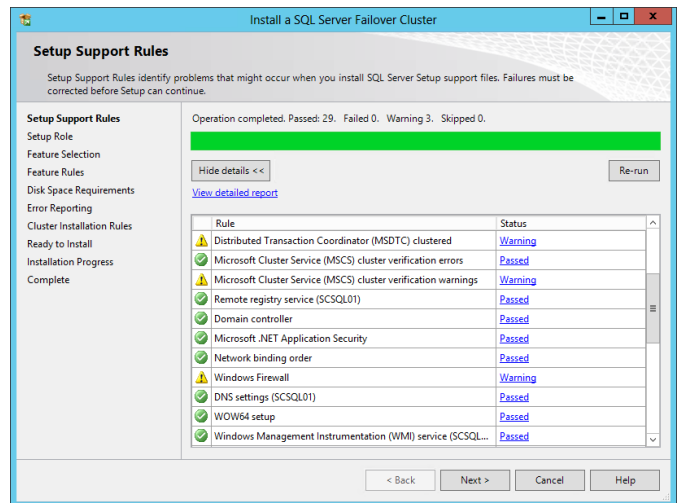


In the **Install Setup Files** dialog, click **Install** and allow the support files to install.

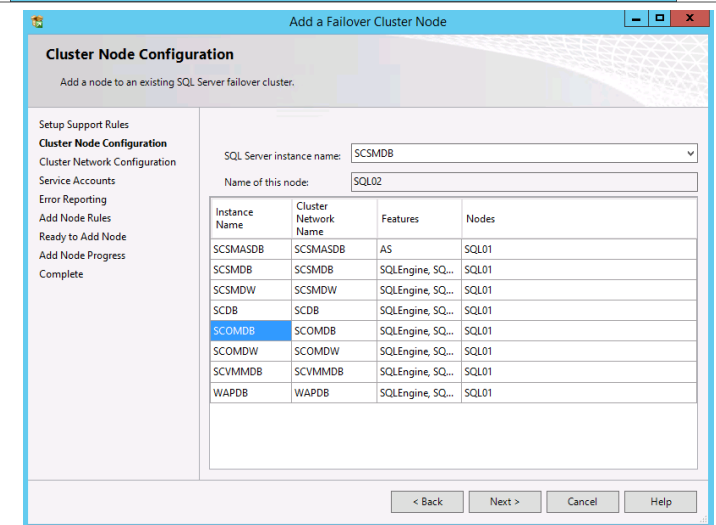


In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Click **Next** to continue.

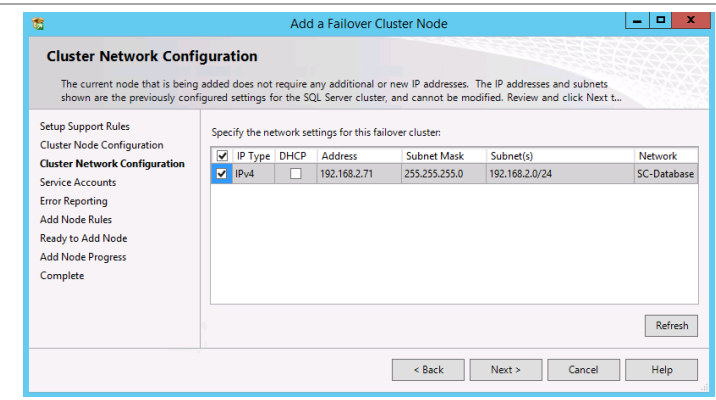
**Note:** The use of MSDTC is not required for the System Center 2012 SP1 environment.



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

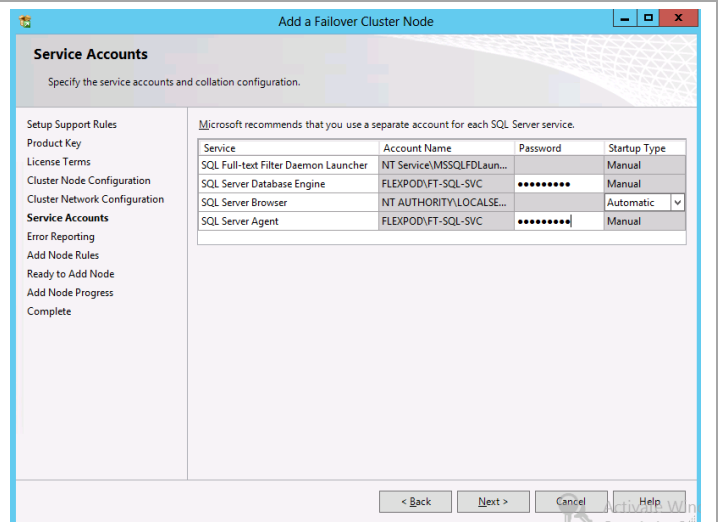


In the **Cluster Network Configuration** dialog, the network configuration values are displayed and set based on the existing failover cluster instance values from the first node and cannot be modified. Click **Next** to continue.

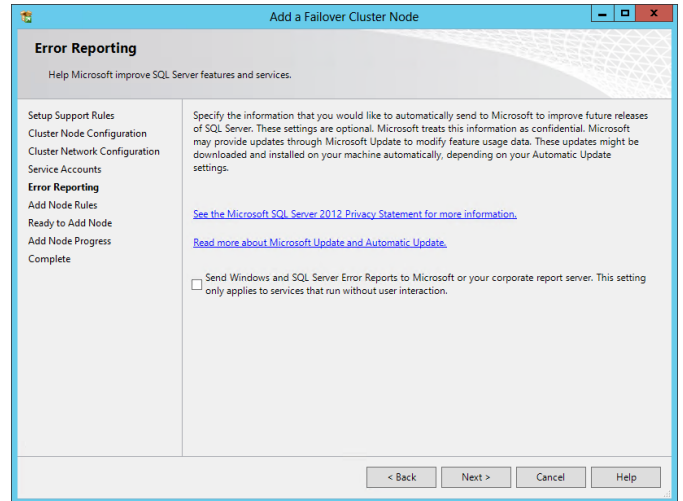


In the **Service Accounts** dialog, specify the Fast Track SQL Server Service Account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services. When complete, click **Next** to continue.

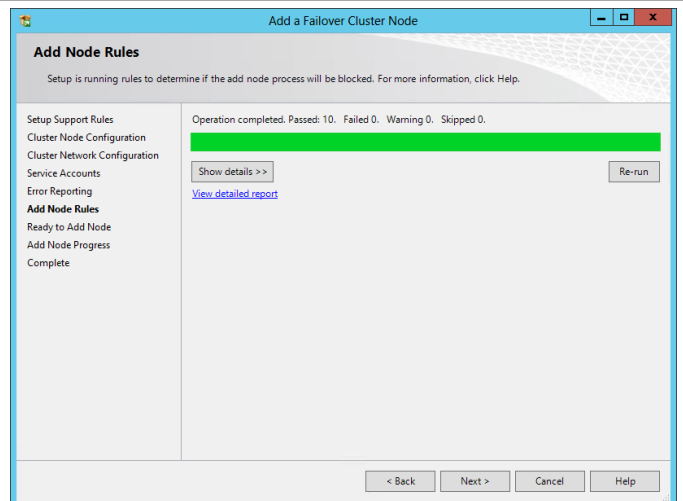
**Note:** For the SCSMAS instance only, an additional password must be supplied for the **SQL Server Analysis Services** service account.



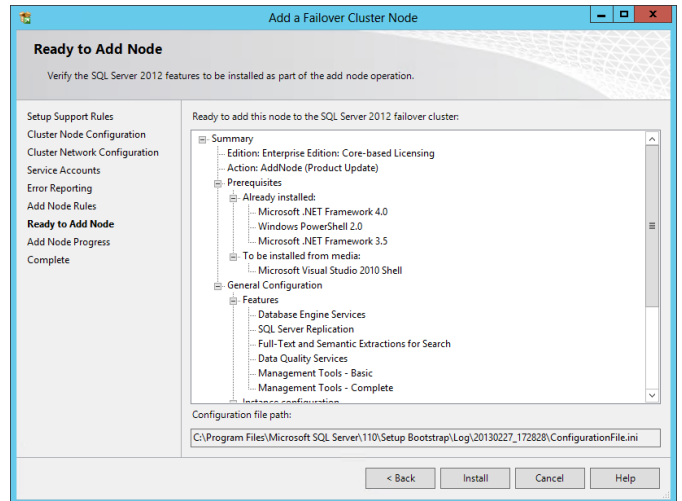
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



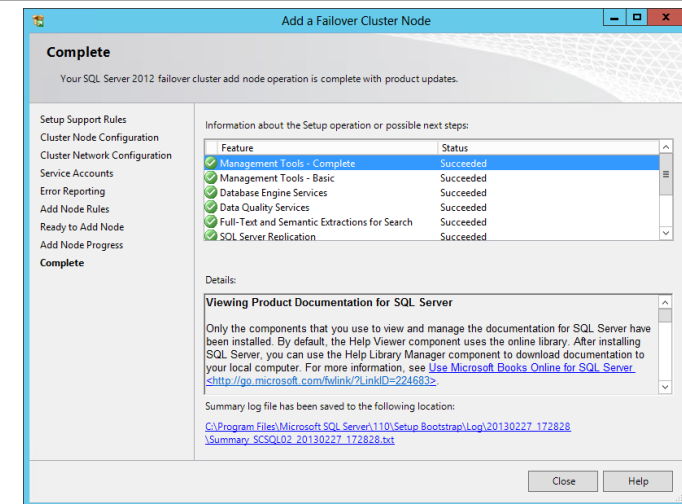
In the **Add Node Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

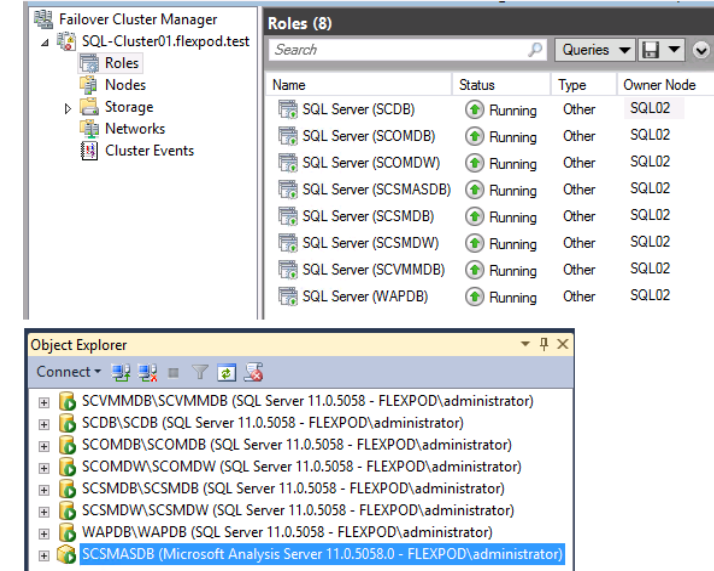


When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



Repeat these steps for each associated SQL Server instance required for Fast Track installation (eight instances total).

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



## 16.4 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.

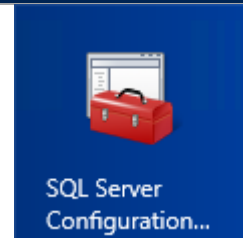
**Note:** This process is described in TechNet<sup>4</sup> and instructions are provided in this document.

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

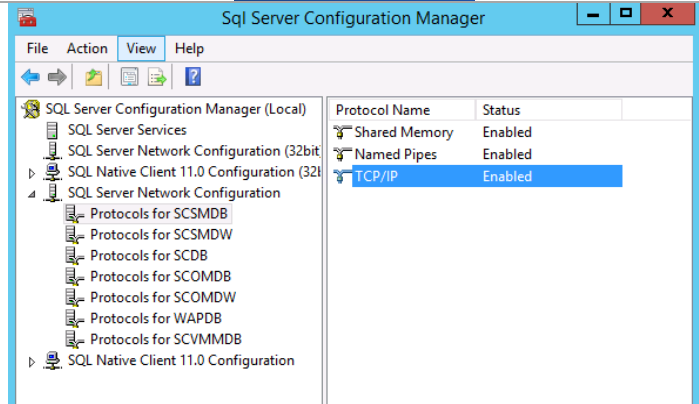
Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt execute the following command:  
**netstat -b**  
 Notice the existing dynamic ports used by the SQLSERVER.EXE sessions.

```
TCP 192.168.2.22:49917 SCDB:60480 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:49929 SCDB:60480 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:49930 SCDB:60480 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:49956 SCOMDB:64796 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:49969 SCOMDB:64796 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:49970 SCOMDB:64796 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:49998 SCOMDW:65186 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:50014 SCOMDW:65186 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50015 SCOMDW:65186 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50066 SCSMDB:63899 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:50081 SCSMDB:63899 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50082 SCSMDB:63899 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50116 WAPDB:54227 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:50129 WAPDB:54227 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50130 WAPDB:54227 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50226 SCSMDW:52501 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:50239 SCSMDW:52501 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50240 SCSMDW:52501 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50494 SCVMMDB:55296 ESTABLISHED
[rhs.exe]
TCP 192.168.2.22:50504 SCVMMDB:55296 ESTABLISHED
[SQLAGENT.EXE]
TCP 192.168.2.22:50505 SCVMMDB:55296 ESTABLISHED
[SQLAGENT.EXE]
```

On the SQL Server node that owns the SQL instances open **SQL Configuration Manager**.



In the **SQL Server Configuration Manager** console pane, expand the **SQL Server Network Configuration** node and then expand the **Protocols for the <instance name>** node. When selected, double-click **TCP/IP** from the available protocol names to observe its properties.



<sup>4</sup> Configure a Server to Listen on a Specific TCP Port - [http://technet.microsoft.com/en-us/library/ms177440\(v=sql.110\).aspx](http://technet.microsoft.com/en-us/library/ms177440(v=sql.110).aspx)

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

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

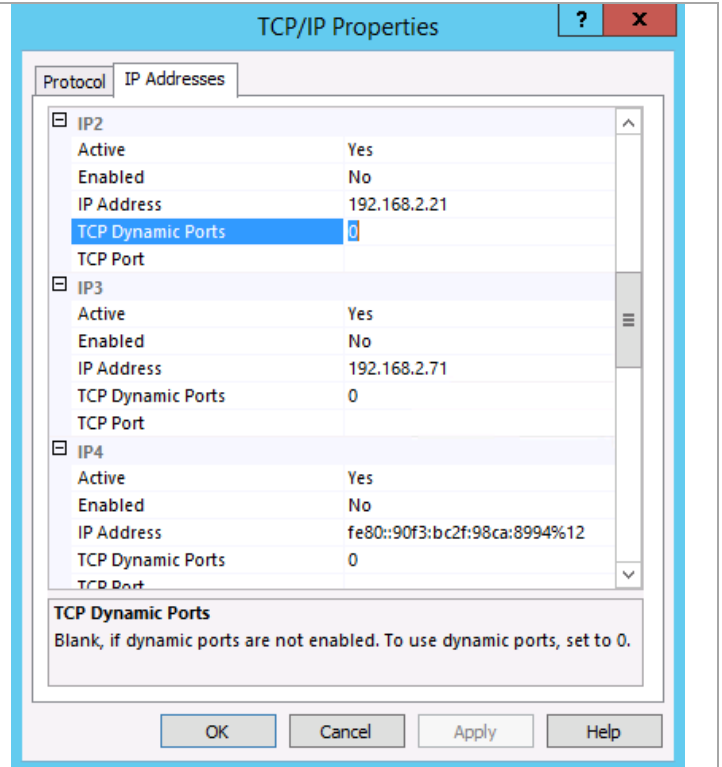
**Enabled** - If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to No, this property indicates whether SQL Server is listening on the IP address. If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to Yes, the property is disregarded. Not available for IPAll.

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

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

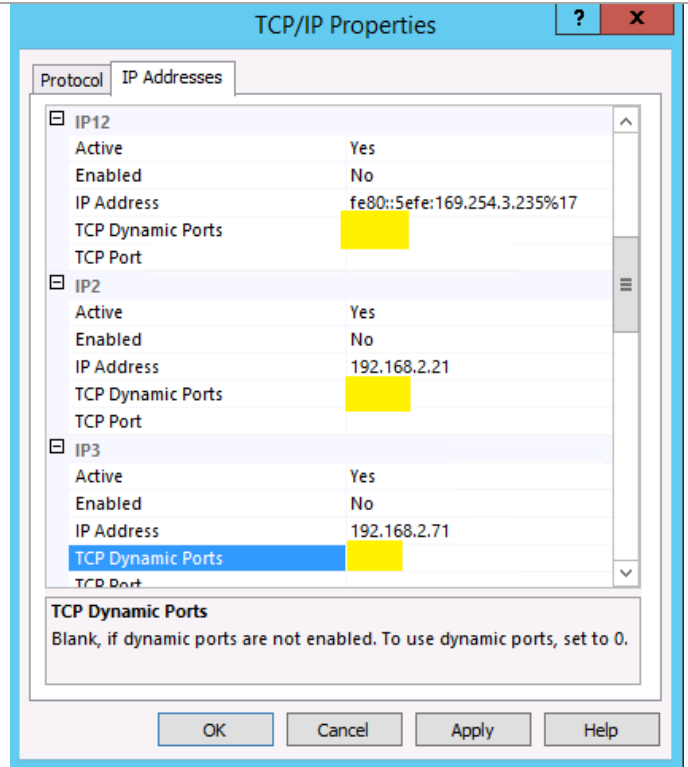
**TCP Port** - View or change the port on which SQL Server listens. By default, the default instance of Database Engine listens on port 1433. Note that the SCDB database must use port 1433 if the Cloud Services Process Pack will be used.

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

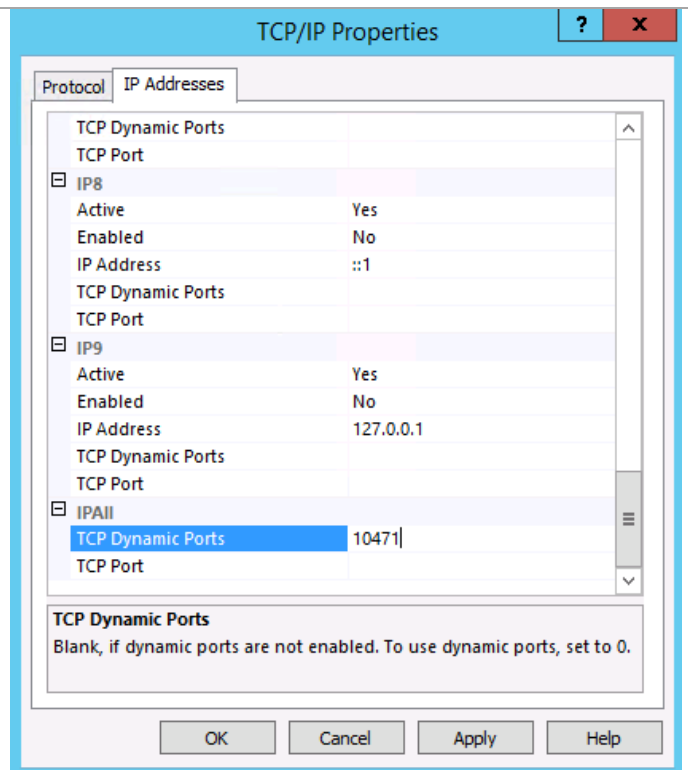




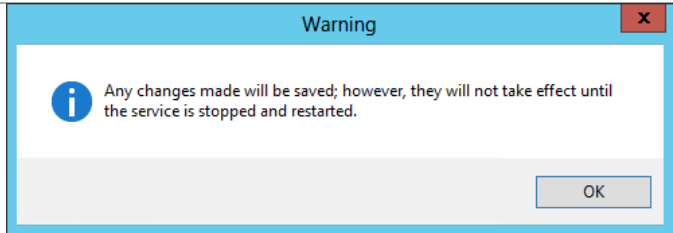
Within the dialog, browse to each IP address section for the instance and delete the numerical value (0) from the **TCP Dynamic Ports** field.



Scroll down to the **IPALL** section and delete the existing dynamic port value from **TCP Dynamic Ports** property. Assign static port value under **TCP Port** to one that is appropriate for the instance and you had previously recorded in your worksheet. For this example, port 10471 was specified. Click **Apply** to save the changes.



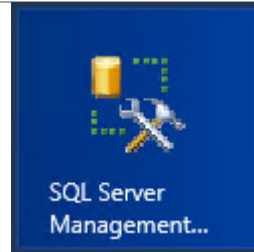
Note that a warning dialog will appear stating that the settings will not take effect until the SQL Server service has been restarted for that instance.



Repeat these steps to set a static port for each database service instance. Reference the SQL settings table at the beginning of this section for the default values used in this guide. 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.

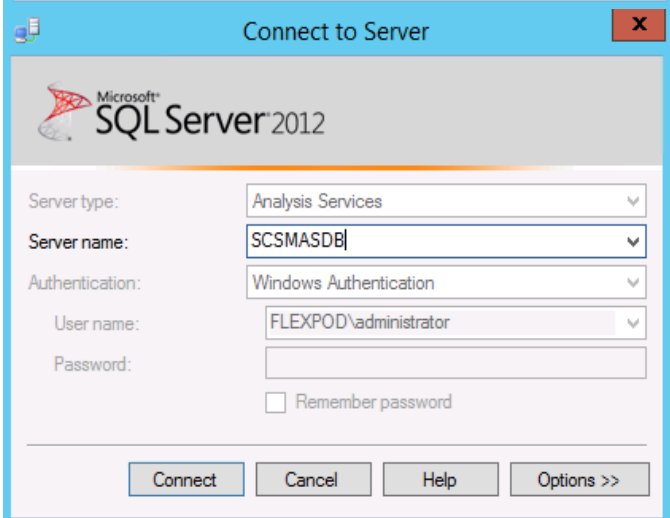
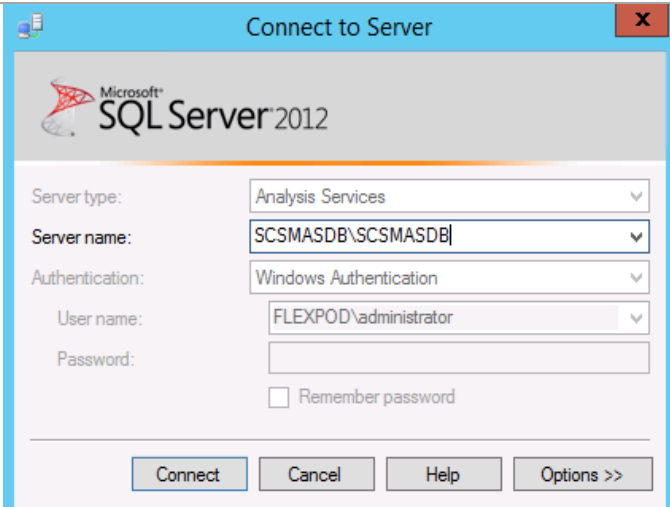
SQL Instance	Listening Port
SCDB	10474
SCVMMDB	10475
SCOMDB	10476
SCOMDW	10477
SCSMDB	10471
SCSMDW	10472
SCSMAS	10473
WAPDB	10478

Open **SQL Server Management Studio**.

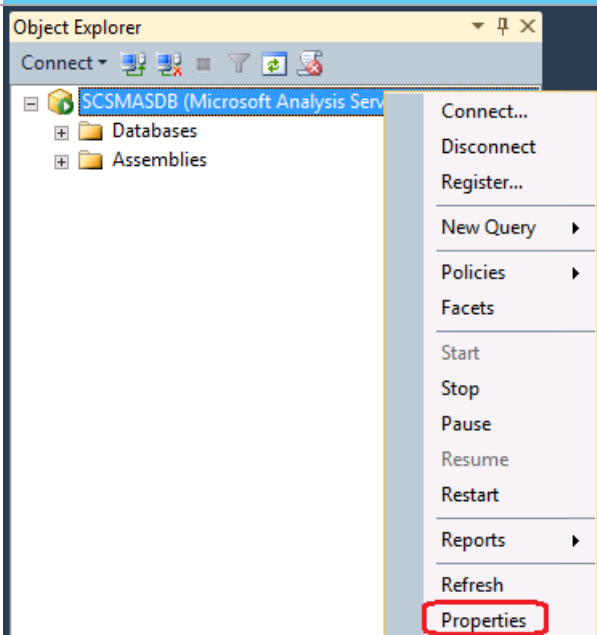


In the **Connect to Server** dialog, input the connection values for the SSAS instance. The default values of SCMAS\SCMAS for the analysis service are incorrect. You must use only the virtual computer object name (SCMAS in this example) as shown here. Click **Connect** to connect to the instance.

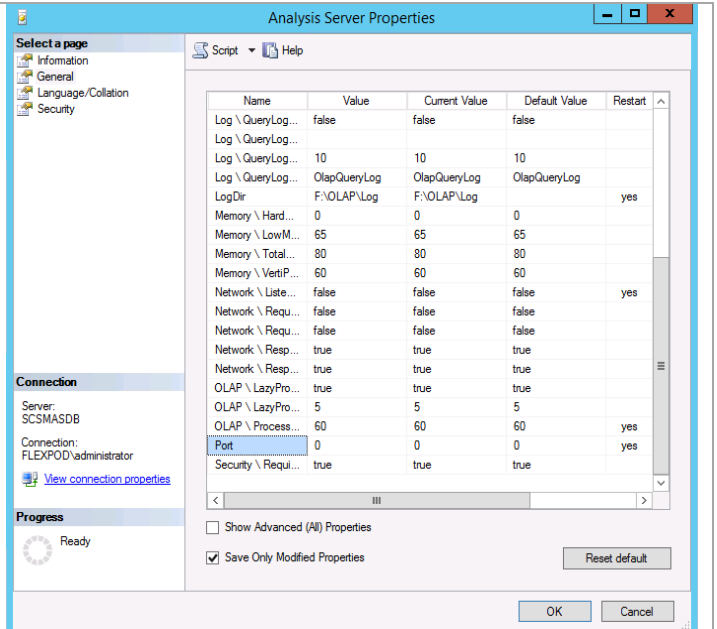
**Note:** Be sure the account you are logged on with is a member of the FT-SQL-Admins domain group or has otherwise been defined as a SQL sysadmin for the instance.



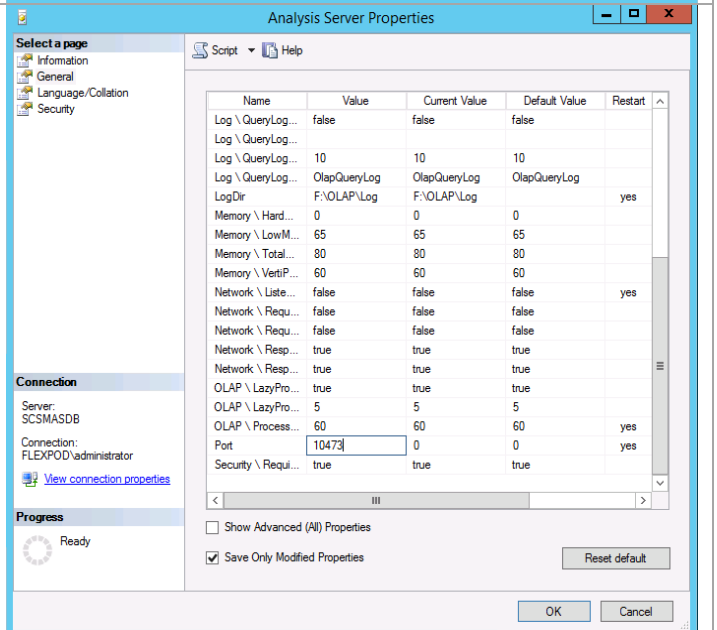
When connected to the instance in **SQL Management Studio**, right-click the SSAS instance and select **Properties**.



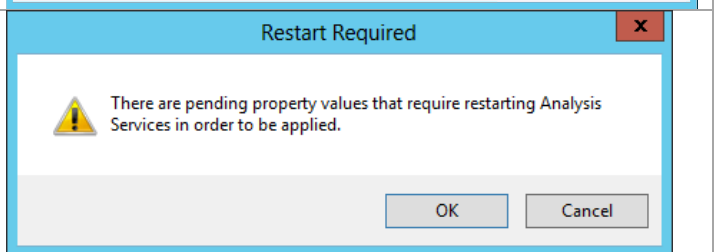
In the Analysis Server Properties dialog, select the **General** tab and then select **Port** (SQL listening port) from the **Name** column. By default the value will be set to “0” (zero) to specify a dynamic port.



In the same dialog, specify an appropriate static port value then click **OK** to save the changes.



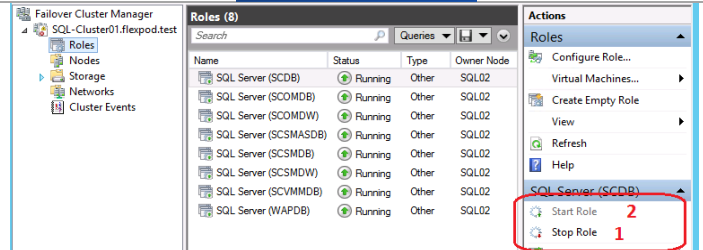
A dialog will appear outlining that a restart is required. Click **OK** and close SQL Management Studio.



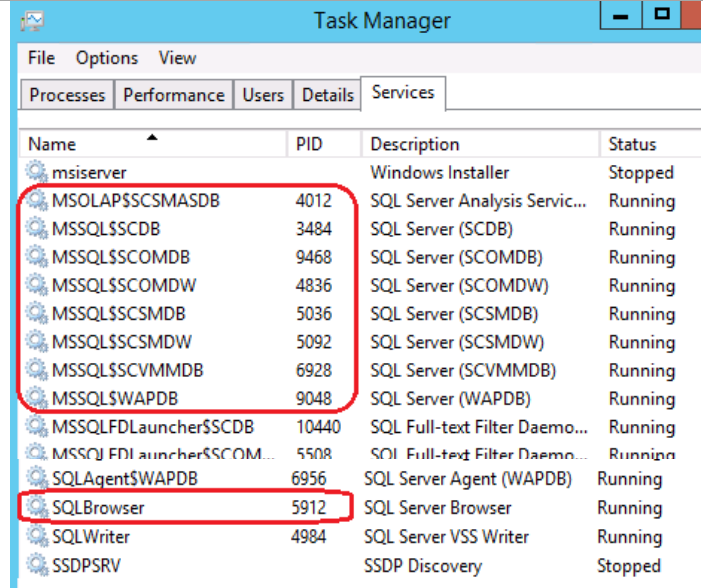
Open **Failover Cluster Manager** and expand the **Roles** node.



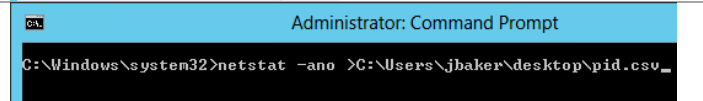
To apply the new port settings, in **Failover Cluster Manager** select each SQL Server instance. In the action pane, select **Stop Role** to stop the service for each instance. Restart each instance by selecting **Start Role** from the action Pane. Close the **Failover Cluster Manager** console.



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



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



Import the CSV file into Excel and then format the data into a table.

Filter on the PID column, selecting only the PIDs you documented from the task manager step previously and then filter on the state column selecting only the listening and blank values. The resulting table should confirm that all of the SQL instances are listening on only the static port assigned previously.

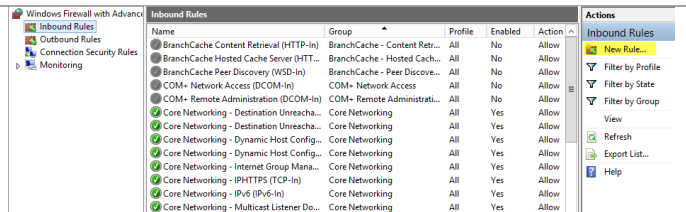
In addition to the static ports for each instance the 2382 TCP/UDP and 1434 TCP/UDP ports for SQL Browser will also be listed and will need to be opened in the firewall settings to support the Analysis and Database Engine instances.

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING	5912
TCP	192.168.2.71:10471	0.0.0.0:0	LISTENING	5036
TCP	192.168.2.72:10472	0.0.0.0:0	LISTENING	5092
TCP	192.168.2.73:10473	0.0.0.0:0	LISTENING	4012
TCP	192.168.2.74:10474	0.0.0.0:0	LISTENING	3484
TCP	192.168.2.75:10475	0.0.0.0:0	LISTENING	6928
TCP	192.168.2.76:10476	0.0.0.0:0	LISTENING	9468
TCP	192.168.2.77:10477	0.0.0.0:0	LISTENING	4836
TCP	192.168.2.78:14078	0.0.0.0:0	LISTENING	9048
TCP	[::]:2382	[::]:0	LISTENING	5912
UDP	0.0.0.0:1434	*.*		5912
UDP	[::]:1434	*.*		5912

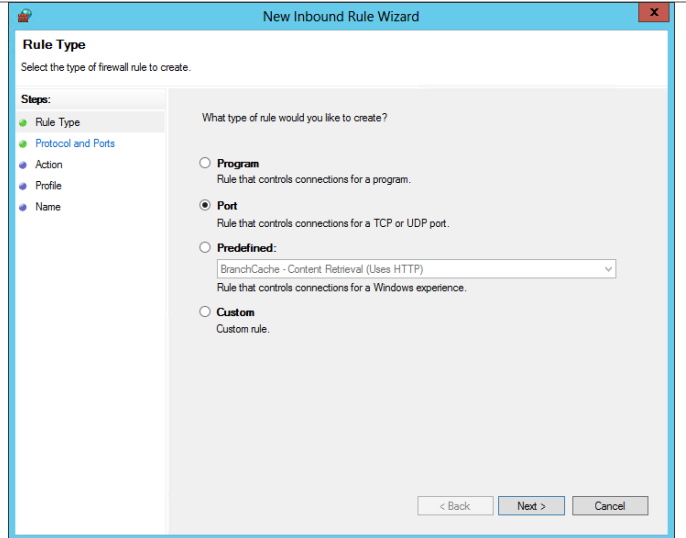
When completed, configure the Windows Firewall Rule for the SQL Browser Service. To perform this action, on each node in the Windows Failover Cluster that will host SQL instances, open the **Windows Firewall with Advanced Security** MMC console.



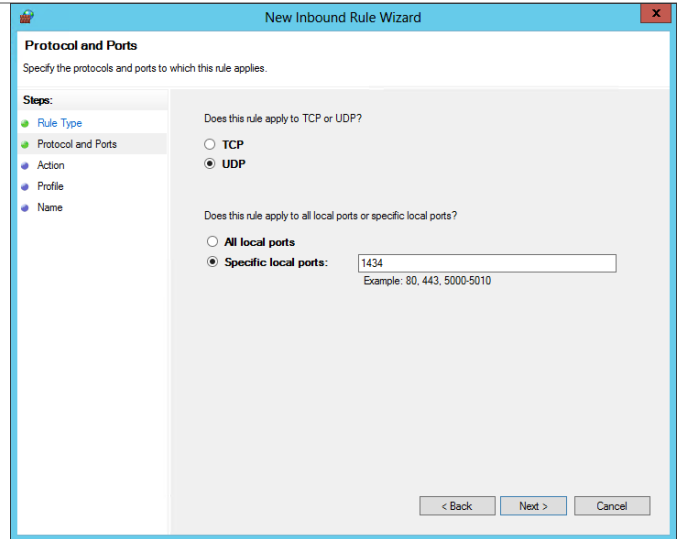
Within the **Windows Firewall with Advanced Security** MMC console, select the **Inbound Rules** node and select **New Rule** from the action pane.



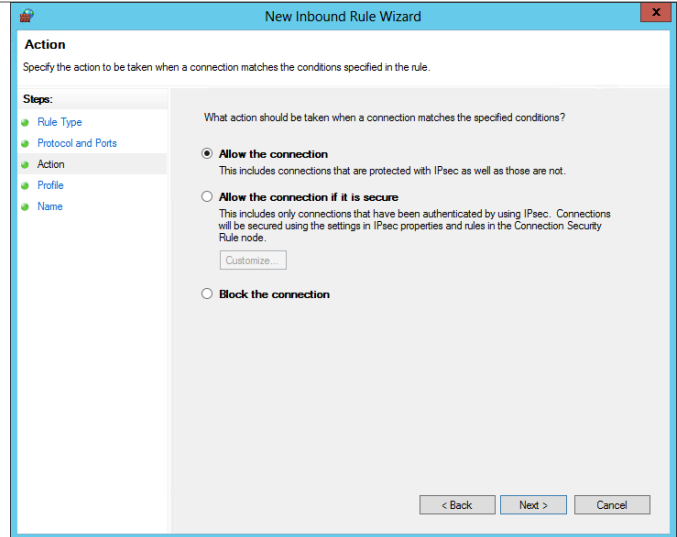
In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.



On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input 1434 to enable access to the SQL Browser service for Database Engine instances. Click **Next** to continue.

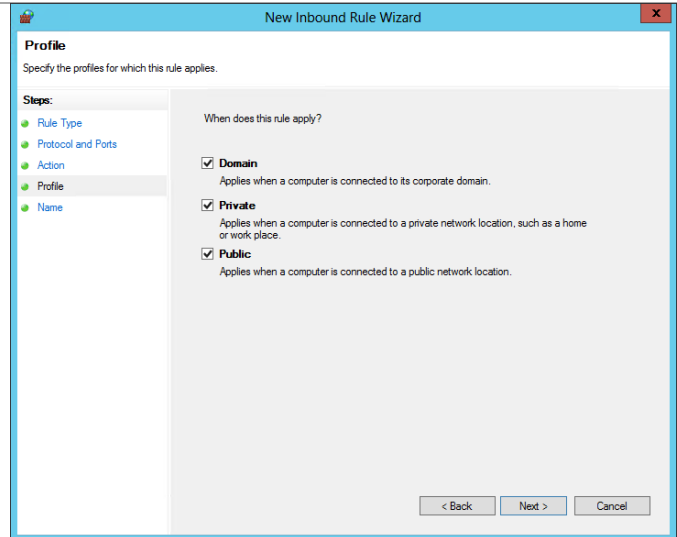


On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.

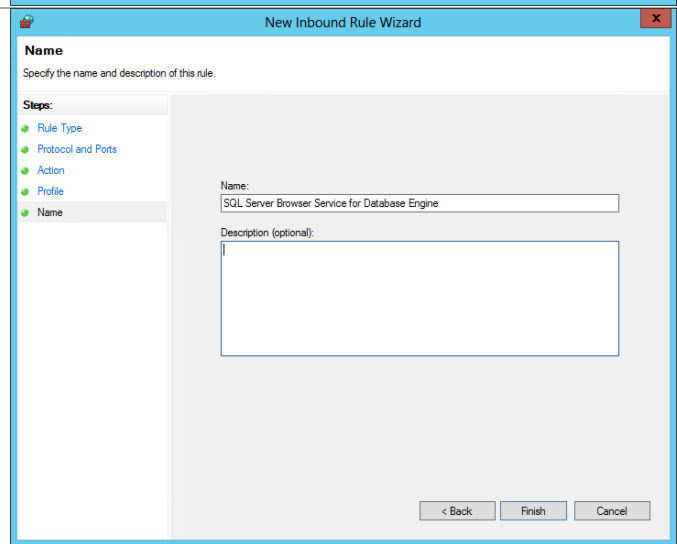


On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.

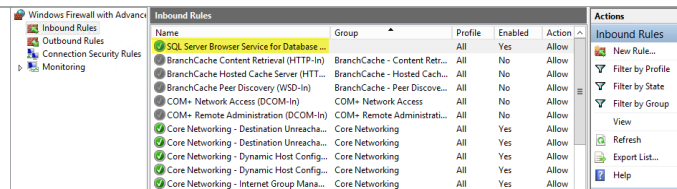
*Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.*



Specify a name for the new rule such as “*SQL Server Browser Service for Database Engine*” and click **Finish**.

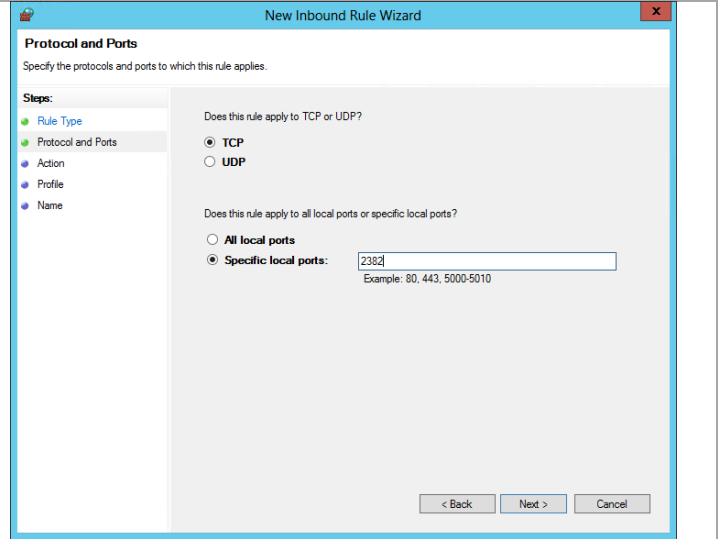


Note the new rule listed in the Inbound Rules pane. Repeat this process by selecting **New Rule** once again from the action pane to create the **SQL Browser Service for Analysis Server** rule.

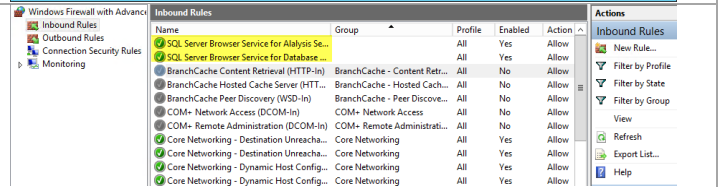




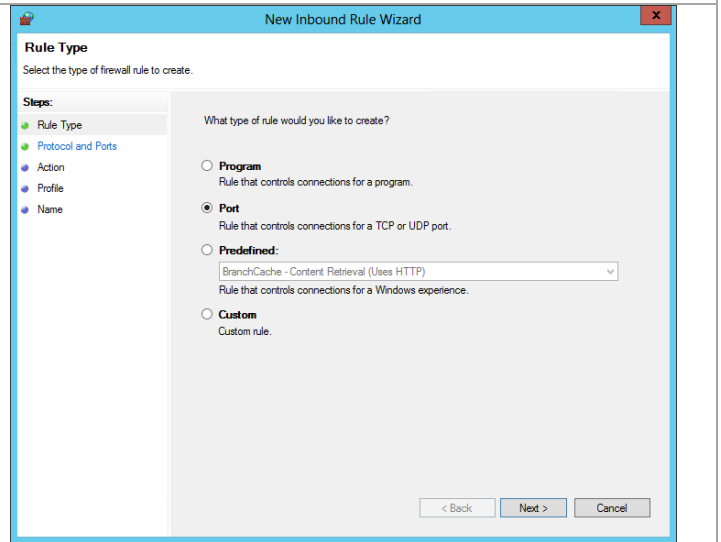
Repeat the previously outlined steps to create the new rule, however on the **Protocol and Ports** page, select both the **TCP** and **Specific local ports** radio buttons. Specify the value of **2382** to enable access to the **SQL Browser service for the Analysis Server** instance.



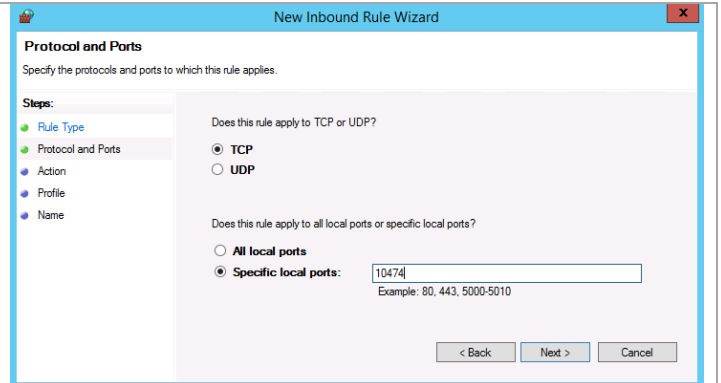
Note the additional new rule listed in the Inbound Rules pane. Next the inbound Windows Firewall rule for each of the SQL instances must be created and configured. From the same dialog, select **New Rule** from the action pane to create the firewall rule for the first named instance.



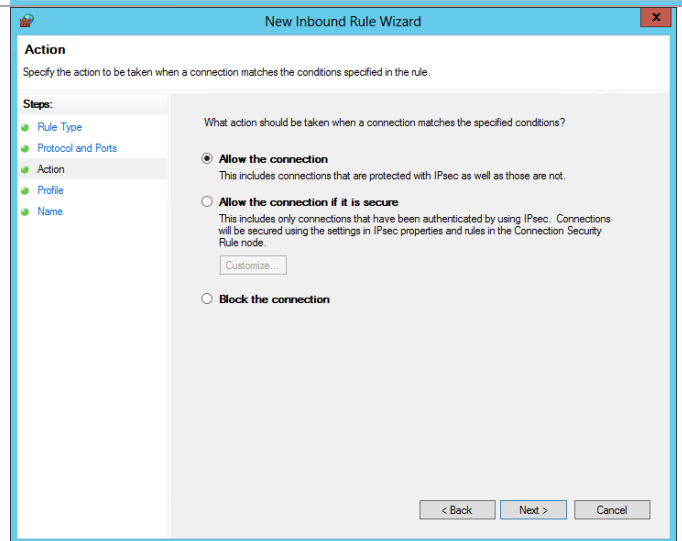
In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.



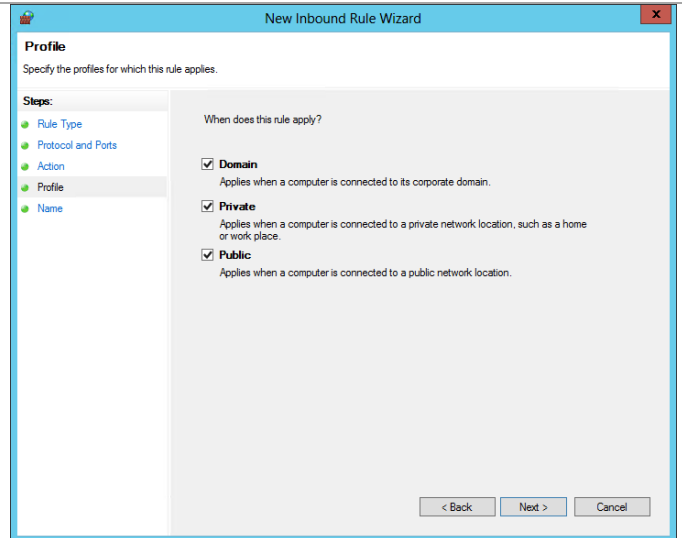
On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input the specific local TCP/IP port to enable access to the first named SQL instance. In this example to enable access to the SQL instance SCDB the port specified is 10474. Click **Next** to continue.



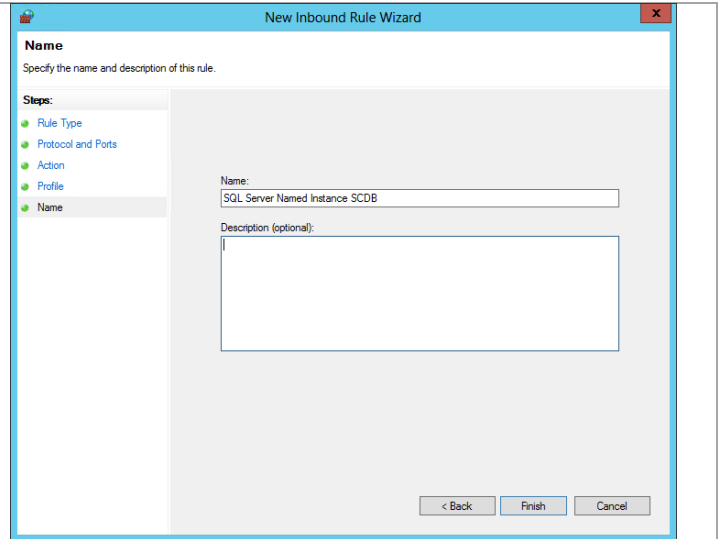
On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.



On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.  
*Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.*



Specify a name for the new rule such as “*SQL Server Named Instance SCDB*” and click **Finish**.



Create an additional rule for each SQL instance. For the reference SQL architecture and instances the rule set would be configured similar to the following diagram.

Name	Group	Local Port	Profile
✓ SQL Server Browser Service for Analysis S...		2382	All
✓ SQL Server Browser Service for Database ...		1434	All
✓ SQL Server Named Instance SCDB		10474	All
✓ SQL Server Named Instance SCOMDB		10476	All
✓ SQL Server Named Instance SCOMDW		10477	All
✓ SQL Server Named Instance SCSMASDB		10473	All
✓ SQL Server Named Instance SCSMDB		10471	All
✓ SQL Server Named Instance SCSMDW		10472	All
✓ SQL Server Named Instance SCVMMDB		10475	All
✓ SQL Server Named Instance WAPDB		10478	All

Alternatively, firewall rules can be created through PowerShell on the local server as shown in the following example. Be sure to replace the port number value with the correct value for your environment.

```
New-NetFirewallRule -DisplayName "SQL Server Browser Service for Database Engine" -LocalPort 1434 -Protocol UDP -Action Allow
```

To create the rules on the remote nodes through PowerShell, the following commands are provided as an example.

This procedure assumes that commands are executed on SQL Server node SQL01.

Repeat for each node in the SQL cluster.

```
$RemoteSession = New-CimSession -ComputerName SQL02
New-NetFirewallRule -DisplayName "SQL Server Browser Service for Database Engine" -LocalPort 1434 -Protocol UDP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Browser Service for Analysis Server" -LocalPort 2382 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Name instance SCDB" -LocalPort 10474 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCVMMDB" -LocalPort 10475 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCOMDB" -LocalPort 10476 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCOMDW" -LocalPort 10477 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMDB" -LocalPort 10471 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMDW" -LocalPort 10472 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance WAPDB" -LocalPort 10478 -Protocol TCP -Action Allow -CimSession $RemoteSession
New-NetFirewallRule -DisplayName "SQL Server Named Instance SCSMAS" -LocalPort 10473 -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.

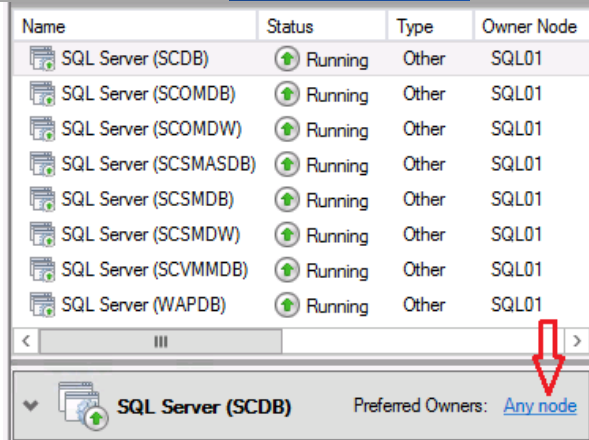
On any SQL Server cluster node, open **Failover Cluster Manager** and expand the **Roles** node.



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

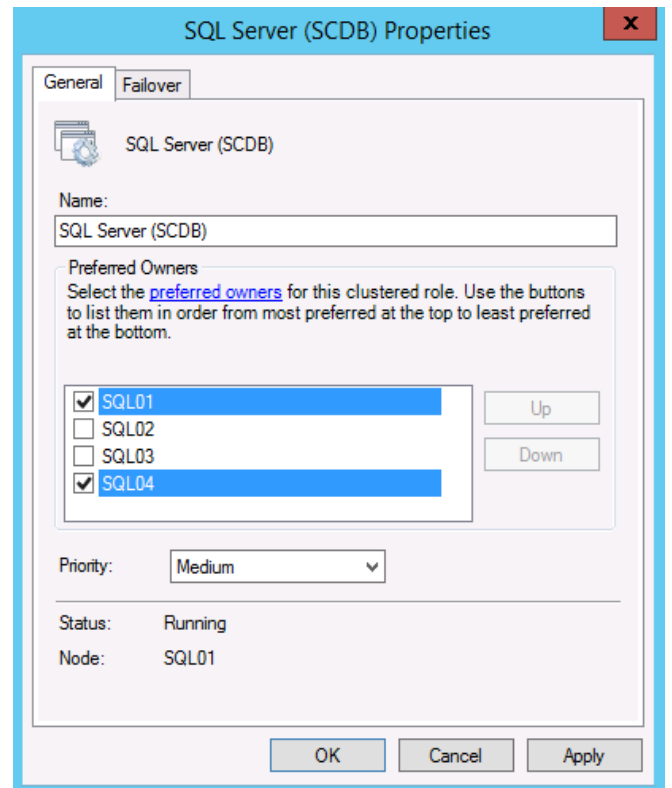
In order to better control failover behavior and distribution of the instances the **Preferred Owners** list must be modified and the owner node must be assigned by failing over the SQL Server instance to that node. Refer to the list created previously.

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

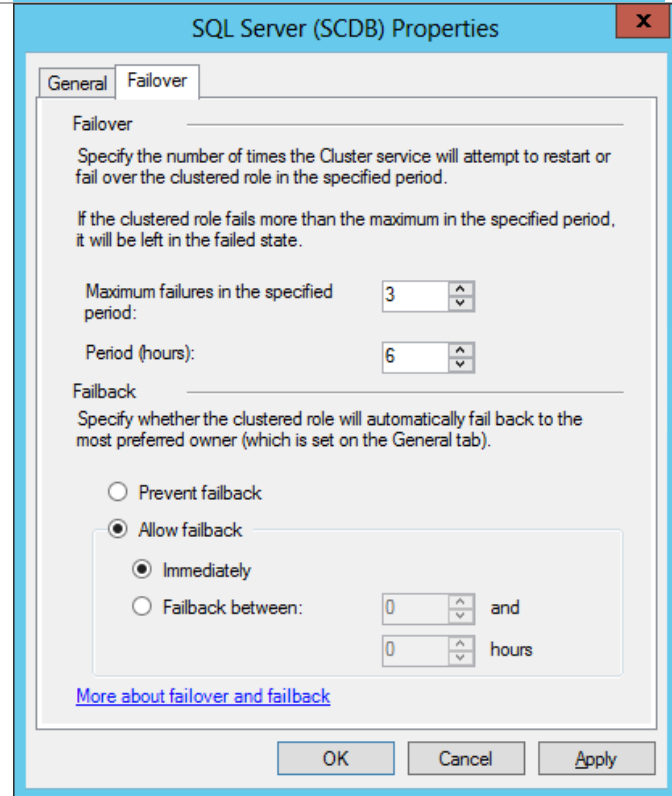


SQL Instance	Preferred Owners
SCDB	Node1, Node4
SCVMMDB	Node1, Node4
SCOMDB	Node3, Node4
SCOMDW	Node3, Node4
SCSMDB	Node2, Node4
SCSMDW	Node2, Node4
SCSMAS	Node2, Node4
WAPDB	Node1, Node3

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



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



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

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL01
SQL Server (SCOMDB)	Running	Other	SQL01
SQL Server (SCOMDW)	Running	Other	SQL01
SQL Server (SCSMASDB)	Running	Other	SQL01
SQL Server (SCSMDB)	Running	Other	SQL01
SQL Server (SCSMDW)	Running	Other	SQL01
SQL Server (SCVMMDB)	Running	Other	SQL01
SQL Server (WAPDB)	Running	Other	SQL01

SQL Server (SC...) Preferred Owners: [User Settings](#)

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

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL01
SQL Server (SCOMDB)	Running	Other	SQL01
SQL Server (SCOMDW)	Running	Other	SQL01
SQL Server (SCSMASDB)	Running	Other	SQL01
SQL Server (SCSMDB)	Running	Other	SQL01
SQL Server (SCSMDW)	Running	Other	SQL01
SQL Server (SCVMMDB)	Start Role		
SQL Server (WAPDB)	Stop Role		

Context menu options: Move, Best Possible Node

When the moves are completed, all Instances should be distributed across Node1, Node 2, and Node3. *Note: With all nodes configured as Possible Owners, failover to nodes not listed as a Preferred Owner can still occur when the preferred owners are not available. However, with Failback enabled the SQL Server instances should always be reassigned on their preferred node when availability returns. This configuration supports a primary dedicated passive node plus two additional active/passive nodes in the case of a failure of two nodes. It is important to note however, that Failback only applies to automatic failover events and not to user initiated moves.*

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL01
SQL Server (SCOMDB)	Running	Other	SQL03
SQL Server (SCOMDW)	Running	Other	SQL03
SQL Server (SCSMASDB)	Running	Other	SQL02
SQL Server (SCSMDB)	Running	Other	SQL02
SQL Server (SCSMDW)	Running	Other	SQL02
SQL Server (SCVMMDB)	Running	Other	SQL01
SQL Server (WAPDB)	Running	Other	SQL01

## 17 Install and Configure the Data ONTAP SMI-S Provider

### 17.1 Prerequisites

The following environment prerequisites must be met before proceeding.

## Accounts

Verify that the following local account has been created:

User name	Purpose	Permissions
FT-SMIS-User	SMI-S access account	This account will not need any special delegation.

## 17.2 Install the SMI-S Provider

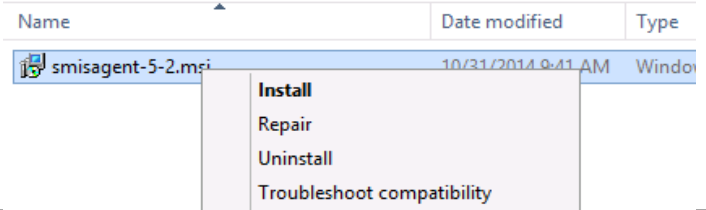
The following steps need to be completed in order to install the NetApp SMI-S provider.

Download the installer from:

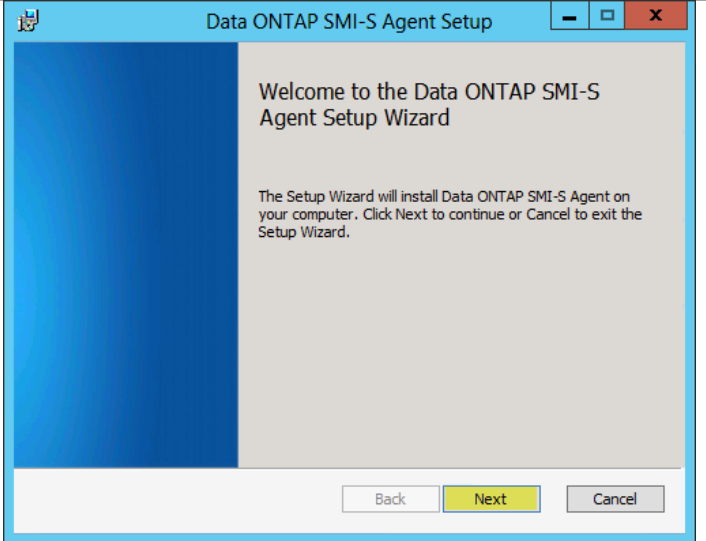
<http://support.netapp.com/NOW/download/software/smis/Windows/5.0/smisagent-5-2.msi>

Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

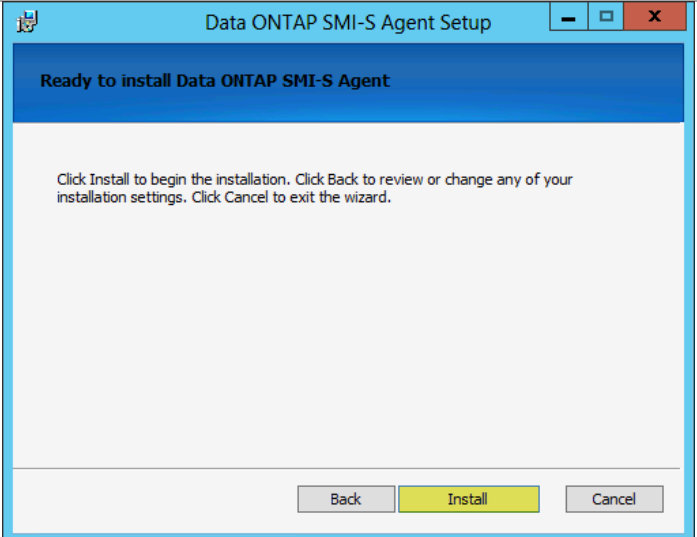
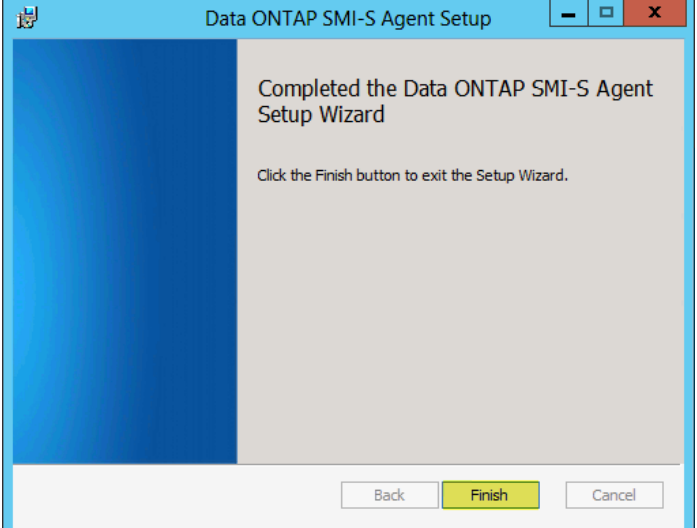
Right-click **smisagent-5-2** and select **Install** from the context menu to begin setup.



On the "Welcome to the Data ONTAP SMI-S Agent Setup Wizard" page, click **Next**



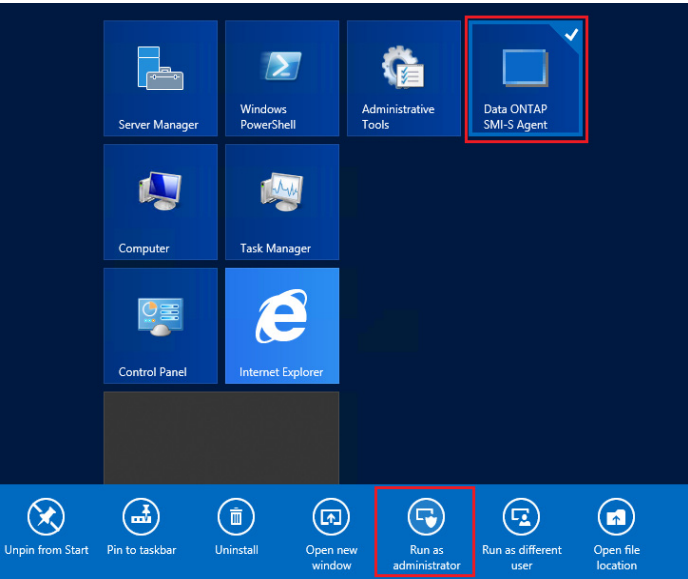
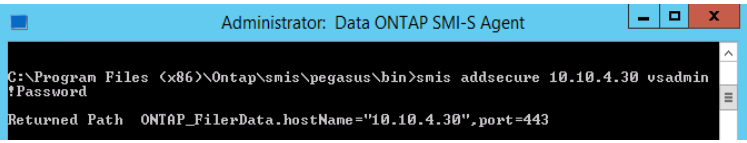
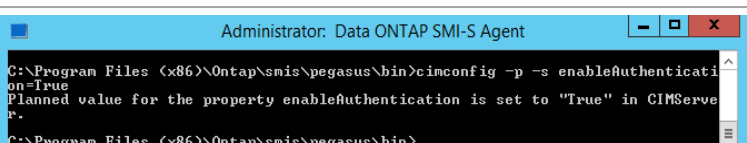
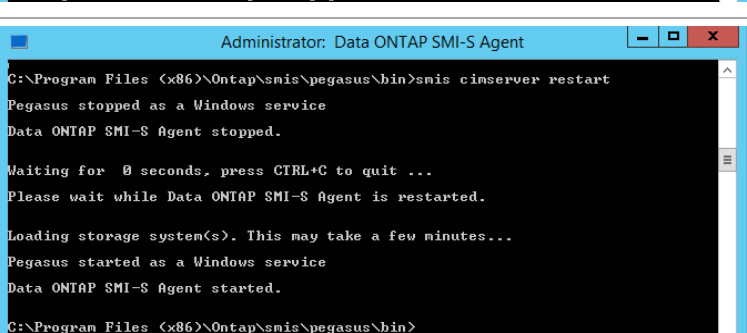
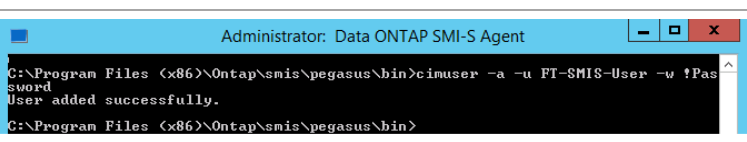


<p>On the “Ready to install Data ONTAP SMI-S Agent” page, click <b>Install</b>.</p>	
<p>On the “Completed the Data ONTAP SMI-S Agent Setup Wizard”, click <b>Finish</b> to complete the installation.</p>	

### 17.3 Configure the SMI-S Provider

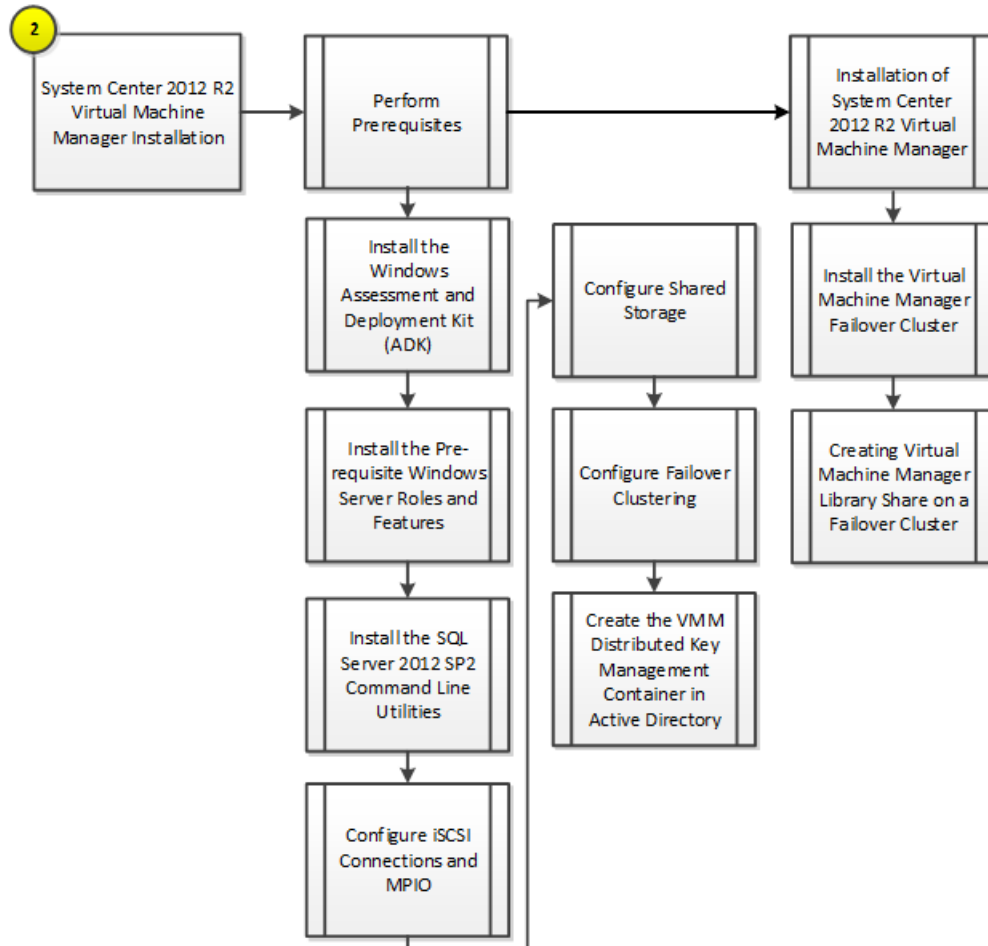
The following steps need to be completed in order to configure the NetApp SMI-S provider.

Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

<p>Open App screen, right-mouse click on <b>Data ONTAP SMI-S Agent</b> and select <b>Run as Administrator</b> at the bottom of the screen.</p>	
<p>Add Vserver to the SMIS configuration.</p>	 <pre>Administrator: Data ONTAP SMI-S Agent C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;smis addsecure 10.10.4.30 vsadmin !Password Returned Path  ONTAP_FilerData.hostName="10.10.4.30", port=443</pre>
<p>Enable user authentication using cimconfig -om-and</p>	 <pre>Administrator: Data ONTAP SMI-S Agent C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;cimconfig -p -s enableAuthentication=true Planned value for the property enableAuthentication is set to "True" in CIMServer. C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;</pre>
<p>Restart the Agent/cimserver</p>	 <pre>Administrator: Data ONTAP SMI-S Agent C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;smis cimserver restart Pegasus stopped as a Windows service Data ONTAP SMI-S Agent stopped.  Waiting for 0 seconds, press CTRL+C to quit ... Please wait while Data ONTAP SMI-S Agent is restarted.  Loading storage system(s). This may take a few minutes... Pegasus started as a Windows service Data ONTAP SMI-S Agent started. C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;</pre>
<p>Add SMI-S Run As account to the SMI-S configuration.</p>	 <pre>Administrator: Data ONTAP SMI-S Agent C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;cimuser -a -u FT-SMIS-User -w !Password User added successfully. C:\Program Files (x86)\Ontap\smis\pegasus\bin&gt;</pre>

## 18 Virtual Machine Manager

The System Center 2012 Virtual Machine Manager installation process includes the following high-level steps:



### 18.1 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 R2 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 SMB shares for storage and file share witness.
  - Requires a dedicated virtual network adapter for cluster communication
- 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 R2 installed.

- The target virtual machine must have the Windows Server Update Services (WSUS) 4.0 console installed (available on Windows Server 2012R2).
  - 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 SP2).
  - 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.

## 18.2 Prerequisites

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 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<sup>5</sup>.

## Configure the Virtual Machine Manager Cluster File Share Witness Share

Perform the following tasks to create the witness share on the NetApp Storage Array:

1. Open an SSH connection to NetApp cluster IP or host name and log in to the admin user with the password you provided earlier.

2. Create a qtree in the SCVMM pool to house the infrastructure virtual machines (VMs)–

```
qtree create -volume witness -qtree vmm-witness -security-style ntfs -vserver infra_svm
```

3. Create the qtree quota policy for the infrastructure VM share.

```
quota policy rule create -policy-name default -volume witness -type tree -disk-limit 5g -target vmm-witness -vserver infra_svm
```

4. Create the SMB share to store the vmm witness database

```
share create -share-name vmm-witness -path /witness/vmm-witness -share-properties browsable, oplocks -vserver infra_svm
```

5. Remove the Everyone permission from the Witness share.

```
cifs share access-control delete -share sql-witness -user-or-group Everyone -vserver infra_svm
```

6. Add Permissions the following accounts with NTFS full control permissions over the Share:

VMM Node 1

VMM Node 2

VMM Cluster Name Object (CNO)

```
share access-control create -share vmm-witness -user-or-group NETAPP\SCVMM01$ -permission full_Control -vserver infra_svm
```

```
share access-control create -share vmm-witness -user-or-group NETAPP\SCVMM02$ -permission full_Control -vserver infra_svm
```

```
share access-control create -share vmm-witness -user-or-group NETAPP\scvmm-cluster01$ -permission full_Control -vserver infra_svm
```

```
share access-control create -share vmm-witness -user-or-group NETAPP\administrator -permission -Read -vserver infra_svm
```

## 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](http://www.microsoft.com/en-us/download/details.aspx?id=39982) from <http://www.microsoft.com/en-us/download/details.aspx?id=39982>.

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

---

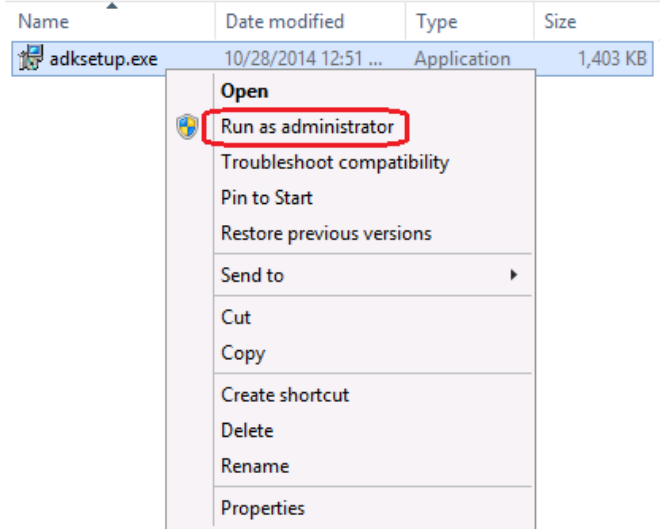
<sup>5</sup> Creating User Roles in VMM - <http://technet.microsoft.com/en-us/library/gg696971.aspx>.

installation details can be found at <http://msdn.microsoft.com/en-us/library/hh825494.aspx>

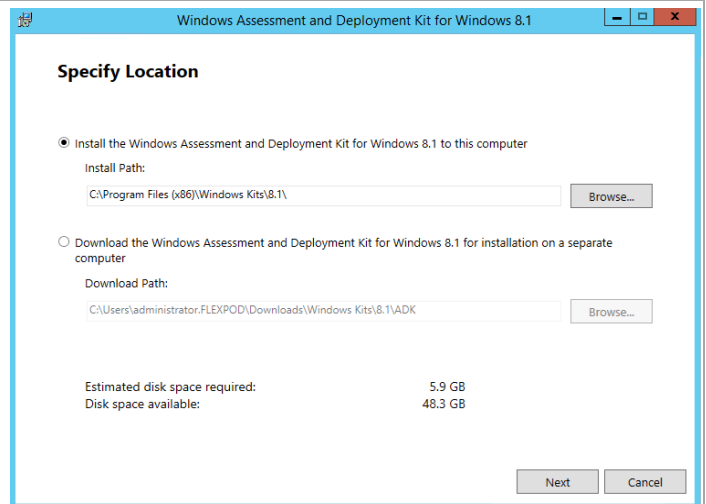
The following steps outline how to install the Windows ADK on the Virtual Machine Manager Management server.

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

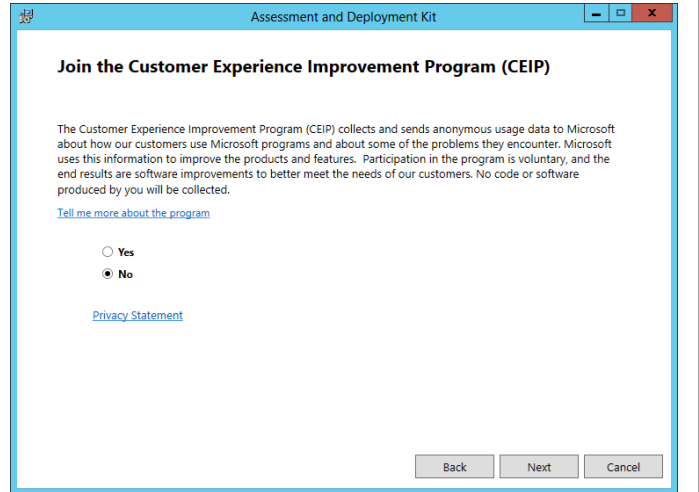
From the Windows ADK installation media source, right-click **adksetup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



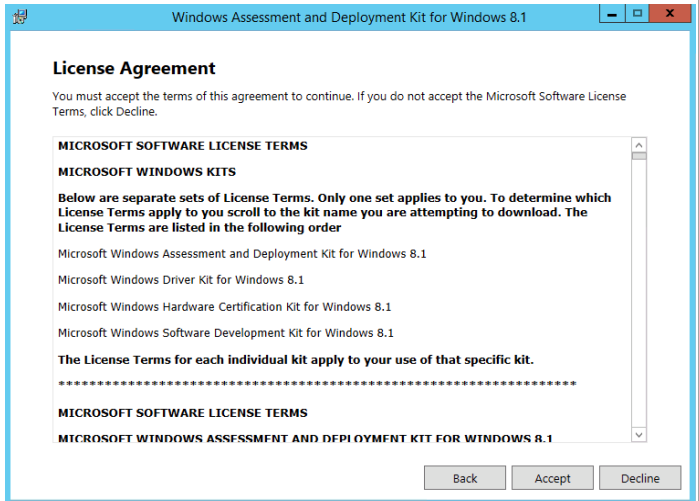
A splash screen will appear. In the **Specify Location** dialog, accept the default folder location of `%ProgramFiles%\Windows Kits\8.0` and click **Next** to continue.



In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



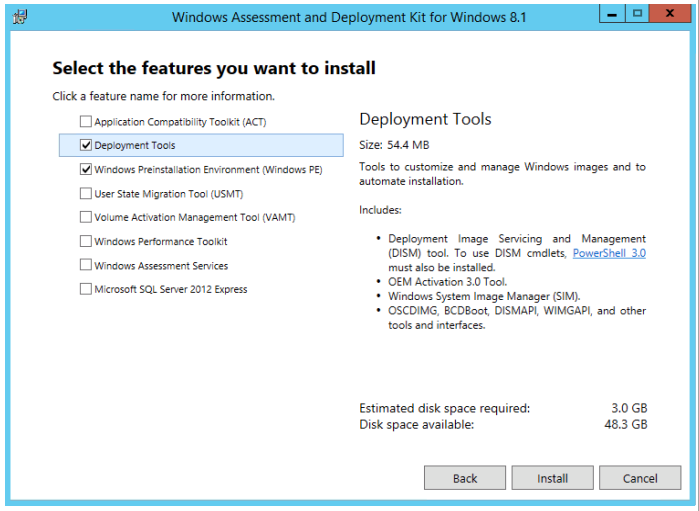
In the **License Agreement** dialog, click **Accept** to continue.



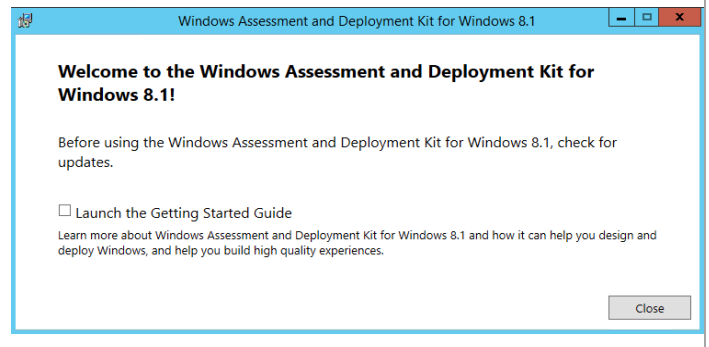
In the **Select the features you want to install** dialog, select the following option checkboxes:

- Deployment Tools
- Windows Preinstallation Environment (Windows PE)

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



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



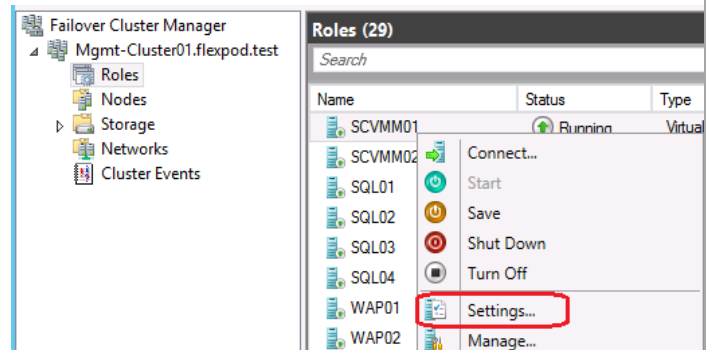
### 18.3 Install the Prerequisite Windows Server Roles and Features

The Virtual Machine Manager installation requires the WSUS Administration Tools to be installed on the Virtual Machine Manager Management servers. In addition, the MPIO and Failover Clustering Features must be installed.

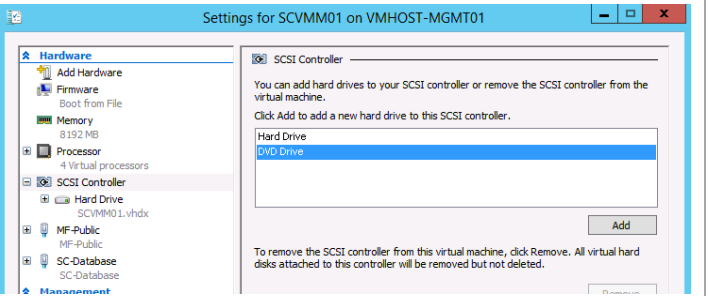
Follow the steps below to install the pre-requisite roles and features on the Virtual Machine Manager Management servers.

Perform the following steps on each **Virtual Machine Manager** virtual machine. (If you included the .NET 3.5 feature in a sysprepped VM used to build all your Fabric Management VMs, this step is not necessary to manually add that feature.)

Verify that the Windows installation disk is mapped to D: drive.  
From the Failover Cluster Manager console, right-click on the SCVMM virtual machine and select **Settings...**

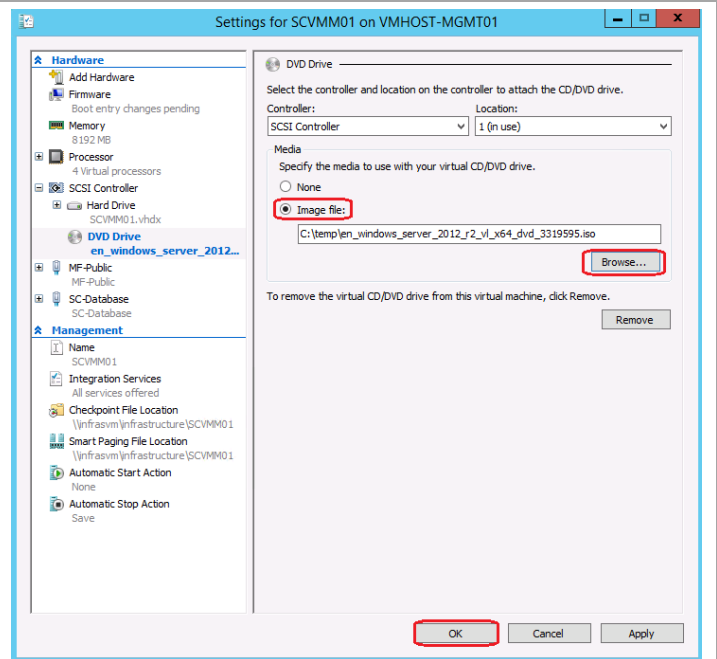


Select **SCSI Controller** under Hardware, then select **DVD Drive** and click **Add** to add a DVD drive to the virtual machine.

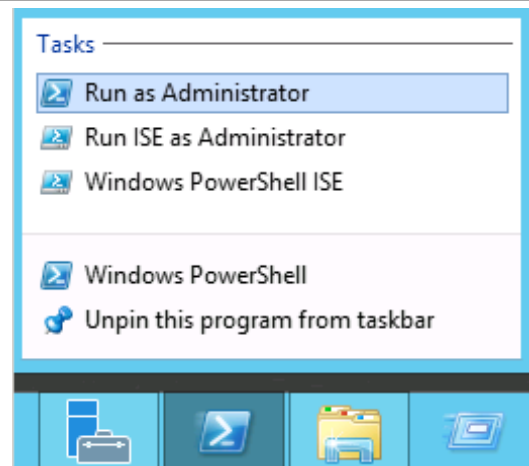




Select the radio button by **Image file**. Browse to the location where you have the Windows Server 2012 R2 installation media. Click **OK** to add the DVD with the mounted media to the VM.

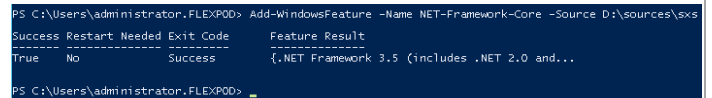


Launch a PowerShell prompt by right clicking the PowerShell icon in the taskbar, and selecting **Run as Administrator**.

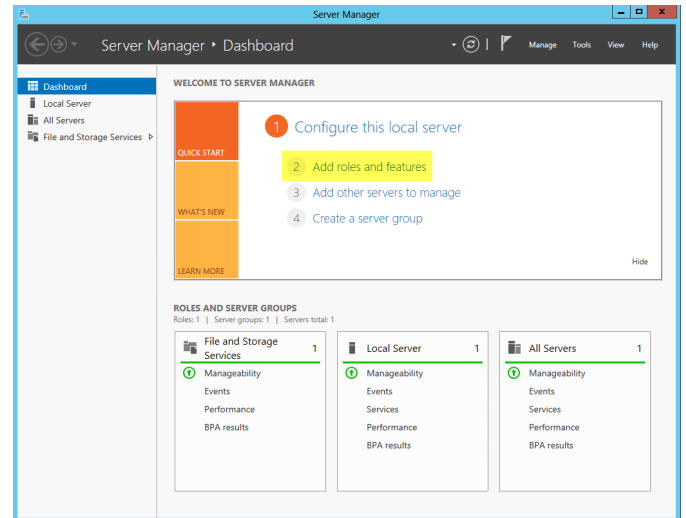


Add the .Net 3.5 feature by entering the following command:

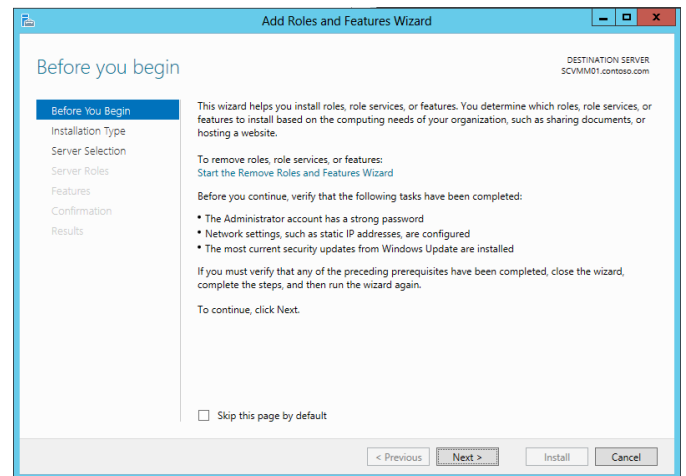
```
Add-indowsFeature -Name NET--ramework-Core -Source D:\sources\sxs
```



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



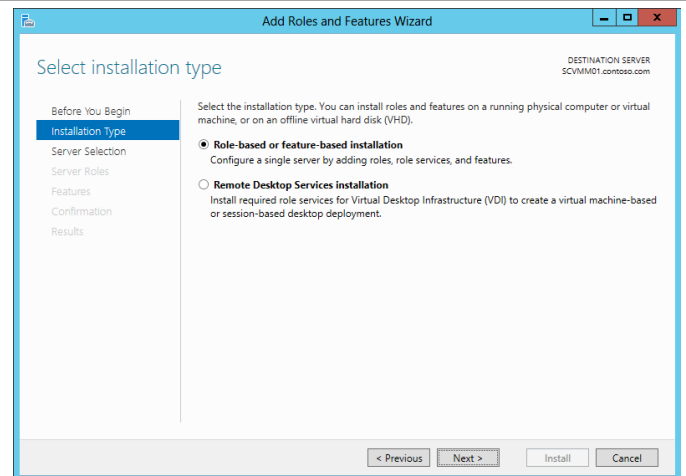
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, click **Next** to continue.



In the **Select Installation Type** dialog, you are presented with two options:

- **Role-based or Feature-based installation** – Traditional installation of roles and features to enable discrete functionality on the operating system.
- **Remote Desktop Services scenario-based installation** – Installation of a pre-determined combination of roles, features and configurations to support a Remote Desktop (Session Virtualization) or VDI scenario

Select the **Role-based or Feature-based installation** radio button and click **Next** to continue.

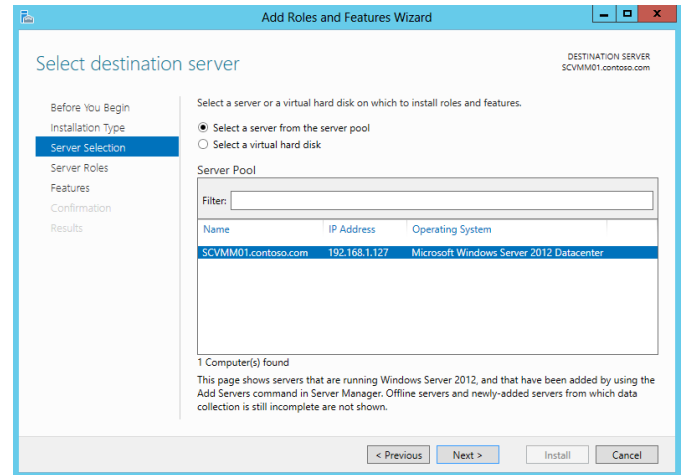


In the **Select destination server** dialog, you are presented with two options:

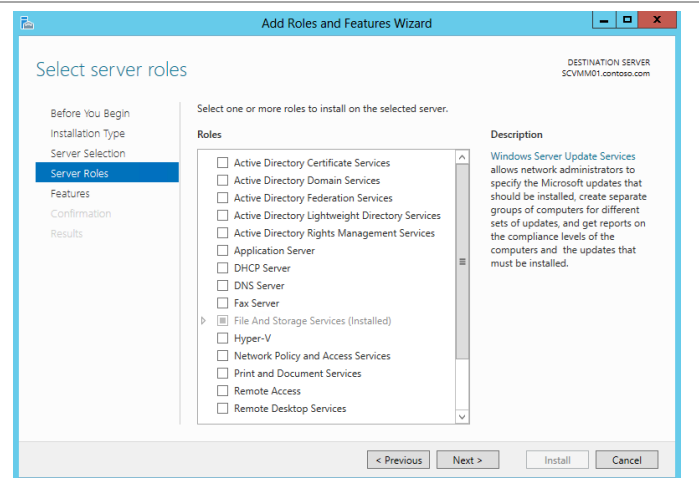
- *Select a server from the server pool* – This option allows you to select a server from the managed pool of systems defined within Server Manager.
- *Select a virtual hard disk* – This option allows for roles to be installed to staged VHD files for offline servicing purposes.

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

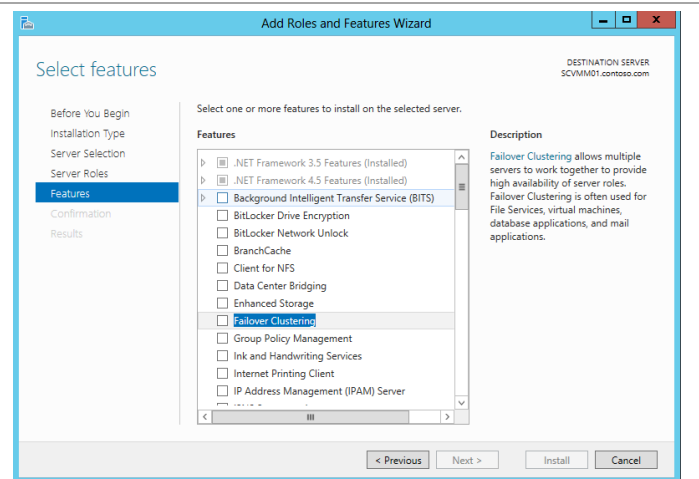
*Note that while many servers may be presented in the Select a server from the server pool option, only one can be selected at a time for role and feature installation operations. To enable installs across multiple hosts, the configuration can be saved at the end of the wizard and applied to multiple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



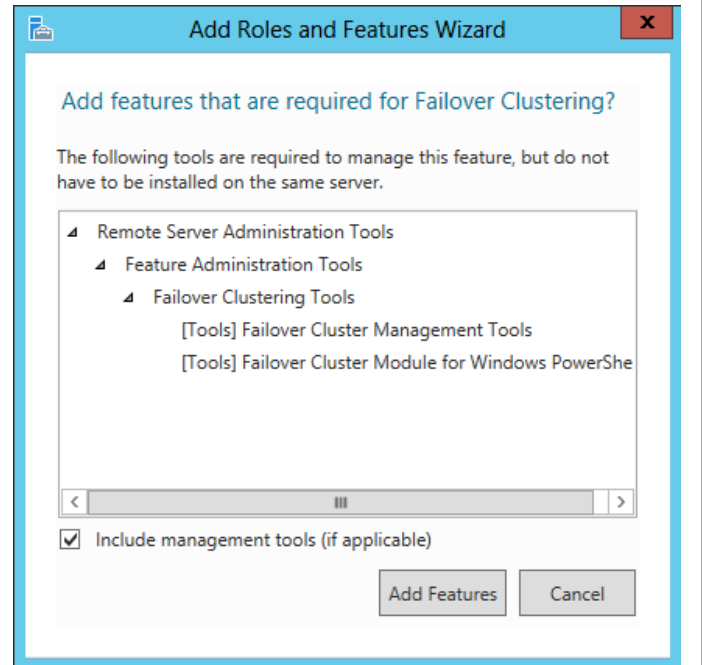
In the **Select Server Roles** dialog, do not make any additional selections and click **Next** to continue.



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

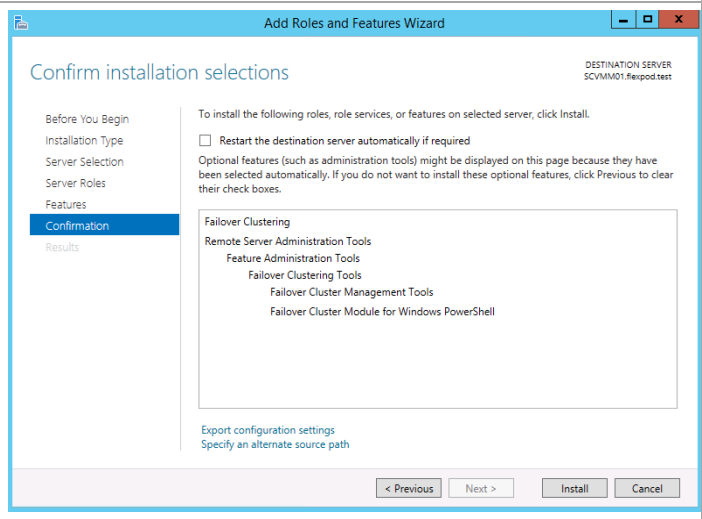


The **Add features that are required for Failover Clustering** dialog will appear. Check the **Include management tools (if applicable)** checkbox, then click the **Add Features** button.

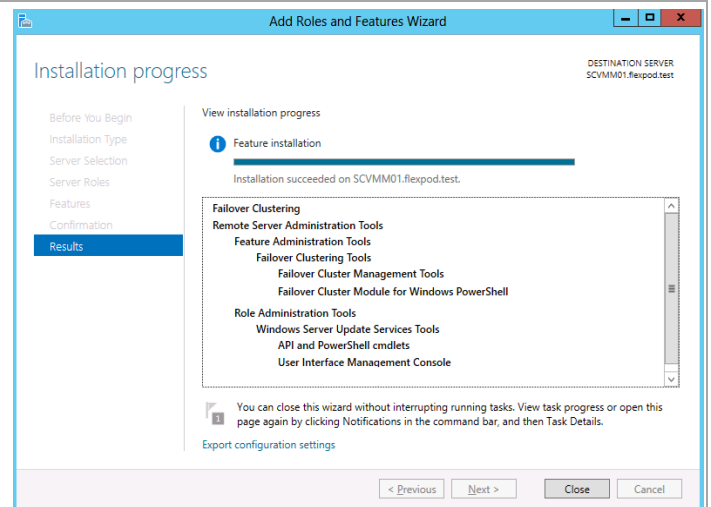


In the **Confirm installation selections** dialog, verify that the Multipath I/O and Failover Clustering features are selected. Make sure that the **Restart each destination server automatically if required** is selected. This is especially important for remote role/feature installation. Click **Install** to begin installation.

*Note that 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.*

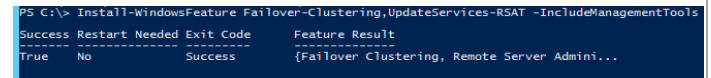


The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



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

```
Install-WindowsFeature -Name Failover-Clustering, Updat-Services-RSAT -IncludeManagementTools -Restart
```



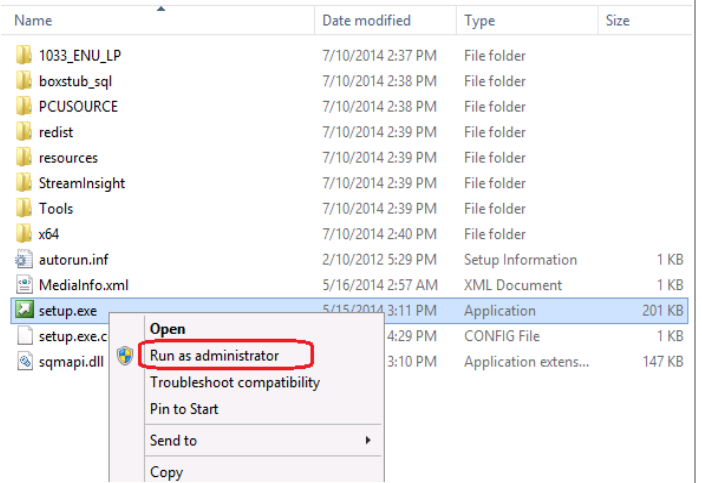
## Install the SQL Server 2012 SP2 Command Line Utilities

The Virtual Machine Manager installation requires that the SQL Server 2012 SP2 Command Line Utilities and Management Tools be installed on the Virtual Machine Manager Management server.

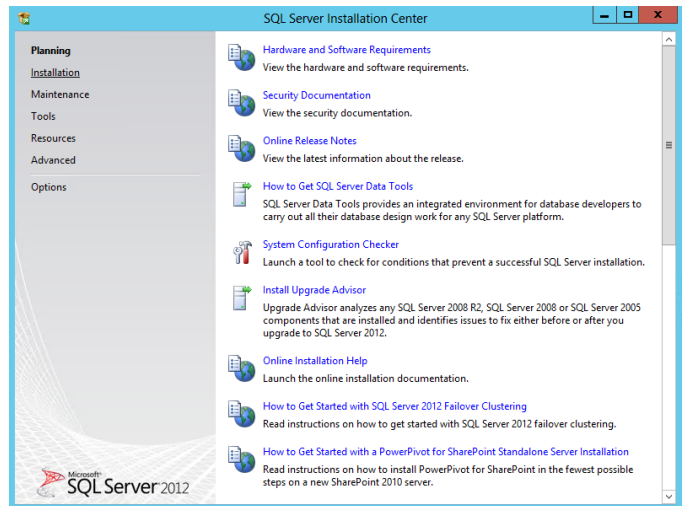
Follow the steps below to install the Command Line Utilities and Management Tools on the Virtual Machine Manager management server.

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

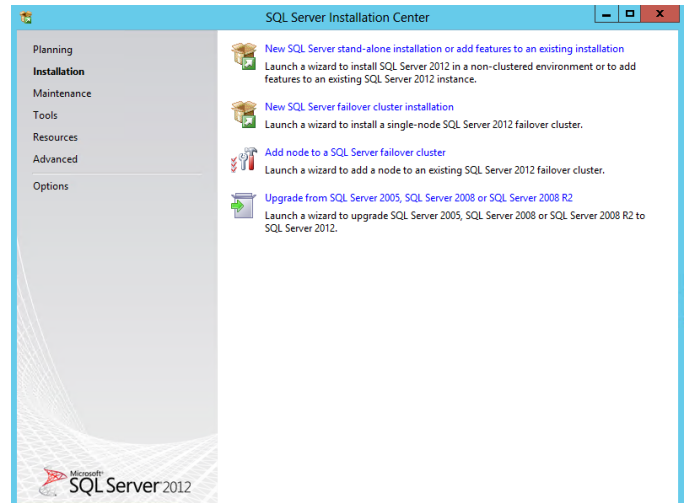
From the SQL Server 2012 with SP1 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



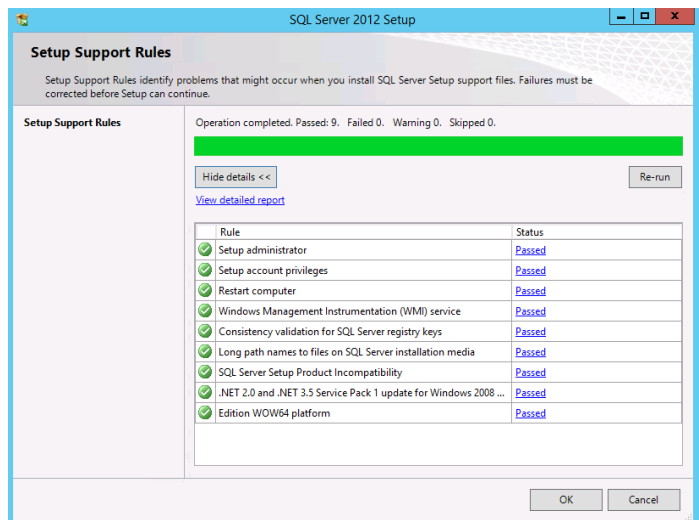
The **SQL Server Installation Center** will appear. Select **Installation**.



From the **SQL Server Installation Center**, click the **New SQL Server stand-alone installation or add features to an existing installation** link.

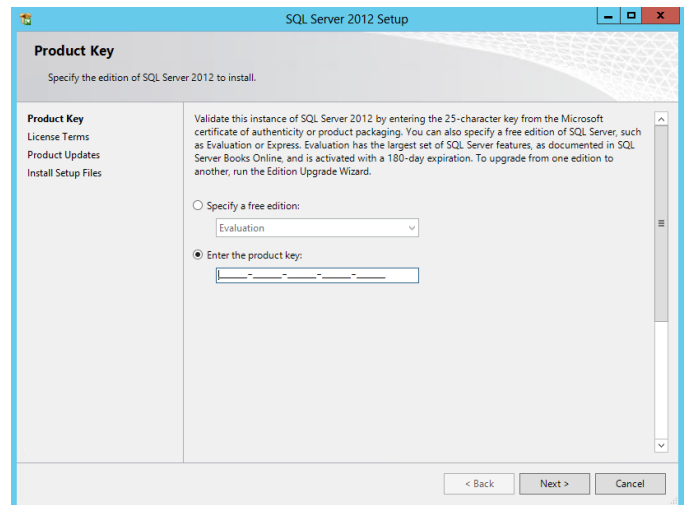


The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

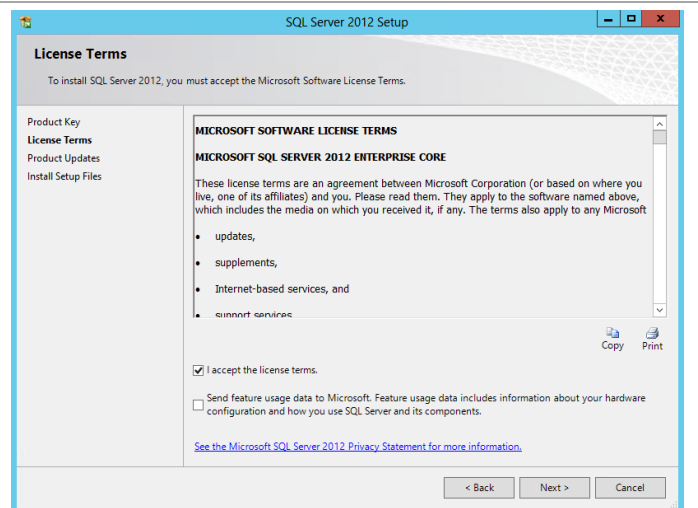


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

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

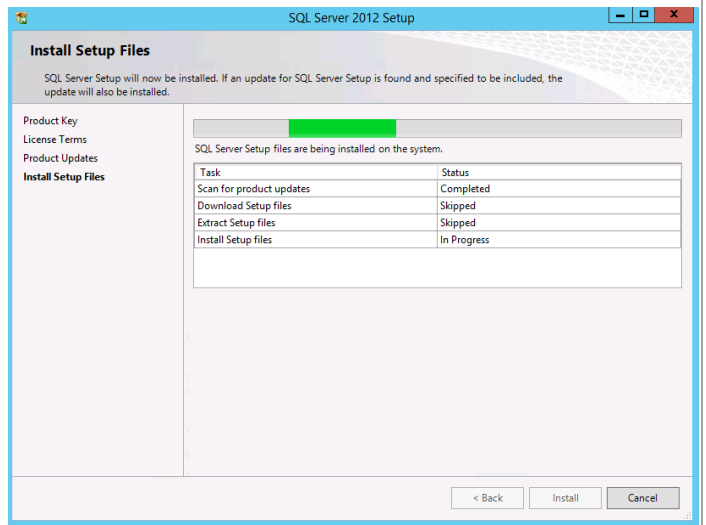


In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.

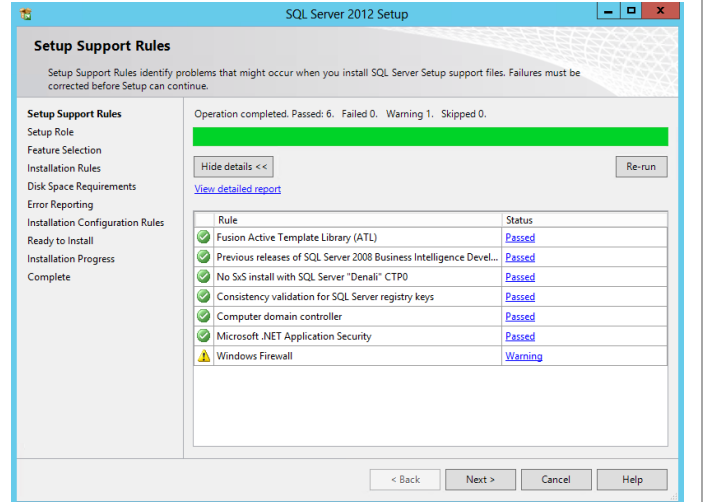




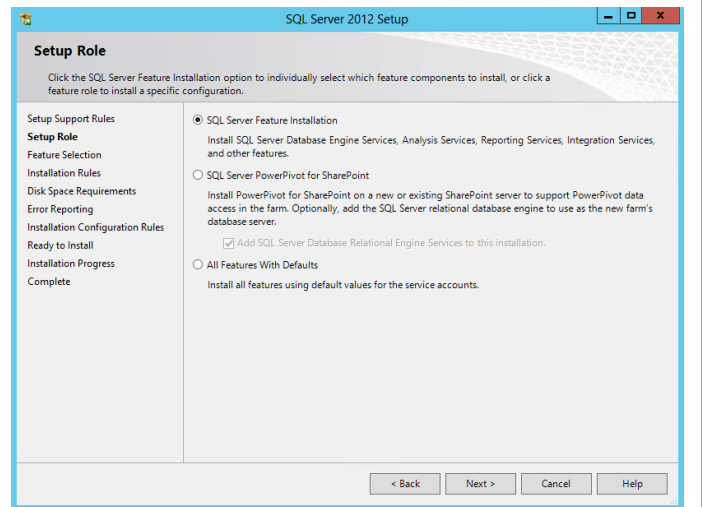
On the **Install Setup Files** dialog the update and install process will be displayed.



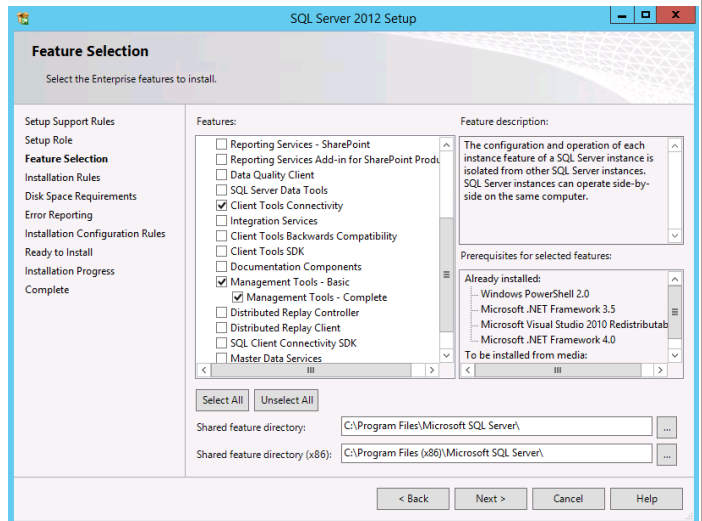
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



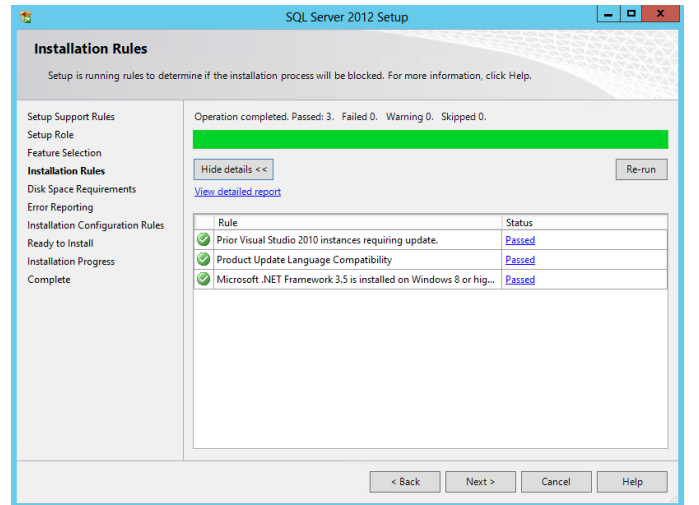
In the **Setup Role** dialog, select the **SQL Server Feature Installation** option and click **Next** to continue.



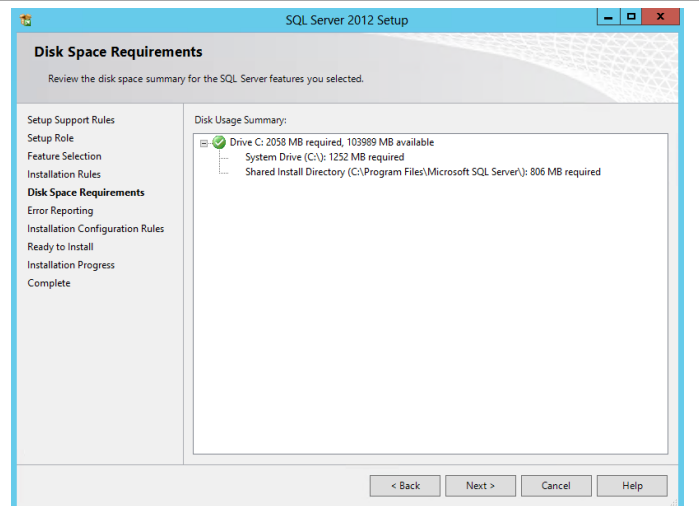
In the **Feature Selection** dialog, select the **Client Tools Connectivity, Management Tools – Basic** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.



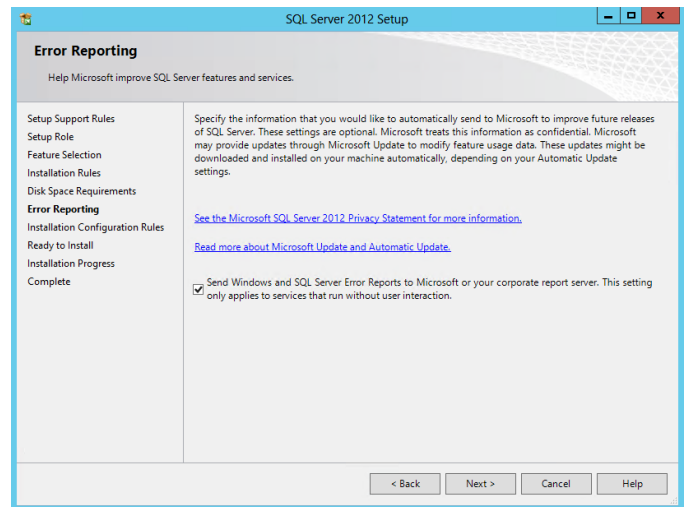
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



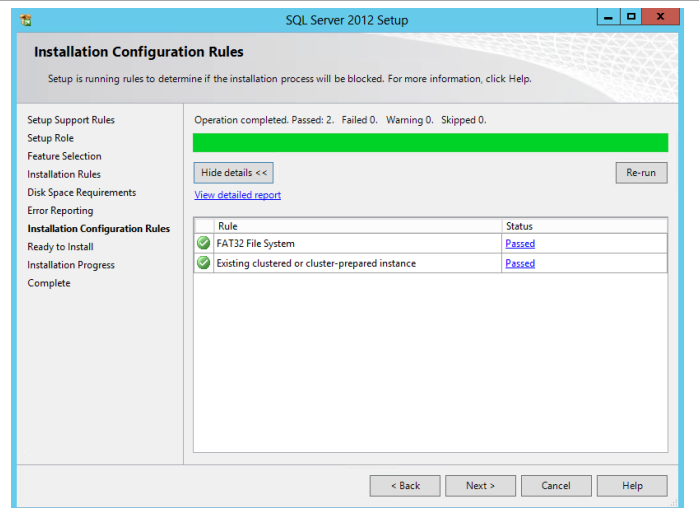
In the **Disk Space Requirements** dialog, verify that the installation has enough space on the target drive and click **Next** to continue.



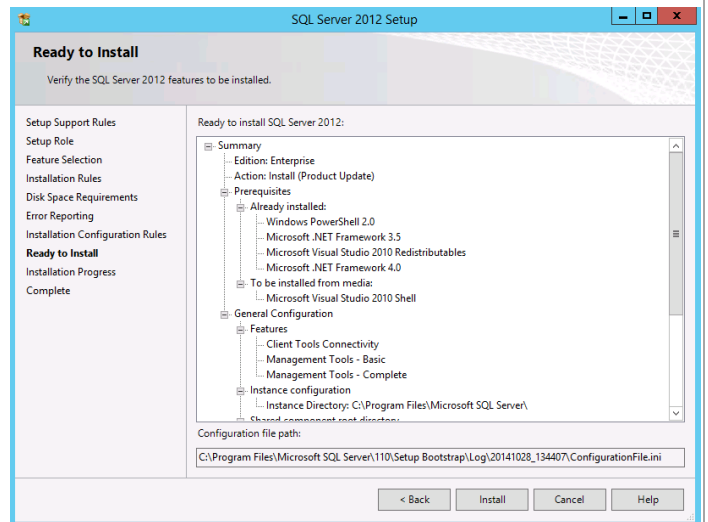
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



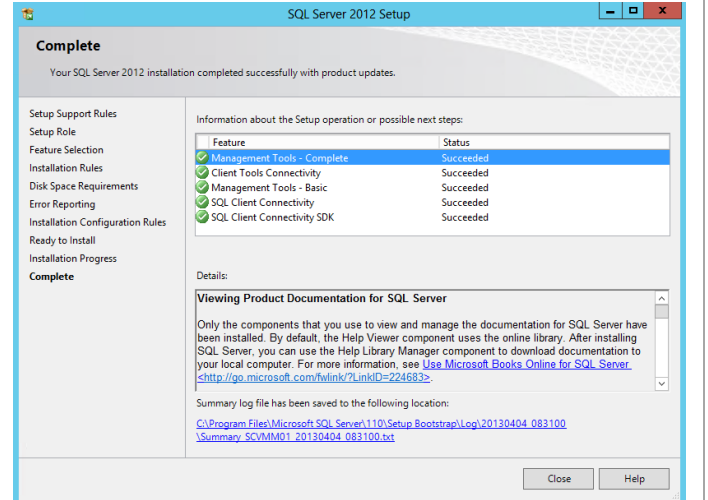
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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



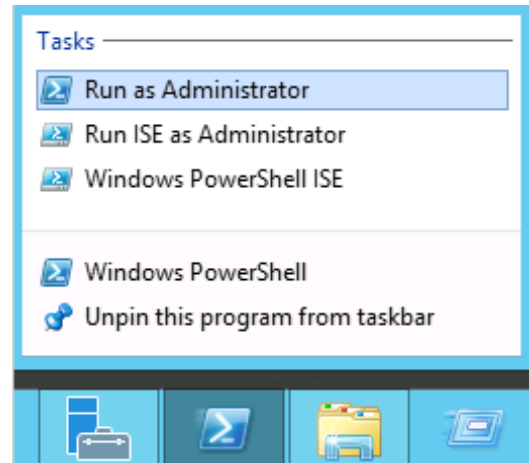
When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of SQL Server tools.



## 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.

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



Create a new cluster by executing the following command

```
New-Cluster -Name <cluster_name> -Node
<Node1>, <Nod-2> -NoStorage -
StaticAddress <cluster_ip_address>
```

```
PS C:\> New-Cluster -Name SCVM-Cluster01 -Node SCVM01,SCVM02 -NoStorage -StaticAddress 192.168.2.30
Report File Location: C:\Windows\cluster\Reports\Create Cluster Wizard SCVM-Cluster01 on 2014-10-28 At 15:09:43.mht
Name
----
SCVM-Cluster01
```

Rename the cluster networks to match their function.

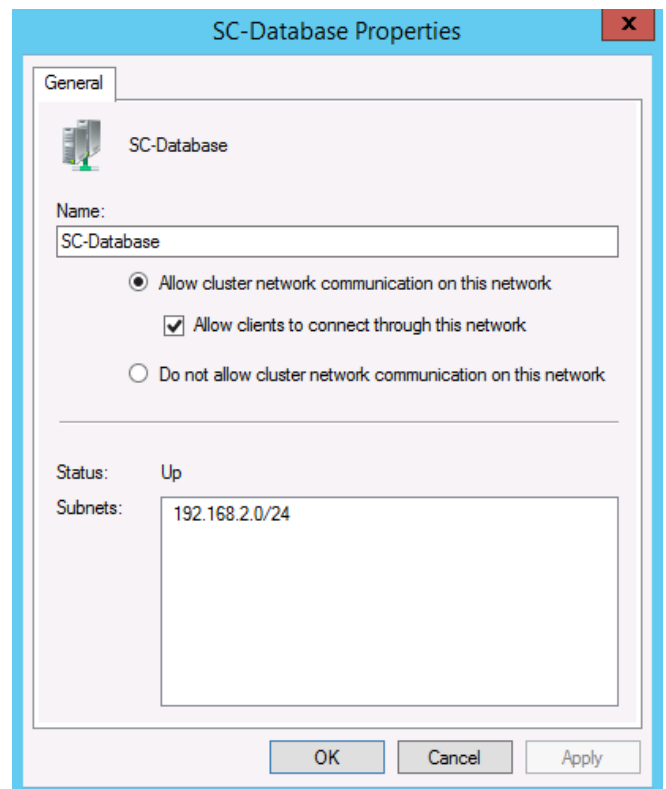
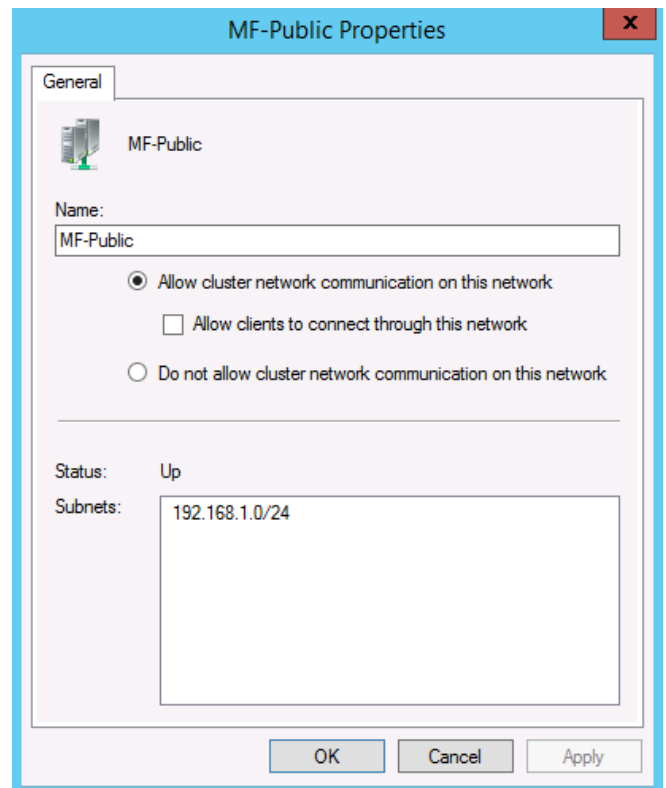
```
Get-ClusterNetworkInterface | ? Name -
like *SC-Database* | Group Network | %{
(Get-ClusterNetwork $'.Name).Name = 'SC-
Database'}
```

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

Using Failover Cluster Manager, expand the Networks object in the left tree view. Right-click each network and select properties.

**Uncheck** Allow clients to connect through this network for the MF-Public network.

**Check** Allow clients to connect through this network for the SC-Database network.

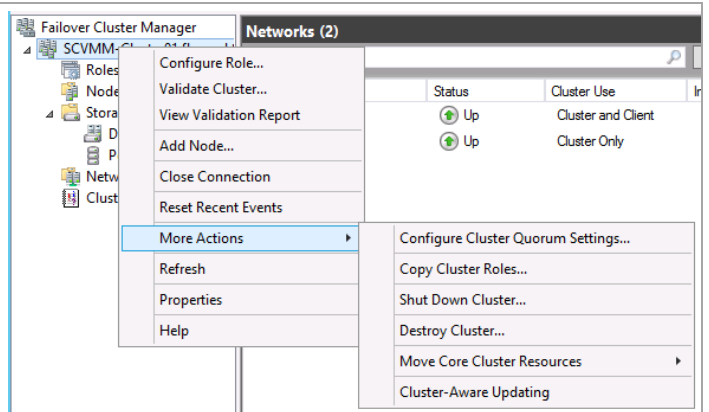


## Configure VMM Server Cluster to Use a File Share Witness

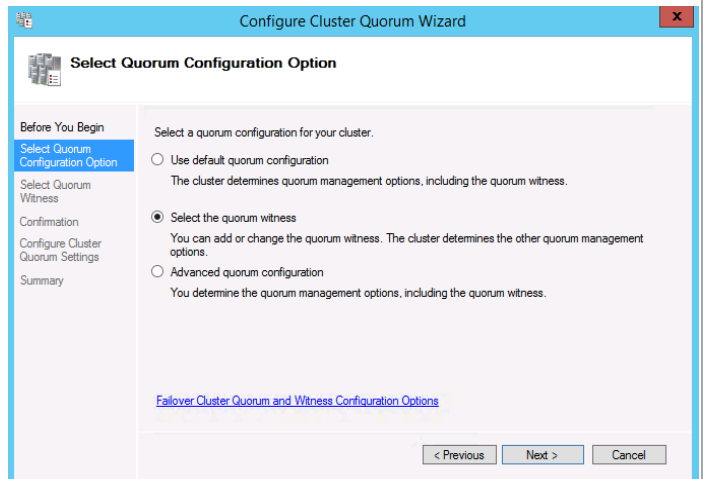
In failover cluster manager, select **More Actions** in the action pane and click **Configure Cluster Quorum Settings...**

The following cmdlet can be used to assign the quorum disk as an alternative to using Failover Cluster Manager.

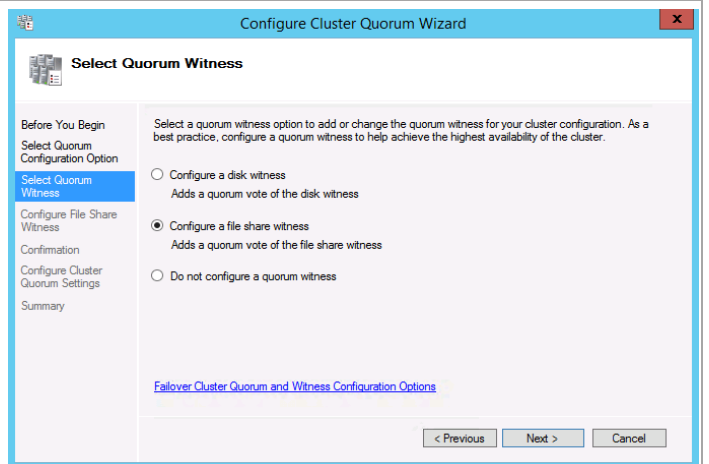
```
Set-ClusterQuorum -FileShareWitness
<Fileshare UNC>
```



Click Select **the quorum witness**, and click **Next**.

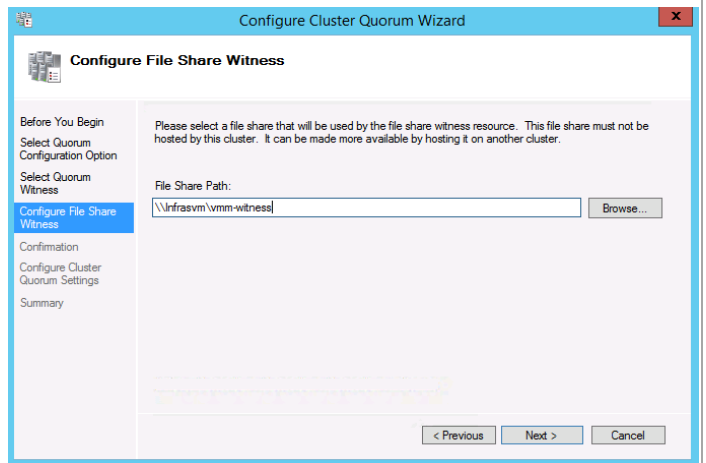


Select **Configure a file share witness** and click **Next**.

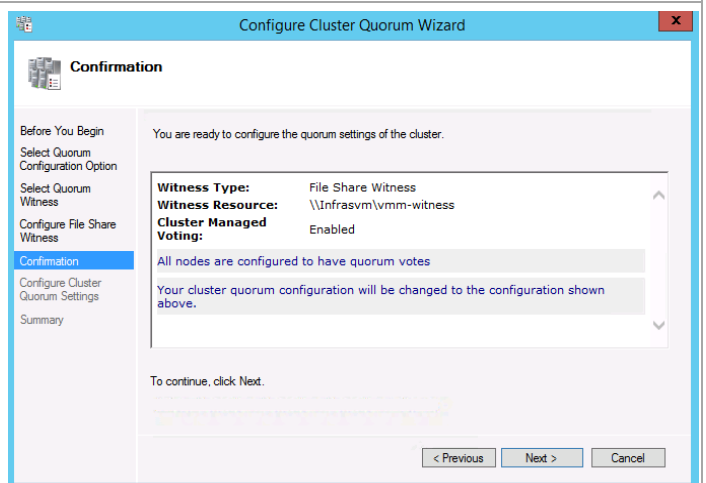




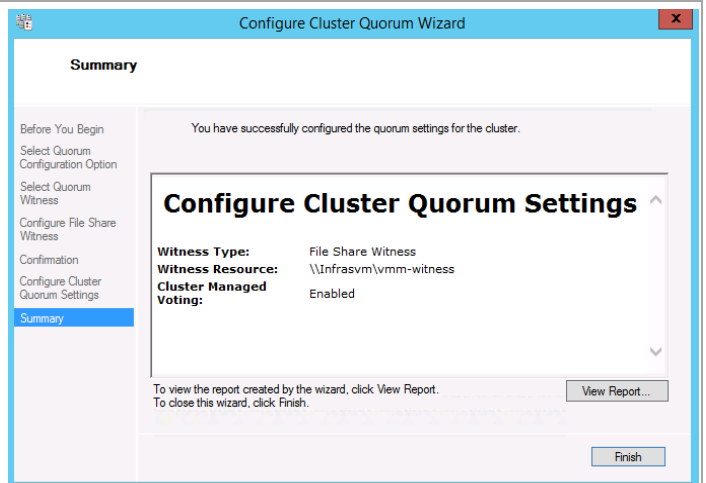
Enter the UNC for the file share witness. Click **Next**.



Confirm the settings and click **Next**.

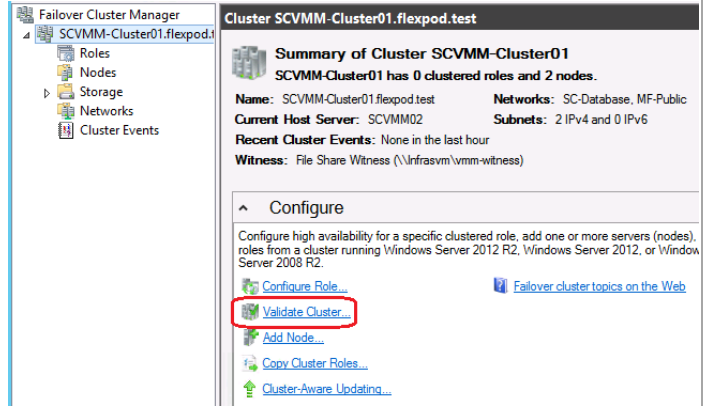


Review the results and click **Finish** to close the wizard screen.

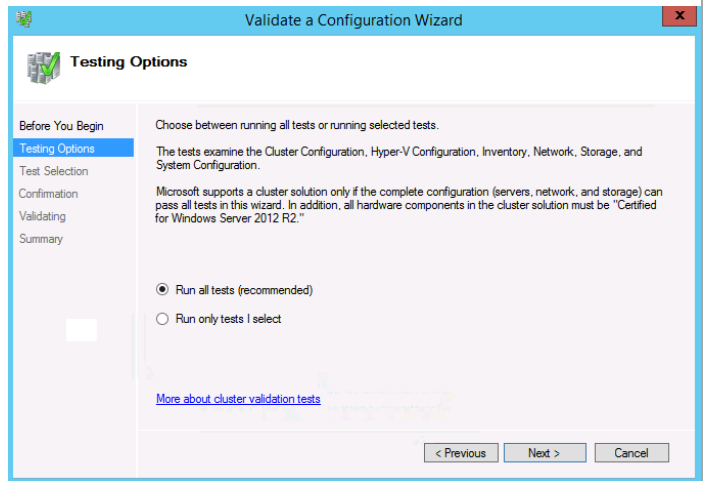


## Validate the VMM Server Cluster

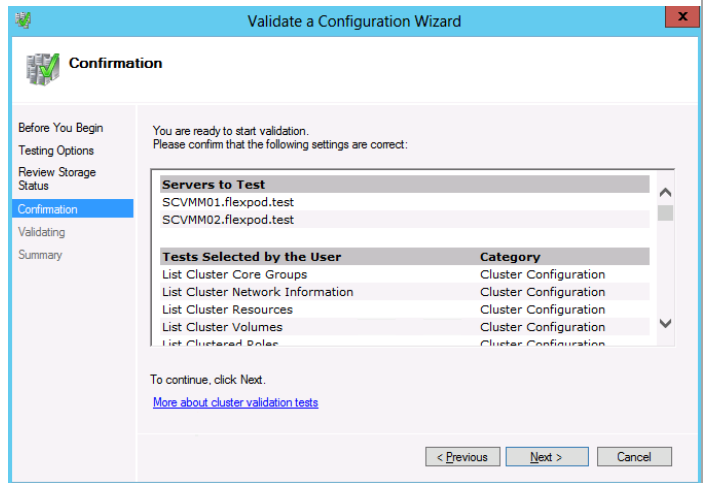
Select the SQL Server cluster in the left tree view and click Validate Cluster.



Select **Run all tests (recommended)** and click **Next**.

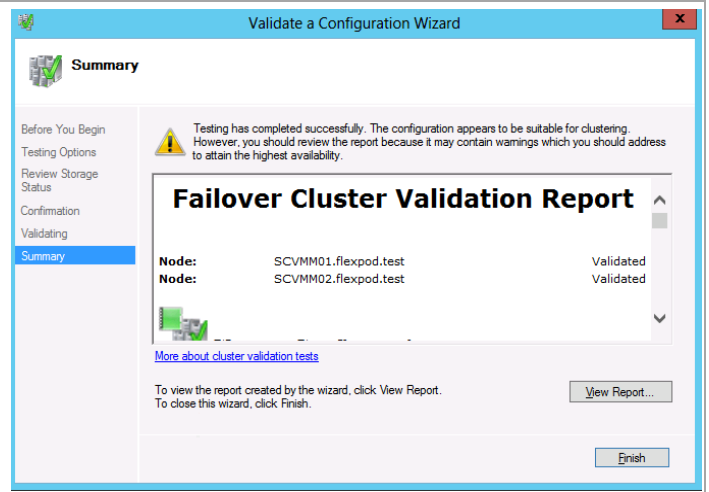


Confirm the selected options and click **Next**.



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

As one of the networks is configured with a default gateway, it is expected to receive warnings about lost packets. This is an acceptable warning.



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

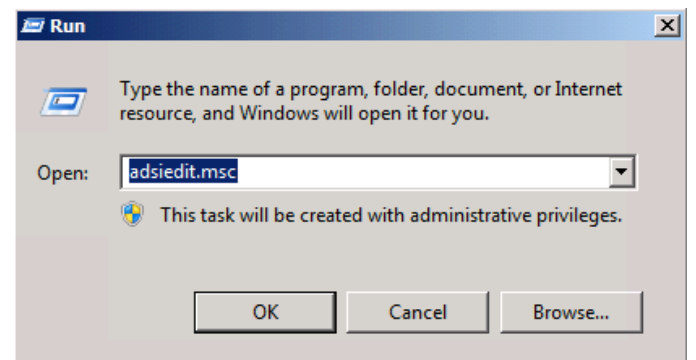
The Virtual Machine Manager installation requires that an Active Directory container be created to house the distributed key information for Virtual Machine Manager.<sup>6</sup>

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

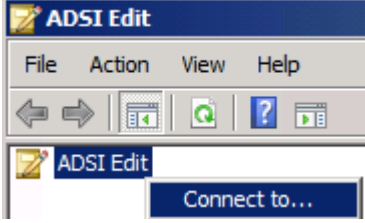
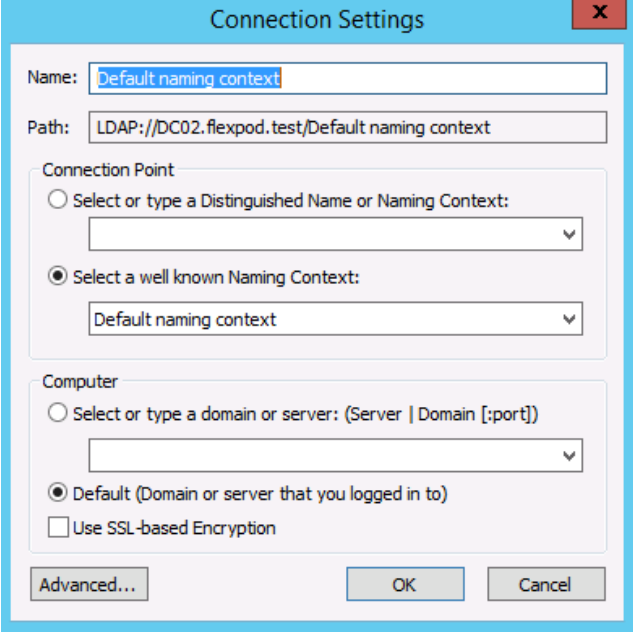
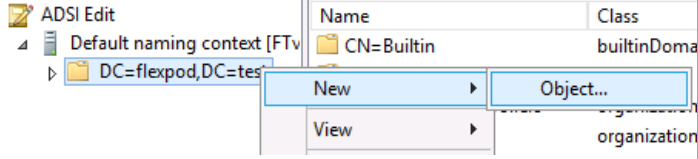
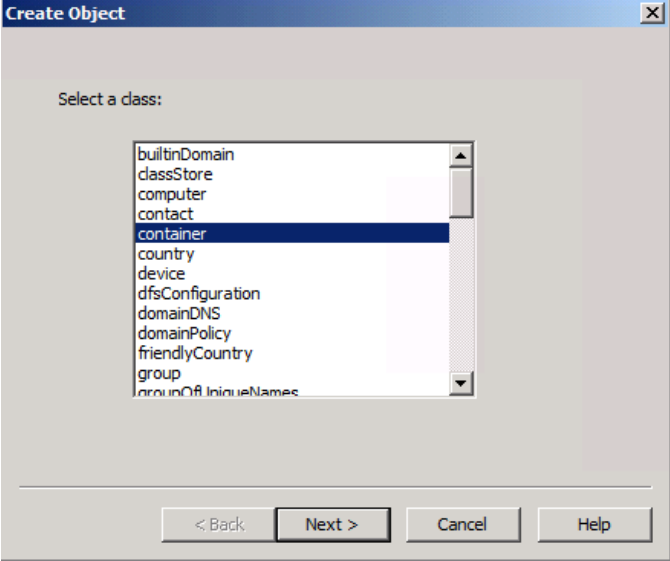
Perform the following steps to create an AD DS container to house the distributed key information. These instructions assume a Windows Server 2008 R2 domain controller is in use, similar steps would be followed for other versions of Active Directory including Windows Server 2008, Windows Server 2012,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

**Perform the following steps on a Domain Controller in the domain where Virtual Machine Manager is to be installed.**

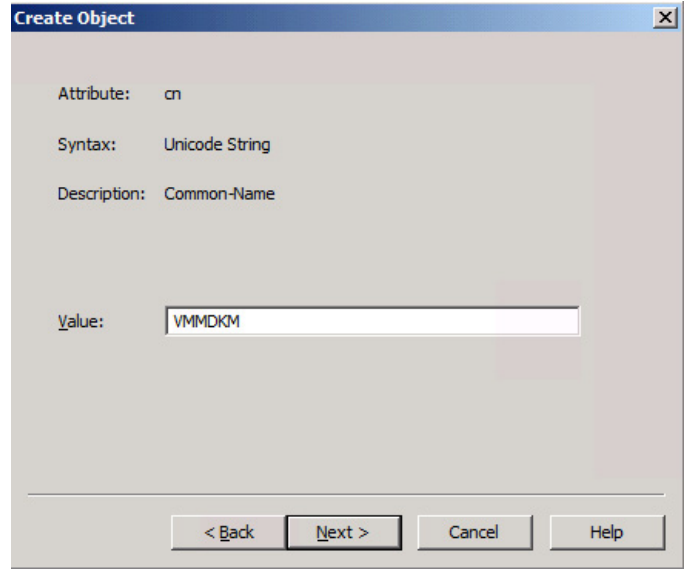
Log on to a Domain Controller with a user that has Domain Admin privileges and run **adsiedit.msc**.



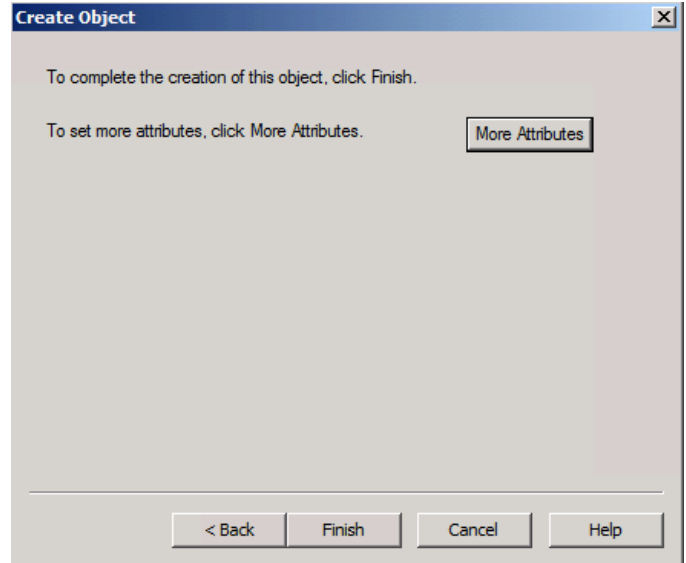
<sup>6</sup> Configuring Distributed Key Management in VMM - <http://technet.microsoft.com/library/gg697604.aspx>.

<p>Right-click the <b>ADSI Edit</b> node and select <b>Connect to...</b> from the context menu.</p>	
<p>In the <b>Connections Settings dialog</b> in the <b>Connection Point</b> section, select the <b>Select a well known Naming Context</b> option. Select <b>Default naming context</b> from the drop-down menu and click <b>OK</b>.</p>	
<p>Expand <i>Domain Default naming context</i> [<i>&lt;computer fully qualified domain name&gt;</i>], expand <i>&lt;distinguished name of domain&gt;</i>, right-click the root node and select <b>New – Object...</b> from the context menu.</p>	
<p>In the <b>Create Object</b> dialog box, select <b>Container</b> and then click <b>Next</b>.</p>	

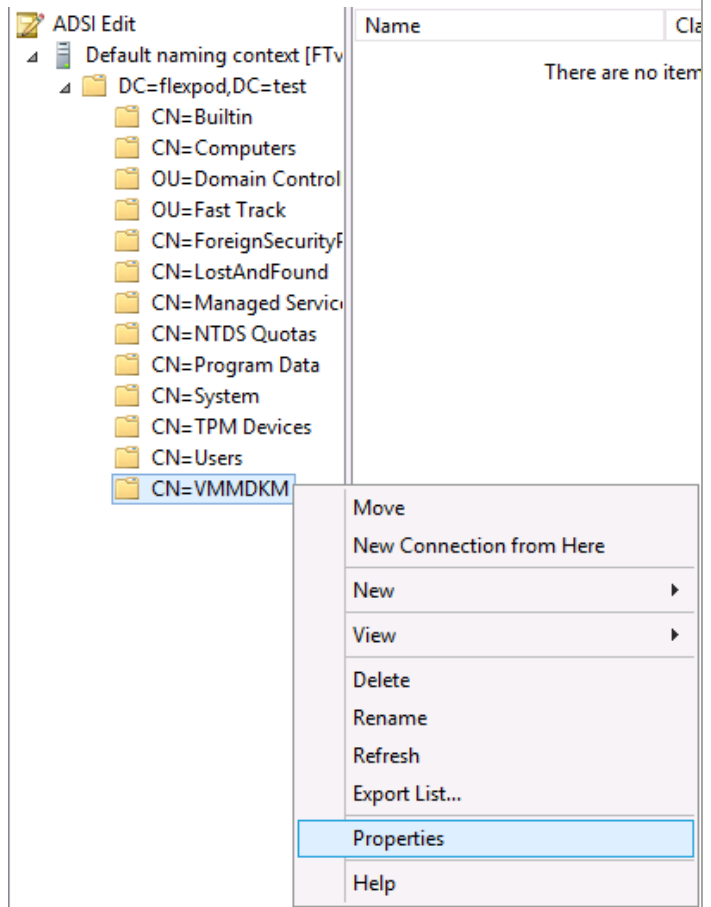
In the **Value** text box, type *VMMDKM* and then click **Next**.



Click **Finish** to create the container object.

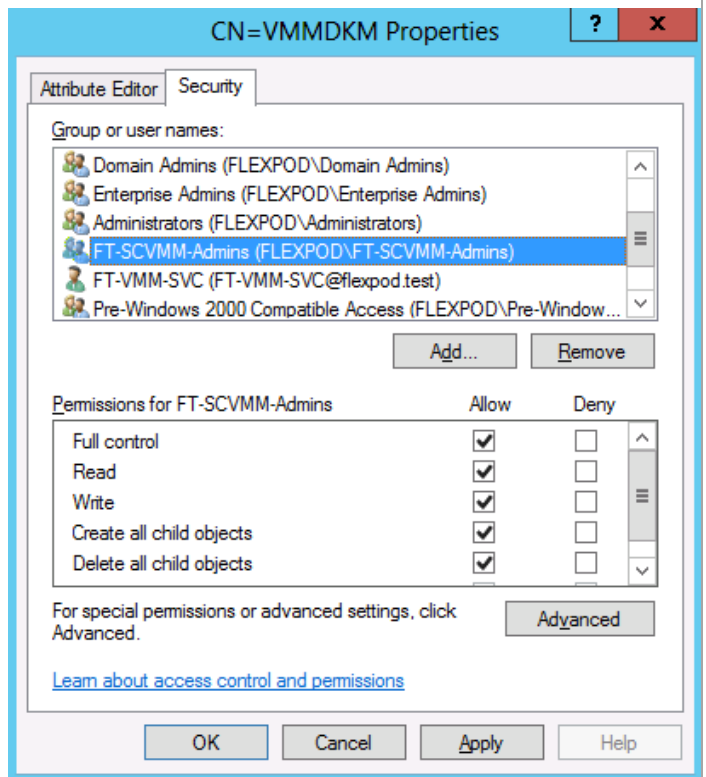


Within ADSI Edit, right-click the new **VMMDKM** object and then click **Properties**.



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

Click **OK** three times and close ADSI Edit.



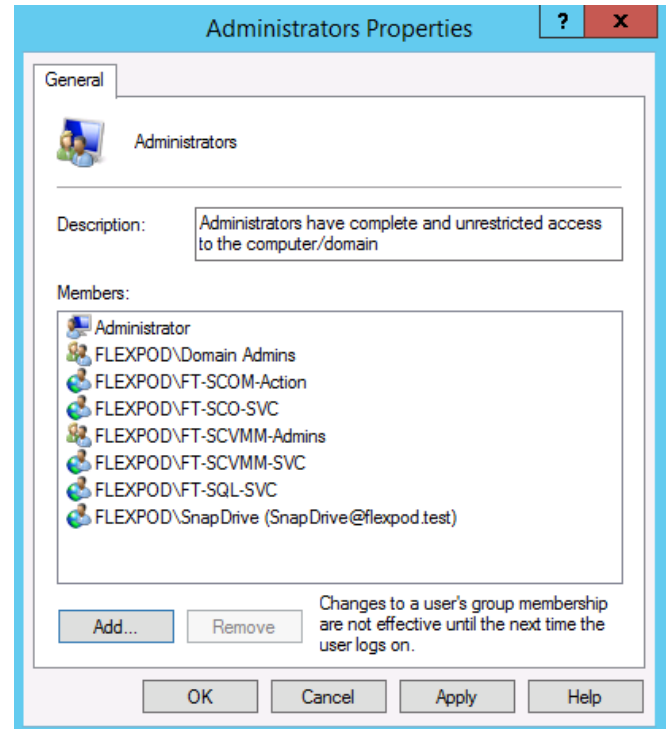
## 18.4 Installation

### Install the Virtual Machine Manager Failover Cluster Nodes

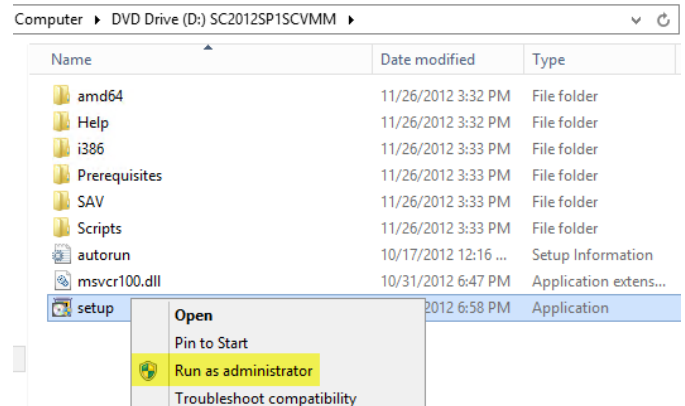
Perform the following steps on the **first Virtual Machine Manager** virtual machine.

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

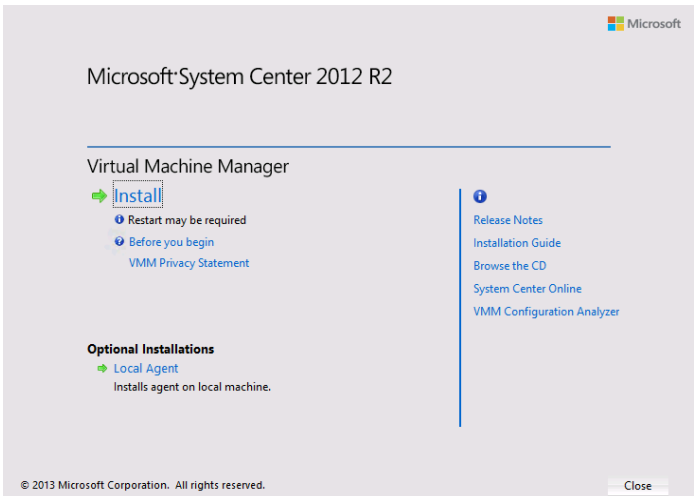
- Orchestrator service account.
- Operations Manager action account.
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.
- SQL Server service account.
- NetApp SnapDrive account



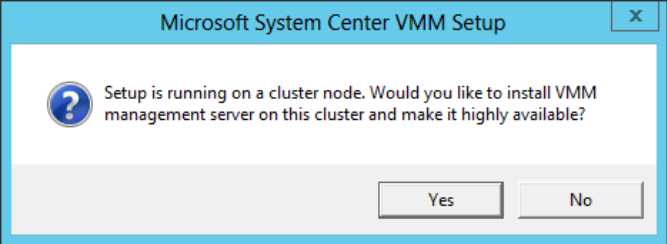
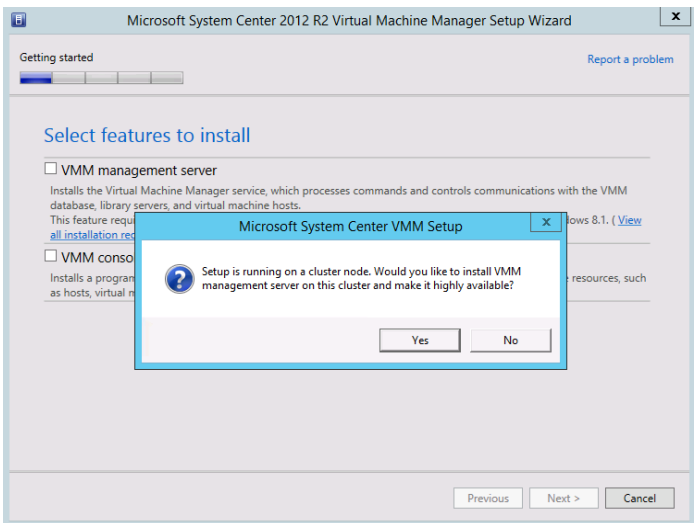
From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.

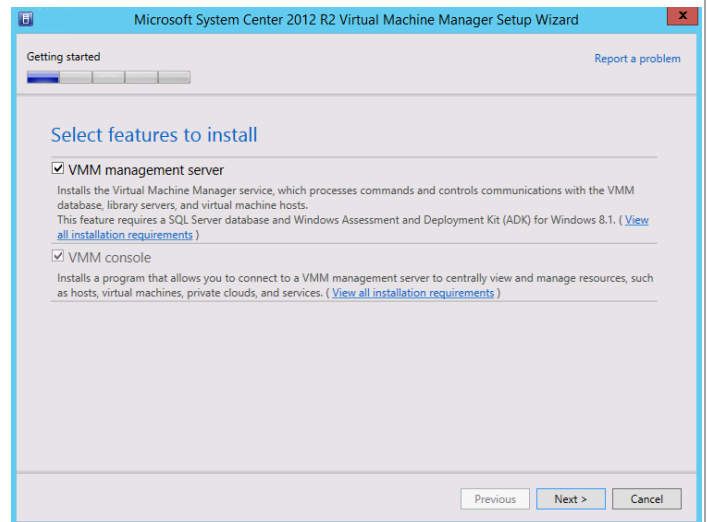


Attempting to select any feature will cause the cluster management server notice to appear. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard.



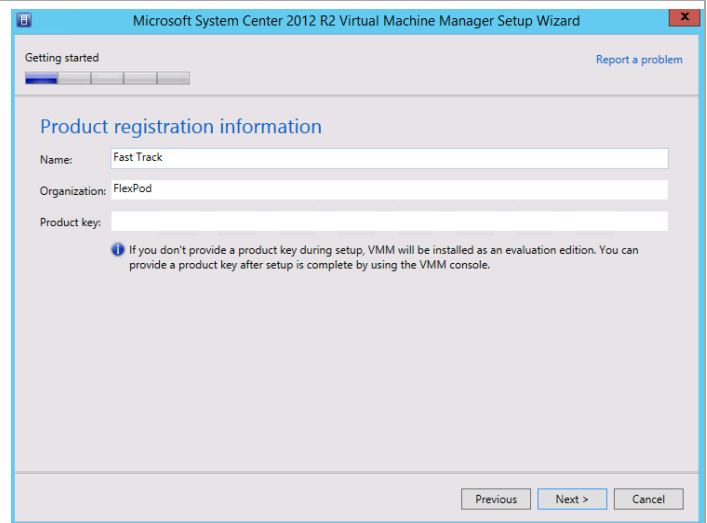


In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **VMM console** installation option check box will be selected by default. Click **Next** to continue.



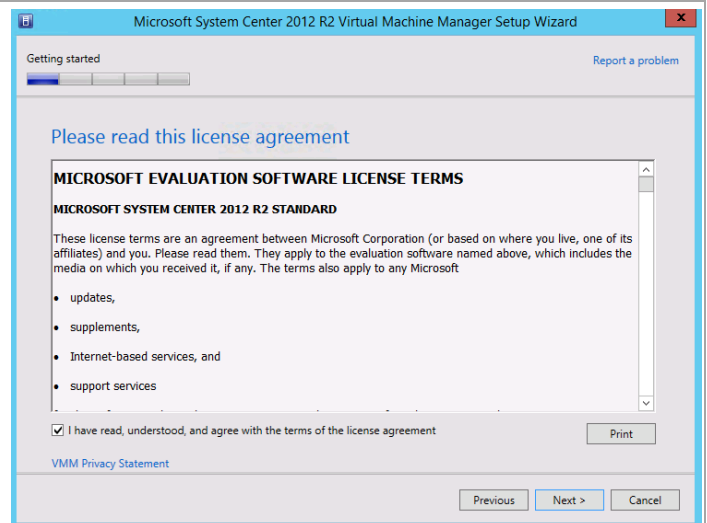
In the **Product registration information** dialog, enter the following information in the provided text boxes:

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

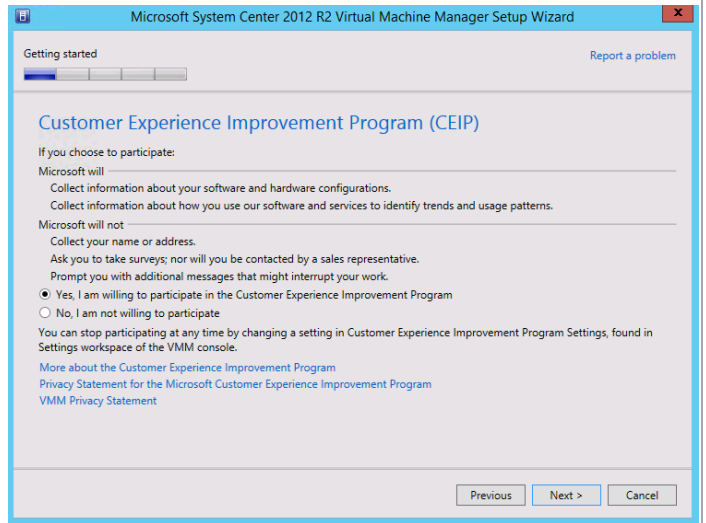


Click **Next** to continue.

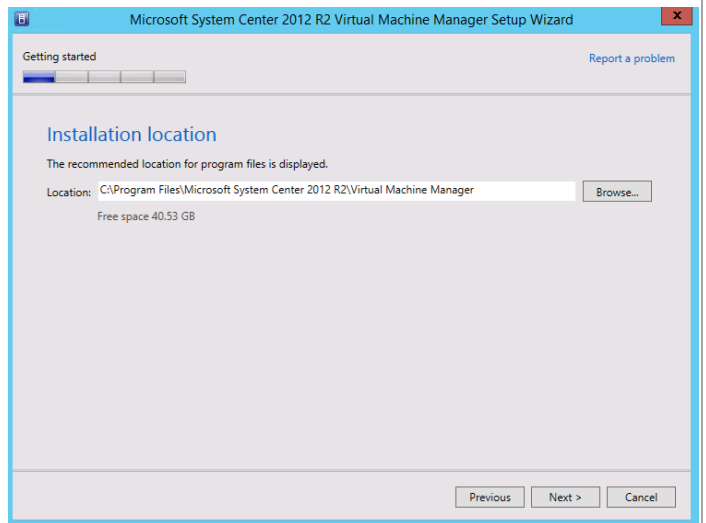
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



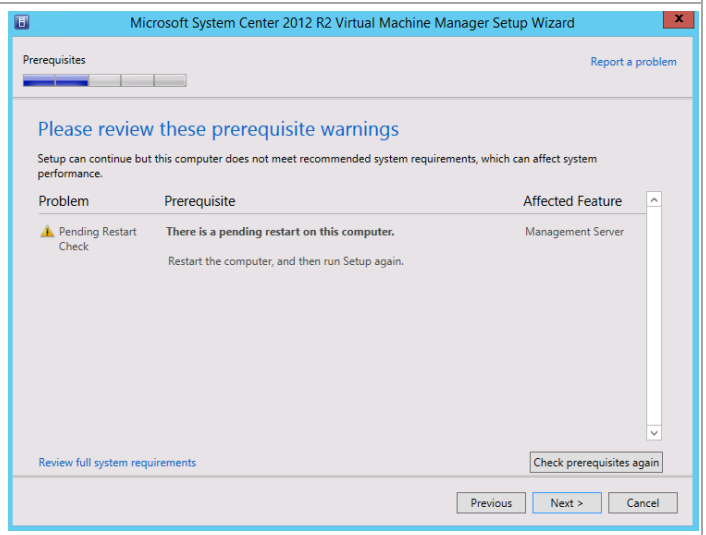
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.



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

**The following is just an example of that UI.**

If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



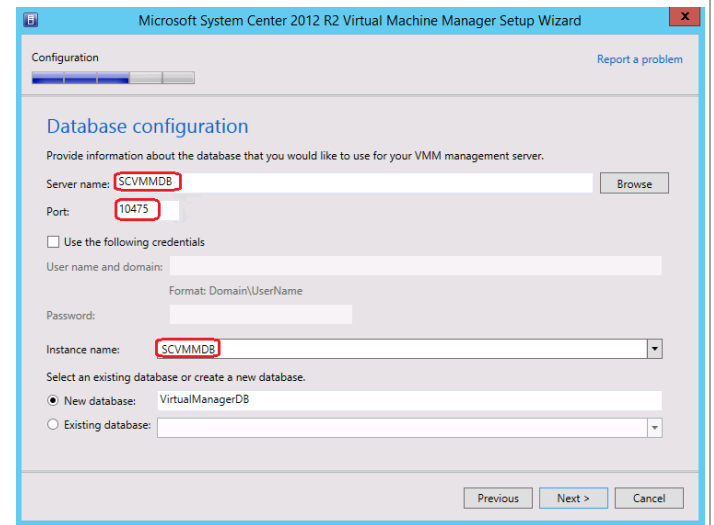
In the **Database configuration** dialog, enter the following information in the provided text boxes:

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

Verify that the **Use the following credentials** check box is clear. In the **Instance name** drop-down menu, select the Virtual Machine Manager database instance deployed earlier in the SQL Server cluster.

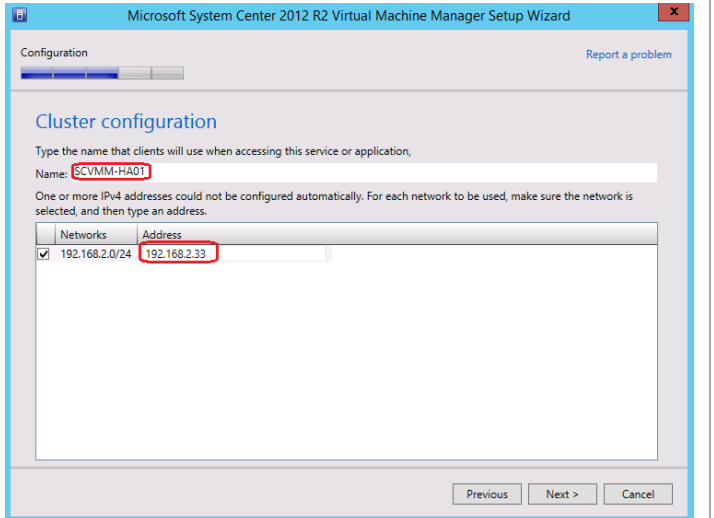
In the **Select an existing database or create a new database** option, select the **New database** option and accept the default database name of *VirtualManagerDB*.

Click **Next** to continue.



In the **Cluster Configuration** dialog, in the **Name** field, provide a name for the Virtual Machine Manager cluster service.

If the cluster node you are installing is configured with static IP addresses you will also need to provide an IP address for the Virtual Machine Manager cluster service. If the cluster node is configured to use DHCP, no additional information is required.

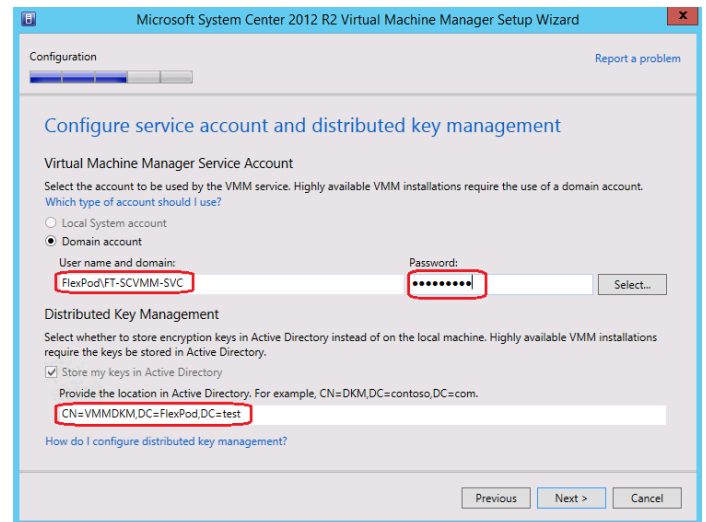


In the **Configure service account and distributed key management** dialog, in the **Virtual Machine Manager Service account** section, select the **Domain account** option. Enter the following information in the provided text boxes:

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

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

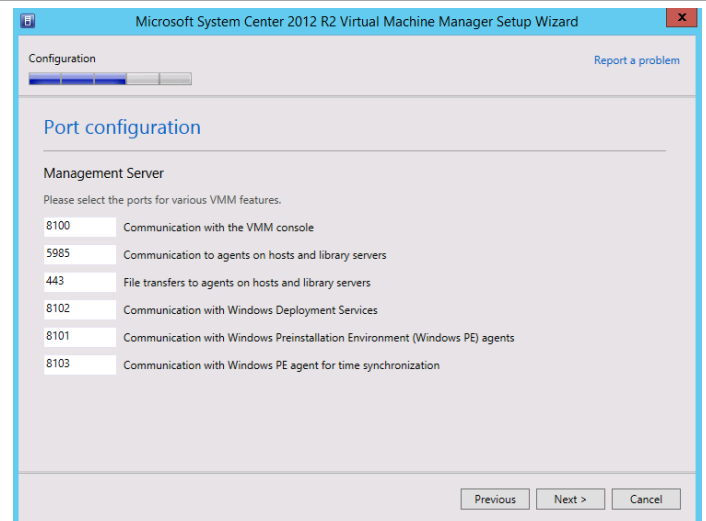
Click **Next** to continue.



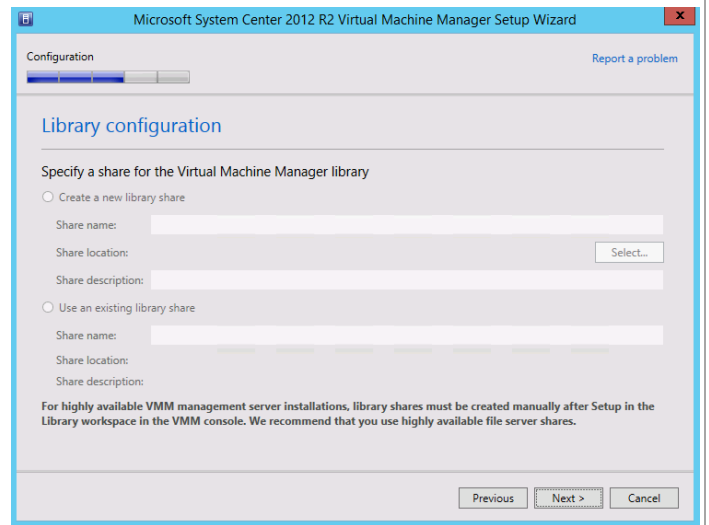
In the **Port configuration** dialog, accept the default values in the provided text boxes:

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

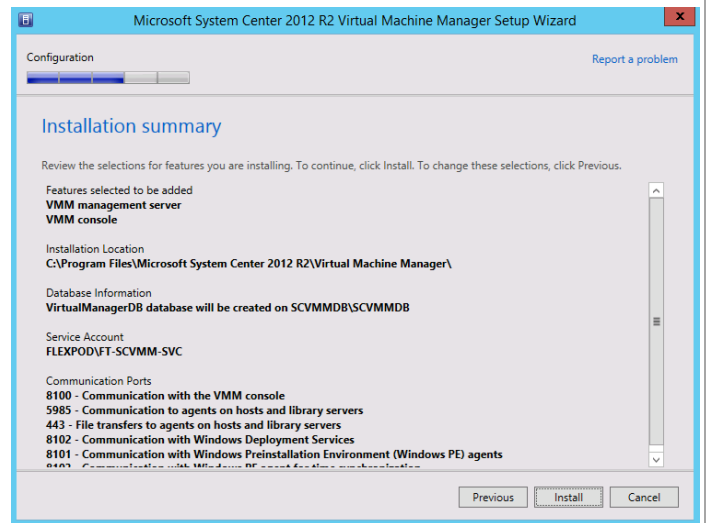
Click **Next** to continue.



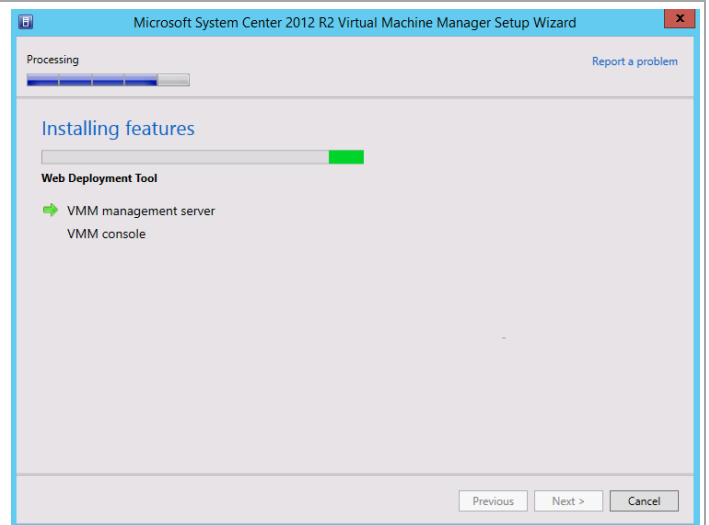
In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.



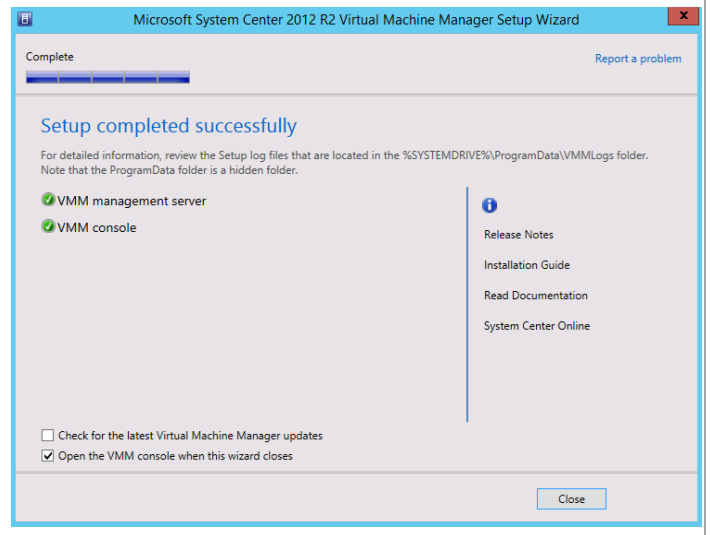
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



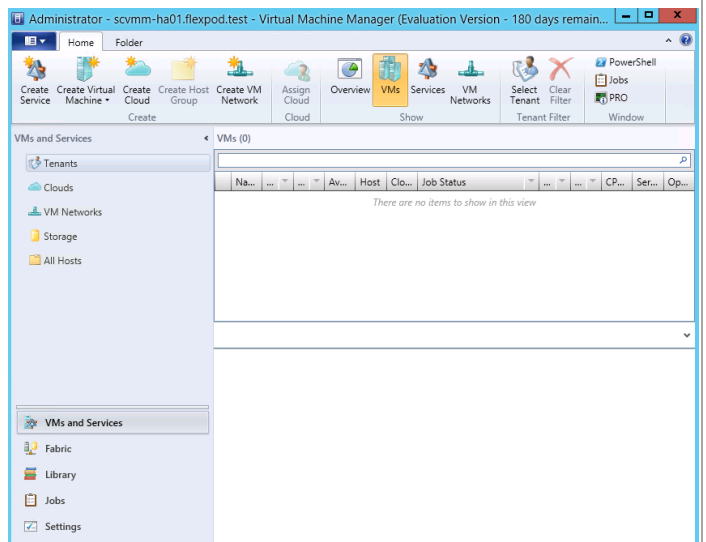
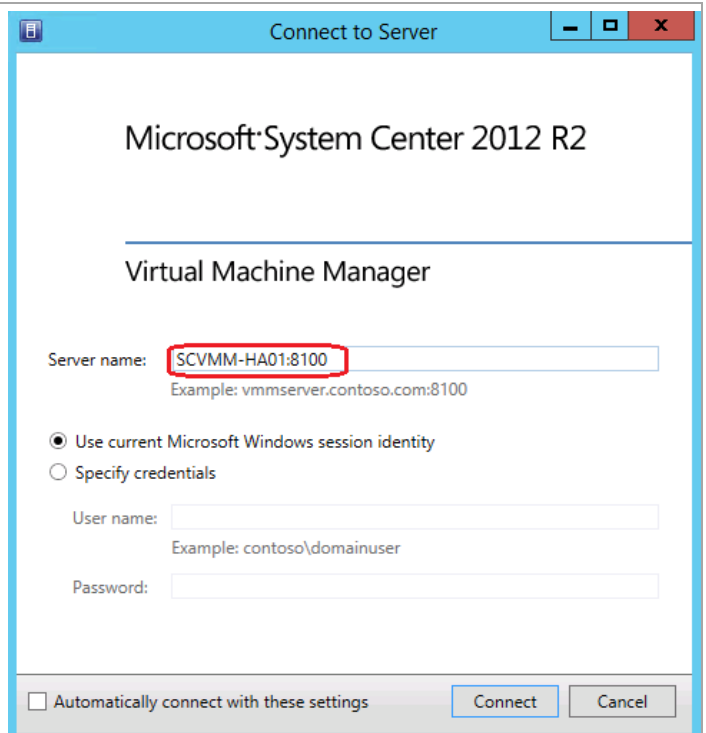
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** dialog. Clear the check box for checking for the latest updates, and click **Close** to complete the installation.



When complete, launch the Virtual Machine Manager console to verify the installation occurred properly. Set the **Server name** value to match the name that was provided for the **Cluster Resource** name during setup (for example, SCVMM-HA01:8100). Verify that the console launches and connects to the Virtual Machine Manager instance installed.

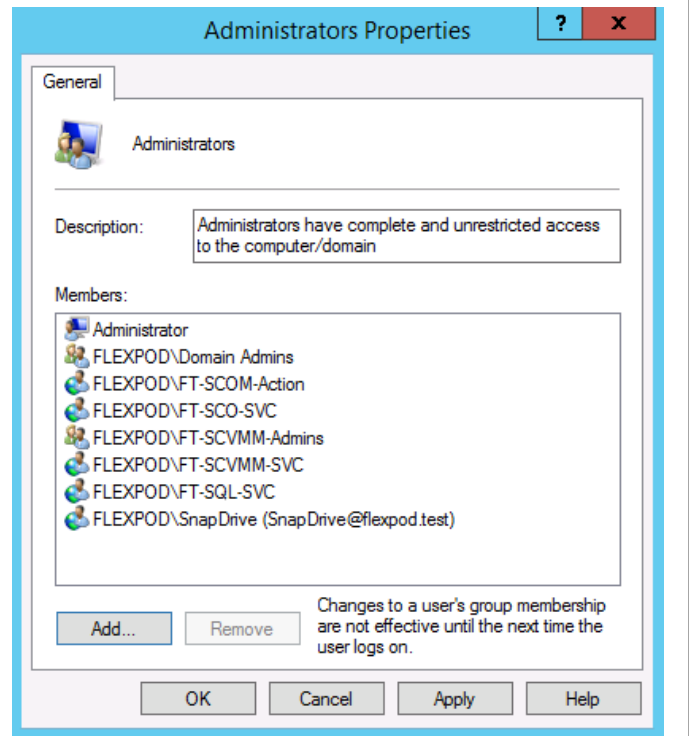


Perform the following steps on the **second Virtual Machine Manager** virtual machine.

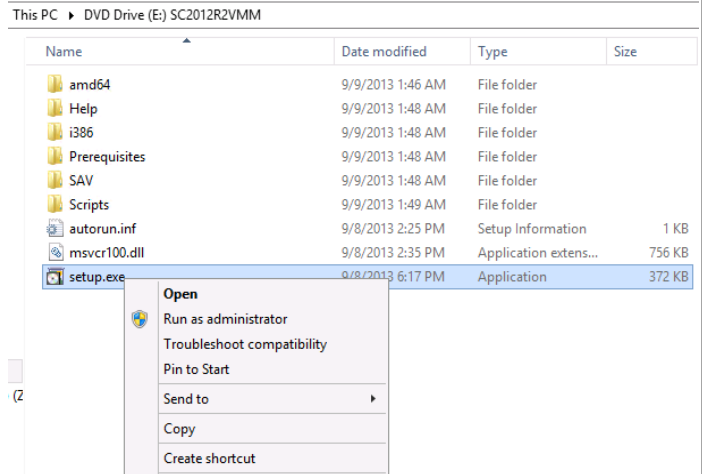
Log on to the **second** Virtual Machine Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager Virtual Machine:

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

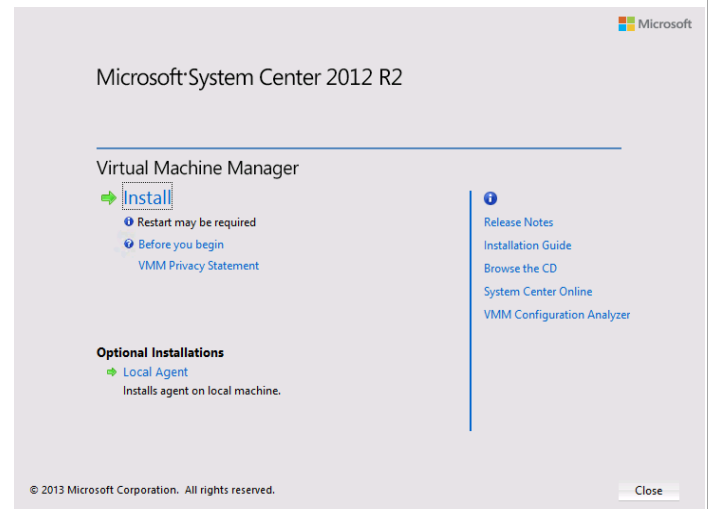


From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



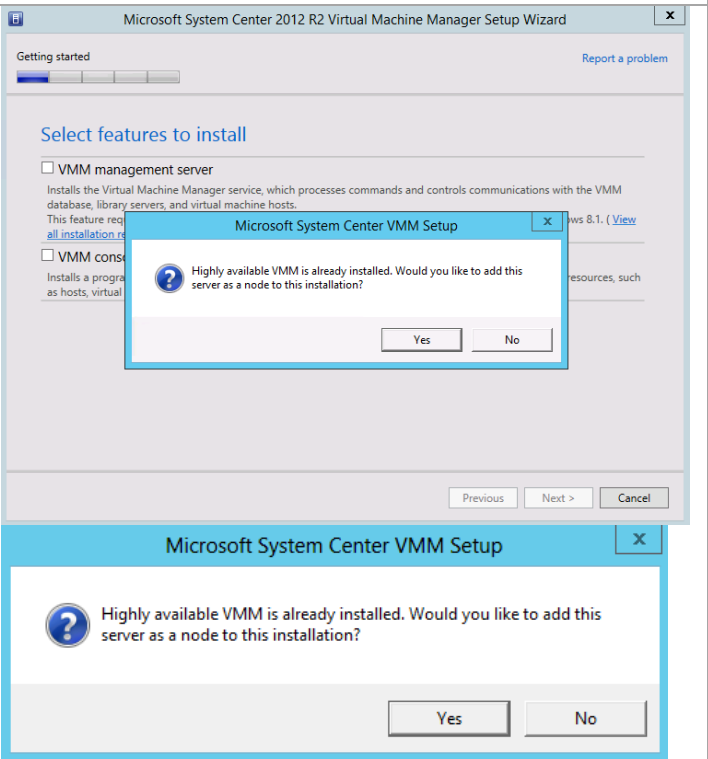


The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.

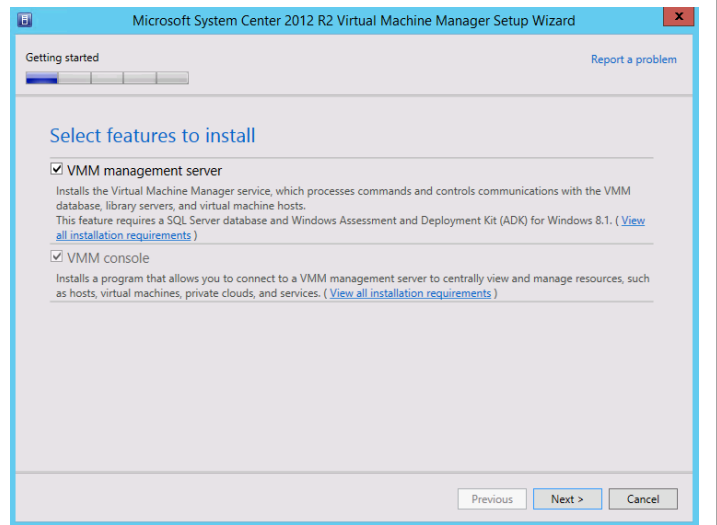


Attempting to select any feature will cause the cluster management server notice to appear. Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard and add the second node.

**Note:** Virtual Machine Manager can be deployed on up to 16 cluster nodes but only a single node can be active at any time.

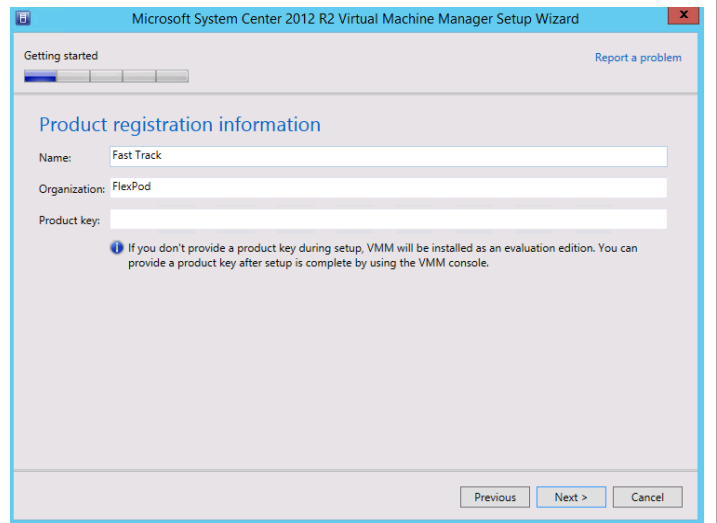


In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **Virtual Machine Manager console** installation option check box will be selected by default. Click **Next** to continue.



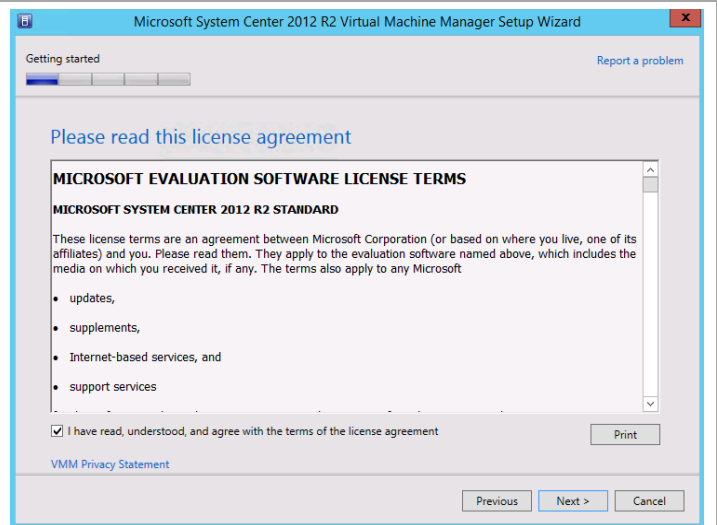
In the **Product registration information** dialog, enter the following information in the provided text boxes:

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



Click **Next** to continue.

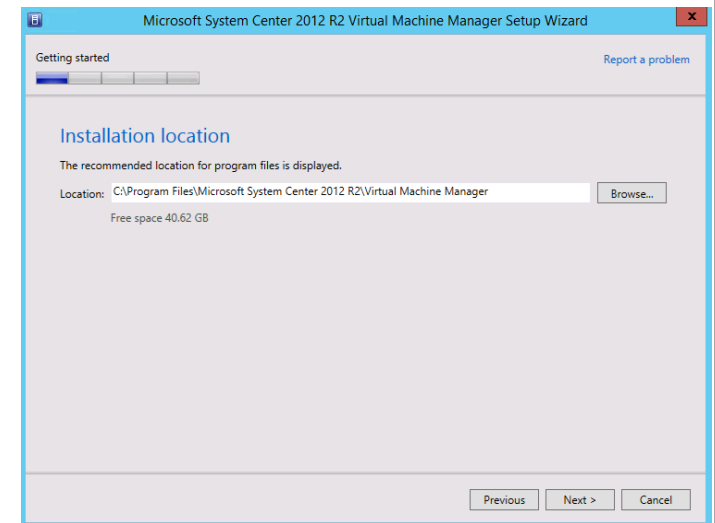
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



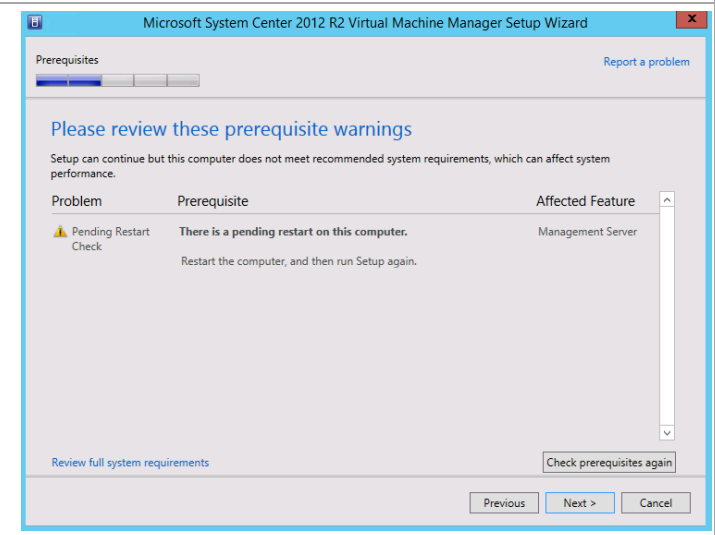
In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.



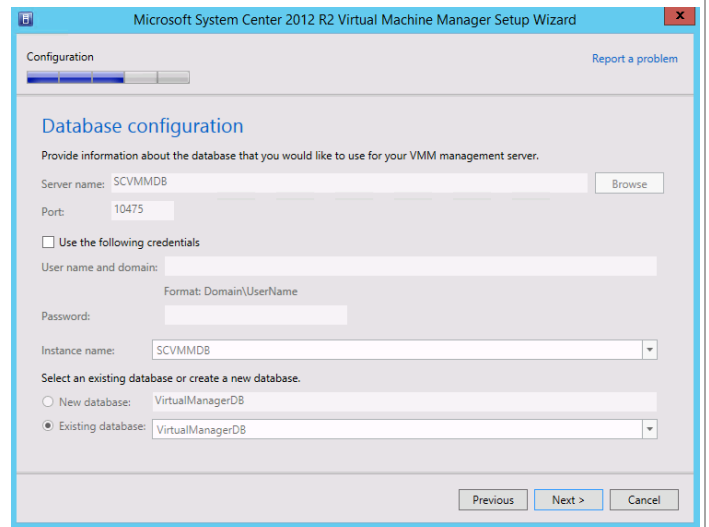
**Note:** The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy.

**The following is just an example of that UI.**

If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



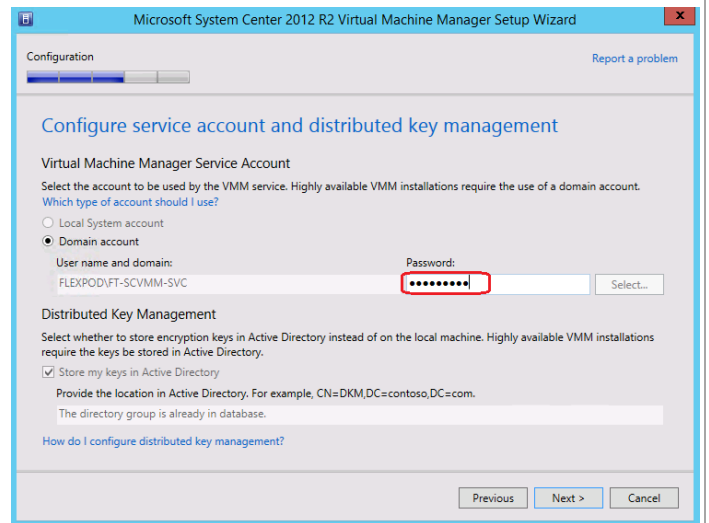
In the **Database configuration** dialog, all options are greyed out when adding an additional node to an existing Virtual Machine Manager cluster. Click **Next** to continue.



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

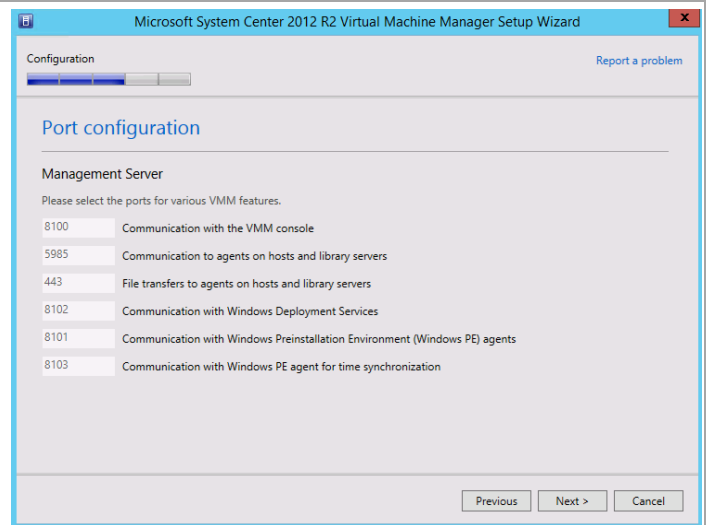
- **Password** – specify the password for the Virtual Machine Manager service account identified above.

Click **Next** to continue.

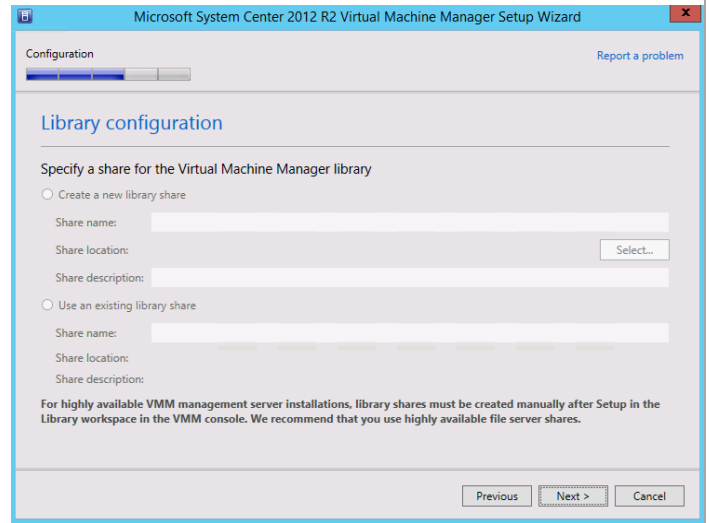


In the **Port configuration** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields are greyed out.

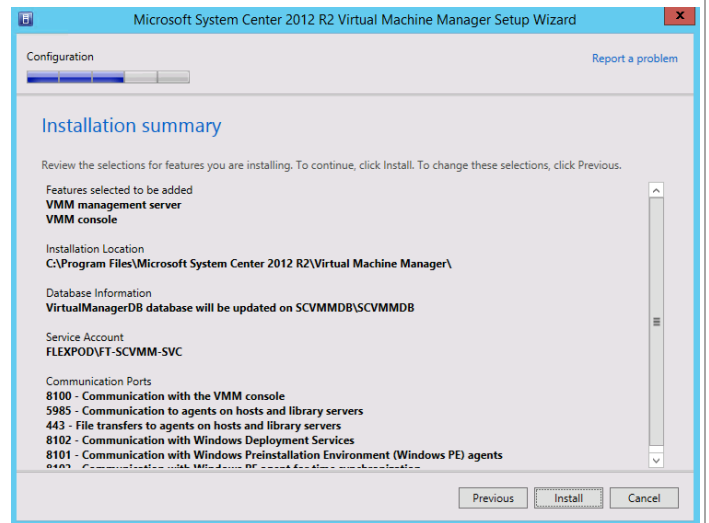
Click **Next** to continue.



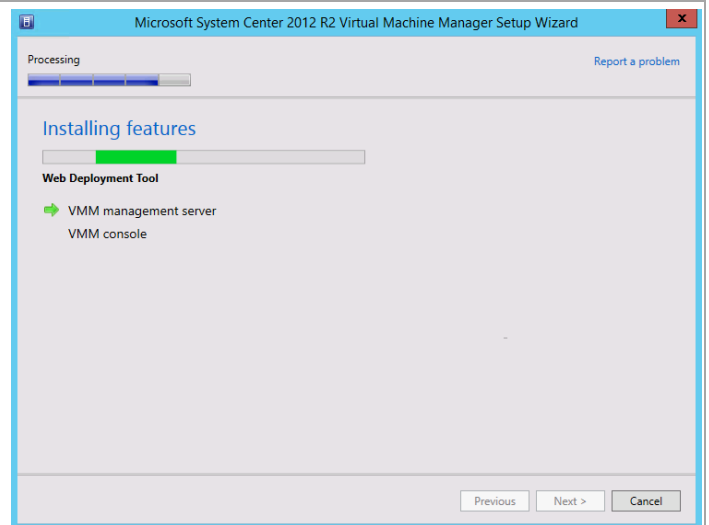
In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.



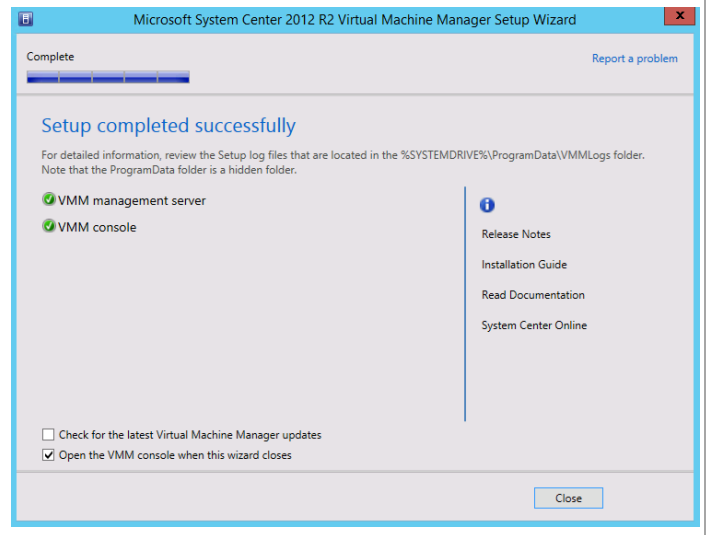
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



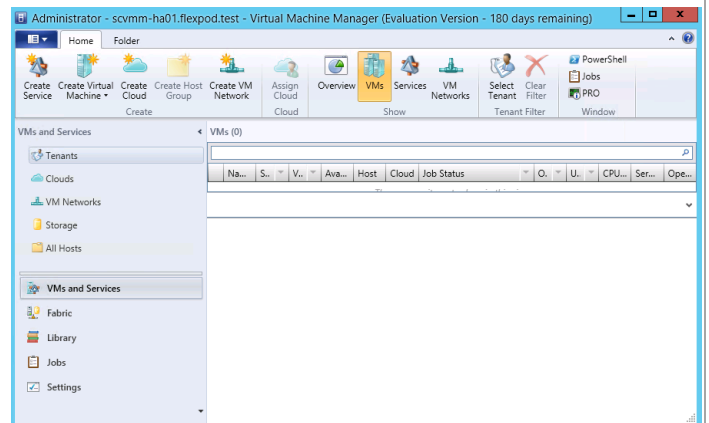
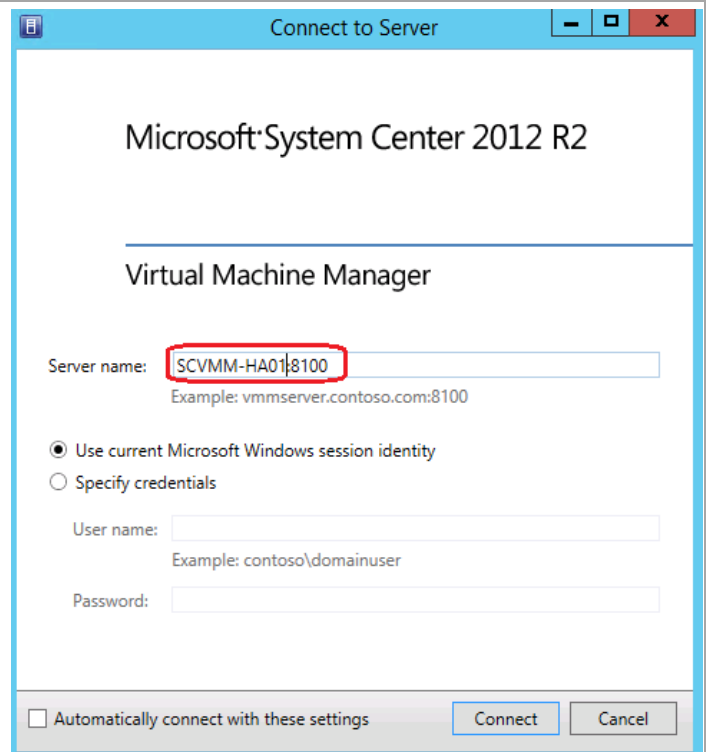
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** dialog. Clear the check box to check for latest updates and click **Close** to complete the installation.

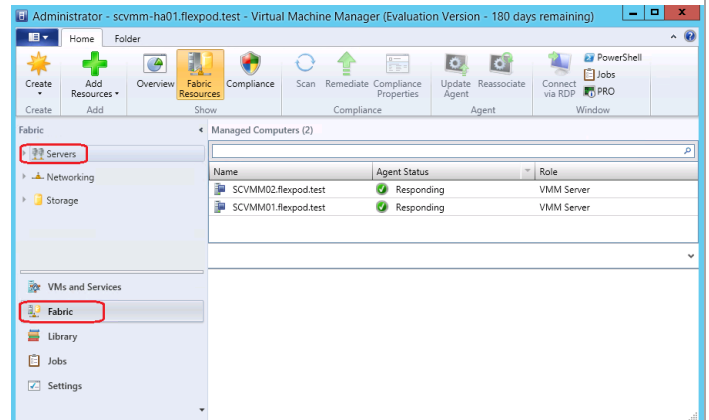


When complete, launch the Virtual Machine Manager console to verify the installation occurred properly. Set the **Server** Name value to match the name that was provided for the **Cluster Resource** name during setup (for example, SCVMM-HA01:8100). Verify that the console launches and connects to the Virtual Machine Manager instance installed.



In the **Virtual Machine Manager Console**, select **Fabric** and then **Servers**.

Verify that both cluster nodes are listed as *VMM Servers* under **Role** and that both nodes are listed as *Responding* under **Agent Status**.



## 18.5 Create Virtual Machine Manager Library Share

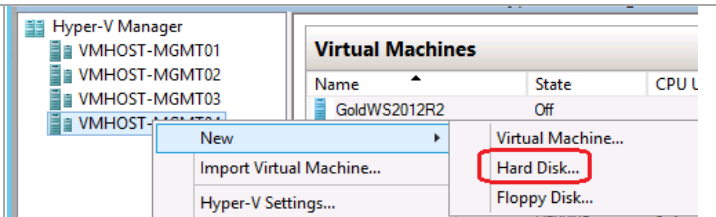
In a highly available installation of Virtual Machine Manager, the Virtual Machine Manager Library must reside on a server outside of the Virtual Machine Manager Cluster infrastructure; it is not a supported configuration to reside upon the Virtual Machine Manager cluster or its nodes. In addition, making the Virtual Machine Manager Library highly available is a recommended practice given that the Virtual Machine Manager servers themselves are highly available. The recommendation is to create this share on a highly available file service. While any file server cluster will suffice, this document will detail the steps required to host the VMM library up on the SQL Server cluster created earlier in this document.

### Create VHDX on Hyper-V Host

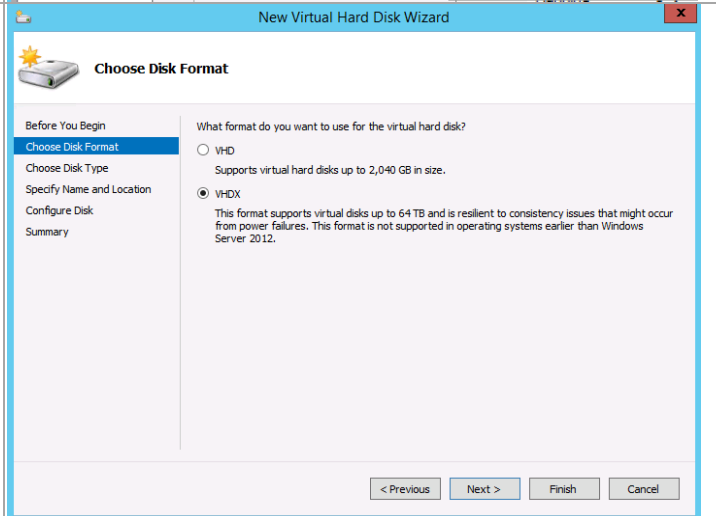
The share needs a virtual hard disk added to the SQL Server cluster on which the information will be stored. The following steps show how to create a new virtual hard disk.

Perform the following steps on one of the **Hyper-V hosts**.

In Hyper-V Manager, right-click on a host and select **New** and then **Hard Disk...**  
Click **Next** on the **Before You Begin** window.

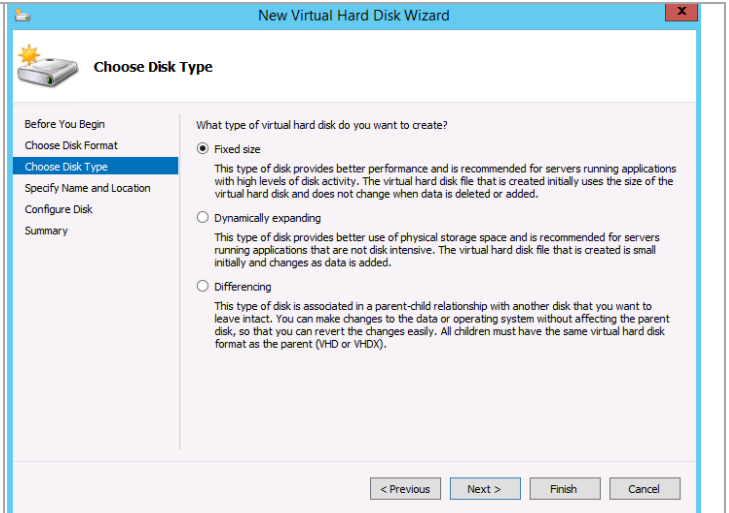


On the **Choose Disk Format** window, ensure the radio button by **VHDX** is selected. Click **Next** to continue.

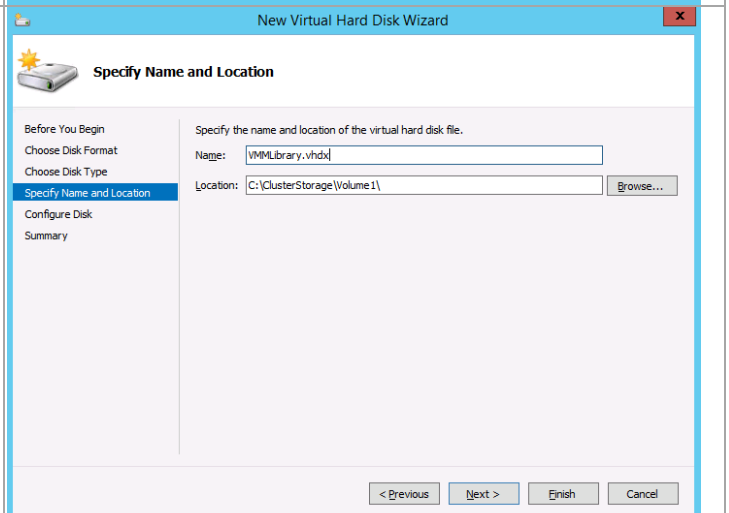




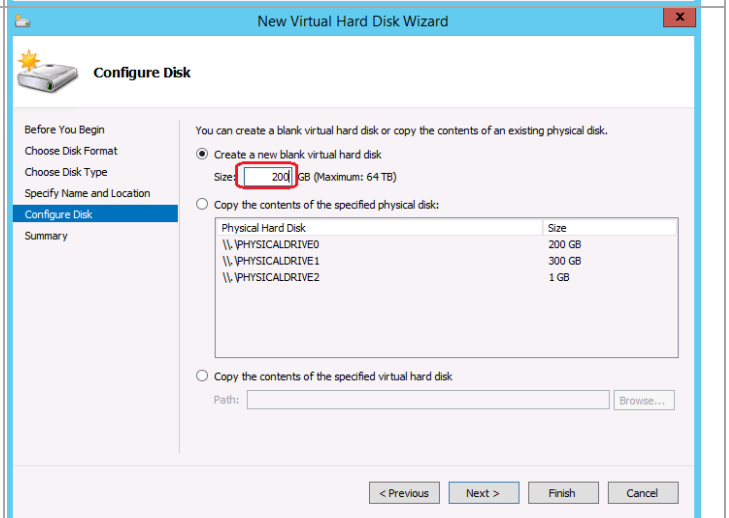
On the **Choose Disk Type** window, select **Fixed Disk**. Click **Next** to continue.



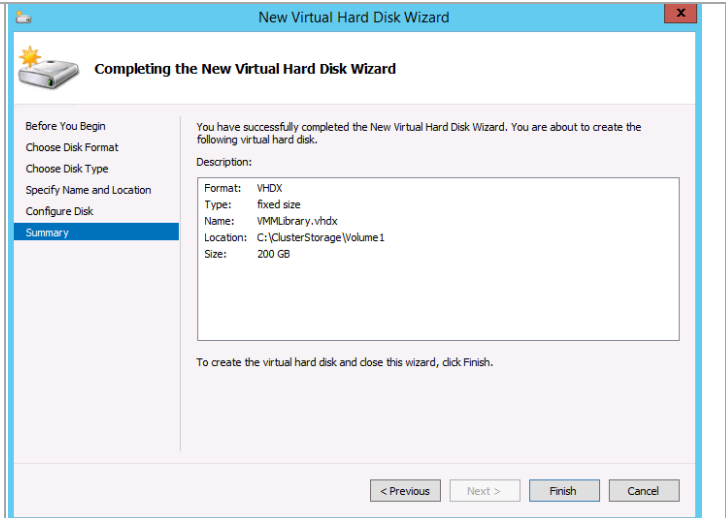
On the **Specify Name and Location** window, enter a name for the VHDX file. Click **Browse...** to browse to the CSV location **C:\ClusterStorage\Volume1**. Click **Next** to continue.



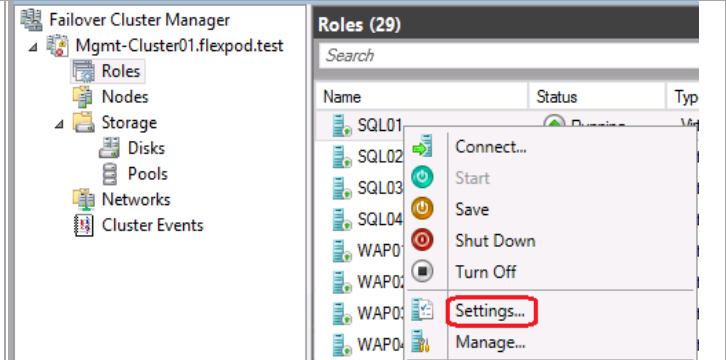
On the **Configure Disk** window, enter an appropriate size for the library disk. A size of 200 GB is a good start. This can be expanded or additional disks added at a later time if your library grows. Click **Next** to continue.



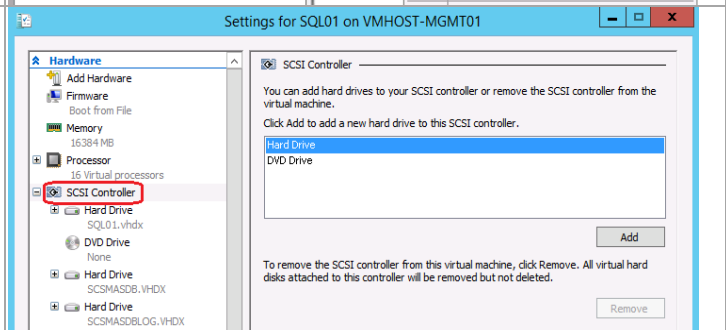
On the summary window, review what you entered and click **Finish** to create the disk.



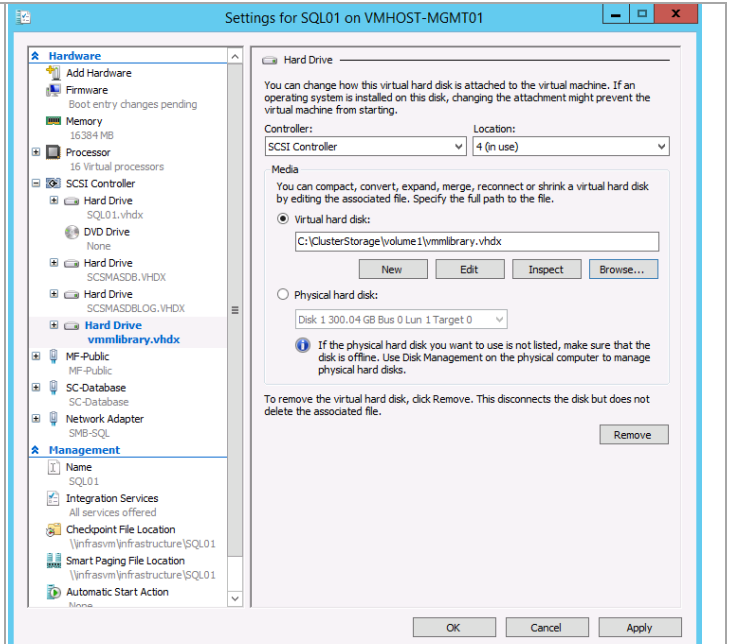
From the **Failover Cluster Manager** console for the Fabric Management cluster, select one of the SQL Server nodes, right-click, and select **Settings...**



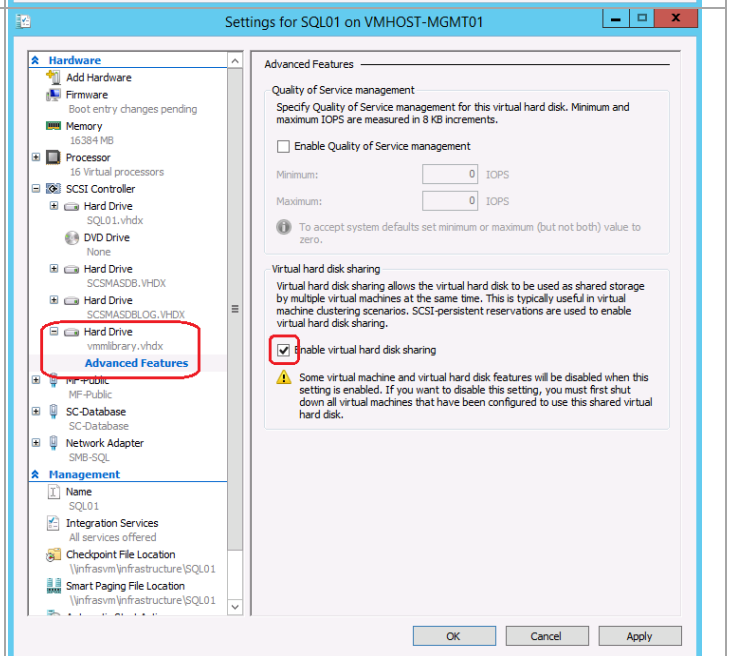
Click **SCSI Controller**. Click **Hard Drive**. Click **Add**.



Click on **Browse...** and navigate to the C:\ClusterStorage location where you created the VHDX. Select the newly created VHDX and click **Apply**.



Expand the newly added Hard Drive and click on **Advanced Features**. Check the box by **Enable virtual hard disk sharing**. Click **OK** to continue.



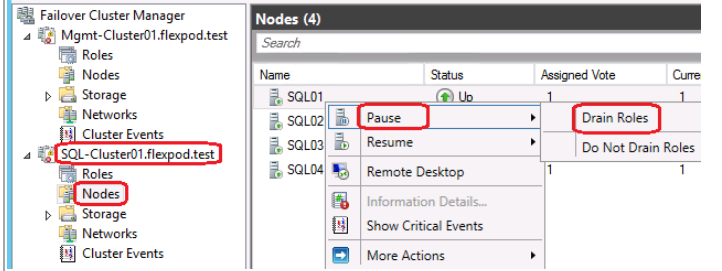
## Add Disk to SQL Server Cluster

The process of adding a shared disk to the cluster requires the node being worked on to be shut down. The following steps illustrate:

- How to drain the SQL Server node of SQL instances
- Shut down the node
- Add the newly created virtual hard disk to the SQL Server cluster for sharing
- Restart the SQL Server node

Note that these steps are easier if you have both the Fabric Management and SQL Server clusters open in the same Failover Cluster Manager console.

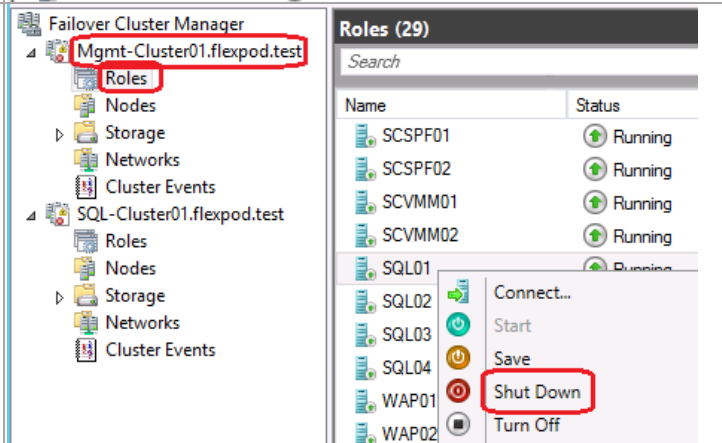
From the Failover Cluster Manager console for the **SQL Server** cluster, select one of the SQL Server nodes, right-click, and select **Pause** and **Drain Roles**. Wait until the node shows a status of **Paused** before proceeding to the next step.



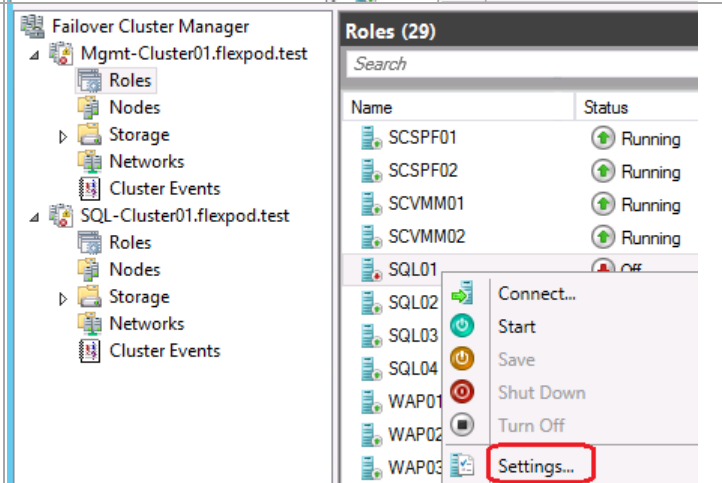
Name	Status	Assigned Vote
SQL01	Paused	1
SQL02	Up	1
SQL03	Up	1
SQL04	Up	1

From the Failover Cluster Manager console for the **Fabric Management** cluster, select the node selected in the previous step. Right-click and select **Shut Down**.

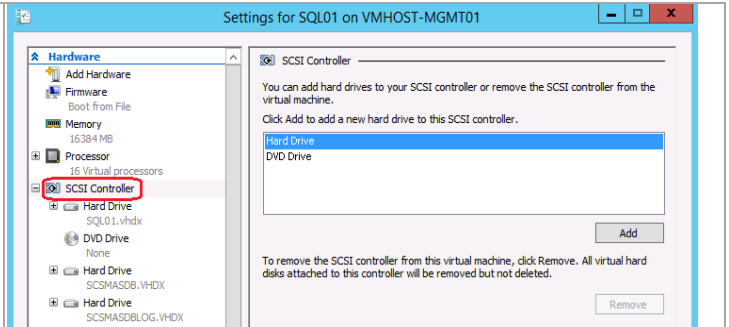
When the virtual machine has the status of **Off**, proceed to the next step.



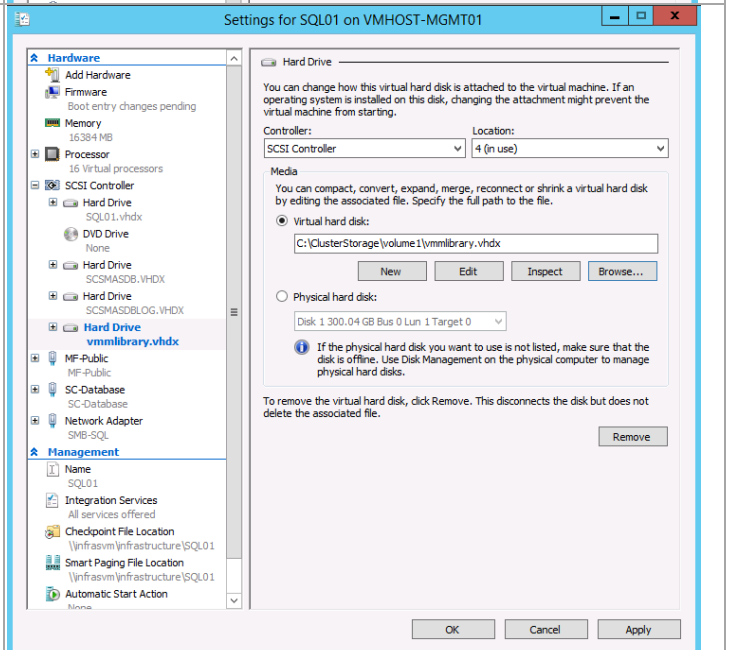
From the Failover Cluster Manager console for the Fabric Management cluster, select one of the SQL Server nodes, right-click, and select **Settings...**



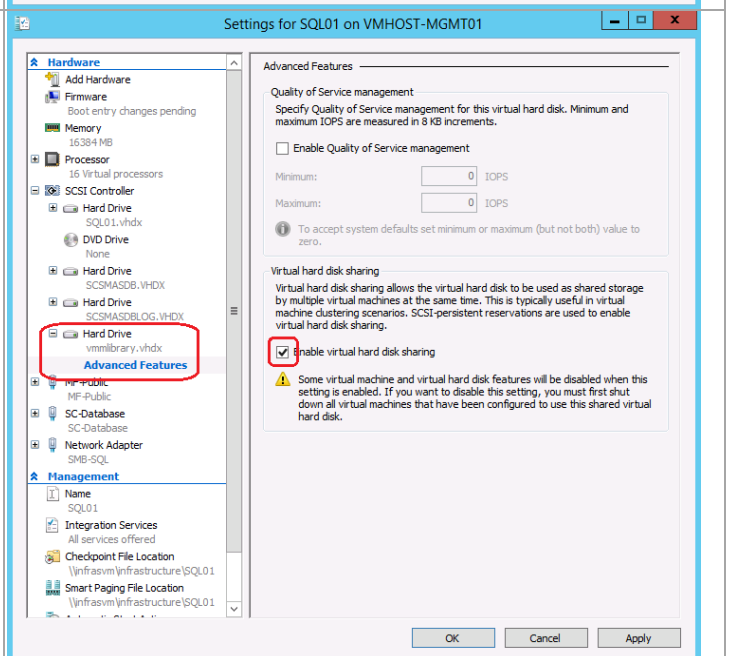
Click on **SCSI Controller**. Click on **Hard Drive**.  
Click on **Add**.



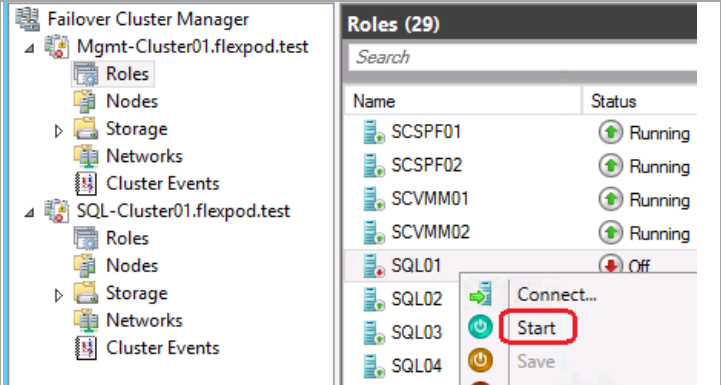
Click on **Browse...** and navigate to the  
C:\ClusterStorage location where you created the  
VHDX. Select the newly created VHDX and click  
**Apply**.



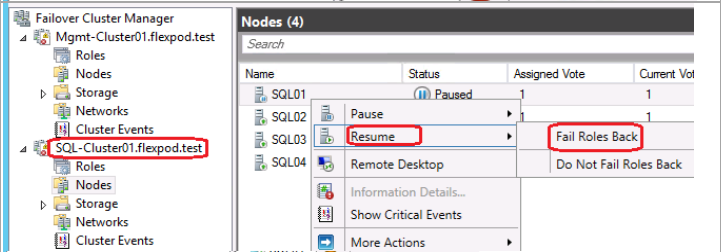
Expand the newly added Hard Drive and click on  
**Advanced Features**. Check the box by **Enable**  
**virtual hard disk sharing**. Click **OK** to continue.



Select the virtual machine, right-click and select **Start** to restart the virtual machine. Wait about 30 seconds before proceeding to the next step. This allows the VM to boot and be ready to regain its role in the SQL Server cluster.



Back in the **SQL Server** cluster, select the **Paused** node, right-click and select **Resume** and **Fail Roles Back**. Wait until the node has a status of **Up** before proceeding.  
Repeat these steps for each node of the cluster.

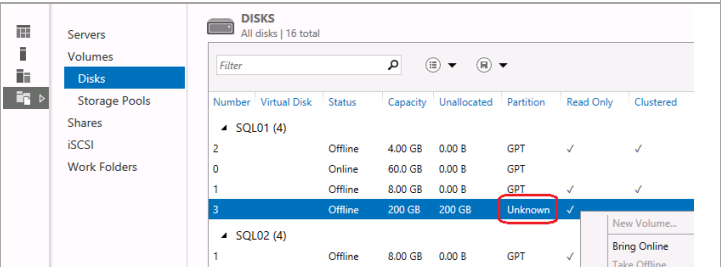


## Format the Disk and Add to the SQL Server Cluster Storage

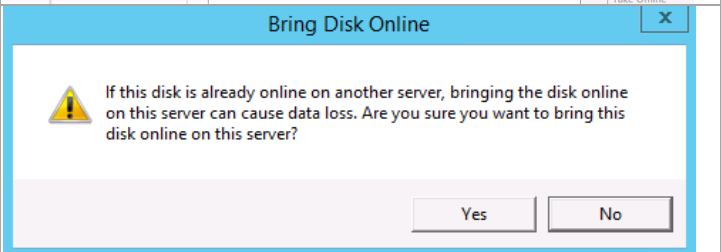
The virtual hard disk just added needs to be initialized and formatted. When it has a valid file system created on it, it can be added to the cluster to be used to storage the VMM library share.

Perform the following steps on **ONLY** one of the **SQL Server** virtual machines.

From Server Manager, select **File and Storage Services**. Select **Disks** and right-click on the newly added disk. It will show an **Unknown** partition. Select **Bring Online**.



A warning window will appear. Click **Yes** to continue.



Right-click the disk you just brought online and select **New Volume...**  
Click **Next** on the **Before You Begin** window.

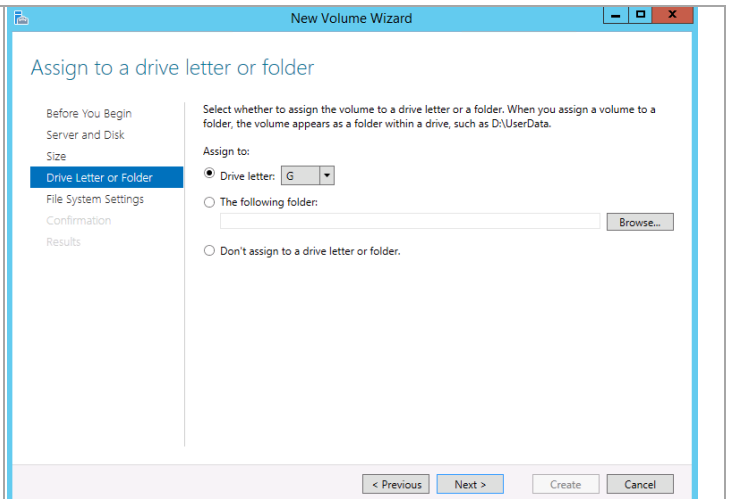
Number	Virtual Disk	Status	Capacity	Unallocated	Partition
SQL01 (4)					
2		Offline	4.00 GB	0.00 B	GPT
0		Online	60.0 GB	0.00 B	GPT
1		Offline	8.00 GB	0.00 B	GPT
3		Online	200 GB	200 GB	Unallocated
SQL02 (4)					
1		Offline	8.00 GB	0.00 B	GPT

On the **Select the server and disk** window, click on **Next** to continue.

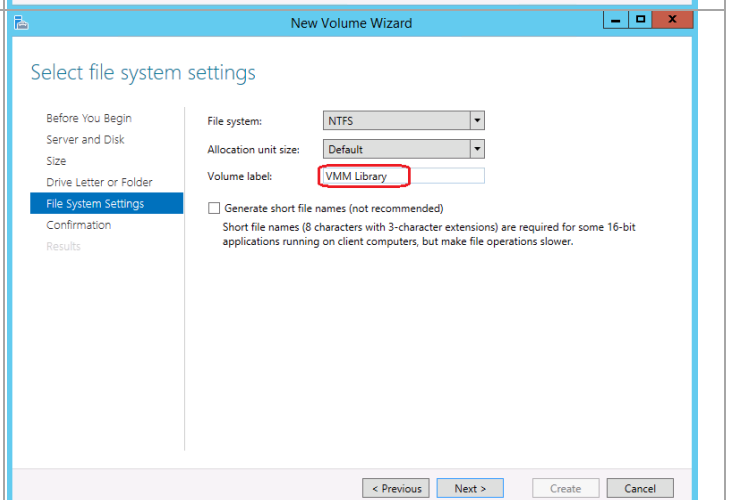
A window stating the disk will be initialized as a GPT disk displays. Click **OK** to start the initialization.

On the **Specify the size of the volume** window, accept what is displayed by clicking **Next**.

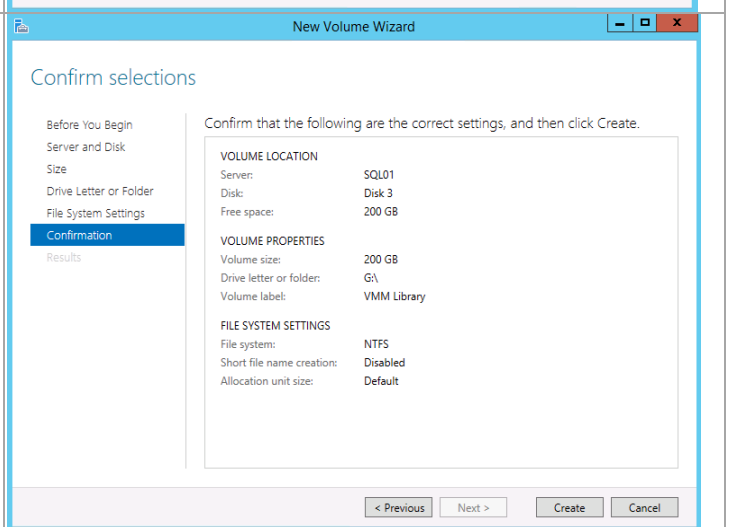
On the **Assign to a drive letter or folder** window, accept what is displayed by clicking **Next**.



If desired, enter an appropriate **Volume label**. Click **Next** to continue.

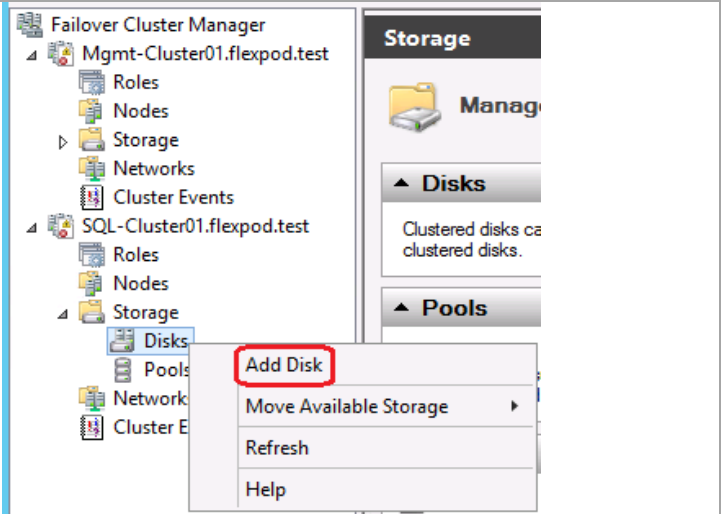


Review your selections on the **Confirm selections** window and click **Create** to create the volume.

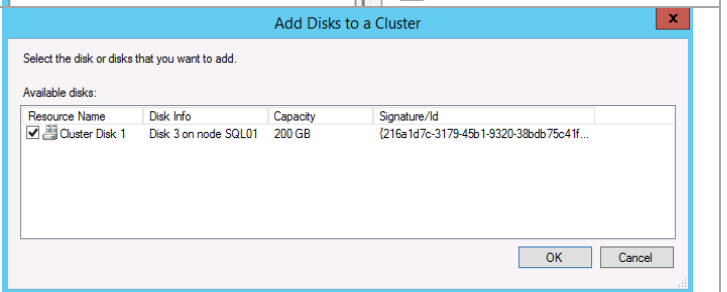




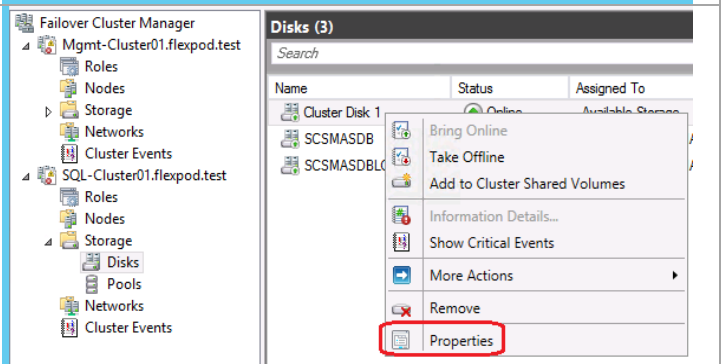
In the **Failover Cluster Manager** console for the **SQL Server cluster**, expand **Storage**. Right-click **Disks** and select **Add Disk**.



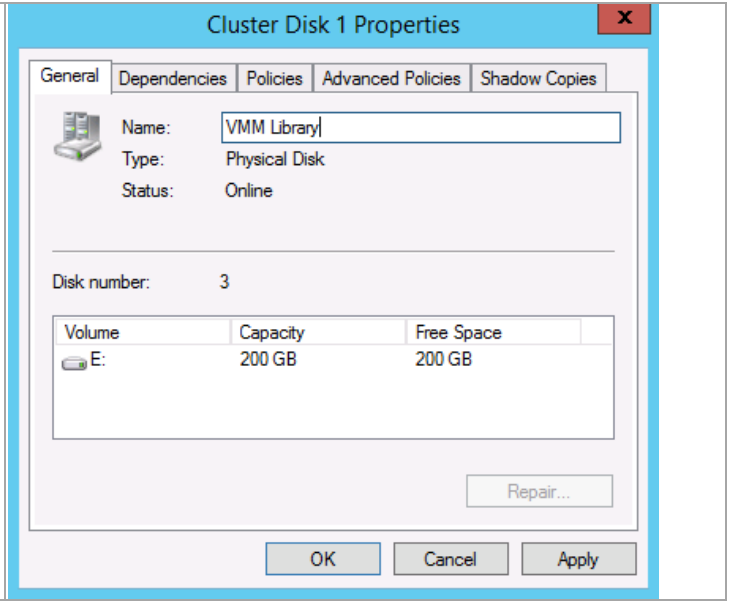
Ensure the check box is selected by the new disk and click **OK**.



Refresh the **Disks** display. Right-click on the newly added disk and select **Properties**.



Assign a meaning **Name** to the disk and click **OK**.

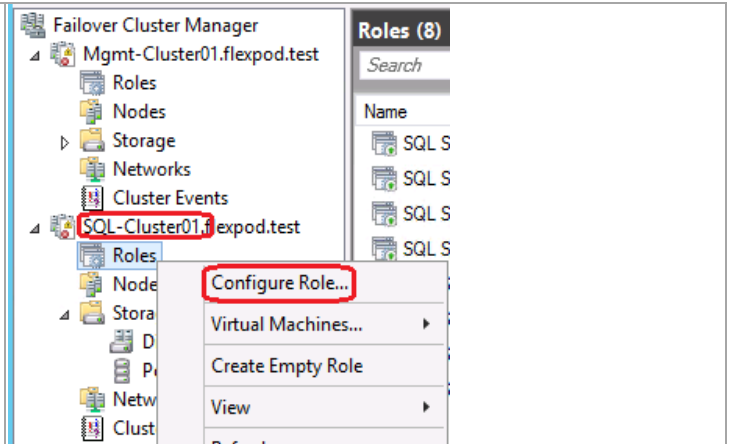


## Add the File Server Role to the SQL Server Cluster

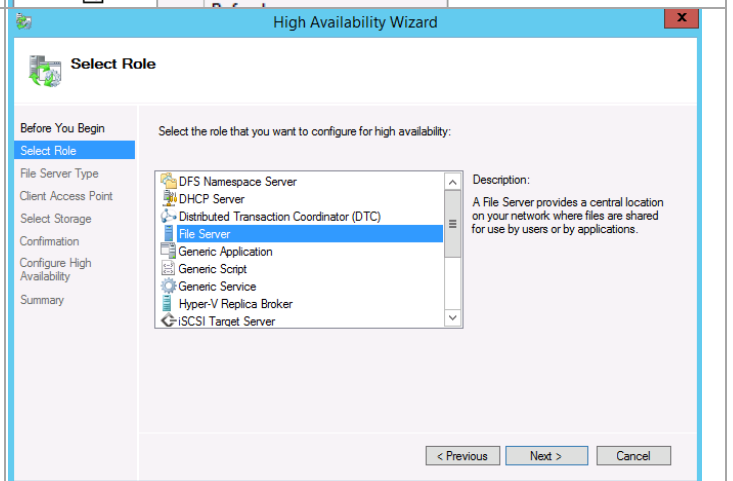
In order to share the newly added disk to SCVMM for its library use, the File Server needs to be added to the cluster and configured to use the disk.

In the **Failover Cluster Manager** console for the **SQL Server** cluster, right-click **Roles** and select **Configure Role...**

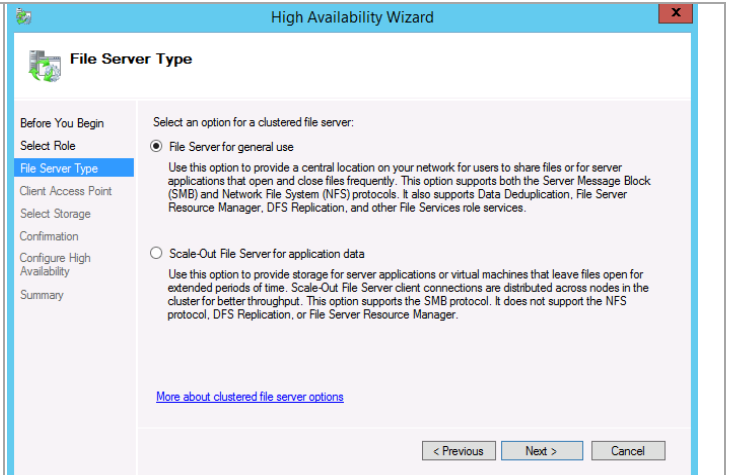
Click **Next** on the **Before You Begin** window.



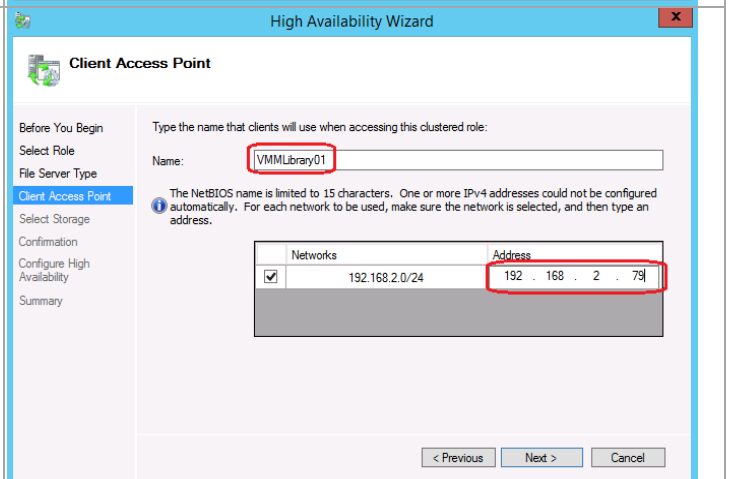
On the **Select Role** window, select **File Server**. Click **Next** to continue.



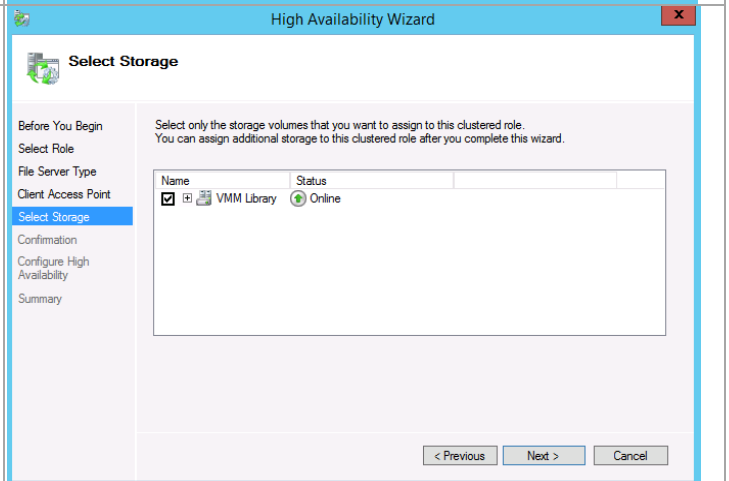
On the **File Server Type** window, select the radio button by **File Server for general use**. Click **Next** to continue.



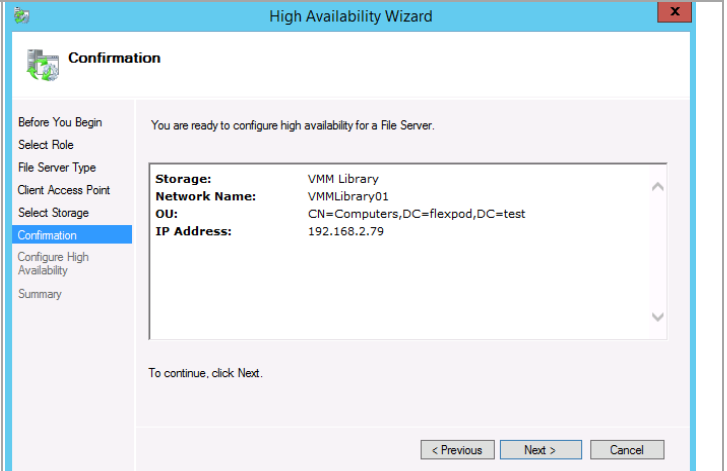
On the **Client Access Point** window, specify a name to be used to access this service and the IP address associated with it. Click **Next** to continue.



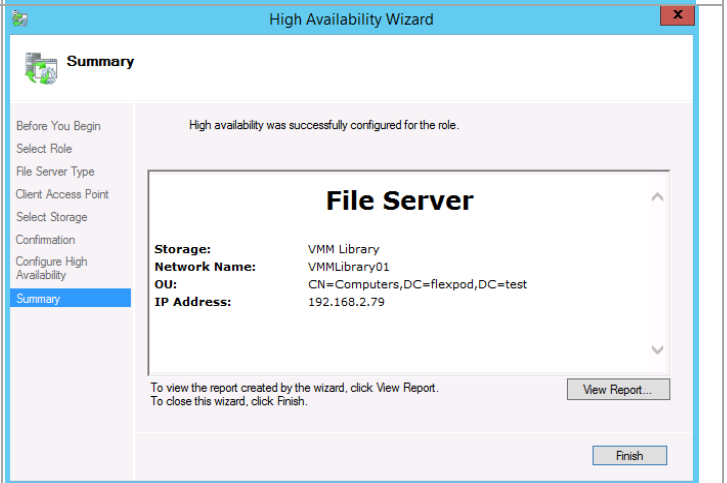
On the **Select Storage** window, check the box by the newly added storage. Click **Next** to continue.



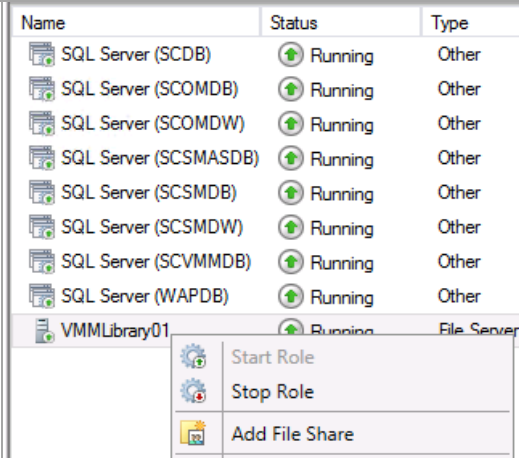
Review your entries on the **Confirmation** window. Click **Next** to continue.



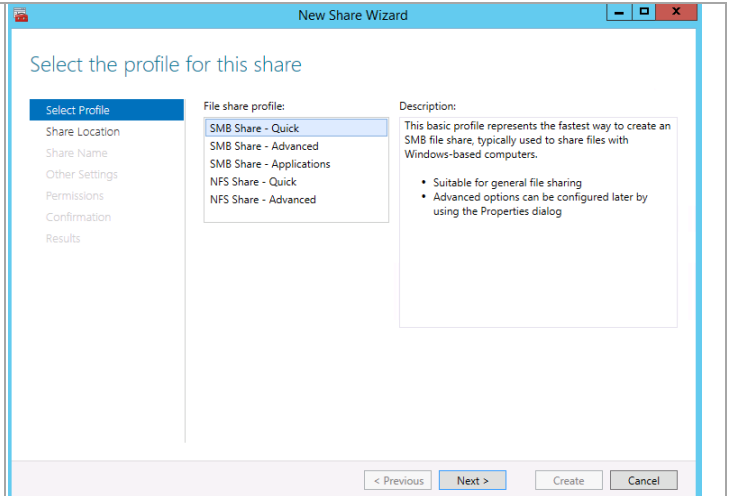
A summary window displays after the high availability of the service is configured. If you wish, you can click on **View Report...** to see the results. Click **Finish** to complete the process.



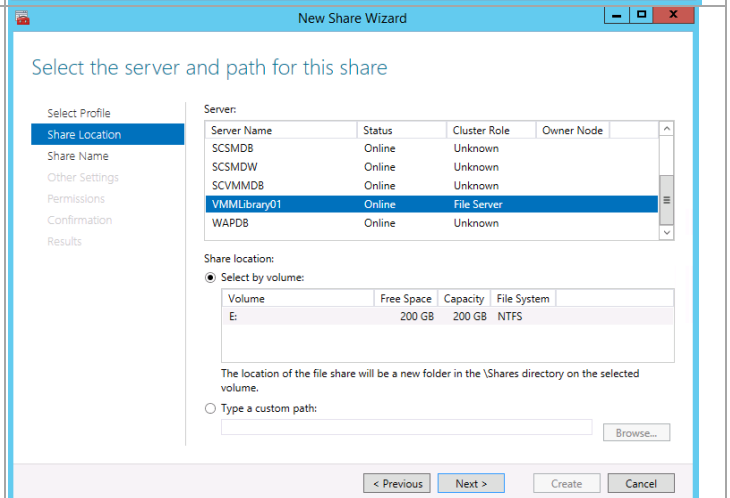
Right-click on the new created File Server role and select **Add File Share**.



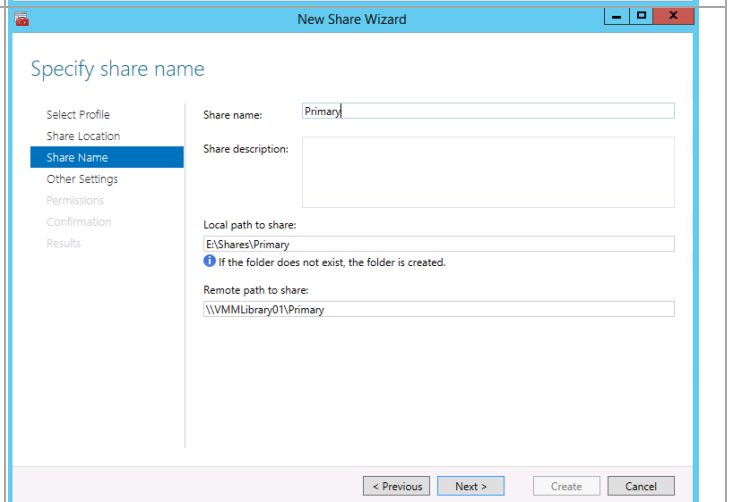
On the **Select the profile for this share** window select **SMB Share – Quick**. Click **Next** to continue.



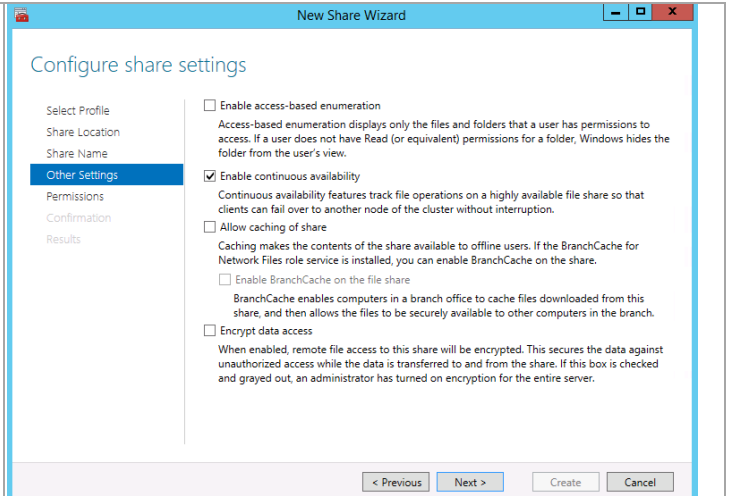
On the **Select the server and path for this share** window, scroll down to the newly created File Server role and click on it to select it. Under **Share location** select the radio button by **Select by volume** as the whole volume will be used as the library share. Click **Next** to continue.



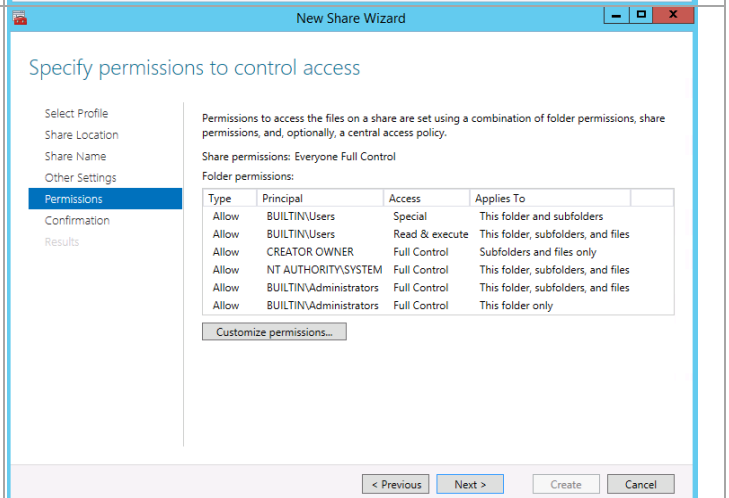
On the **Specify share name** window, enter an appropriate name for the share and click **Next** to continue.



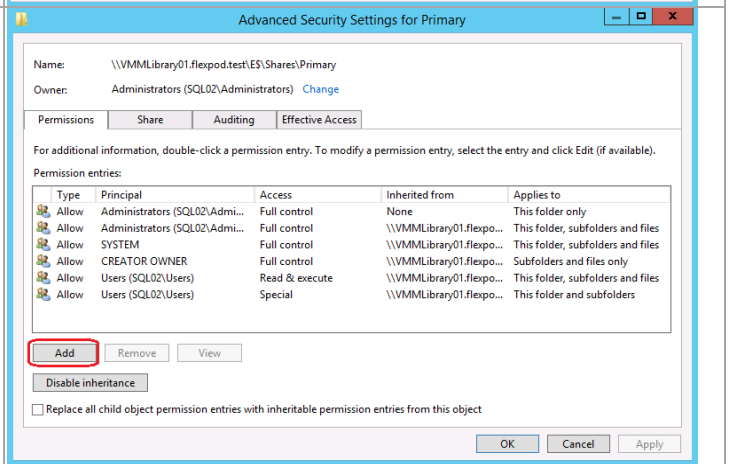
On the **Configure share settings** window, select only **Enable continuous availability**. Click **Next to continue**.



On the **Specify permissions to control access** window, click on **Customize permissions...**

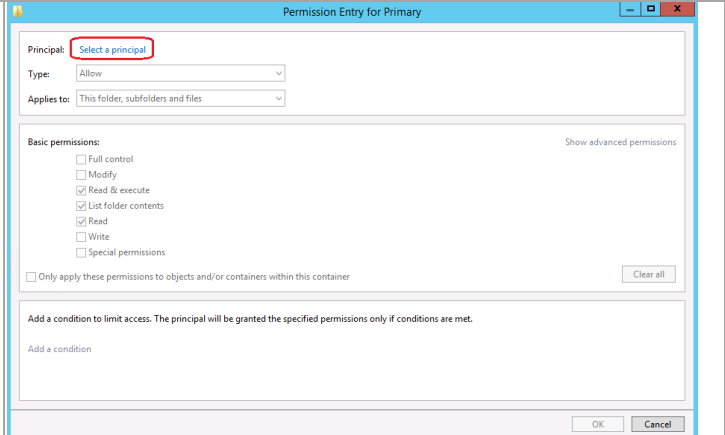


On the **Advanced Security Settings** window, click **Add**.

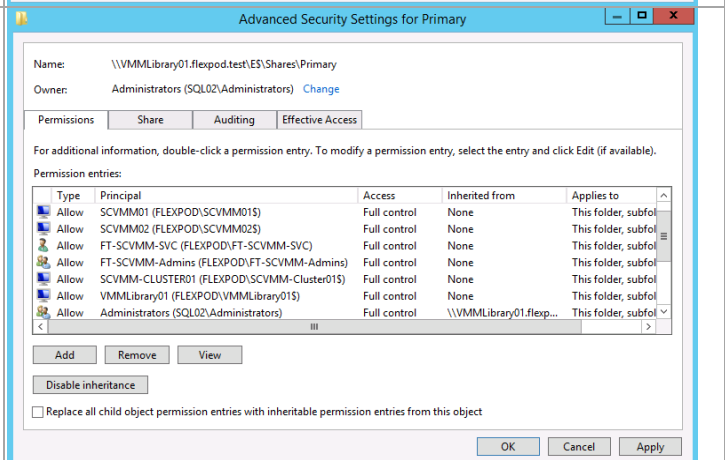


On the **Permission Entry** window, click on **Select a Principal**. This brings up a window that will allow selection of entries from Active Directory and the local computer. Add the following accounts with NTFS Full Control permissions:

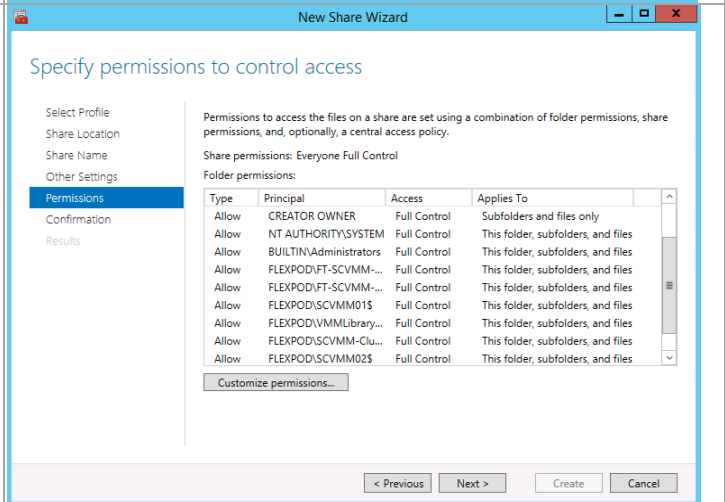
- SCVMM service account
- SCVMM Admins group
- Both SCVMM computer accounts
- SCVMM cluster name object computer account
- Library server cluster name object computer account



Verify you have all the accounts added and click **OK** to continue.

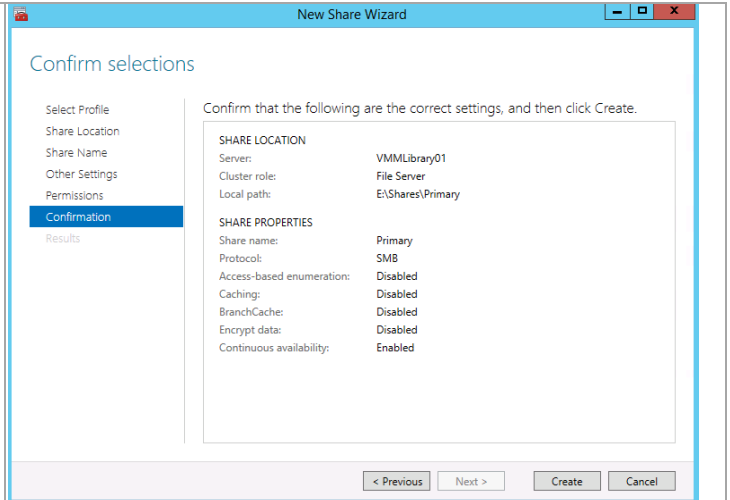


On the **Specify permissions to control access** window select **Next** to continue.



Validate your entries on the **Confirm selections** window and click **Create**.

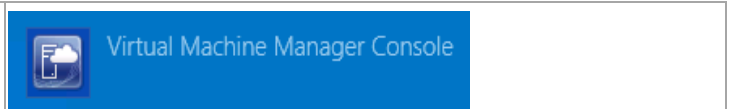
Click **Close** on the following **View Results** window.



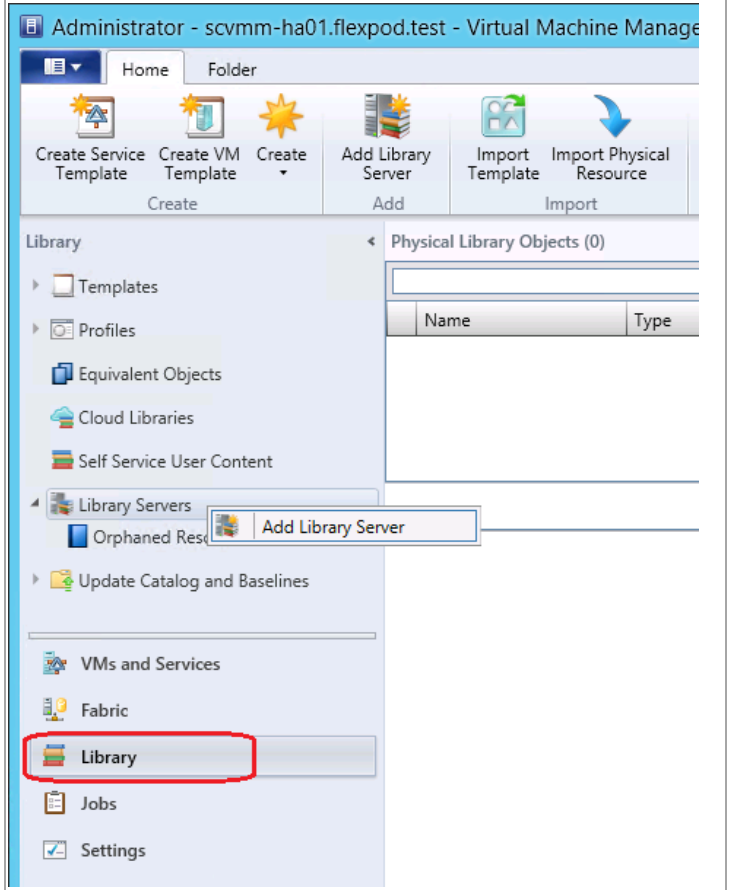
## Configure the Library in SCVMM

Now that a highly available file service has been configured, the following steps show how to configure the VMM library.

From one of the System Center Virtual Machine Manager virtual machines launch the SCVMM console

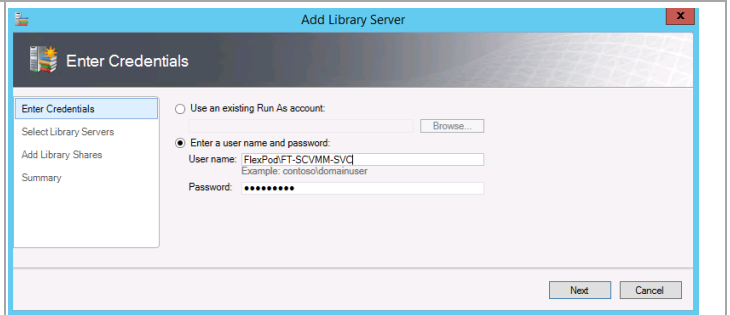


Select **Library**, then right-click on **Library Servers**. Select **Add Library Server**.

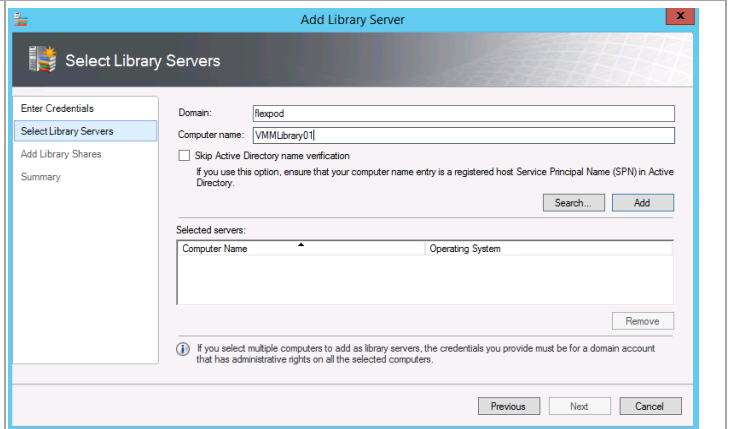




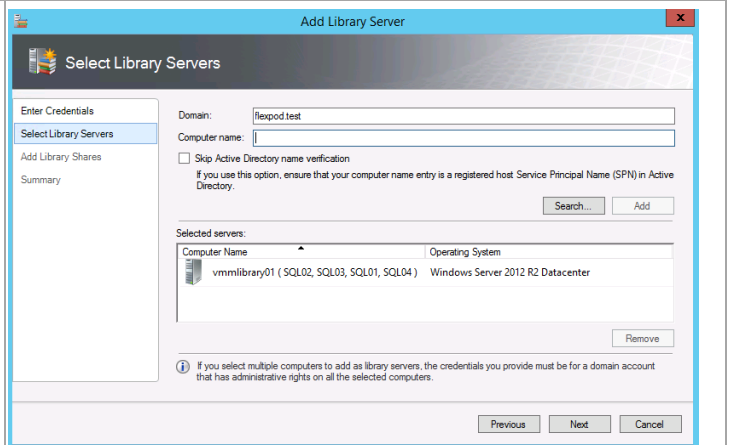
The **Add Library Server** wizard appears. On the **Enter Credentials** page, select the **Enter a user name and password** option. In the **User name** and **Password** text boxes, type credentials that have administrative rights for the Virtual Machine Manager Library share. Click **Next** to continue.



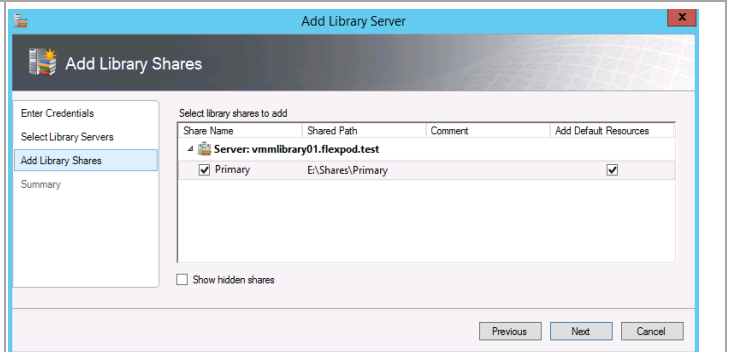
On the **Select Library Servers** page, in the **Domain** text box, specify the FQDN of the target domain. In the **Computer name** text box, type the name of the **File Server Cluster object** and click **Add**.



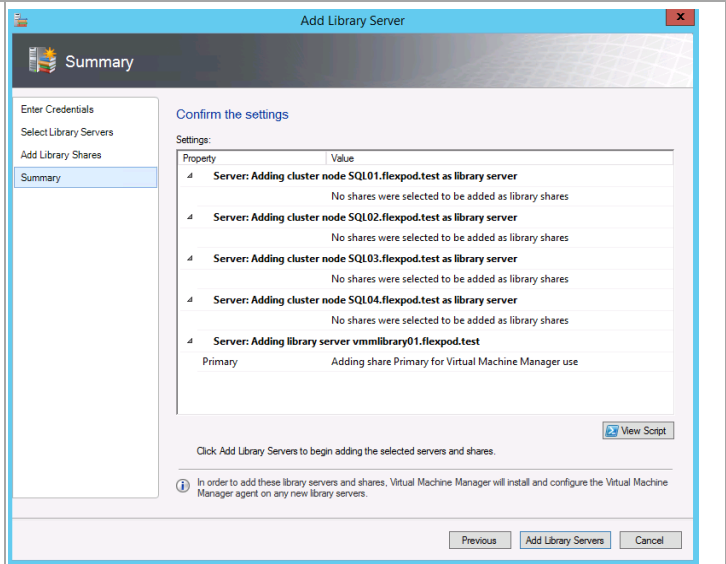
When the cluster object has been discovered, click **Next** to continue.



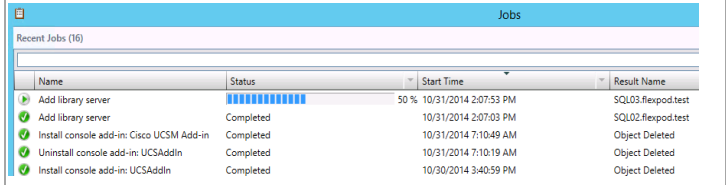
On the **Add Library Shares** window, select the previously created share. Also check the box for **Add Default Resources**. Click **Next** to continue.



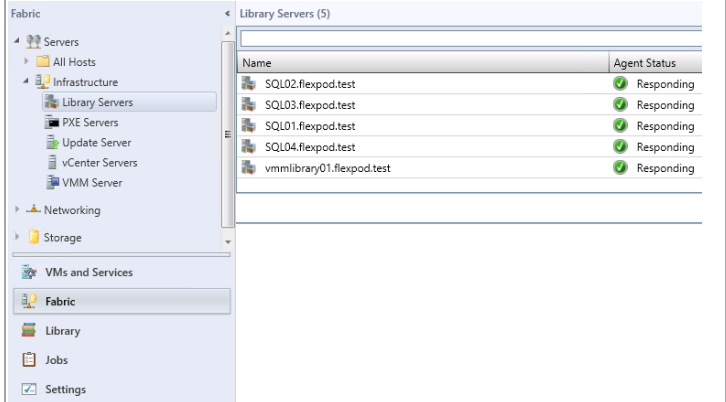
Review the contents of the **Summary** window and click **Add Library Servers** to complete creation of the VMM library.



The Jobs dialog window will open allowing you to monitor the progress of the addition.



When the jobs complete, navigate to **Fabric** in the VMM console. Expand **Server** and **Infrastructure** and click on **Library Servers** to see that all are responding.

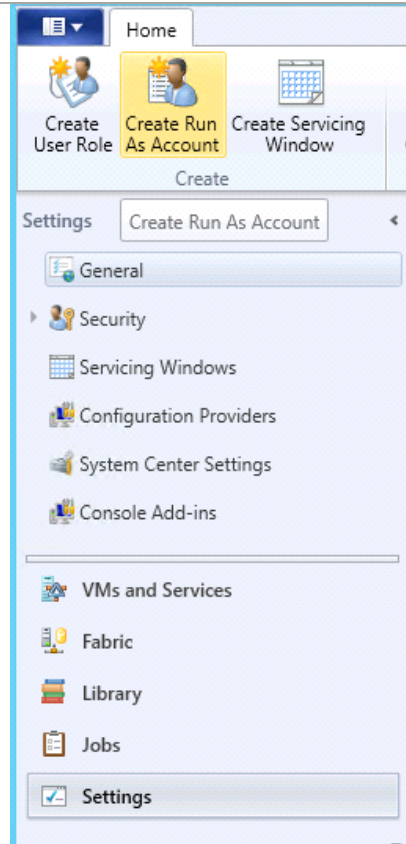


## Add a Run As Account to VMM

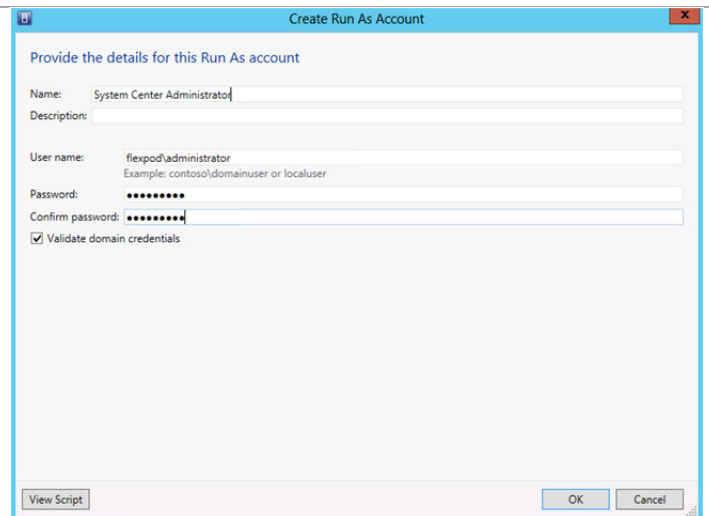
In System Center Virtual Machine Manager, the credentials that a user enters for any process can be provided by a Run As account. A Run As account is a container for a set of stored credentials. This enables role-based access controls to be supplied to different users with different access requirements or restrictions.

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

Click **Settings** in the left tree view and click **Create Run As Account** on the ribbon.



Name the account. Provide an active directory account name and password with administrator rights. Click **OK** to create the Run As Account



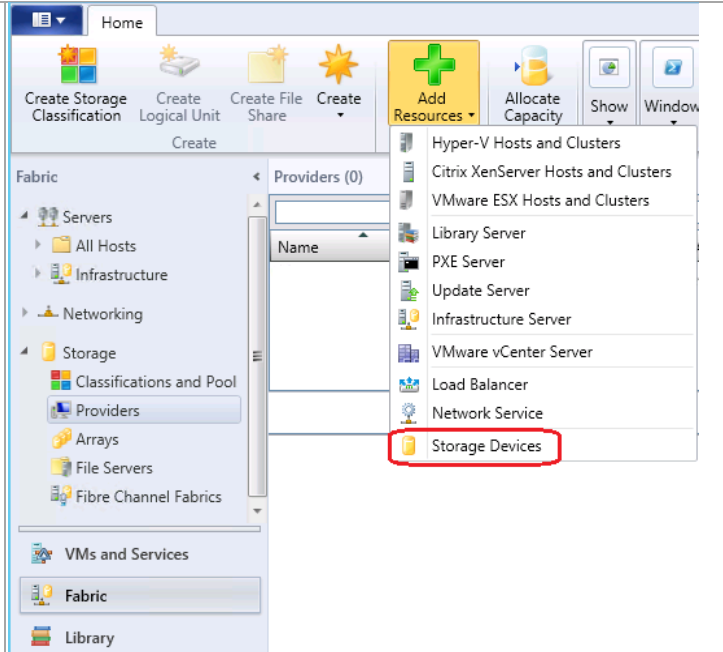
## 18.6 Register SMI-S in SCVMM

The following steps need to be completed in order to register the NetApp SMI-S provider in SCVMM.

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

In the **Virtual Machine Manager** console, navigate to the **Fabric** pane and expand the **Storage** node. Select the **Providers** sub-node.

From the ribbon select **Add Resources**, and select **Storage Devices** from the drop down.



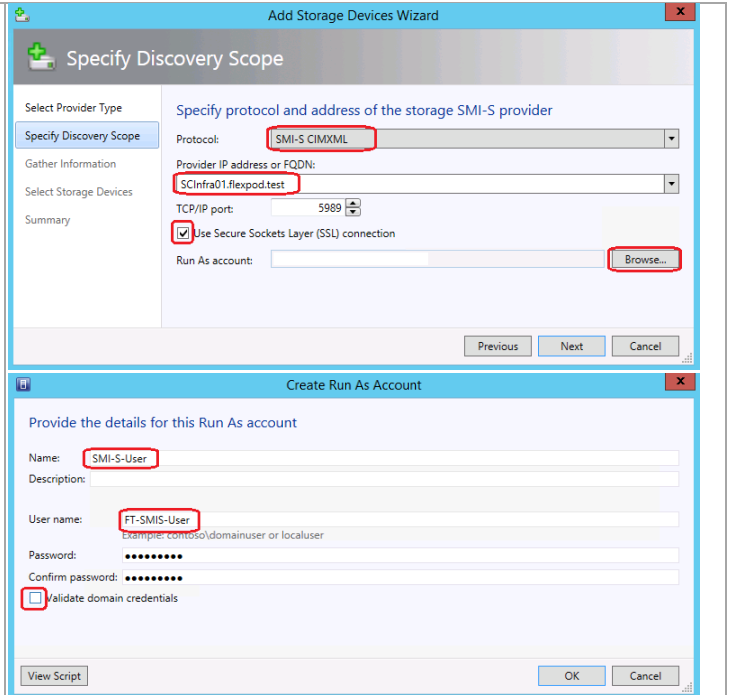
On the Add Storage Devices Wizard select **SAN and NAS devices discovered and managed by a SMI-S provider**, and click **Next**.



On the Specify Discovery Scope page.

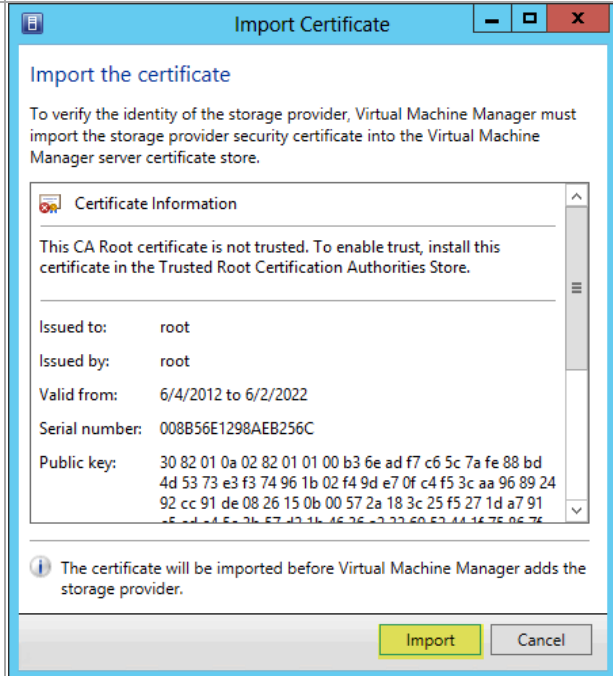
- Select **SMI-S CIMXML** for the Protocol
- Enter the **IP or FQDN** for the SMI-S provider
- Check the **Use Secure Sockets Layer** check box
- Click **Browse**, and in the resulting popup select **Create Run As Account**
  - Enter a **Display Name**
  - Enter the **User Name**
  - Enter the **Password**
  - Uncheck **Validate Domain Credentials**
  - Click **OK**.

Click **Next**



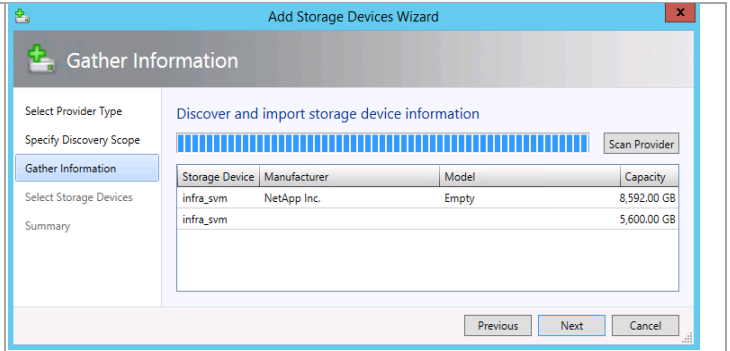
During the discovery phase a popup will open asking to Import the SMI-S providers Certificate.

Click **Import**



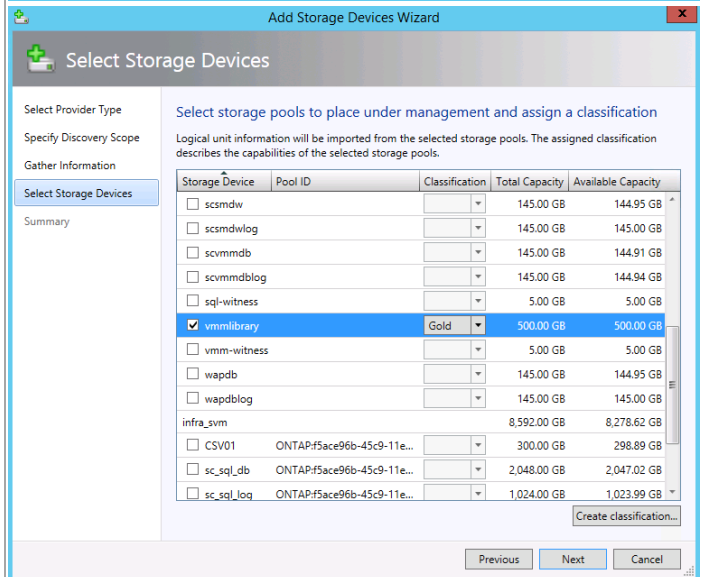
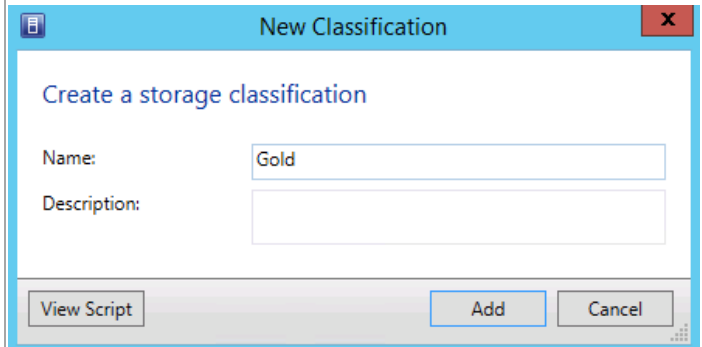
Once Discovery is completed the Wizard will show every storage controller registered with the SMI-S provider

Click **Next**.

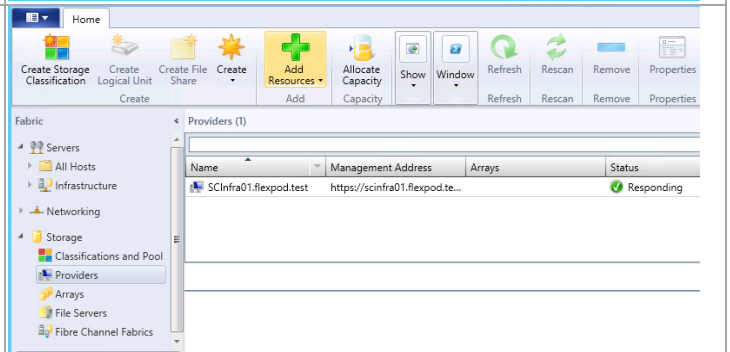


On the Select Storage Devices page.

- Click the **Create Classification** button. In the resulting popup enter a name for the storage pool.
- Check **vmmlibrary** and set the **classification**.
- Click **Next**, and **Finish** to close out the wizard.



In the SCVMM console you will be able to see the added provider.

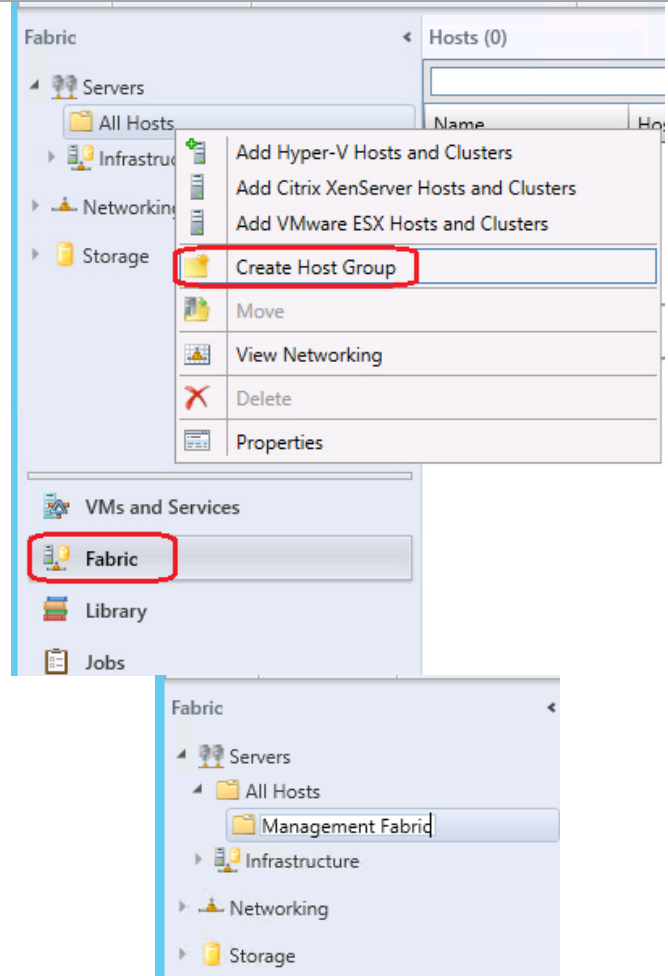


## 18.7 Add Fabric Management Resources Virtual Machine Manager

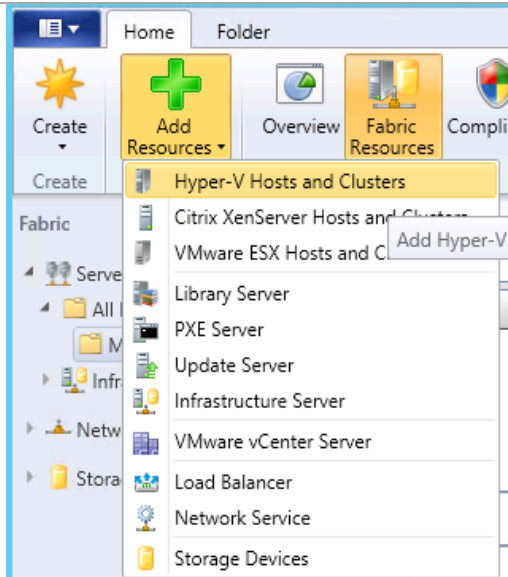
Complete the following steps to Add the Fabric Management Hyper-V hosts to VMM.

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

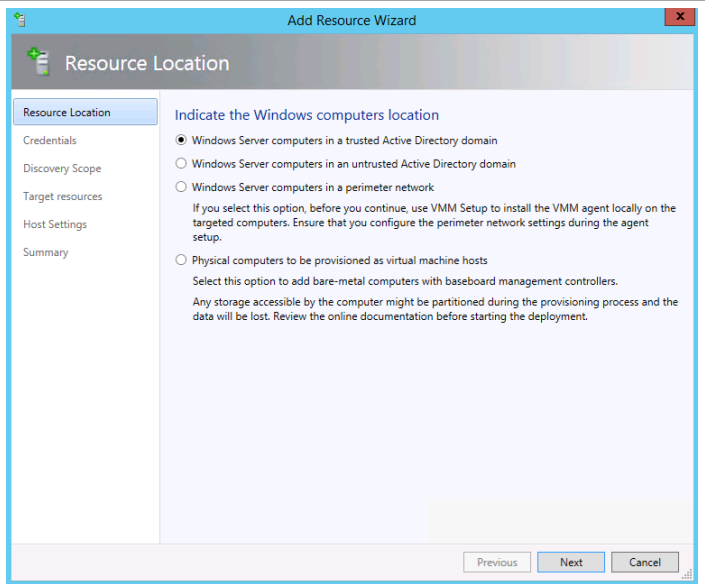
Click **Fabric** in the left tree view, expand **Servers**, and right click **All Hosts**. Select **Create Host Group**. Name the new Host Group.



From the ribbon click **Add Resources** and select **Hyper-V Hosts and Clusters**.

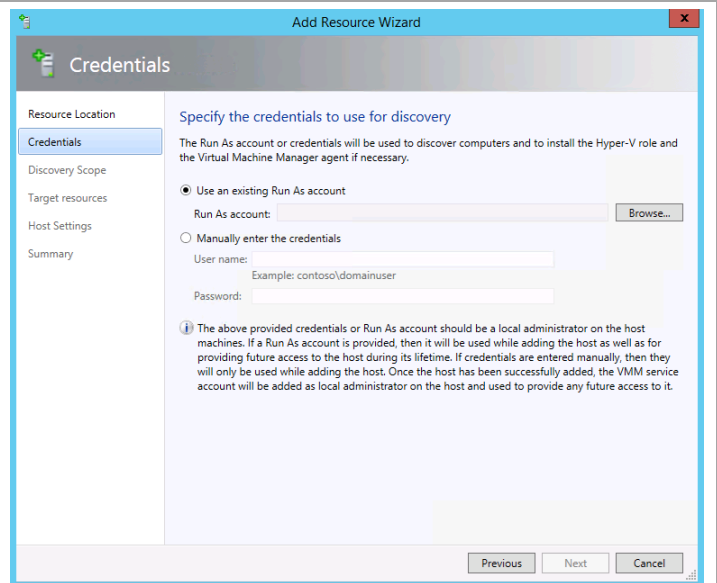


In the Indicate the Windows computer location windows select **Windows Server computers in a trusted Active Directory domain**.

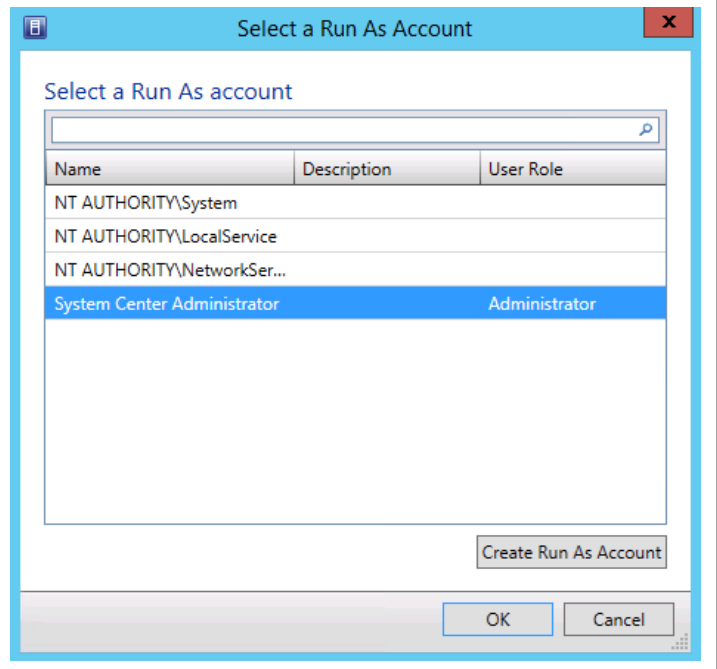




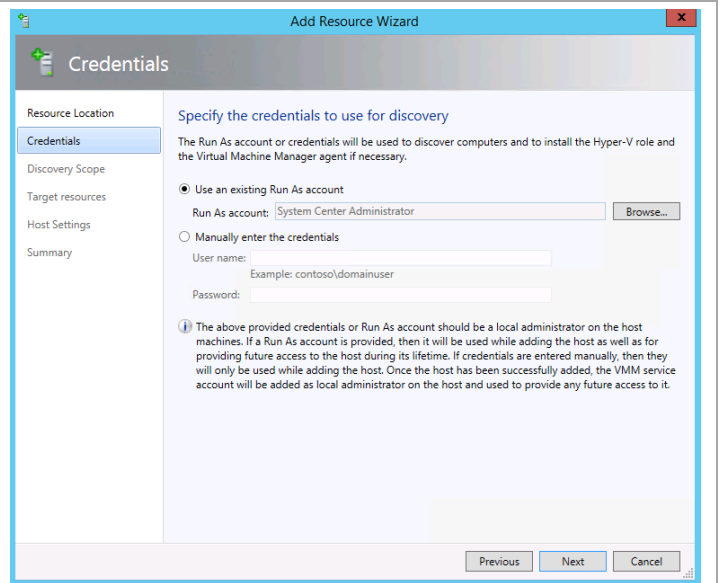
Select Use an Existing Run As account and click browse.



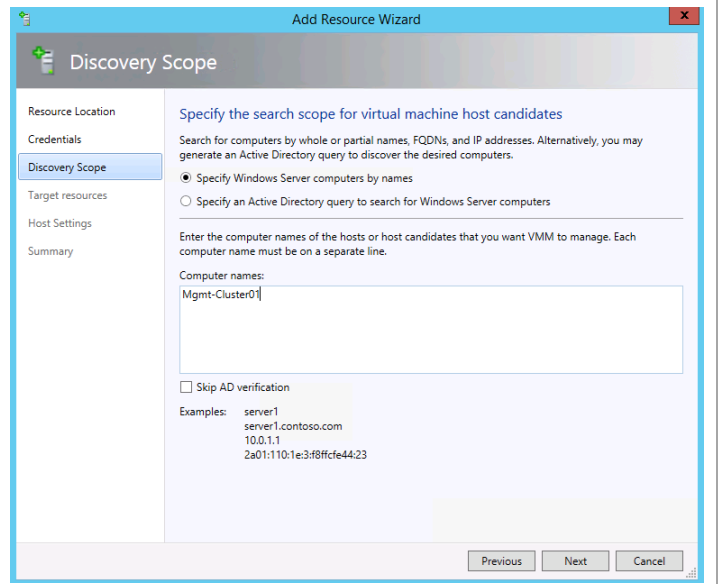
Select the previously created account and click OK.



Click **Next** to proceed to the next screen.

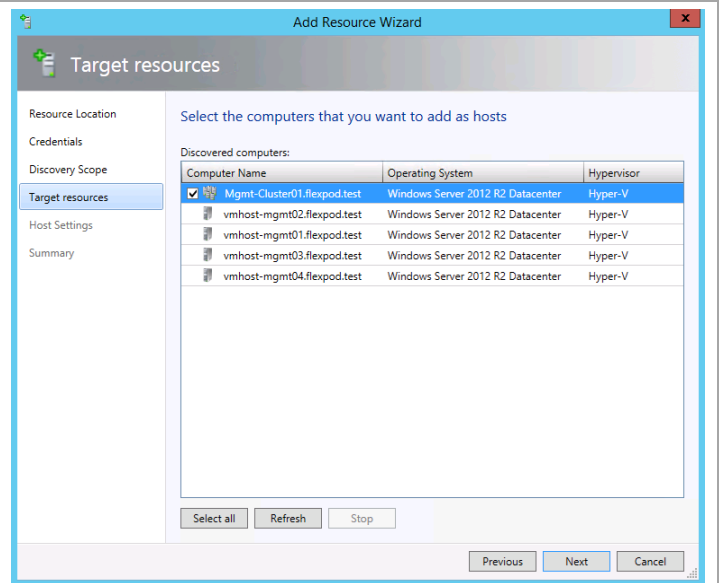


Enter the cluster name and click **Next**.

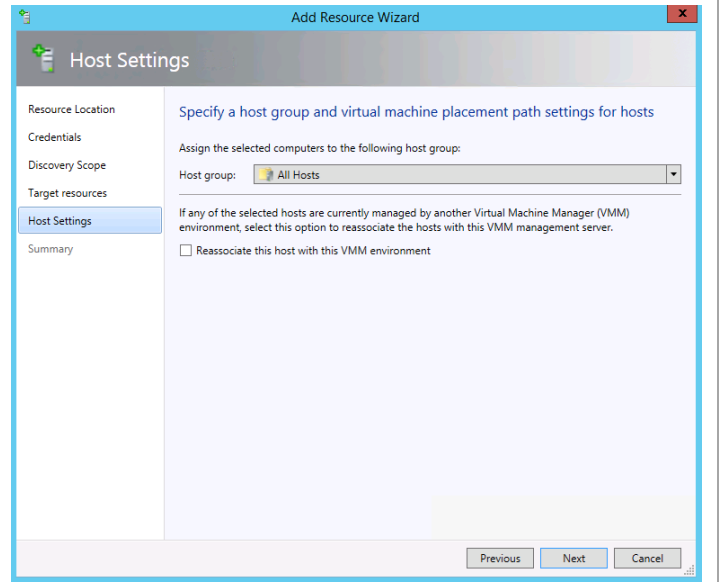


Click **Select All** and click **Next**.

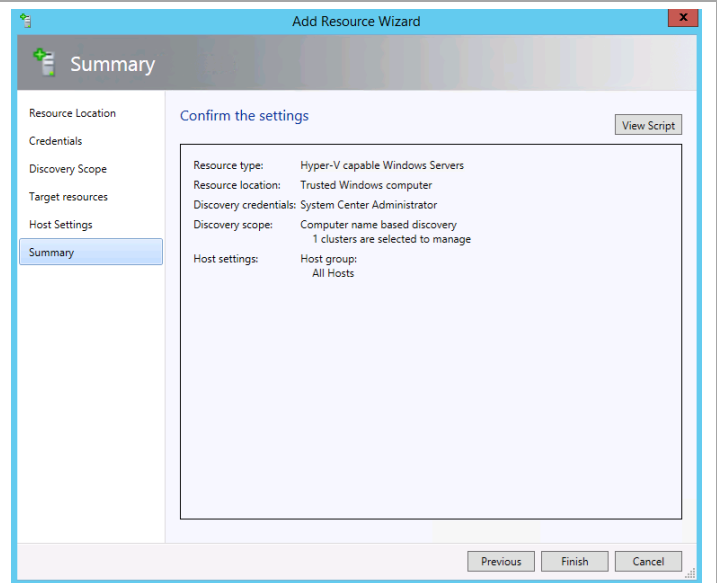
If you receive an error, try clicking **Refresh** to try again.



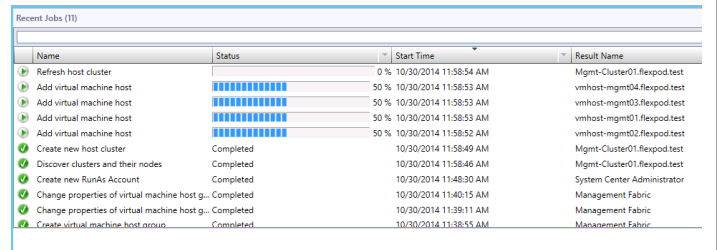
Click **Next** to accept placing the management hosts into the previously created Host group.



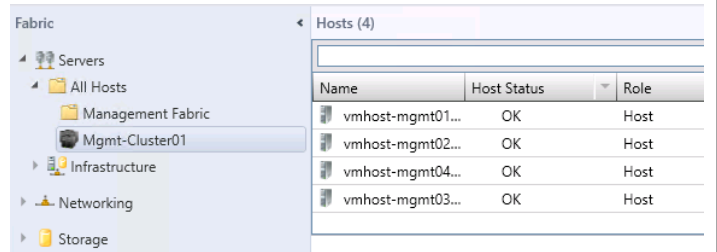
Click **Finish**.



A Jobs window will open showing the status of adding the nodes to SCVMM.



Verify that the hosts are added.

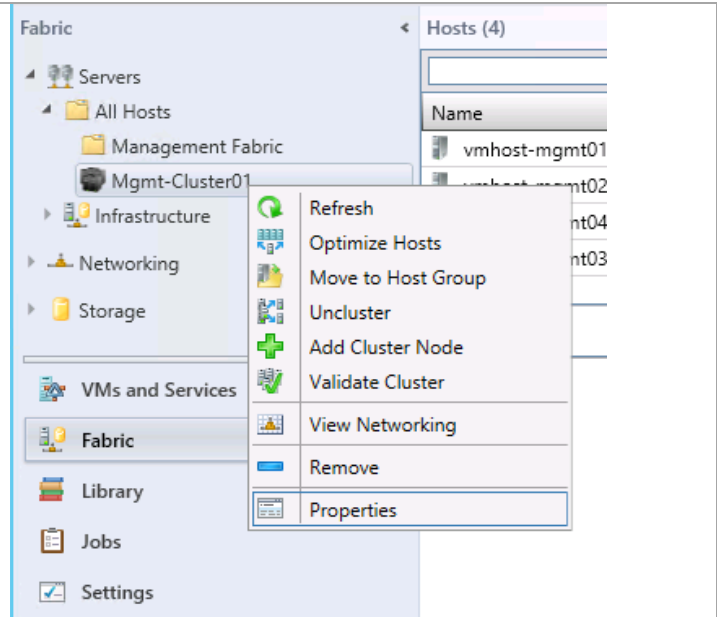


## 18.8 Register the File Share to the Management Cluster

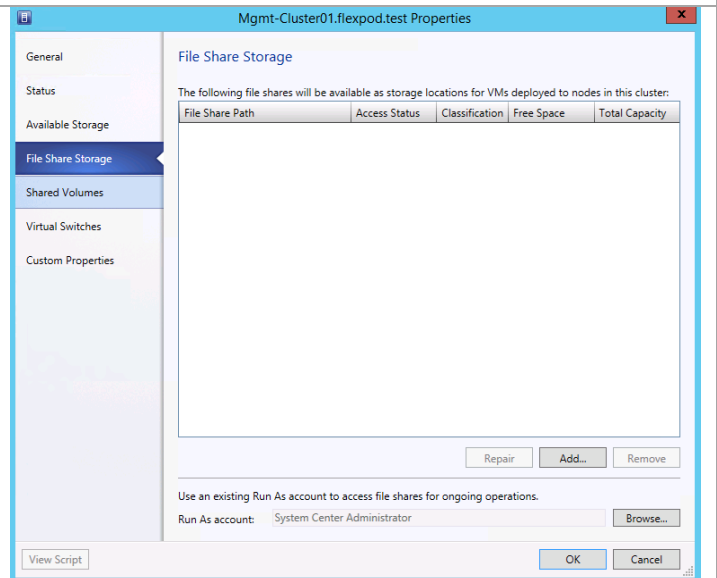
Complete the following steps to Add the Fabric Management Hyper-V hosts to VMM.

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

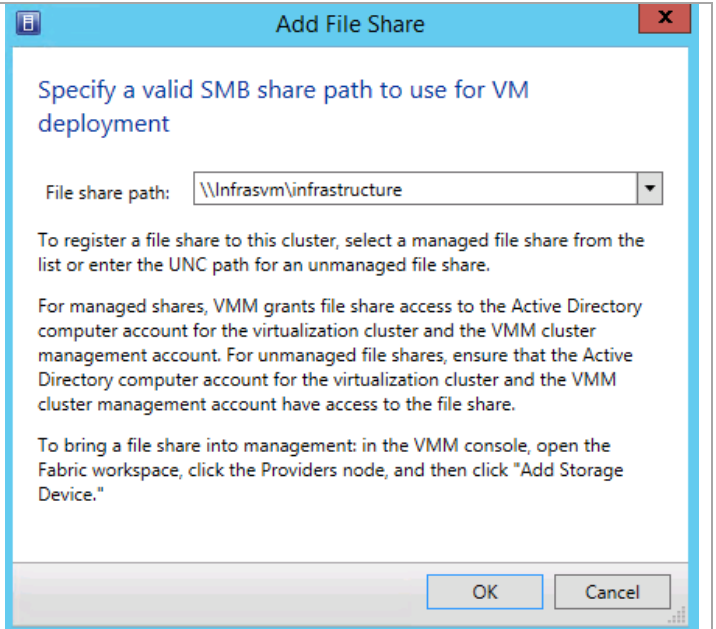
Click **Fabric** in the left tree view. Expand **Servers**, **All Hosts**, and **Management Fabric**. Right click the **Management Cluster** and select **Properties**.



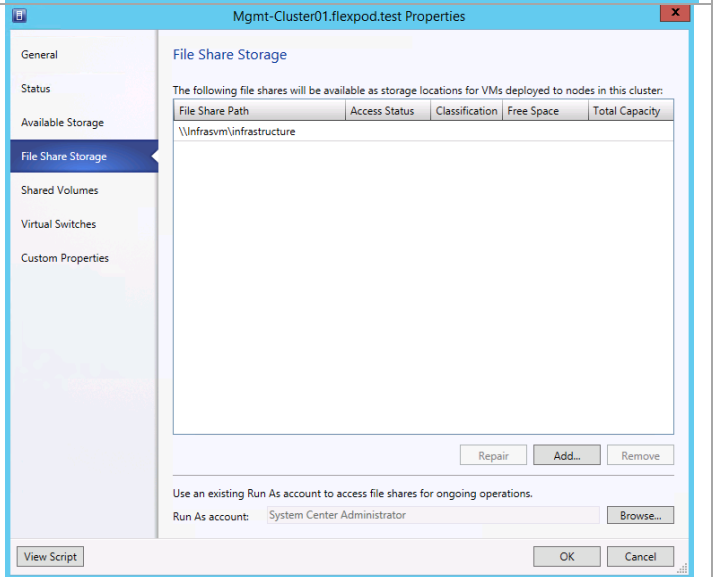
Select **File Share Storage** and click **Add**.



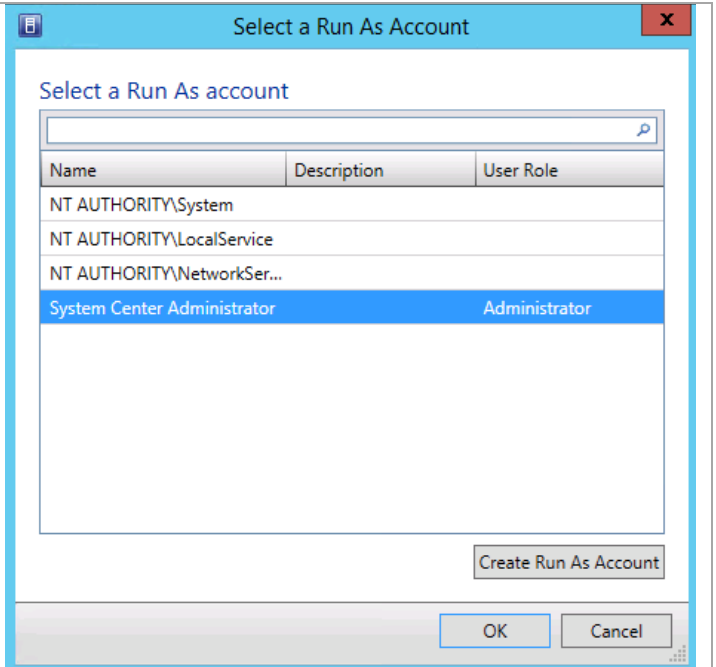
Enter the UNC path to the file share that stores the cluster VHDs and click **OK**.



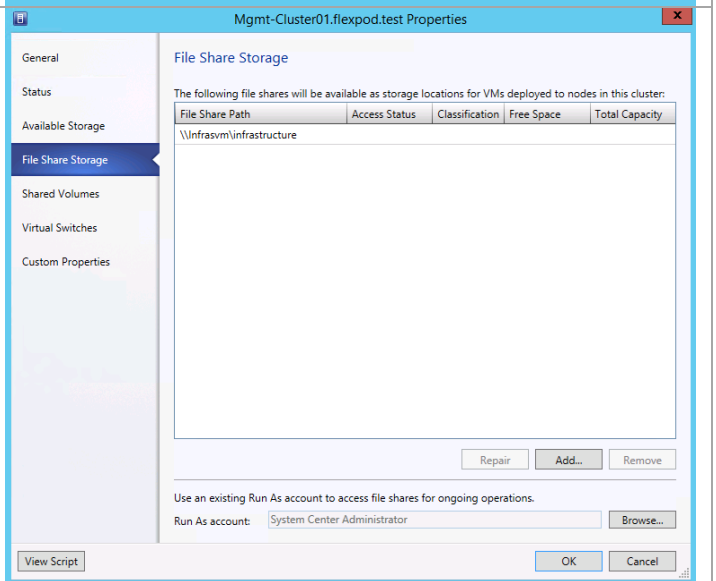
Click **Browse** to add a **Run As** account.



Select the Run As account and click **OK**.



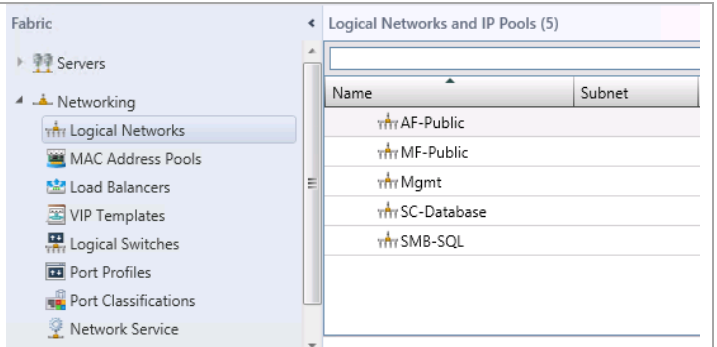
Click **OK** to register the file share.



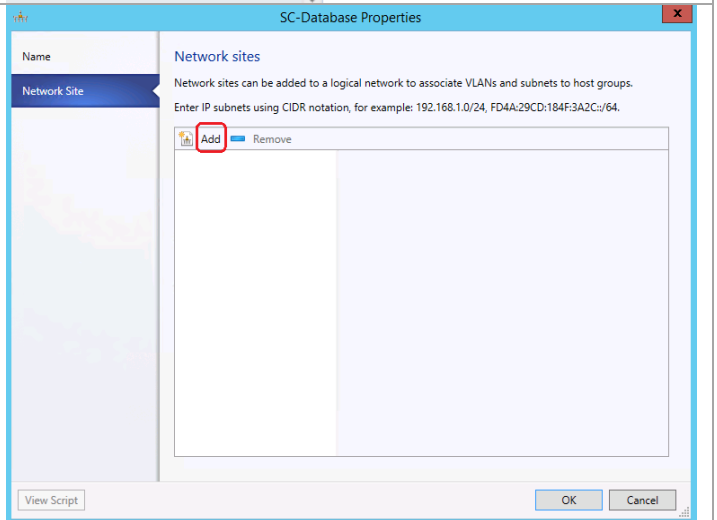
## 18.9 Configure Logical Networks

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

Select **Fabric** and expand **Networking**. Right-click each Logical Networks and select **Properties**.



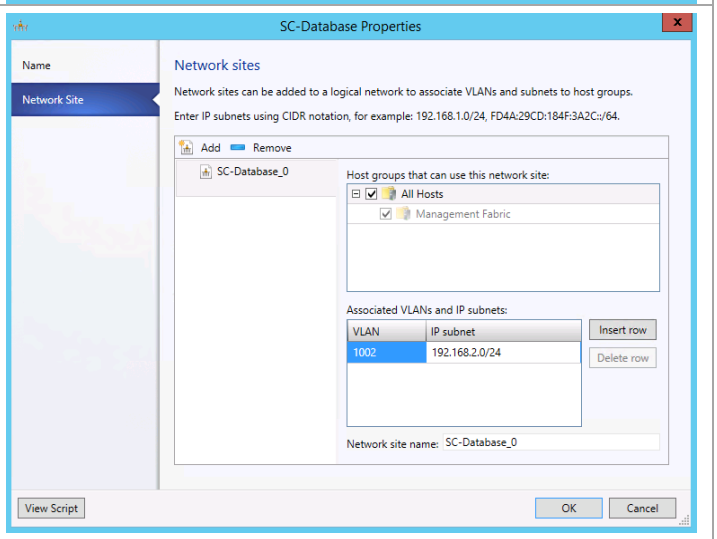
Select **Network Site** and click **Add**.



Check **All Hosts**. Click **Insert row**. Enter the **VLAN ID** and **IP subnet** the network site. Click **OK**.

Repeat this procedure for each Logical Network.

**Note:** Enter 0 for the VLAN ID for the native VLAN.



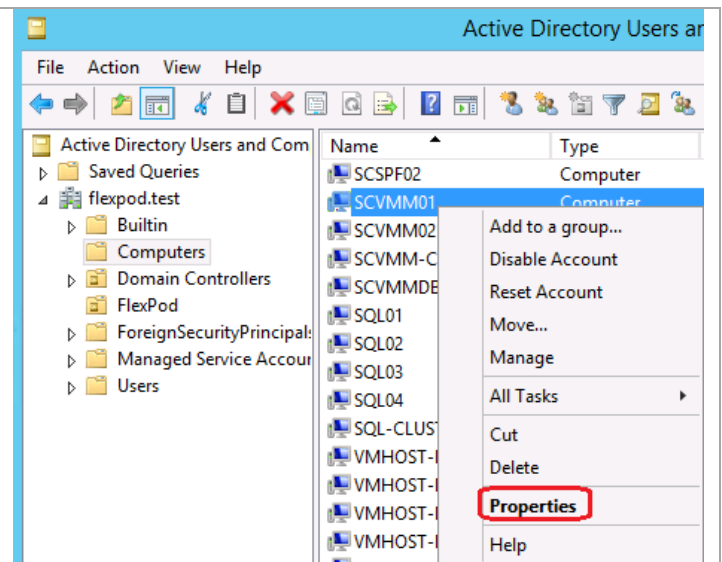


## 18.10 Configure Constrained Delegation

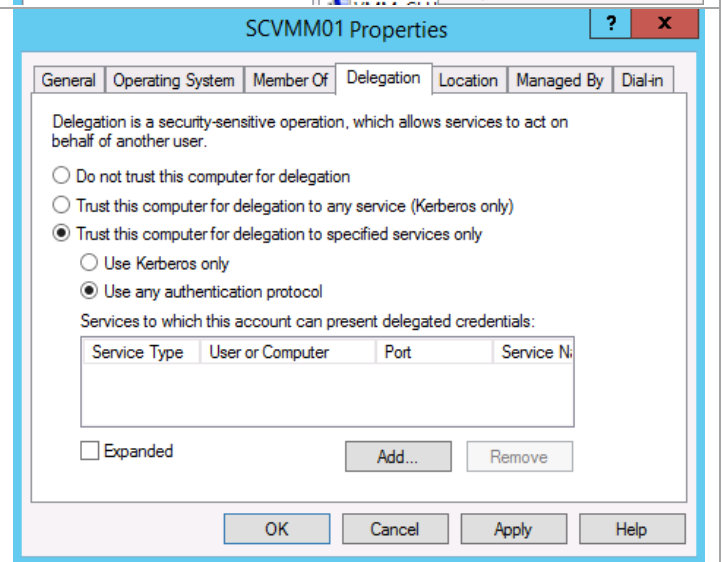
By default, when VMM is creating a virtual machine, and you are using an ISO file from the library for installation purposes, the ISO file is copied and made part of the virtual machine's definition. This wastes time copying the file and it takes extra space. It also means that different versions of installation media may end up getting stored all over. Sharing ISO items across nodes requires additional configuration of the VMM hosts and any system that runs the VMM console. This is called constrained delegation which allows the VMM host to operate on behalf of the virtual machine being created.

This is a security change to a default installation, so it should be reviewed with your security department before deployment.

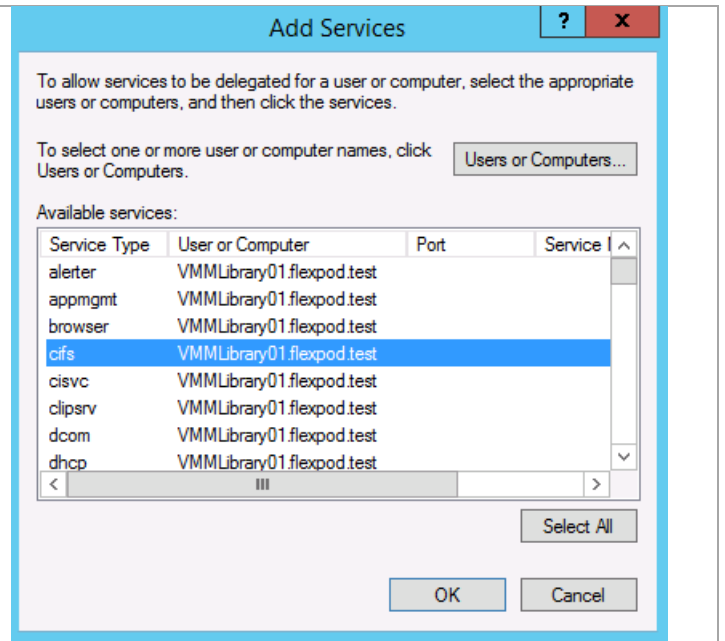
On your domain controller (or a system that has the proper Remote Server Administration Tools installed), launch **Active Directory Users and Computers**. Expand your domain and expand **Computers**. Right-click on your VMM host and select **Properties**.



On the **Delegation** tab, click the radio button by **Trust this computer for delegation to specified service only**. Select the radio button by **Use any authentication protocol**. Click the **Add...** button.



On the **Add Services** window, click the **Users or Computers...** button. Select the SCVMM library server in the **Select Users or Computers** window. Click **OK** to show the list of services available for the selected server. Select the **cifs** service and click **OK** to continue. Then click **OK** on the server Property page to update the services. Repeat for each SCVMM server or any server from which you plan to run the VMM console, such as your remote management workstation.



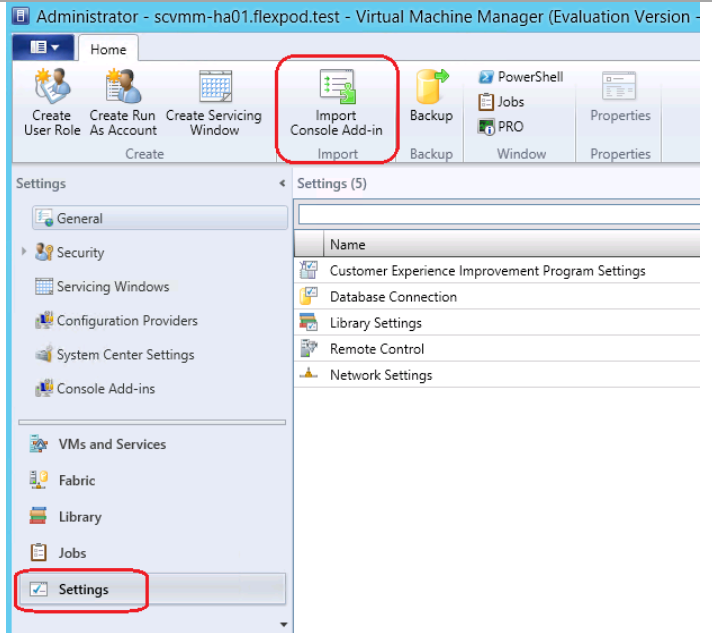
## 18.11 Install Cisco UCS User Interface Extensions for Virtual Machine Manager

The UCS User Interface Extensions for Virtual Machine Manager can be downloaded from the following link:

<http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574016&release=1.1.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

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

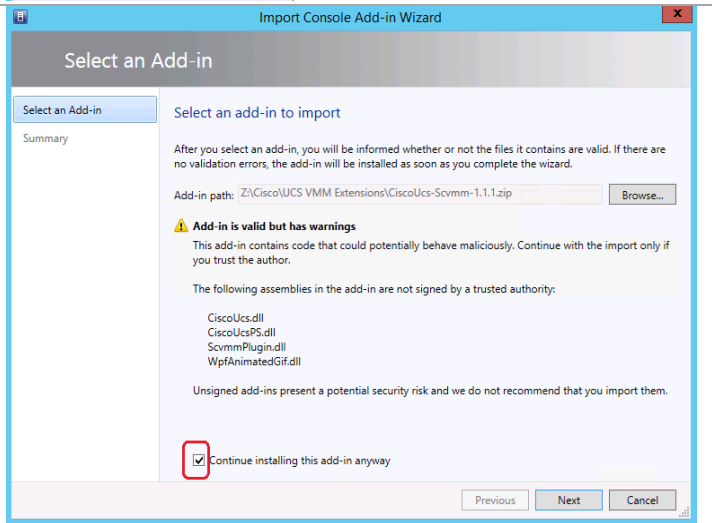
In the **Virtual Machine Manager** console, navigate to the **Settings** pane and select the **Import Console Add-in**



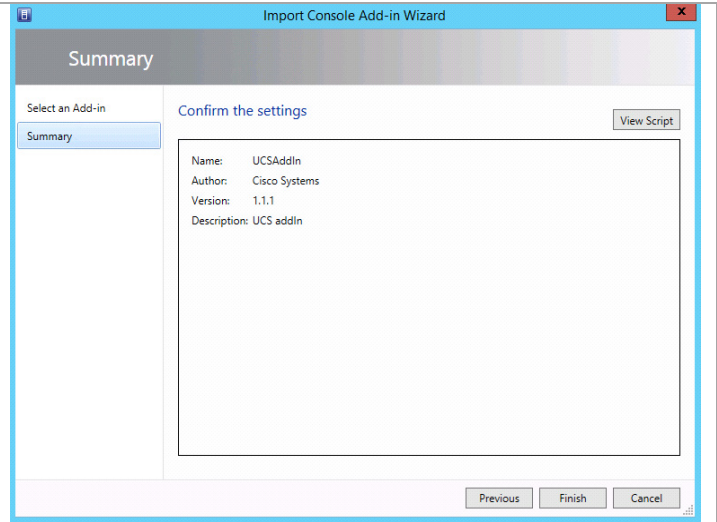
On the Import Console Add-in Wizard, click **Browse** on the Add-in Path. Select the **Cisco UCS UI Extensions for Virtual Machine Manager** package and click **Open**.

**Note:** The warning about signed binaries can safely be ignored in this case.

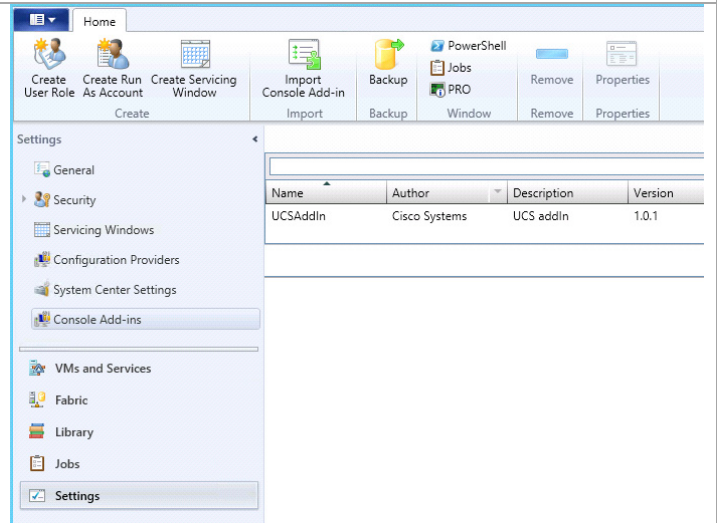
Click the check box **“Continue installing this add-in anyway”** and click **Next** to continue.



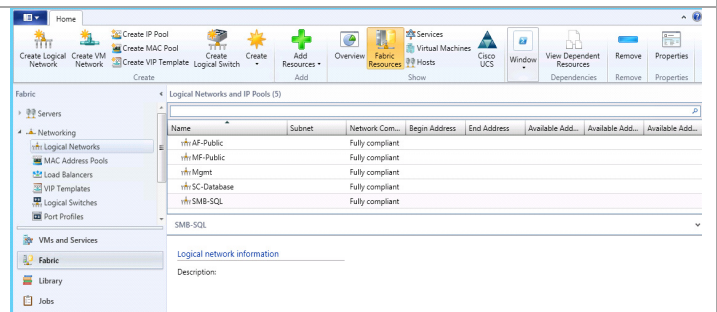
Review the summary information and click **Finish**.



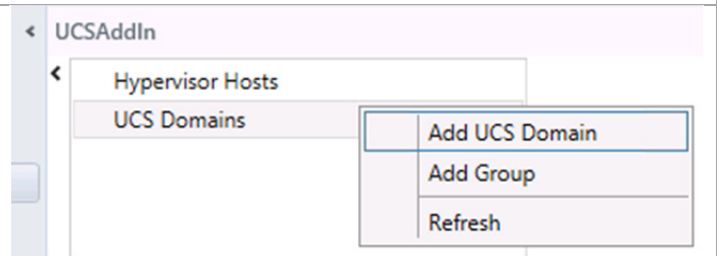
Click Console Add-ins to view the installed UCS User Interface Extensions.



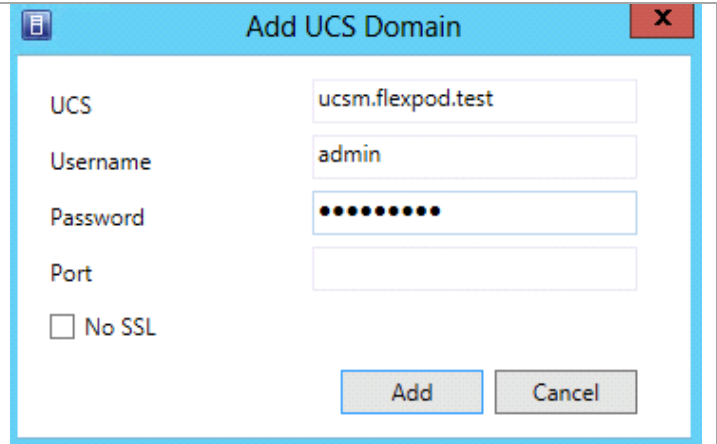
Select **Fabric** in the left pane and click the **Cisco UCS** icon.



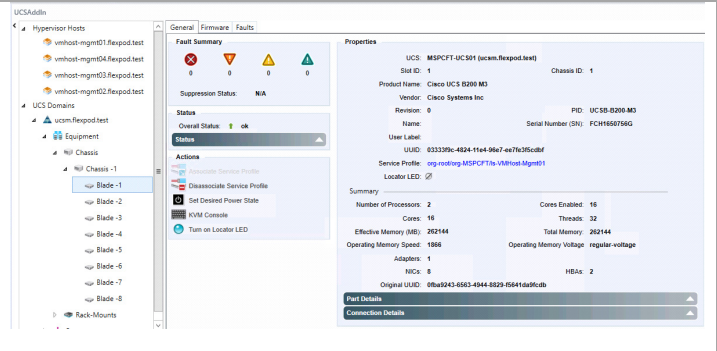
Right-click **UCS Domain** and select **Add UCS Domain**.



Enter the **UCS Manager host name, admin account, and password**. Click **Add**.



The UCS Manager objects are displayed in the review view pane.



## 19 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. Extract the contents of the zip file and find the location of these components:

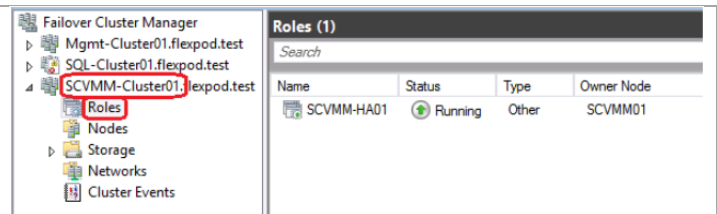
- Virtual Supervisor Module (VSM) ISO located in VSM\Install subdirectory
- Virtual Ethernet Module (VEM) MSI package located in VEM subdirectory
- Cisco VSEM Provider MSI package located in VMM subdirectory

Cisco Nexus 1000V for Hyper-V can be downloaded at the following link:

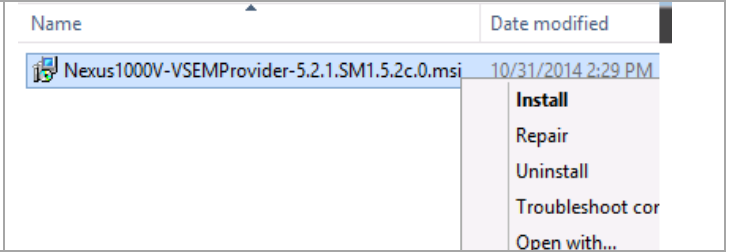
[http://software.cisco.com/download/release.html?mdfid=284786025&flowid=42792&softwareid=282088129&release=5.2\(1\)SM1\(5.2c\)&reind=AVAILABLE&rellifecycle=&reltype=latest](http://software.cisco.com/download/release.html?mdfid=284786025&flowid=42792&softwareid=282088129&release=5.2(1)SM1(5.2c)&reind=AVAILABLE&rellifecycle=&reltype=latest)

### 19.1 Install the Virtual Supervisor Modules Virtual Machine Template

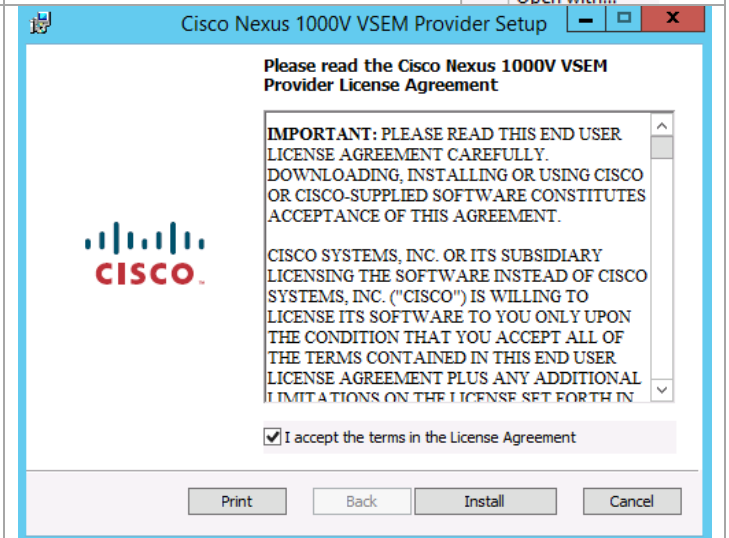
Determine the node of the SCVMM cluster that is hosting the cluster resource and work from that node.



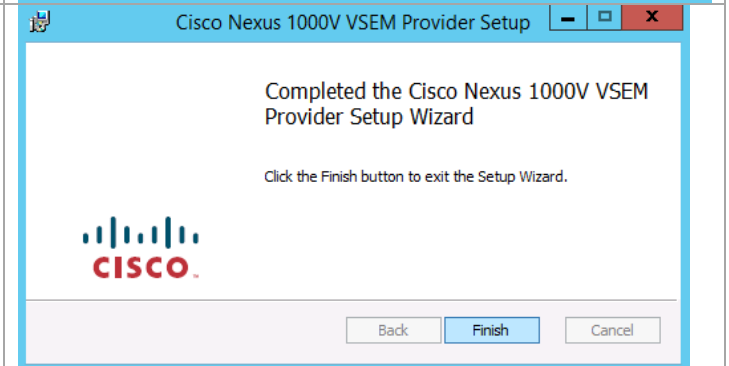
Find the VSEMProvider installation package in the VMM subdirectory and install it.



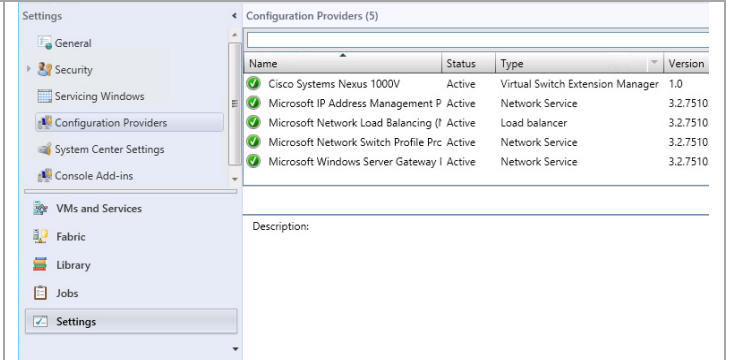
Click the check box for **I accept the terms in the License Agreement** and click **Install**.

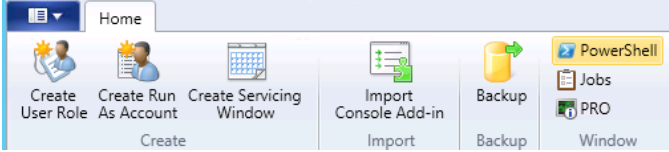
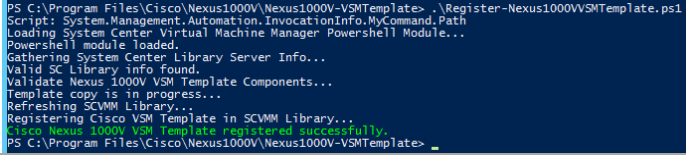
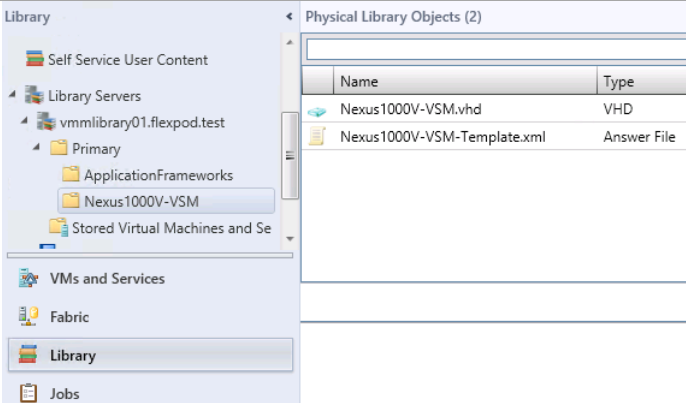
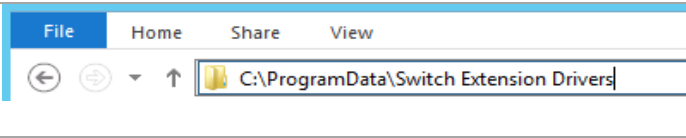
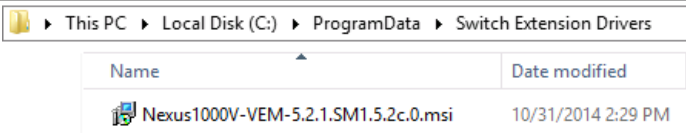


A status screen will show the progress of the installation. When you receive the completion screen, click **Finish** to complete the installation. The installation will restart the VMM service, so you will lose the connection to the service. Just wait and you will be reconnected to the VMM console.

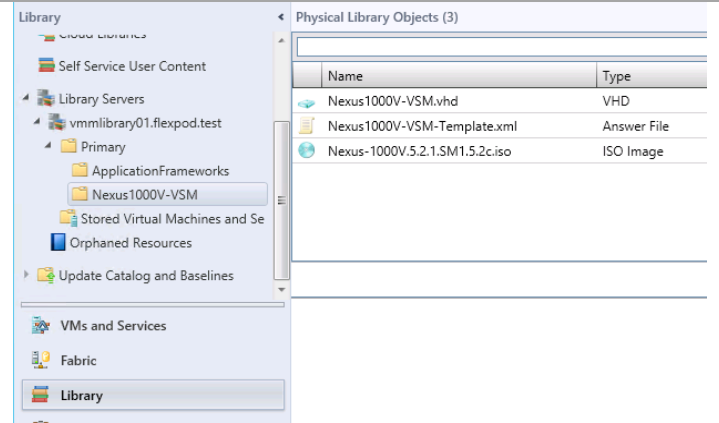


In the VMM console navigate to **Settings > Configuration Providers** to validate the installation of the Cisco Nexus 1000V.



<p>From the VMM Console launch a PowerShell window. This must be launched from the VMM Console in order for the proper PowerShell modules to be loaded. Be patient – it takes a little time for the modules to load.</p> <p>By default the execution policy for execution of scripts is too strict to allow for the execution of a script downloaded from the web. To allow execution of the next installation script, run this PowerShell cmdlet.</p>	 <p><b>Set-ExecutionPolicy Bypass -Force</b></p>
<p>Within the PowerShell window navigate to C:\Program Files\Cisco\Nexus1000V\Nexus1000V-VSMTemplate. When there execute this PowerShell cmdlet. Notice it starts with a period(.).</p>	<p><b>.\Register-Nexus1000VSMTemplate.ps1</b></p> 
<p>You can verify the success by looking in the VMM Library. You should see a new sub-directory name Nexus1000V-VSM and two elements stored in it.</p>	
<p><b>Perform this copy on <u>each</u> VMM management server. DO NOT EXECUTE – JUST COPY.</b></p>	
<p>The destination directory is a hidden directory, so unless you have configured your system to show hidden directories, you need to type its location in the top of the Windows Explorer window.</p>	
<p>The Nexus1000V-VEM-5.2.1.SM1.5.2c.0.msi file is located in the \VEM subdirectory of the expanded files. Copy it to the Switch Extension Driver directory.</p>	
<p><b>Perform this copy on <u>one</u> VMM management server.</b></p>	

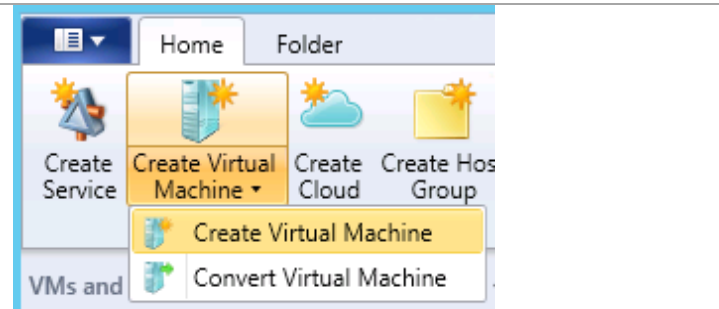
Copy the VSM ISO file to the SCVMM Library. The VSM ISO file is found in the \VSM\Install subdirectory of the expanded files. The SCVMM library is a standard file share, so you just have to copy the file to the appropriate file share location.



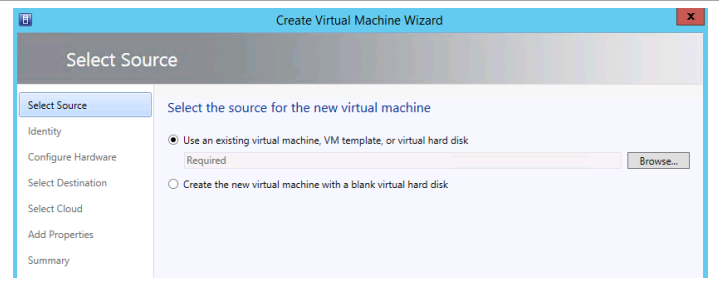
## 19.2 Create Two Virtual Supervisor Modules Virtual Machines

The Cisco Nexus 1000V is deployed as a pair of highly available virtual machines. Each machine will have its own unique management IP address, and the highly available service will have its own virtual IP address separate from the individual machines. It is necessary to add, at a minimum, the virtual IP address to DNS. SCVMM uses the virtual IP address for communication.

From the VMM console, select **VMs and Services**. Select **Create Virtual Machine** from the menu ribbon, and select **Create Virtual Machine**.

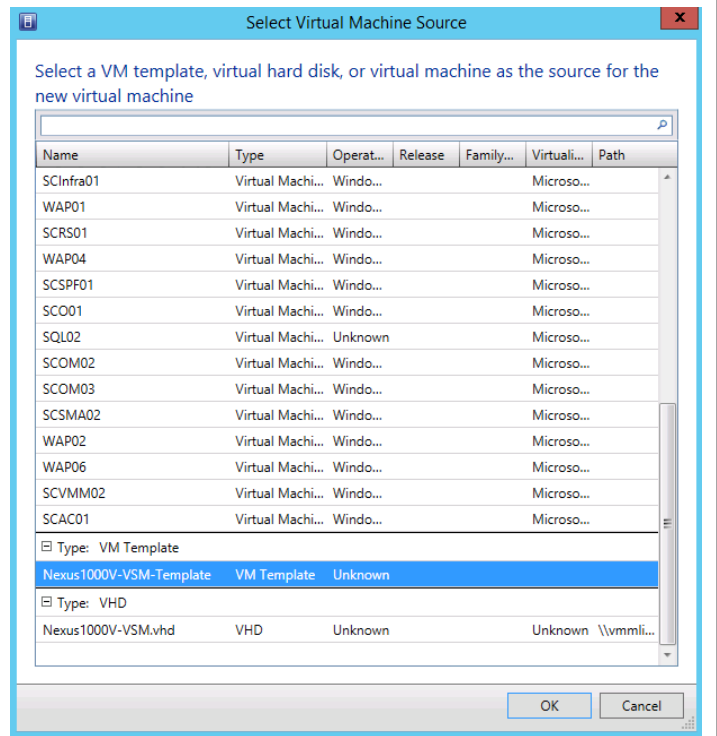


On the **Select Source** window, select the radio button by **Use an existing virtual machine, VM template, or virtual hard disk**. Click the **Browse...** button.

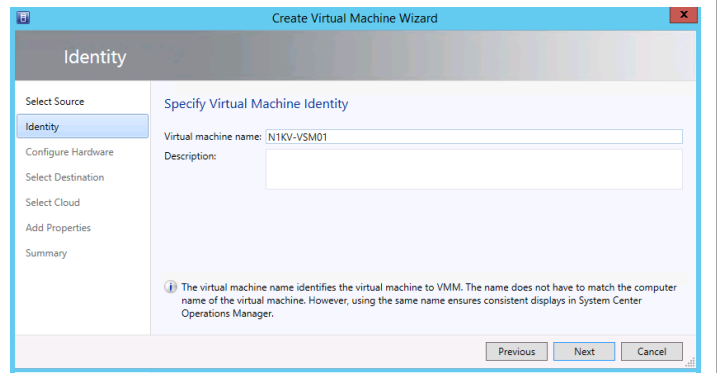




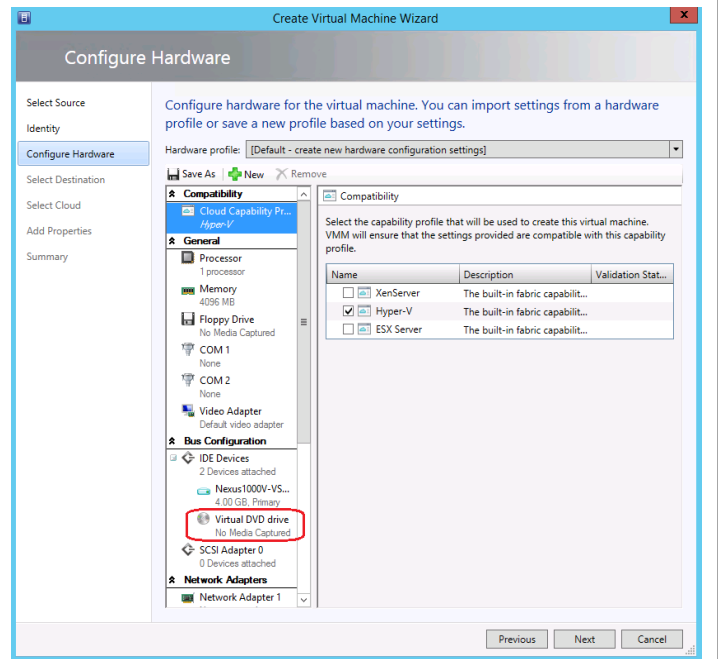
On the **Select Virtual Machine Source** window, scroll to the bottom to find the Type: VM Template. Select the **Nexus1000v-VSM-Template**. Click **OK** to continue. Then click **Next** when you are back on the Select Source page.



On the **Identity** window, enter a name for the virtual machine you are creating. Click **Next** to continue.

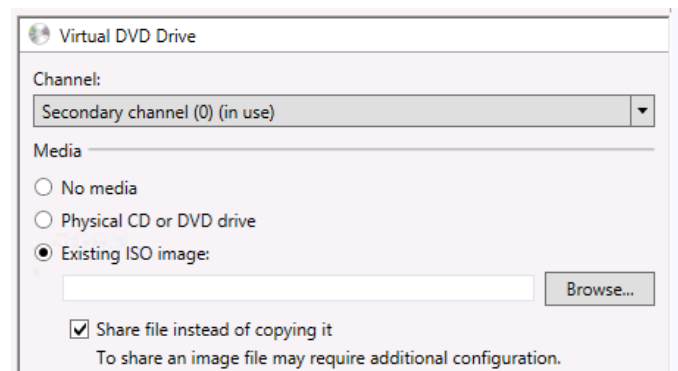


On the **Configure Hardware** window, under Compatibility, select the check box by **Hyper-V**. Almost everything should already be configured from the template. However, you must still assign the ISO file for installation. Click on **Virtual DVD drive**.

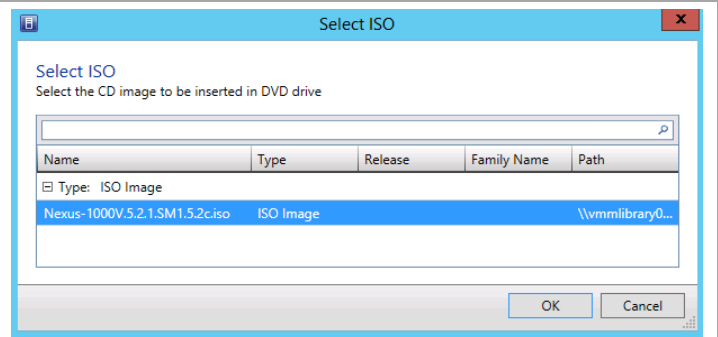


The right-hand side of the page will change to allow you to configure the Virtual DVD Drive. Select the radio button by **Existing ISO image**. Click the **Browse...** button.

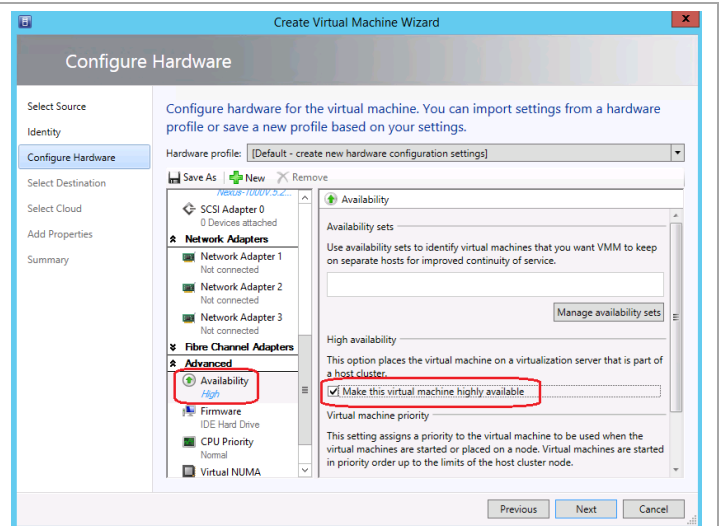
**Note:** Note: If you have configured your systems for Constrained Delegation, you can also select the check-box by **Share file instead of copying it**.



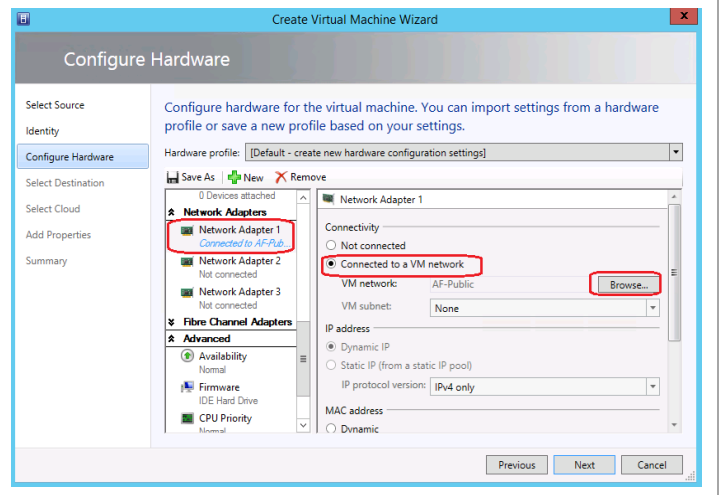
On the **Select ISO** window, select the **Nexus-1000V.5.2.1.SM1.5.2c.iso** file. Click **OK** to continue.



Scroll down to the Advance objects in the middle pane and select **Availability**. Check the box **Make this virtual machine highly available**.

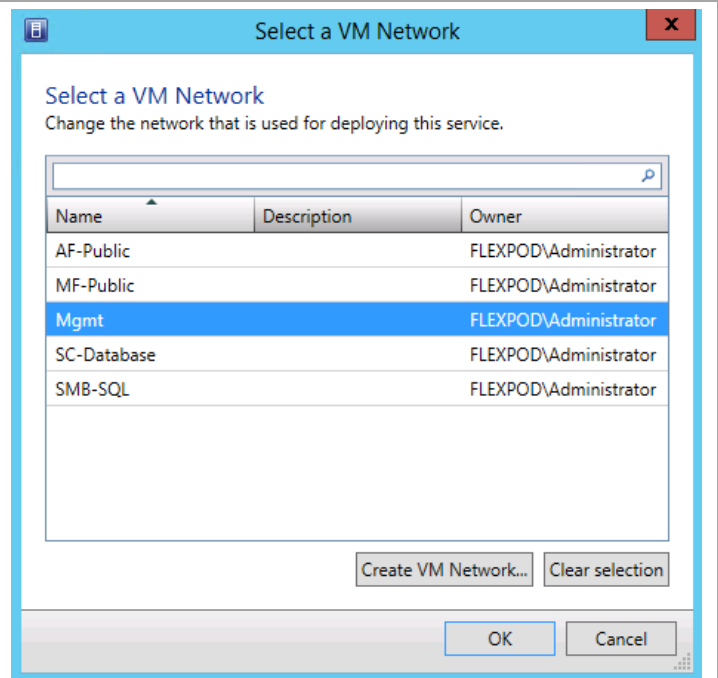


Scroll down to the **Network Adapters** objects in the middle pane and select the first network adapter. In the right pane select the radio button by **Connected to a VM network** and click **Browse...**

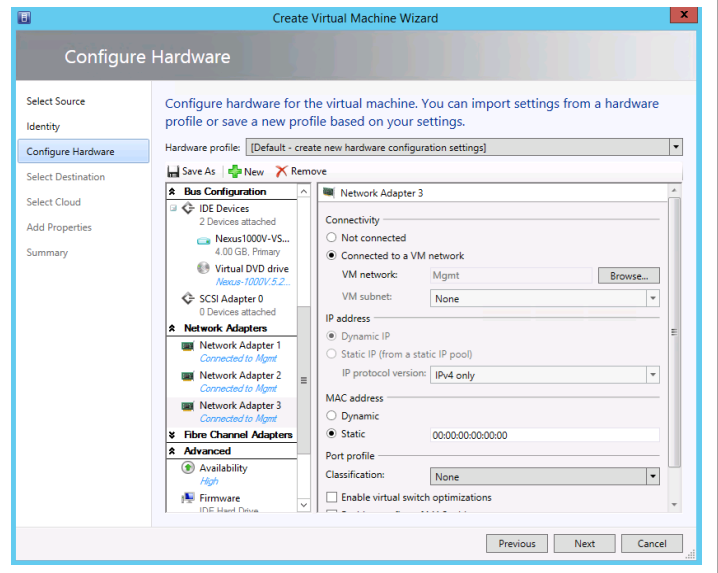


Select the management network shared between hosts and VMs and click **OK**.

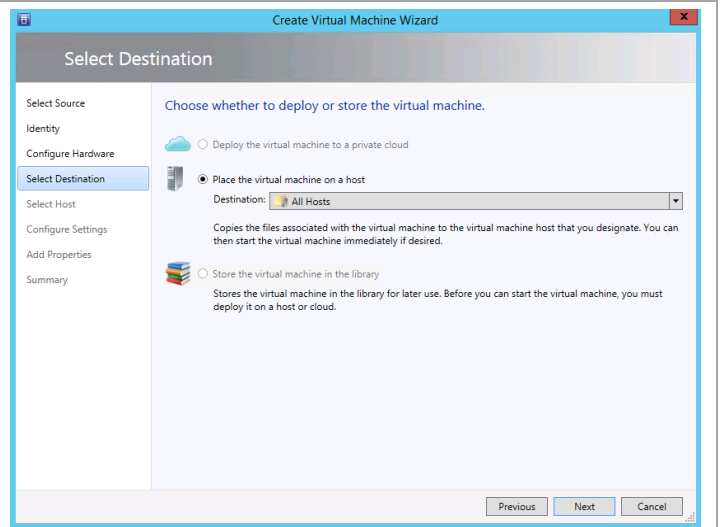
Repeat for all three network adapters; all three network adapters are on the same VM network.



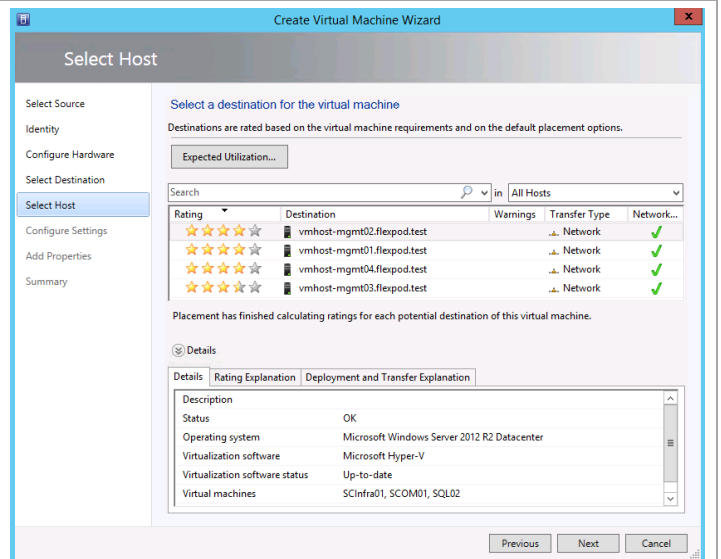
Click **Next** to proceed.



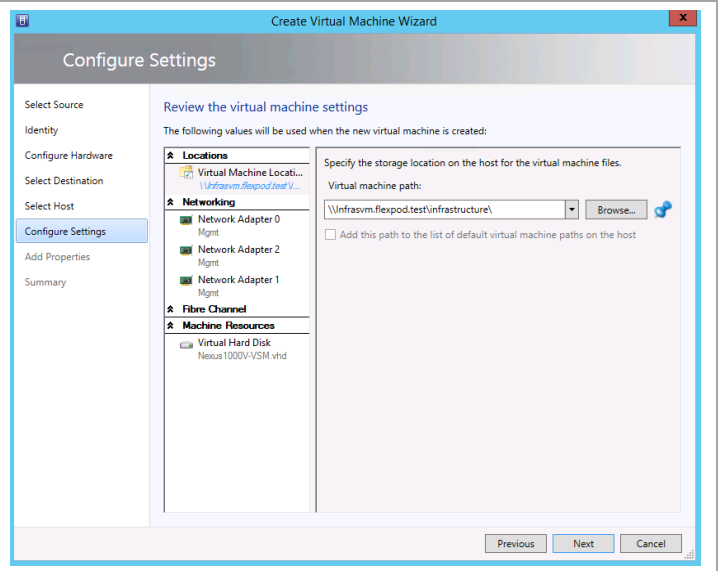
Select the default placement option to place the virtual machine on **All Hosts** and click **Next**.



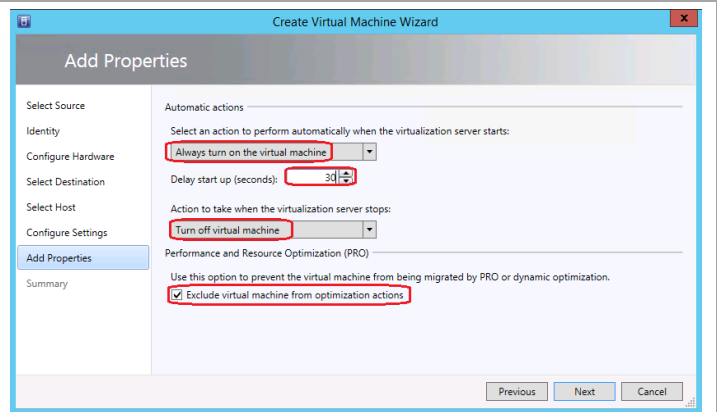
In the **Select Host** window, click **Next**.



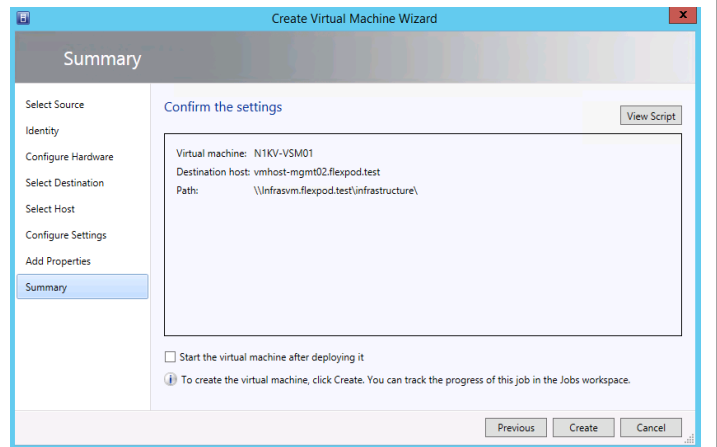
Review the path to store the virtual machine configuration and VHD. Click **Next** to proceed.



In the **Add Properties** window select “**Exclude virtual machine from optimization actions**”. As the Nexus 1000V is critical to the operation of the overall network, select the option to **Always turn on the virtual machine** when the server starts and set a startup delay of 30 seconds. Set the option to **Turn off virtual machine** when the server stops. Click **Next** to proceed.



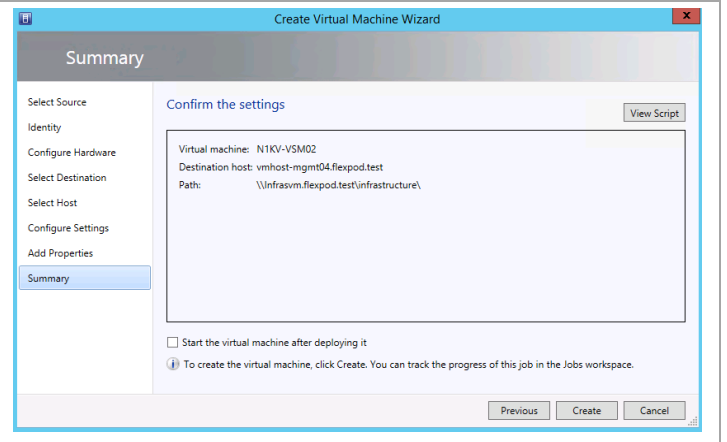
Review the summary and click **Create**.



Verify that virtual machine is created successfully.

Name	Status	Start Time	Result Name
Remove resource	Completed	11/3/2014 8:20:11 AM	Object Deleted
Create virtual machine	Completed	11/3/2014 8:20:10 AM	N1KV-VSM01
Update the placement settings of a VM depl...	Completed	11/3/2014 8:14:25 AM	N1KV-VSM01
Modify existing VM deployment configurati...	Completed	11/3/2014 8:14:25 AM	N1KV-VSM01
Update the placement settings of a VM depl...	Completed	11/3/2014 8:13:25 AM	N1KV-VSM01
Modify existing VM deployment configurati...	Completed	11/3/2014 8:13:24 AM	N1KV-VSM01
Create virtual machine			
Step	Name	Status	Start Time
1	Create virtual machine	Completed	11/3/2014 8:20:10 AM
1.1	Create virtual machine	Completed	11/3/2014 8:20:14 AM
1.2	Deploy file (using LAN)	Completed	11/3/2014 8:20:18 AM
1.3	Deploy file (using LAN)	Completed	11/3/2014 8:20:18 AM
1.4	Change properties of virtual machine	Completed	11/3/2014 8:20:25 AM
1.5	Fix up differencing disks	Completed	11/3/2014 8:20:25 AM

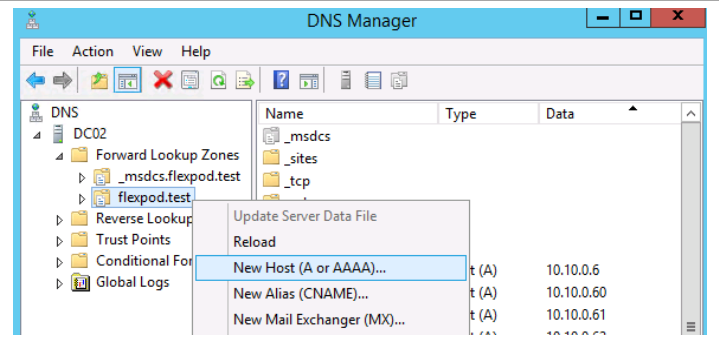
Repeat this procedure to create the second VSM virtual machine. Place the second VSM on a different host from the first VSM.



### 19.3 Add a Domain Name Service Record for the Virtual Supervisor Module VMs

Perform the following configuration operation on the server running Domain Name Service.

Open DNS Manager and navigate the forward lookup zone for the domain. Right click the forward lookup zone and select **New Host (A or AAAA) ...**

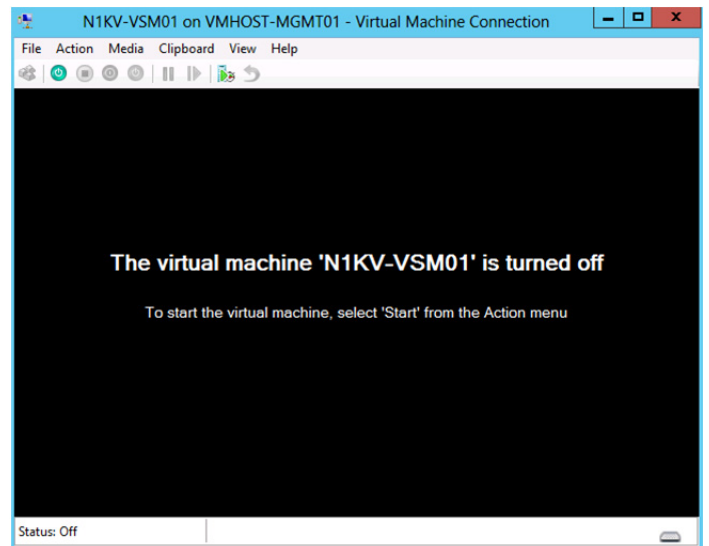


Enter the VMS host name and IP address. Click **Add Host**.  
 Click **OK** to acknowledge the DNS record creation.  
 Click **Done** to close the New Host window.

## 19.4 Configure Virtual Supervisor Modules in the VSM Virtual Machines

Perform the following configuration operation on the first VSM virtual machine.

In VMM or Hyper-V Manager console, connect to the first VSM01 VM and power it on.



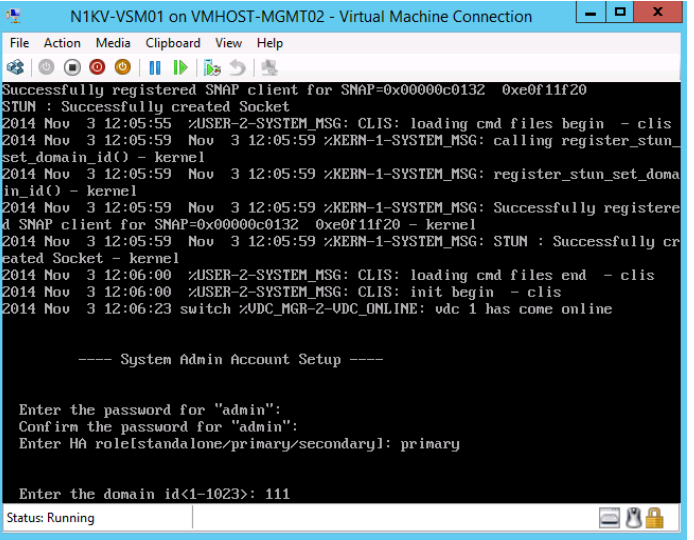
There are three questions asked, all of which have short timers on them. If you do not answer, they automatically continue using the defaults. The defaults are the answers you want.



The installation asks for a password for the admin account. Enter the password and confirm it. If the password is not considered 'strong', you will be prompted for a different password.

The next question is the HA role. Enter **primary**.

The next question is the domain ID. Enter a value between 1-1023.



```
N1KV-VSM01 on VMHOST-MGMT02 - Virtual Machine Connection
File Action Media Clipboard View Help
Successfully registered SNAP client for SNAP=0x00000c0132 0xe0f11f20
STUN : Successfully created Socket
2014 Nov 3 12:05:55 %USER-2-SYSTEM_MSG: CLIS: loading cmd files begin - clis
2014 Nov 3 12:05:59 %KERN-1-SYSTEM_MSG: calling register_stun_
set_domain_id() - kernel
2014 Nov 3 12:05:59 %KERN-1-SYSTEM_MSG: register_stun_set_doma
in_id() - kernel
2014 Nov 3 12:05:59 %KERN-1-SYSTEM_MSG: Successfully registere
d SNAP client for SNAP=0x00000c0132 0xe0f11f20 - kernel
2014 Nov 3 12:05:59 %KERN-1-SYSTEM_MSG: STUN : Successfully cr
eated Socket - kernel
2014 Nov 3 12:06:00 %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2014 Nov 3 12:06:00 %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2014 Nov 3 12:06:23 switch %UDC_MGR-2-UDC_ONLINE: udc 1 has come online

---- System Admin Account Setup ----

Enter the password for "admin":
Confirm the password for "admin":
Enter HA role[standalone/primary/secondary]: primary

Enter the domain id<1-1023>: 111
Status: Running
```

Enter **Y** to enter the basic configuration.

Enter **N** to creating another login account.

Enter the switch name : N1KV-VSM01

Enter **Y** to configure Out-of-Band management interface.

Enter the Mgmt0 IPv4 address: 10.10.0.16

Enter the IPv4 netmask: 255.255.255.0

Enter **Y** to configure the default gateway.  
Enter the IPv4 gateway address: 10.10.0.1

Enter **Y** to configure advance options.

Enter **Y** to configure advanced IP options.

Enter **N** not to configure a static route.

Enter **N** not to configure the default network.

Enter **Y** to configure DNS IP Address: 10.10.4.61

Enter **Y** to configure default domain name:  
flexpod.test

Enter **N** not to configure read-only SNMP  
community string.

Enter **N** not to configure read-write SNMP  
community string.

Enter **Y** to enable telnet service.

Enter **Y** to enable ssh service.

Enter **rsa** as the type of ssh key.

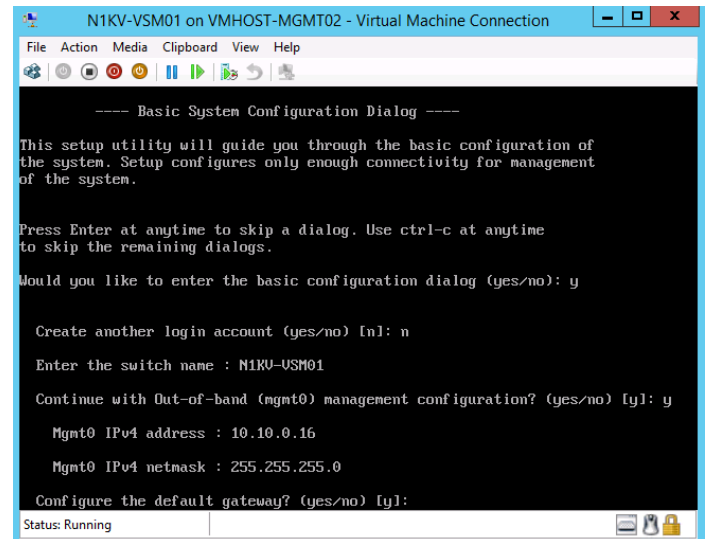
Enter **1024** for the number of rsa key bits.

Enter **Y** to configure NTP server address.

Enter **N** to reconfigure option.

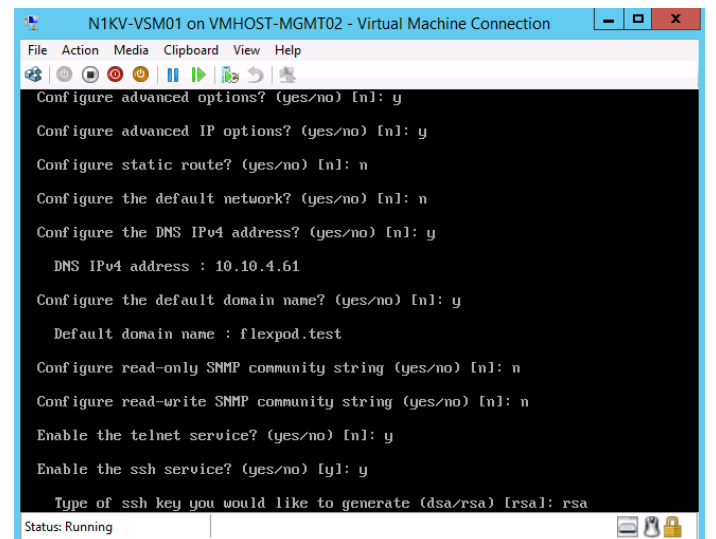
Enter **N** not to edit the configuration.

Enter **Y** to save the configuration and use it.



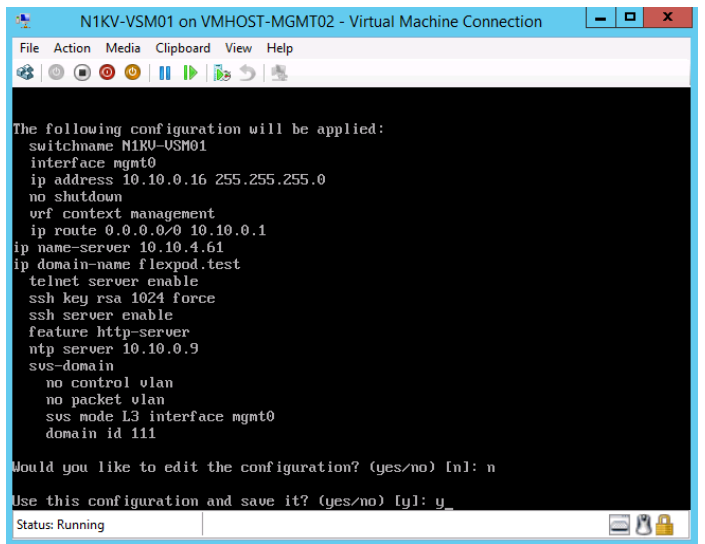
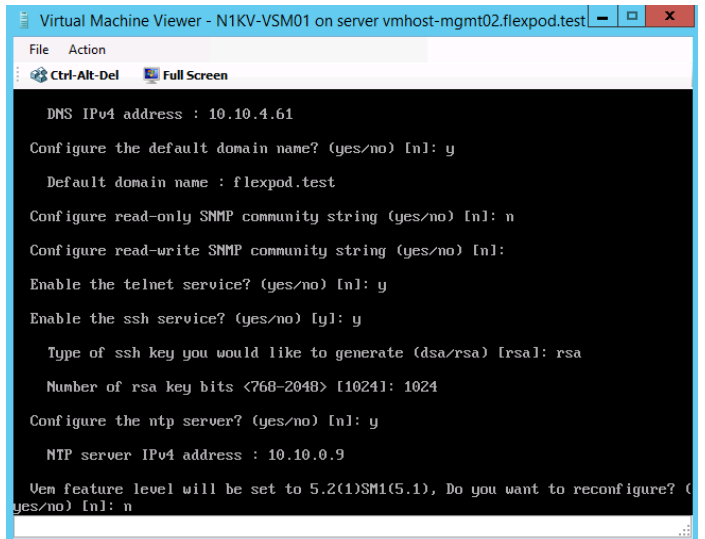
```
N1KV-VSM01 on VMHOST-MGMT02 - Virtual Machine Connection
File Action Media Clipboard View Help
----- Basic System Configuration Dialog -----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y

Create another login account (yes/no) [n]: n
Enter the switch name : N1KV-VSM01
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y
  Mgmt0 IPv4 address : 10.10.0.16
  Mgmt0 IPv4 netmask : 255.255.255.0
Configure the default gateway? (yes/no) [y]:
Status: Running
```

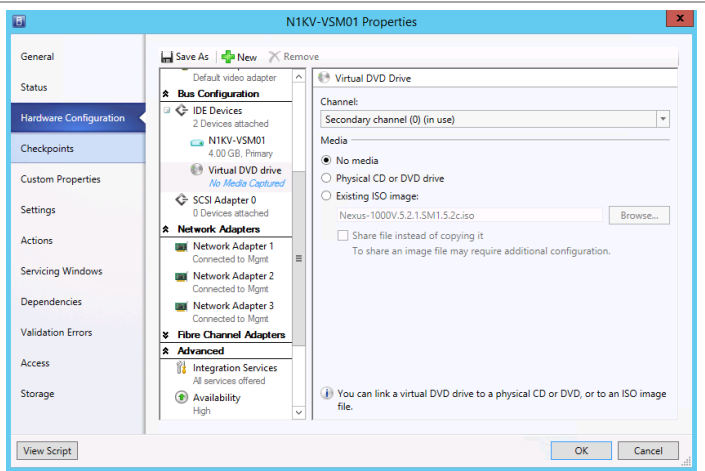


```
N1KV-VSM01 on VMHOST-MGMT02 - Virtual Machine Connection
File Action Media Clipboard View Help
Configure advanced options? (yes/no) [n]: y
Configure advanced IP options? (yes/no) [n]: y
Configure static route? (yes/no) [n]: n
Configure the default network? (yes/no) [n]: n
Configure the DNS IPv4 address? (yes/no) [n]: y
  DNS IPv4 address : 10.10.4.61
Configure the default domain name? (yes/no) [n]: y
  Default domain name : flexpod.test
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: y
Enable the ssh service? (yes/no) [y]: y
  Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Status: Running
```

Enter **Y** to configure NTP server address.  
 Enter IPv4 NTP server address:  
 Enter **N** to reconfigure  
 Review your entries and select **N** to edit the configuration.  
 Enter **Y** to use this configuration and save it.

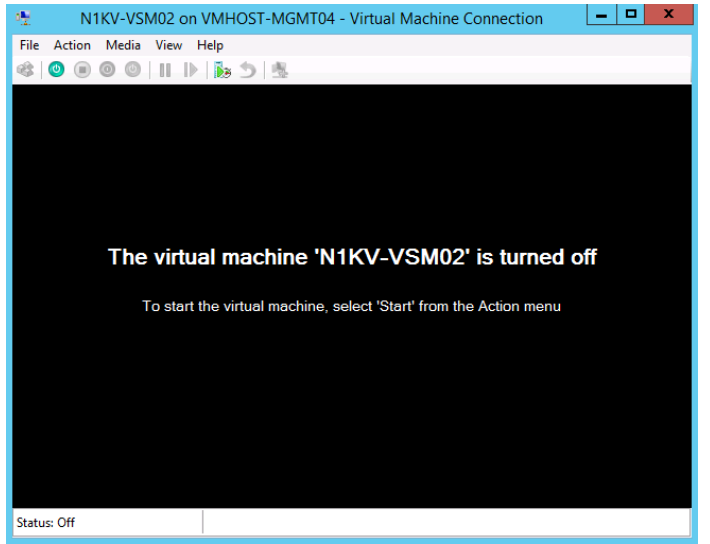


Remove the ISO from the first VSM VM.

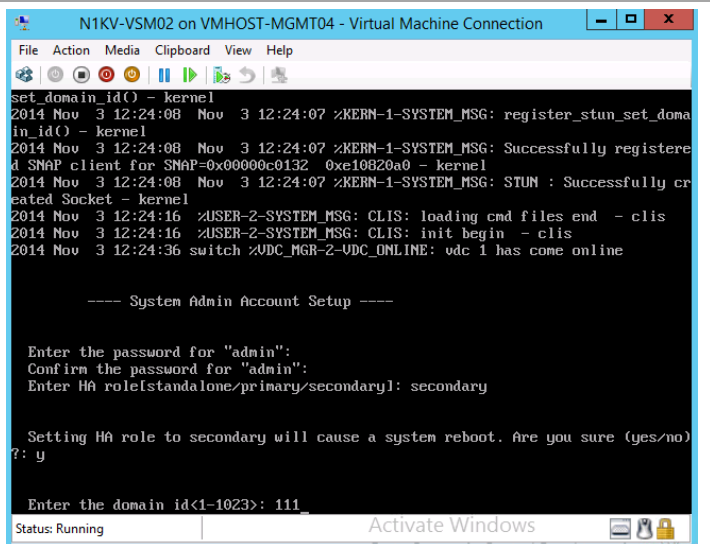


**Perform the following configuration operation on the second VSM virtual machine.**

In VMM or Hyper-V Manager console, connect to the second VSM VM and power it on. Again, there are three questions at the beginning of the process for which you can let the defaults be taken.

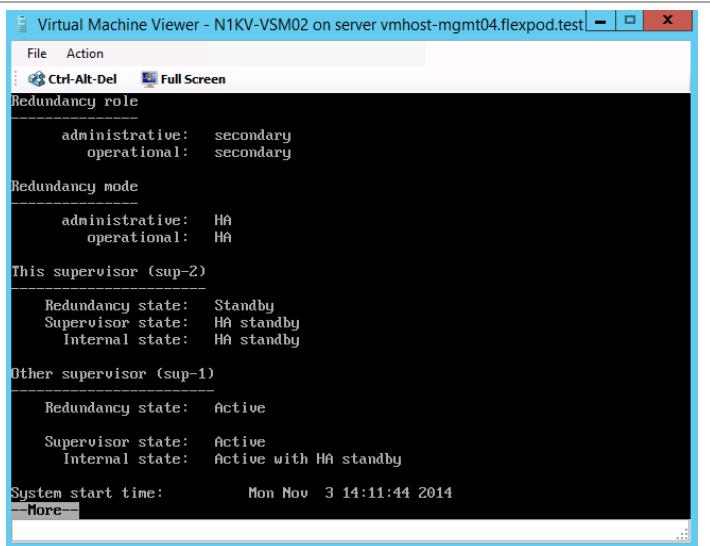


Enter the admin password. Select **secondary** for the role. Enter **Y** to the prompt on the reboot. Enter the domain id entered on the primary node.

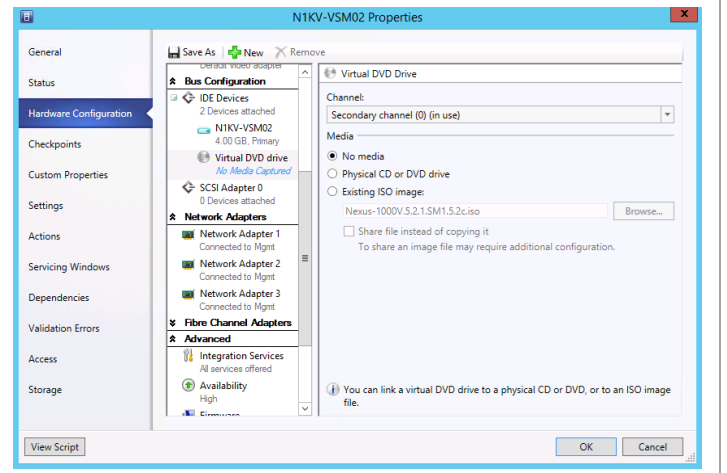


Login to the VMS and verify the redundancy status:

Show redundancy status



Remove the ISO from the second VSM VM.



## 19.5 Configure Nexus 1000V VSM For Use With Virtual Machine Manager

Enter the following configuration commands on The primary VSM.

```
configure terminal

nsm logical network FastTrack
exit

nsm network segment pool Mgmt-Fabric
member-of logical network FastTrack
exit

nsm ip pool template N1KV-MF-Public-IP-Pool
ip address 192.168.1.100 192.168.1.199
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
exit

nsm network segment N1KV-MF-Public
member-of network segment pool Mgmt-Fabric
switchport access vlan 1001
ip pool import template N1KV-MF-Public-IP-Pool
publish network segment
exit

port-profile type vethernet AllAccess1
no shutdown
state enabled
publish port-profile
exit

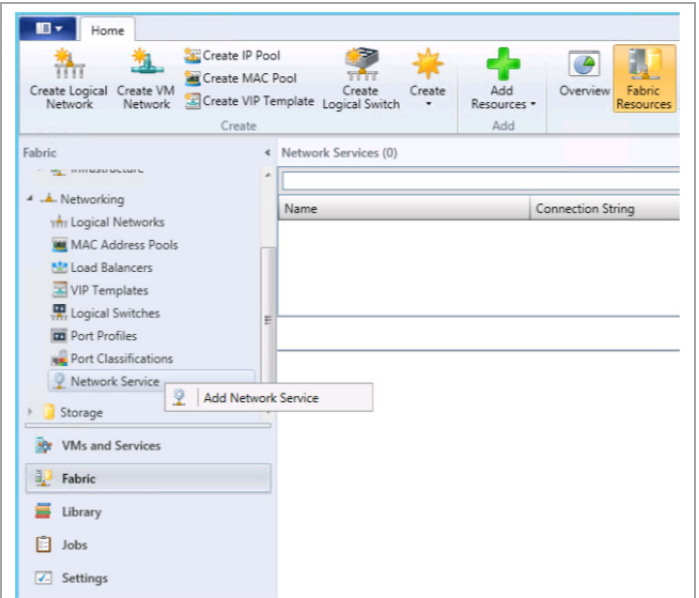
port-profile type ethernet N1KV-Uplink-Policy-FastTrack
channel-group auto mode on mac-pinning
no shutdown
state enabled
exit

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

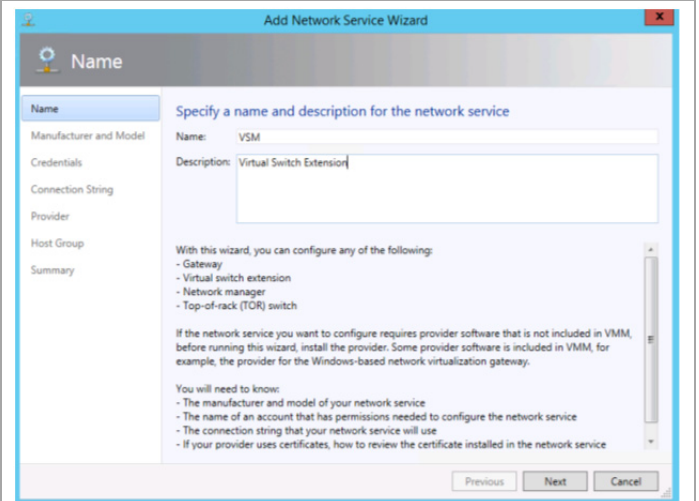
copy running-config startup-config
```

## 19.6 Connect SCVMM to VSM

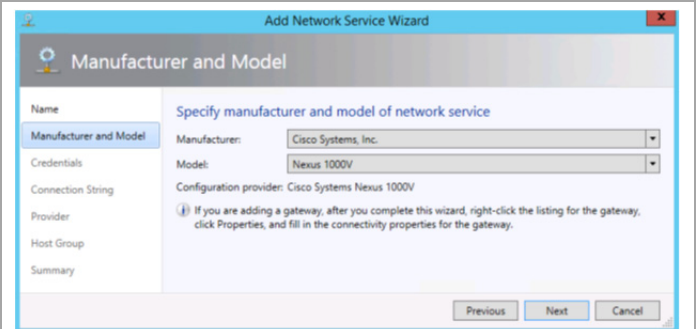
In the left pane of Virtual Machine Manager select **Fabric**. Expand **Networking** and select **Network Service**. Right-click and select **Add Network Service**.



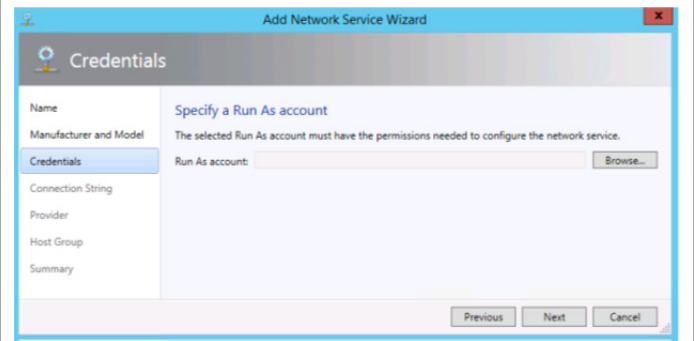
Enter a name for the network service. Optionally enter a description. Click **Next** to continue.



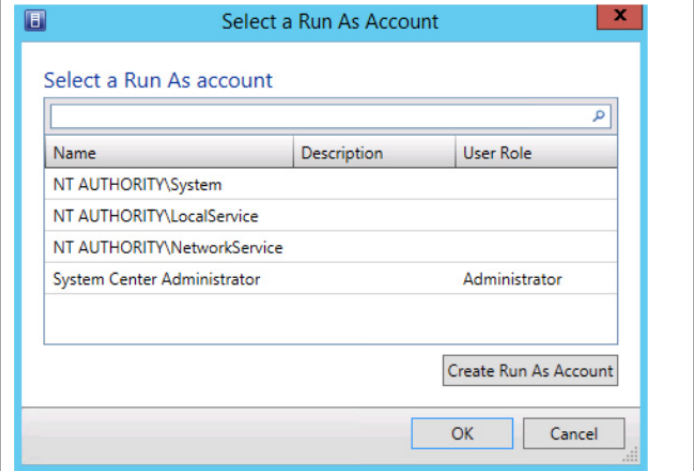
Accept Cisco as the Manufacturer and Nexus 1000V as the Model. Click **Next** to continue.



On the **Credentials** window, click **Browse...**

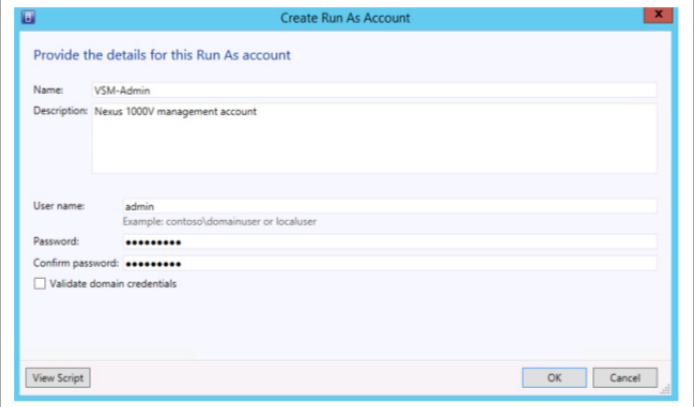


Click **Create Run As Account**.



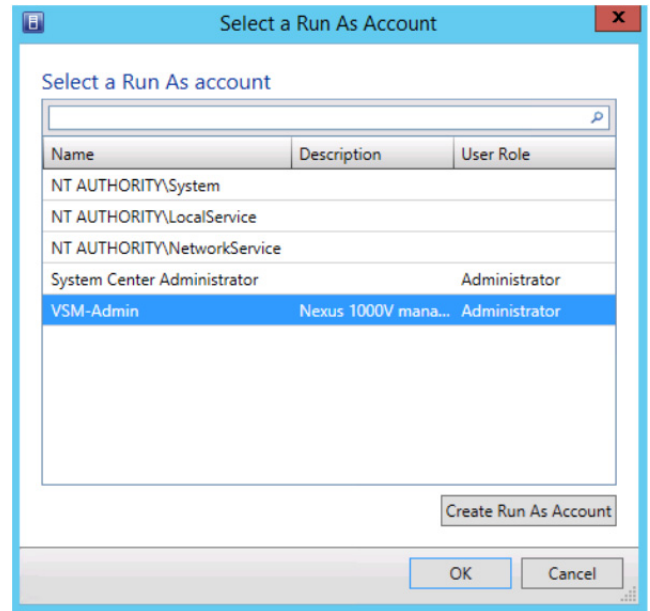
Enter the **Run As account name** and description.  
Enter the **user name** with rights to manage the Nexus 1000V VSM. This is the account and password configured during Cisco Nexus 1000V VSM installation.

Clear the check box for validating the domain credentials. Click **OK** to continue.

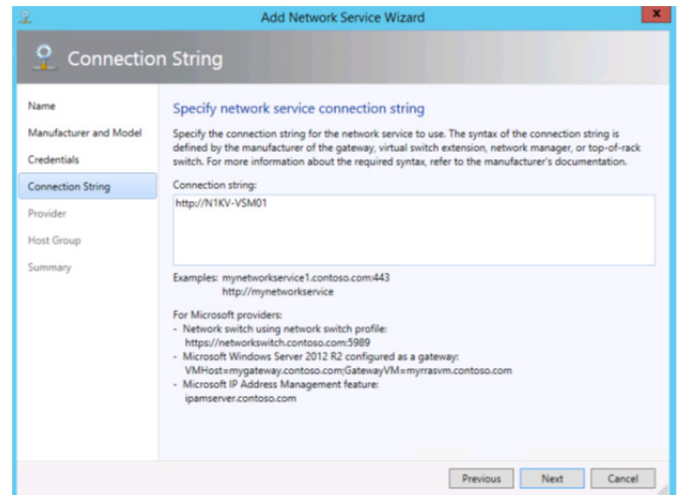


Select **VSM-Admin** account and click **OK**.

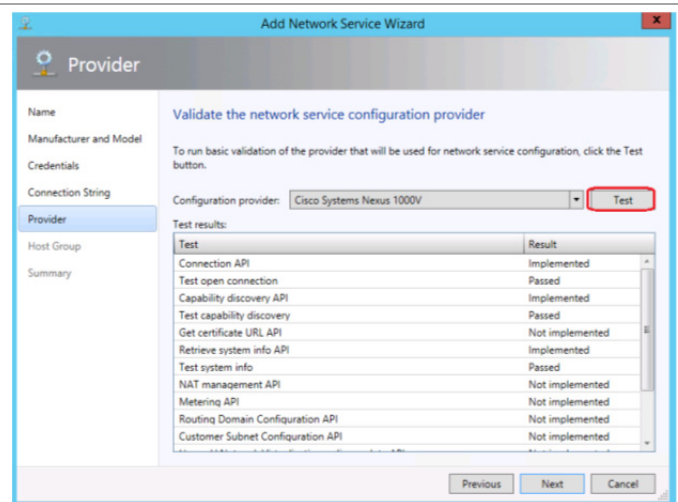
Back on the **Credentials** window, click **Next** to continue.



On the **Connection String** window enter the URL to access the created VSM. In this example that is <http://N1KV-VSM01>. Click **Next** to continue.

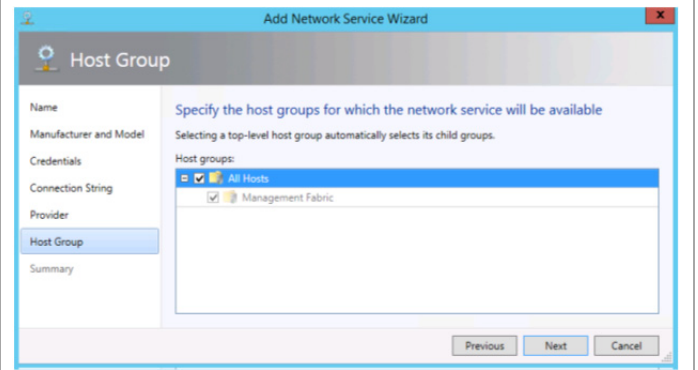


On the **Provider** window click the **Test** button to run basic validation. Check the test results to make sure any test run passed. Click **Next** to continue.

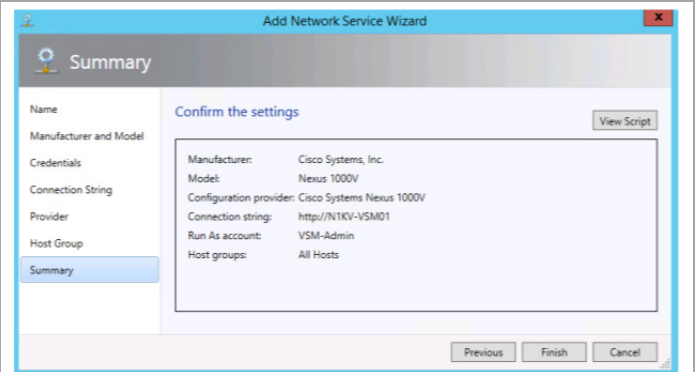




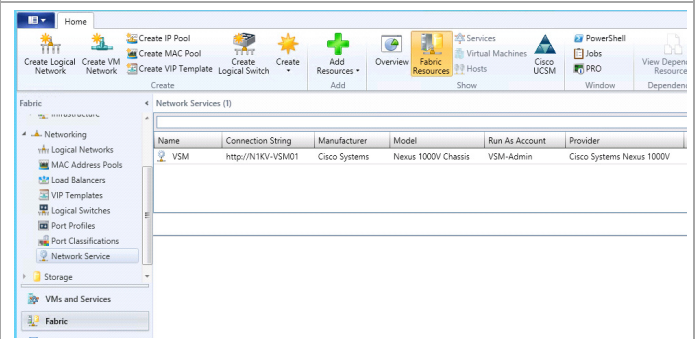
On the **Host Group** window select **All Hosts** group. Click **Next** to continue.



Review the contents of the Summary page and click **Finish**.

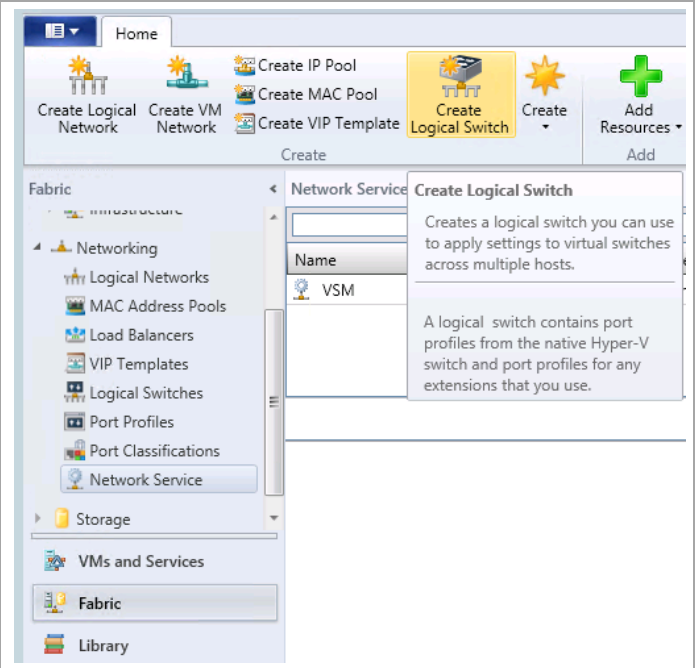


From within the VMM console, validate that the Network Service is installed.

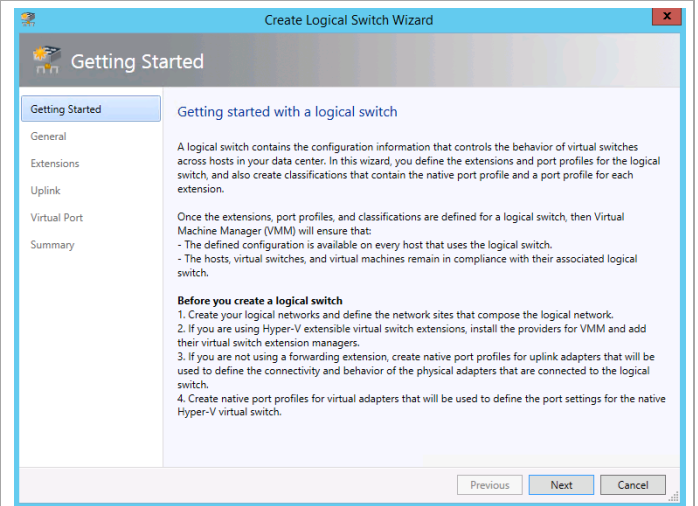


## 19.7 Configure a Logical Switch In Virtual Machine Manager

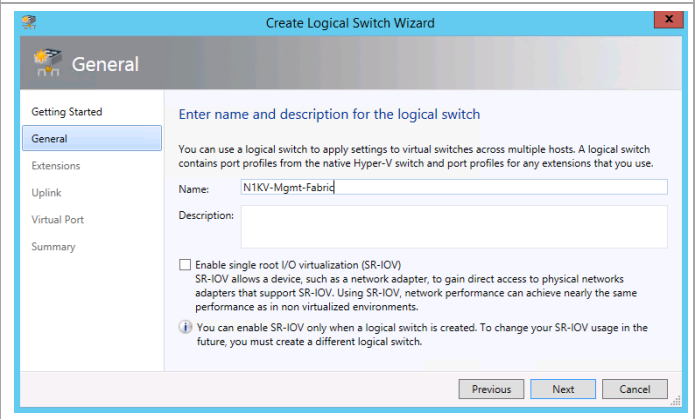
In the left pane of Virtual Machine Manager select **Fabric > Networking > Logical Switches**. Click **Create Logical Switch**.



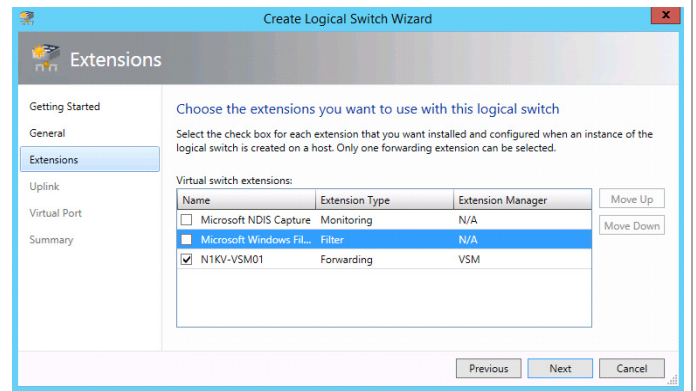
Click **Next**.



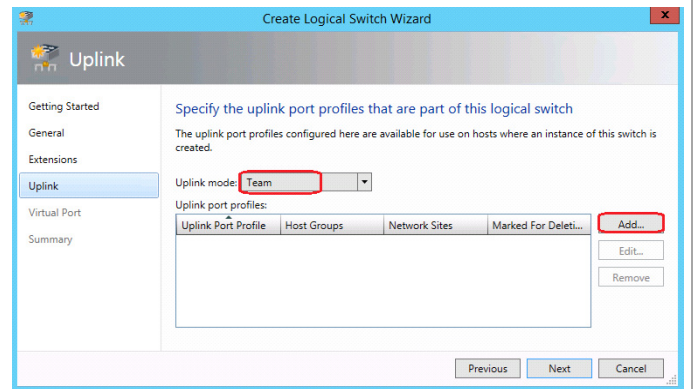
Enter a **logical switch name** for the Nexus 1000V and click **Next** to continue.



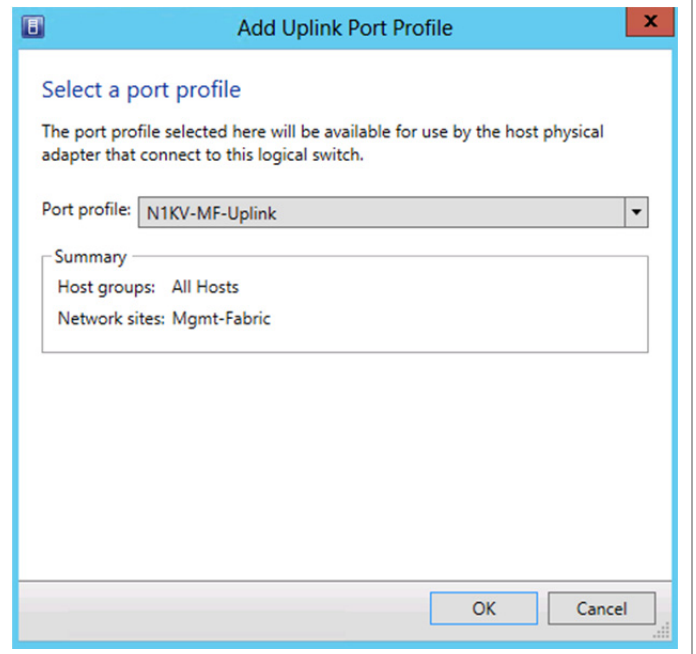
Uncheck **Microsoft Windows Filtering Platform**.  
 Check **N1KV-VSM01** forwarding extension type.  
 Click **Next** to continue.



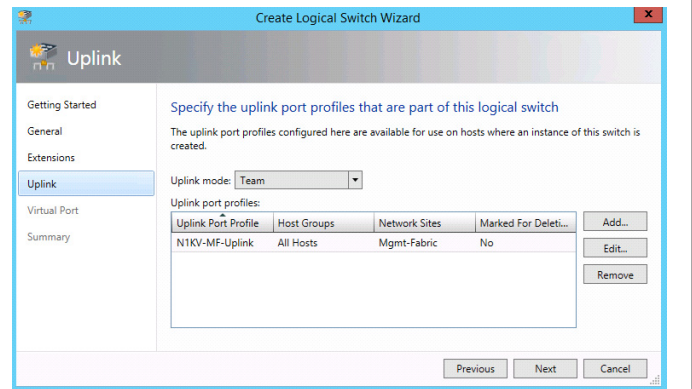
Select the **Team** Uplink mode in the dropdown text box. Click **Add** to add the uplink port profile.



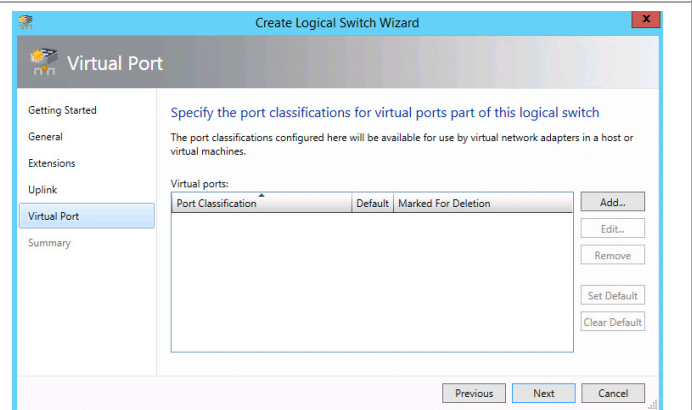
Select the **Port Profile** and click **OK**.



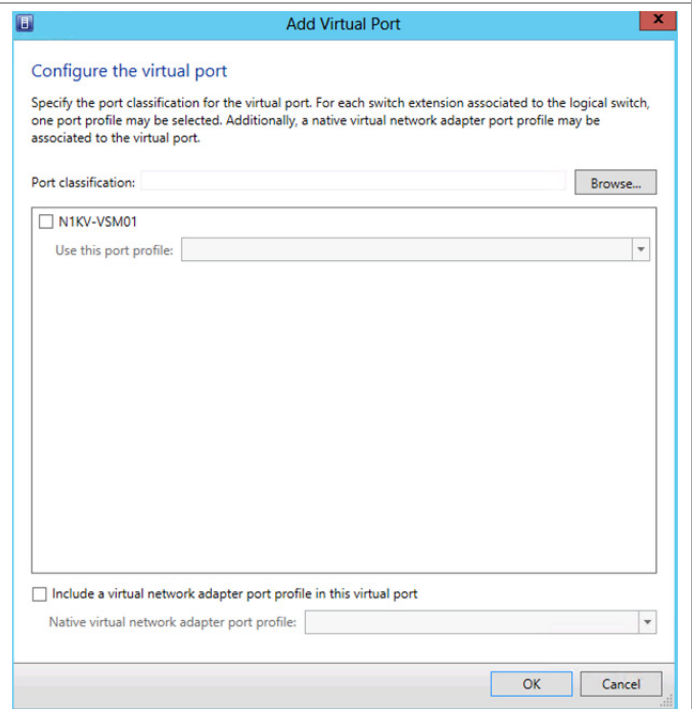
Review the added uplink port profile and click **Next** to continue.



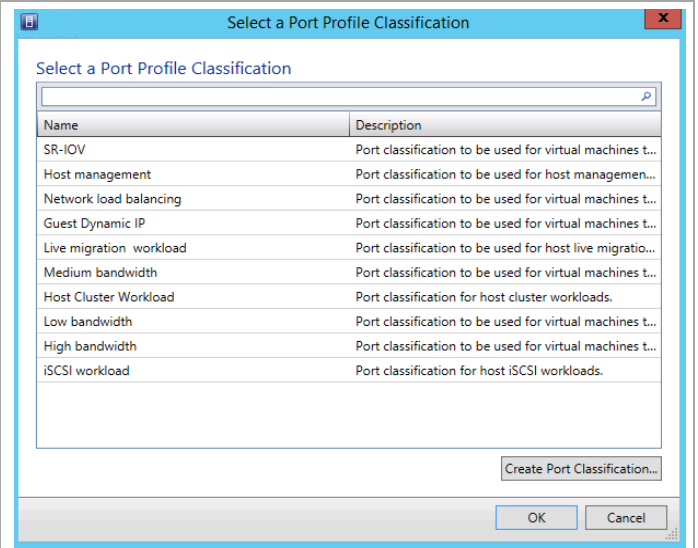
Click **Add** to add the virtual port classification.



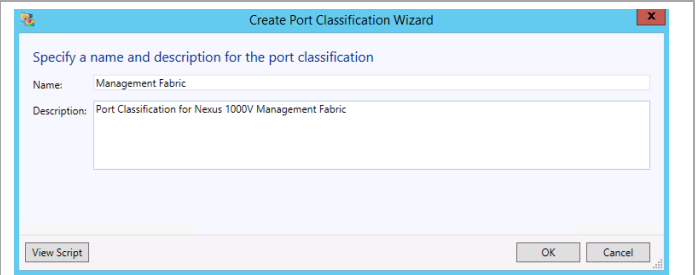
Click **Browse...**



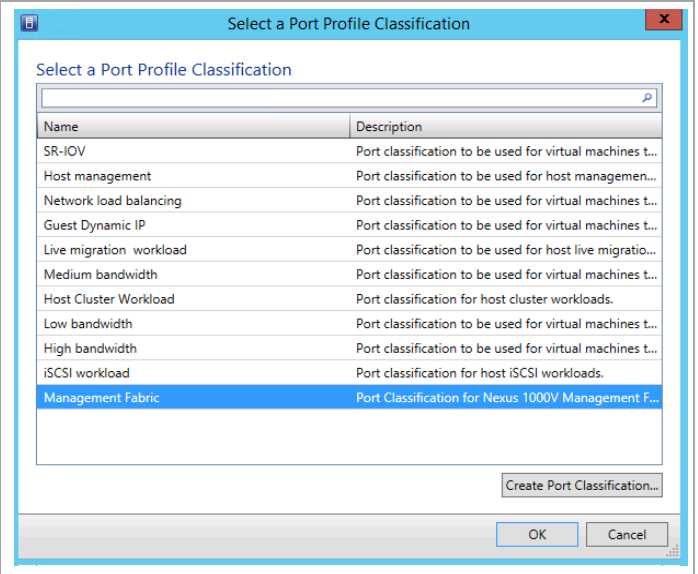
Click **Create Port Classification**.



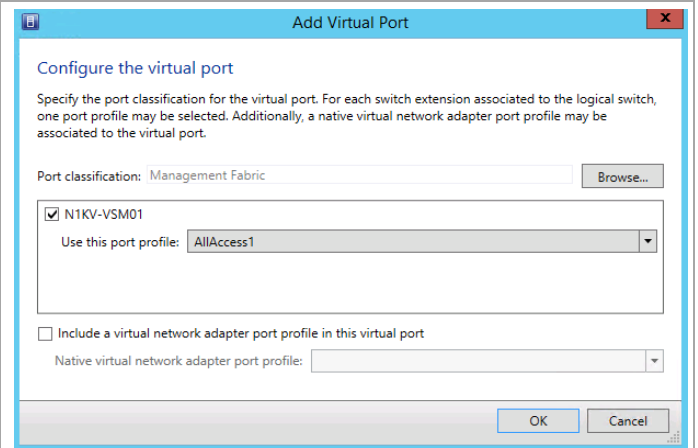
Enter the port classification name and description.  
Click **OK**.



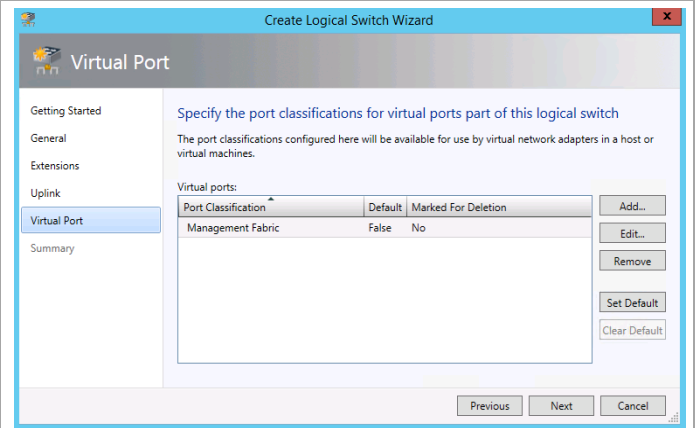
Select the new **Management Fabric** port classification and click **OK**.



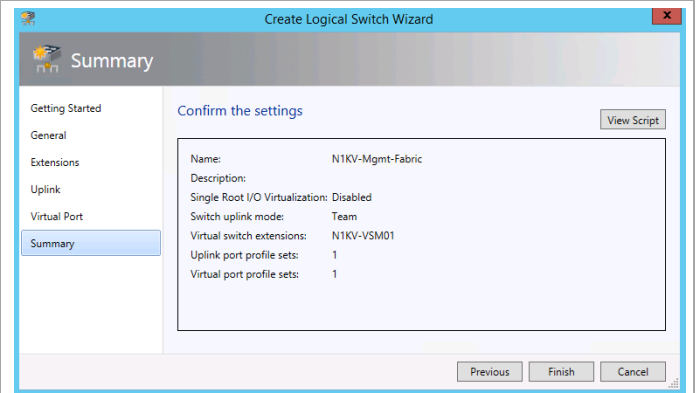
Check N1KV-VSM01 and select the port profile from the dropdown text box. Click **OK**.



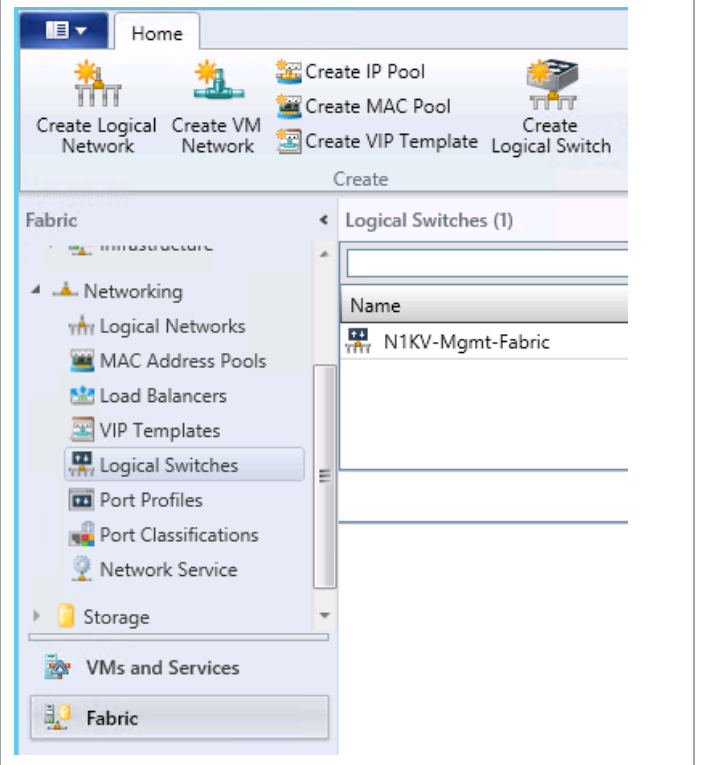
From the **Virtual Port** window click **Next** to continue.



Confirm the configuration setting and click **Finish** to create the logical switch.



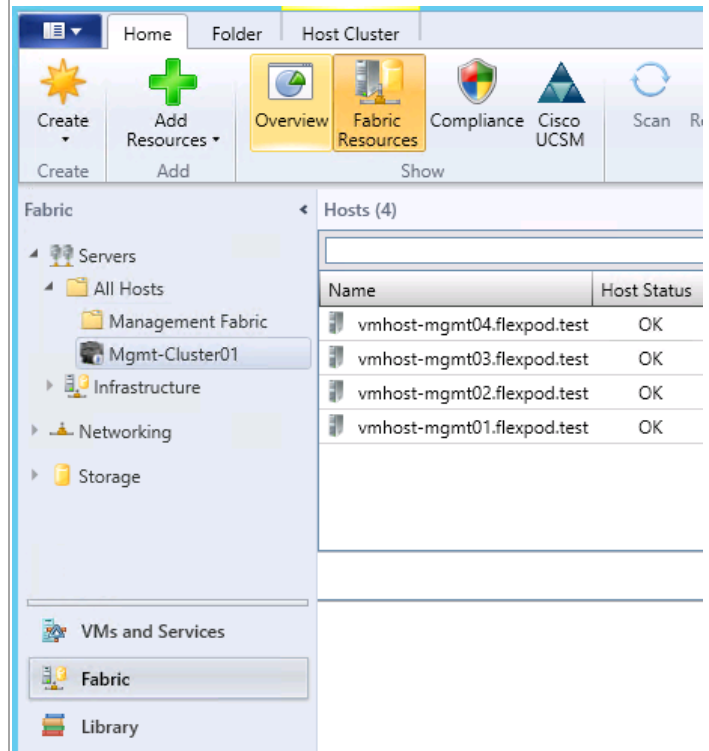
Within the VMM console validate the Cisco Nexus 1000V virtual switch is created.



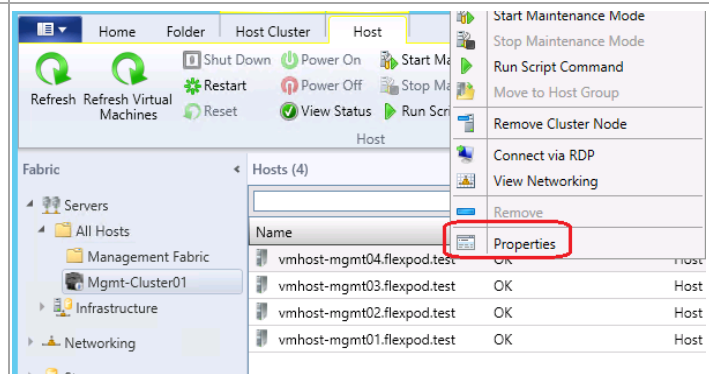
## 19.8 Creating the Logical Switch on the Hyper-V Hosts

Perform the following procedure on each Management Fabric Cluster node.

In the active Virtual Machine Manager instance, select **Fabric**. Expand **All Hosts** and the Fabric Management Cluster.

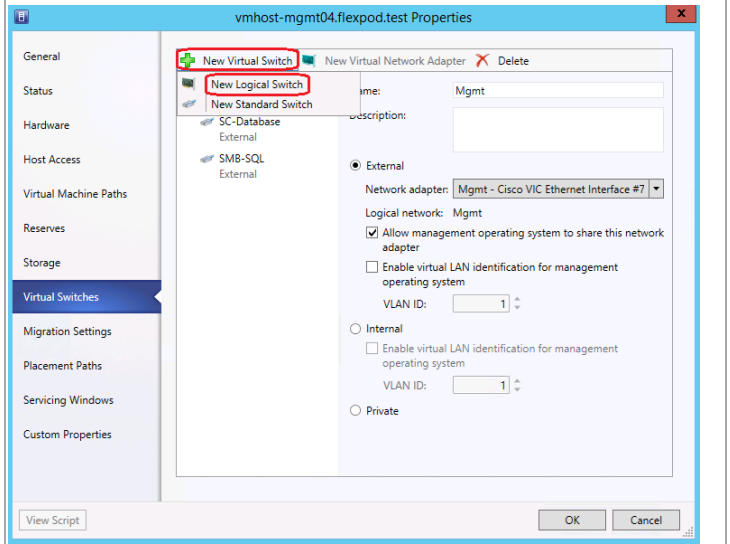


Select the first management fabric host and click **Properties**.

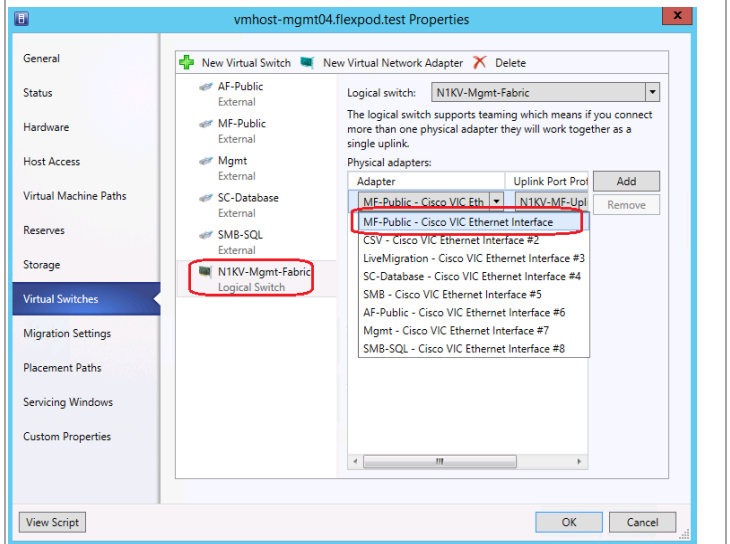




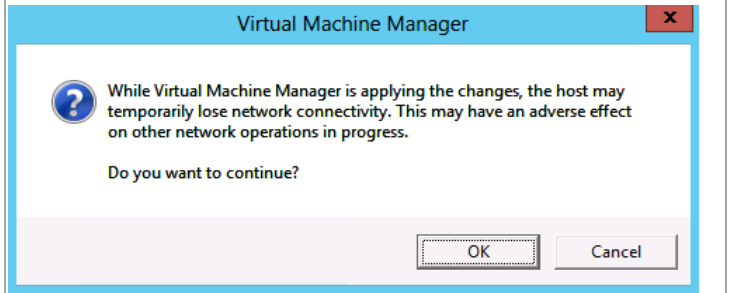
Select **Virtual Switch** in the left pane and **New Virtual Switch**. Select **New Logical Switch**.



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**.



Click **OK** to invoke the configuration change.



Click Jobs and monitor the job progress. The job will complete with a Status of **Completed w/ Info** until the logical switch is installed on all of the hosts in the cluster. The last job should complete with a Status of **Completed**.

Repeat this procedure on all cluster nodes.

The screenshot shows a job progress window with the following details:

- Status: 99%
- Command: Set-SCVMHost
- Result name: vmhost-mgmt04.flexpod.test
- Started: 11/4/2014 2:26:45 PM
- Duration: 00:00:52
- Owner: FLEXPOD\Administrator

Step	Name	Status
1	Change properties of virtual mac...	99%
1.1	Change properties of host netw...	Completed
1.2	New Host instance of a logical s...	99%
1.2.1	Install virtual switch extension	99%
1.2.1.1	Deploy driver and install virtual s...	99%
1.2.1.1.1	Deploy file (using LAN)	Completed

Information (26844): Virtual switch (N1KV-Mgmt-Fabric) is not highly available because the switch is not available in host (vmhost-mgmt01.flexpod.test).

Open the Mgmt-Cluster01 properties and verify that the N1KV-Mgmt-Fabric Switch is in the list of switches installed on all cluster nodes.

The screenshot shows the 'Mgmt-Cluster01.flexpod.test Properties' dialog box. The 'Virtual Switches (4)' tab is selected, displaying a table of installed virtual switches:

Name	Logical Networks
N1KV-Mgmt-Fabric	FastTrack
Mgmt	Mgmt
SC-Database	SC-Database
SMB-SQL	SMB-SQL

## 19.9 Create a VM Network

In Virtual Machine Manager, select **VMs and Services**. Right click **VM Networks** and click **Create VM Network**.

The screenshot shows the Virtual Machine Manager interface. The 'VMs and Services' pane is open, and the 'VM Networks' folder is right-clicked. The 'Create VM Network' context menu is visible, showing the following options:

- Create Service
- Create Virtual Machine
- Create Cloud
- Create Host Group
- Create VM Network**
- Assign Cloud
- Overview

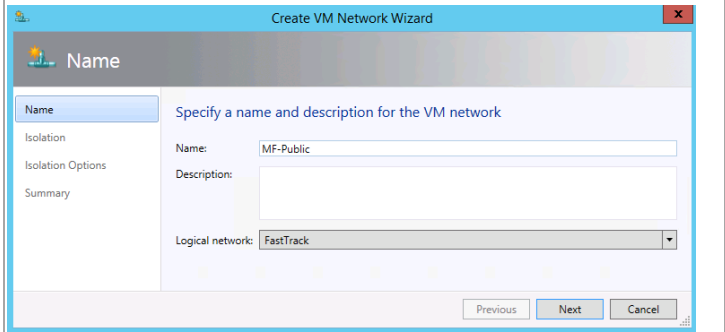
The 'Create VM Network' option is highlighted, and a tooltip is displayed:

**Create VM Network**

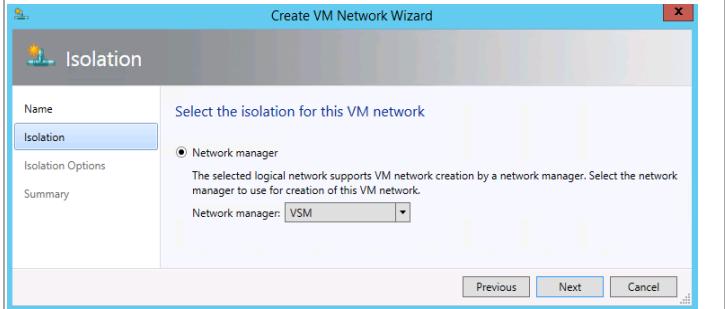
A VM network represents an isolated network that is available for use by virtual machines.

A VM network supports isolation through Hyper-V network virtualization, VLANs or switch extensions.

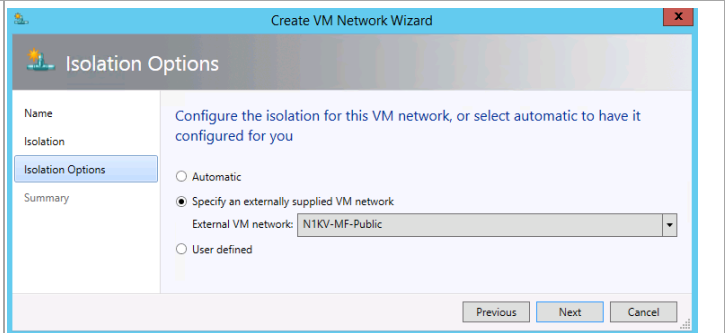
Enter the **network name**. Verify that the logical network FastTrack is selected and click **Next**.



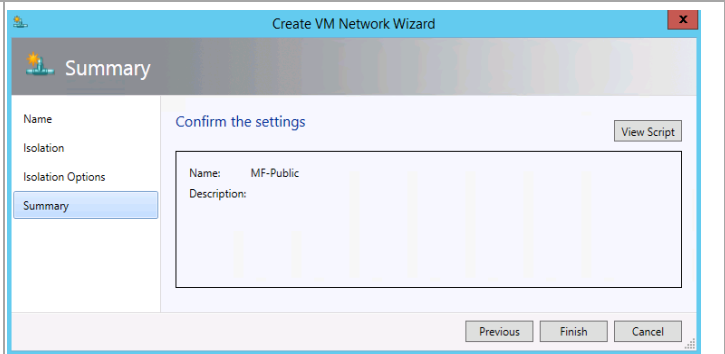
In the Isolation window, select **Network manager** and select the network manager created previously. Click **Next** to continue.



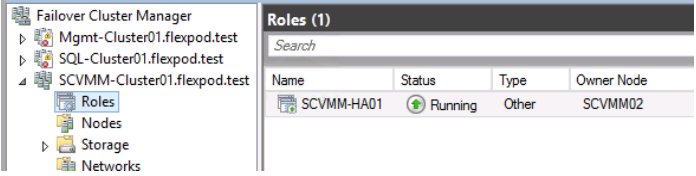
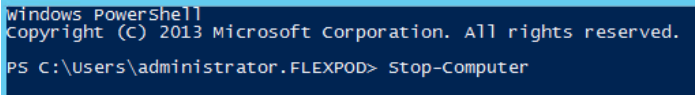
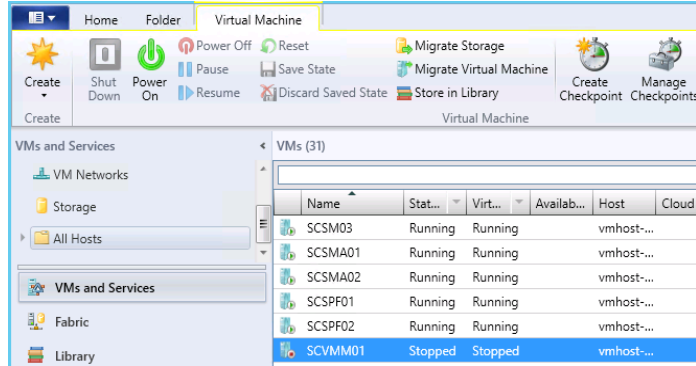
In the Isolation Options window select **Specify an externally supplied VM network** and select the **N1KV-MF-Public** (name configured within the Nexus 1000V) external network. Click **Next** to continue.



In the Summary window click **Finish** to create the VM network.



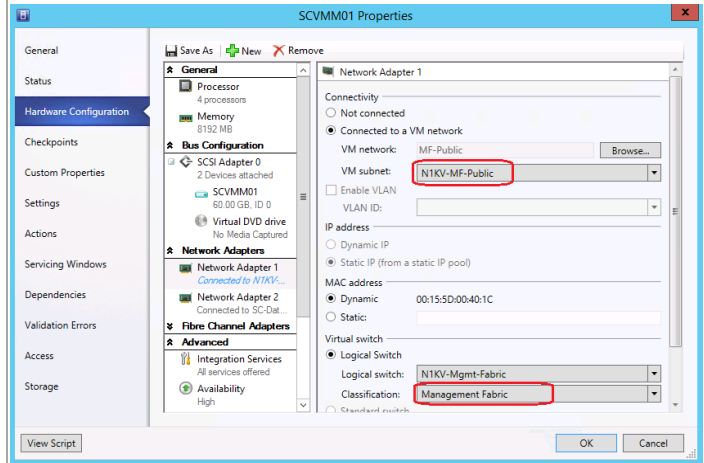
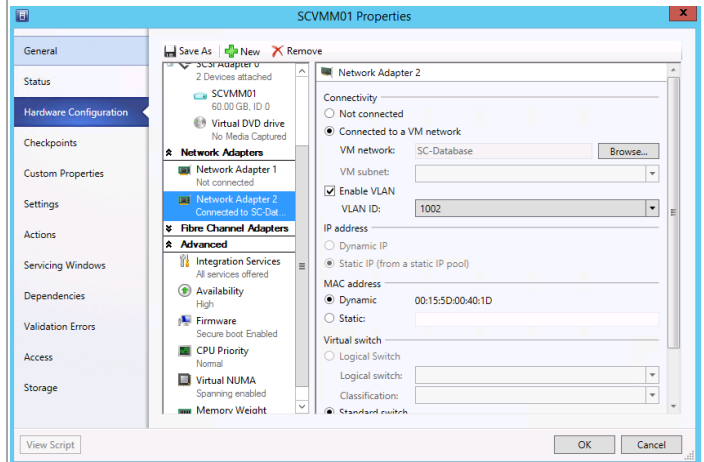
## 19.10 Configure the Virtual Machine Manager Virtual Machine Properties

<p>Perform the following steps on the Virtual Machine Manager virtual machine.</p>	
<p>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.</p>	
<p>Shutdown the first Virtual Machine Manager virtual machine by running following PowerShell command.</p>	
<p>Stop-Computer</p>	
<p>Log into the second Virtual Machine Manager virtual machine and start the Virtual Machine Manager console. Select <b>VMs and Services</b>. Click <b>All Hosts</b>. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select properties.</p>	

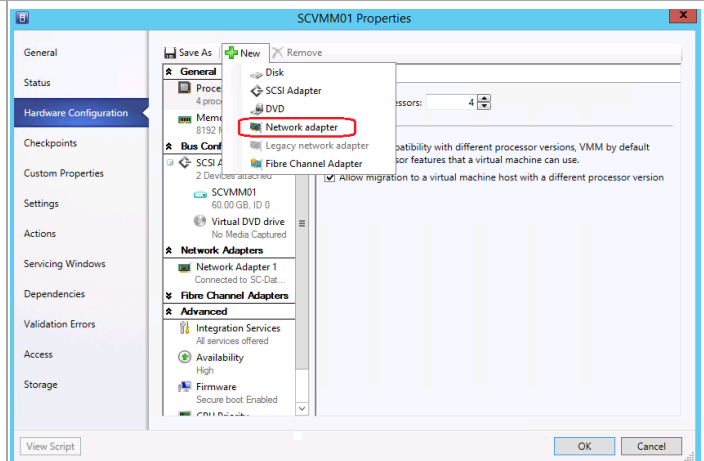
Select **Hardware Configuration** in the left pane and scroll down to the Network adapters in the middle pane.

**Note:** The screen shots to the right show a virtual machine that was created with the automated procedure that created a VM with two adapters – one connected and the other not connected. If you manually created the VMs with a single VM follow the next steps to create another adapter and assign it to the proper network.

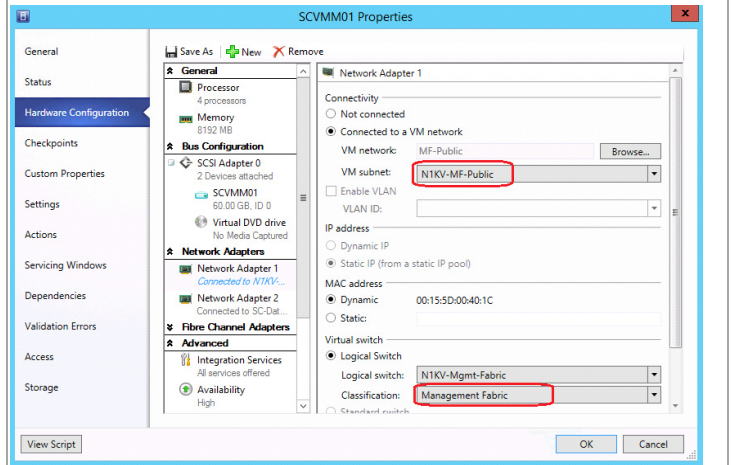
Select the network adapter that is Not connected. Select the radio button by **Connected to a VM network** and select the N1KV network. Under **Logical Switch** select the **Management Fabric** classification. Click **OK** to continue.



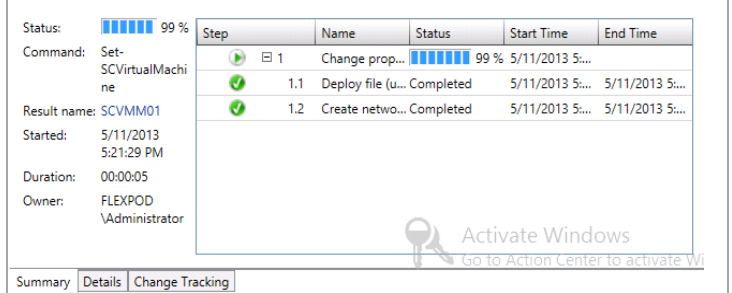
Click **Add** and select **Network Adapter** to create the 2<sup>nd</sup> network adapter.



Select the radio button by **Connect to a VM Network** and select the N1KV network. Under **Logical Switch** select the **Management Fabric** classification. Click **OK** to continue.



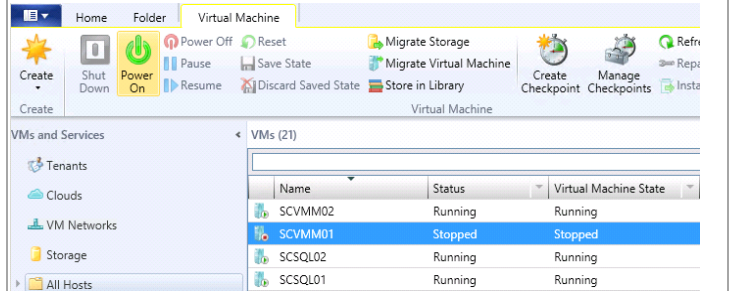
Select Jobs and monitor the job completion progress.



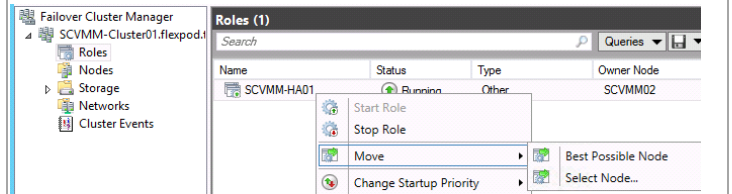
???????????????



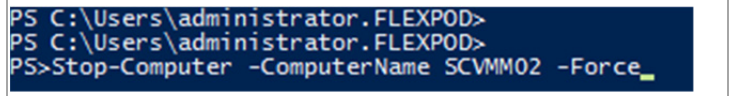
Start the Virtue Machine Manager virtual machine.



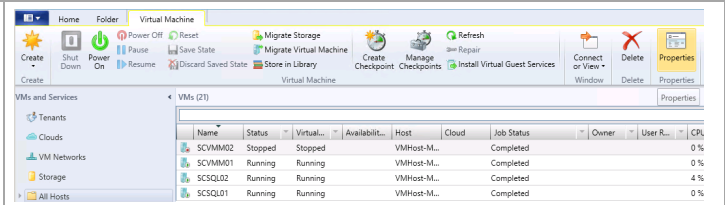
Login to the first Virtual Machine Manager virtual machine. Using Failover Cluster Manager move the Virtual Machine Manager instance to the first node.



Wait until the VMM instance is migrated to SCVMM01 and then shut down SCVMM02 virtual machine.

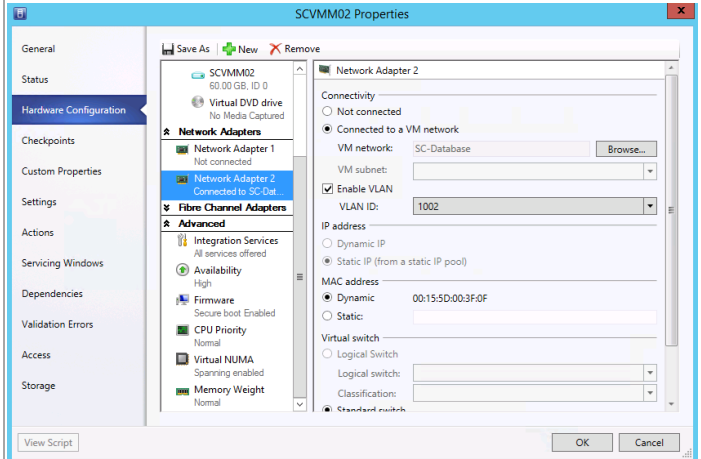


Start the Virtual Machine Manager console. Select **VMs and Services**. Click **All Hosts**. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select **Properties**.

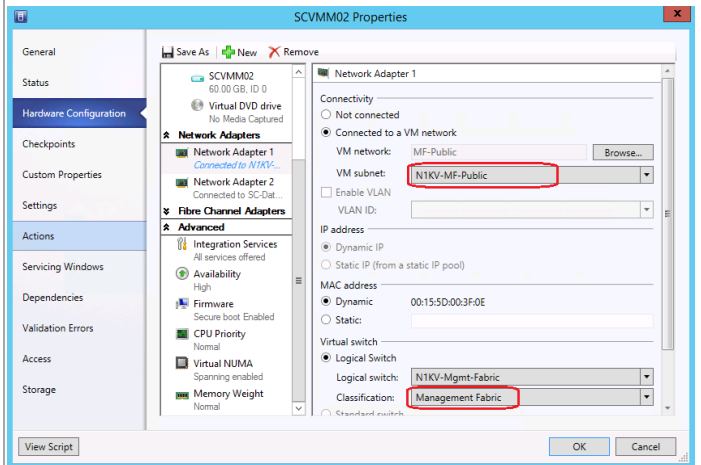


Select **Hardware Configuration** in the left pane and scroll down to the Network adapters in the middle pane.

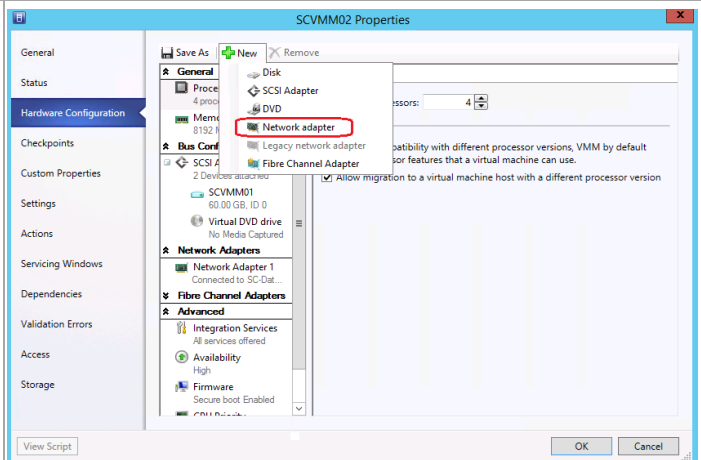
**Note:** The screen shots to the right show a virtual machine that was created with the automated procedure that created a VM with two adapters – one connected and assigned and the other not connected. If you manually created the VMs with a single VM follow the next steps to create another adapter and assign it to the proper network.



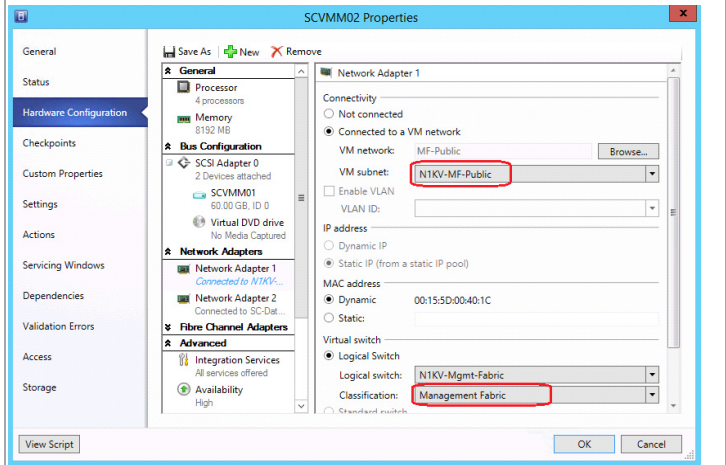
Select the network adapter that is Not connected. Select the radio button by **Connected to a VM network** and select the N1KV network. Under **Logical Switch** select the **Management Fabric** classification. Click **OK** to continue.



Click **Add** and select **Network Adapter** to create the 2<sup>nd</sup> network adapter.



Select the radio button by **Connect to a VM Network** and select the N1KV network. Under **Logical Switch** select the **Management Fabric** classification. Click **OK** to continue.



Select Jobs and monitor the job completion progress.

Status: ■■■■■ 99 %

Command: Set-SCVirtualMachine

Result name: SCVMM02

Started: 5/11/2013 6:59:15 PM

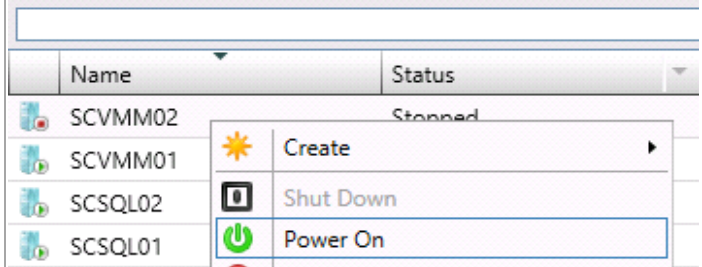
Duration: 00:00:05

Owner: FLEXP0D\Administrator

Step	Name	Status	Start Time	End Time
1	Change prop...	<span style="color: blue;">■■■■■</span> 99 %	5/11/2013 6:5...	5/11/2013 6:5...
1.1	Deploy file (u...	Completed	5/11/2013 6:5...	5/11/2013 6:5...
1.2	Create netwo...	Completed	5/11/2013 6:5...	5/11/2013 6:5...

Summary | Details | Change Tracking

Start the second Virtual Machine Manager virtual machine.



Login to the Cisco Nexus 1000V VSM and verify that the virtual adapters are connected to the Virtual Machine Manager virtual machines.

```
N1RU-USM01# show interface virtual
```

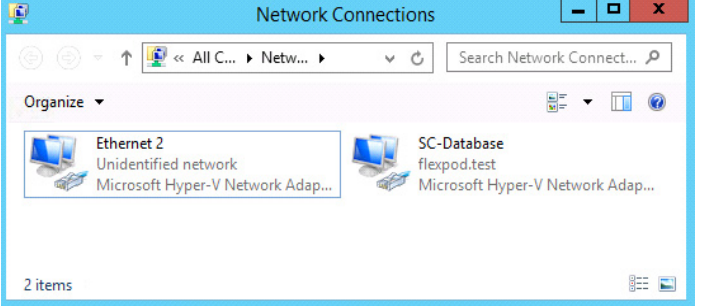
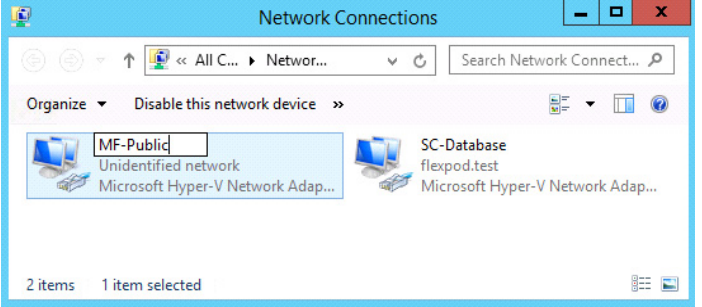
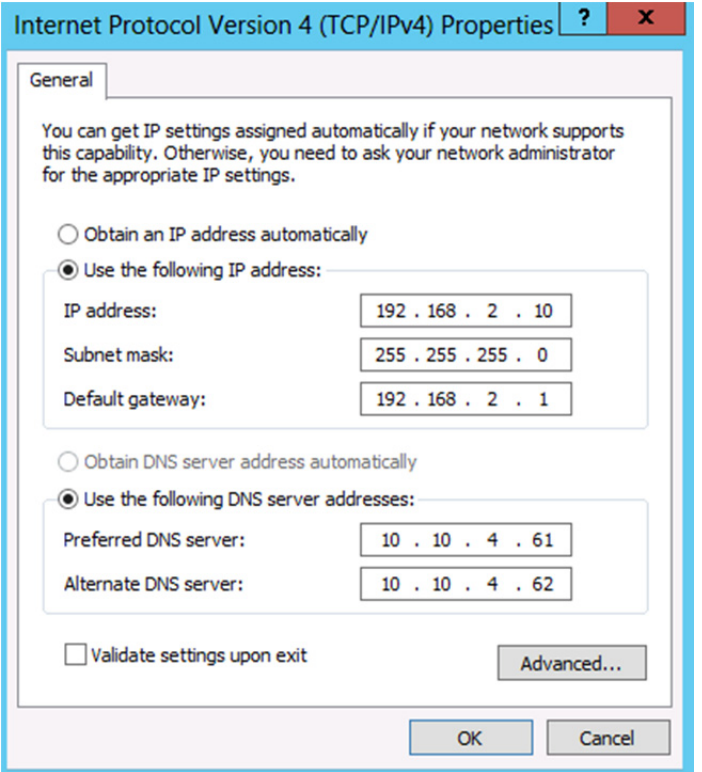
Port	Adapter	Owner	Mod	Host
Ueth1	Net Adapter	SCVMM02	4	UMHOST-MGMT02
Ueth2	Net Adapter	SCVMM01	3	UMHOST-MGMT01

Show interface virtual



## 19.11 Configure Virtual Machine Manager Network Interfaces

Perform the following operation on both Virtual Machine Manager virtual machines.

<p>Open Network Connections.</p>	 <p>The screenshot shows the Windows Network Connections window. The address bar indicates the path is &lt;All C...&gt; &gt; Netw... . There are two network adapters listed: 'Ethernet 2' (Unidentified network, Microsoft Hyper-V Network Adap...) and 'SC-Database' (flexpod.test, Microsoft Hyper-V Network Adap...). The status bar at the bottom shows '2 items'.</p>
<p>Rename the new network interface to match the network interface connection.</p>	 <p>The screenshot shows the Windows Network Connections window. The 'MF-Public' network adapter is selected, and its name is highlighted in a text box. The status bar at the bottom shows '2 items 1 item selected'.</p>
<p>Right-click the previously created SC-Databases network interface, select properties and click <b>Advanced...</b></p>	 <p>The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box. The 'General' tab is active. The text reads: 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.' The 'Use the following IP address:' radio button is selected. The IP address is 192.168.2.10, the subnet mask is 255.255.255.0, and the default gateway is 192.168.2.1. The 'Use the following DNS server addresses:' radio button is also selected. The preferred DNS server is 10.10.4.61 and the alternate DNS server is 10.10.4.62. There is an 'Advanced...' button at the bottom right, and 'OK' and 'Cancel' buttons at the bottom.</p>

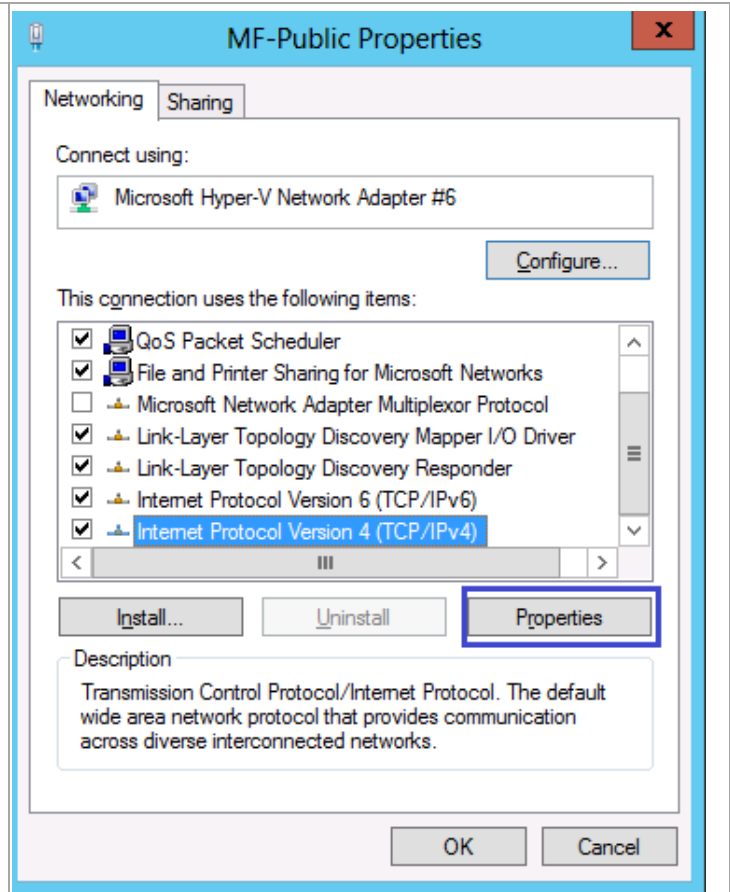
Select the DNS tab. Uncheck **Register this connection's address in DNS**. Click **OK** to save the configuration.

The screenshot shows the 'Advanced TCP/IP Settings' dialog box with the 'DNS' tab selected. The 'DNS server addresses, in order of use:' list is empty. Below it are 'Add...', 'Edit...', and 'Remove' buttons. The section 'The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:' has three radio button options: 'Append primary and connection specific DNS suffixes' (selected), 'Append parent suffixes of the primary DNS suffix' (checked), and 'Append these DNS suffixes (in order):'. Below this is another empty list with 'Add...', 'Edit...', and 'Remove' buttons. The 'DNS suffix for this connection:' field is empty. The checkbox 'Register this connection's addresses in DNS' is unselected and highlighted with a red box. The checkbox 'Use this connection's DNS suffix in DNS registration' is also unselected. 'OK' and 'Cancel' buttons are at the bottom right.

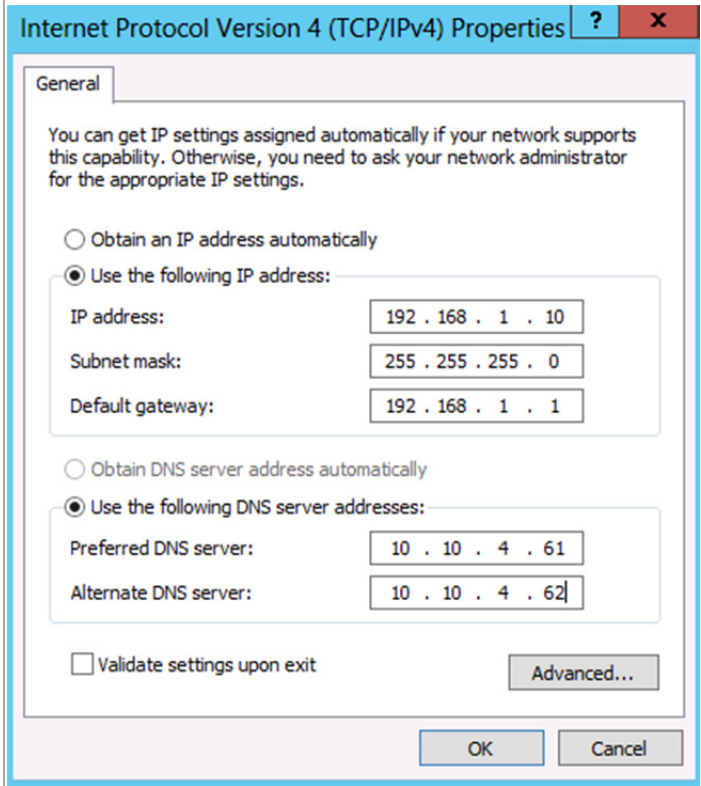
In the general IPv4 TCP/IP properties clear the default gateway and preferred DNS entries. Click **OK** to save the changes.

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'General' tab selected. The text at the top explains that IP settings can be assigned automatically. There are two radio button options: 'Obtain an IP address automatically' and 'Use the following IP address:' (selected). Under the selected option, the 'IP address' field contains '192 . 168 . 2 . 10', the 'Subnet mask' field contains '255 . 255 . 255 . 0', and the 'Default gateway' field contains '| . . .'. Below this are two more radio button options: 'Obtain DNS server address automatically' and 'Use the following DNS server addresses:' (selected). Under the selected option, the 'Preferred DNS server' field contains '. . .' and the 'Alternate DNS server' field contains '. . .'. There is a checkbox for 'Validate settings upon exit' which is unselected. An 'Advanced...' button is located to the right of the 'Validate settings upon exit' checkbox. 'OK' and 'Cancel' buttons are at the bottom right.

Right-click on the new network interface, select properties. Select the TCP/IPv4 item and click **Properties**.

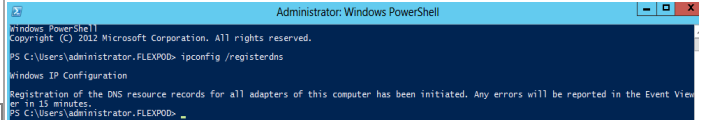


Configure the TCP/IP properties. Specify the IP Address, Subnet mask, Default gateway, and Preferred DNS servers. Click **OK** to save changes.



Open a command prompt. Run the following command.

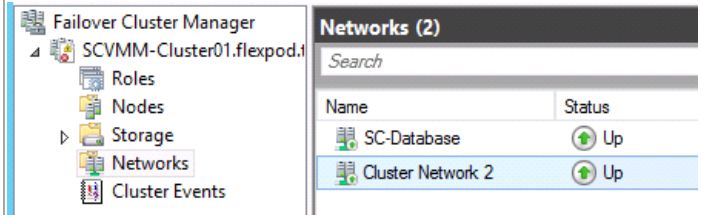
```
ipconfig /registerdns
```



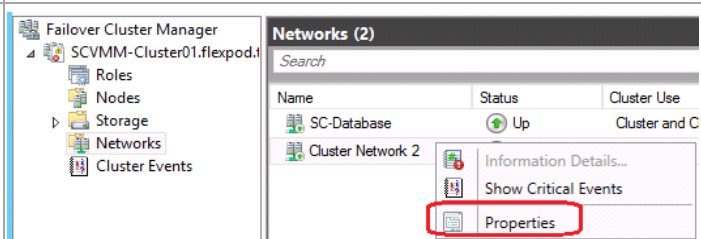
## 19.12 Rename the New Cluster Network

Perform the following operation on one Virtual Machine Manager virtual machines.

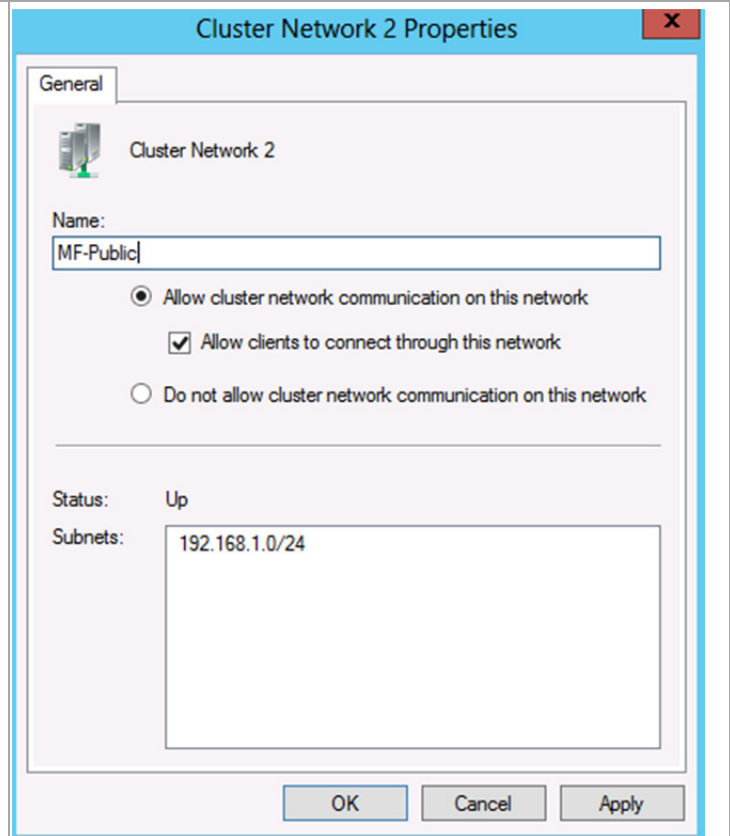
Open Failover Cluster Manager. Select the Virtual Machine Manager Cluster and expand the Networks object.



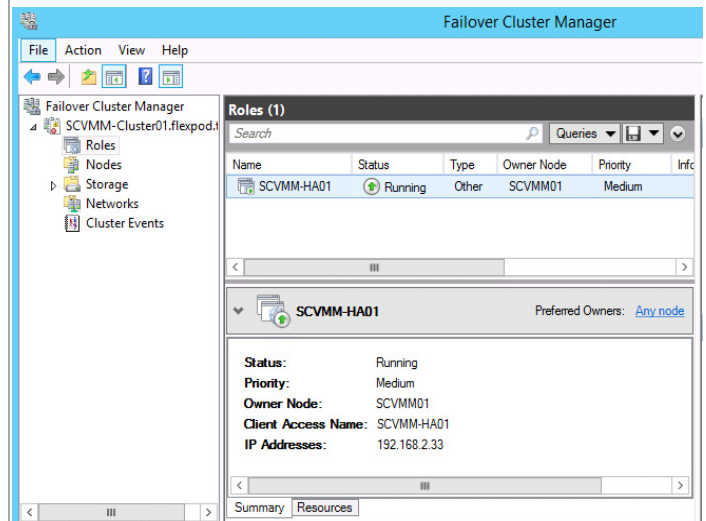
Right-click Cluster Network 2 and open **Properties**.



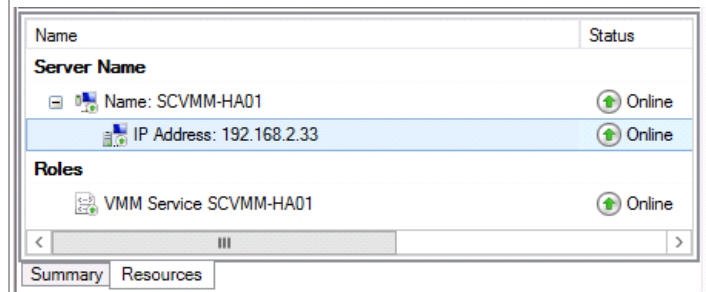
**Rename** the network name to match the connected network. Click **OK** to save changes.



Select **Roles** in the left pane and select the highly available Virtual Machine Manager instance in the top middle pane.



In the middle lower pane click the **Resources** tab and double click the IP address to open its properties page.



Update the Name, Network, and static IP address to use the MF-Public network.

IP Address: 192.168.2.33 Properties

General Dependencies Policies Advanced Policies

Name: IP Address 192.168.1.33  
Type: IP Address  
Status: Online

Network: 192.168.1.0/24  
Subnet mask: 255.255.255.0

IP Address

DHCP Enabled  
Address: 0.0.0.0  
Lease Obtained: <not configured>  
Lease Expires: <not configured>

Static IP Address  
Address: 192 . 168 . 1 . 33

Enable NetBIOS for this address

OK Cancel Apply

Click **Yes** to take the IP Address resource offline, apply the changes. Click **OK** to bring the IP Address resource back online.

Please confirm action

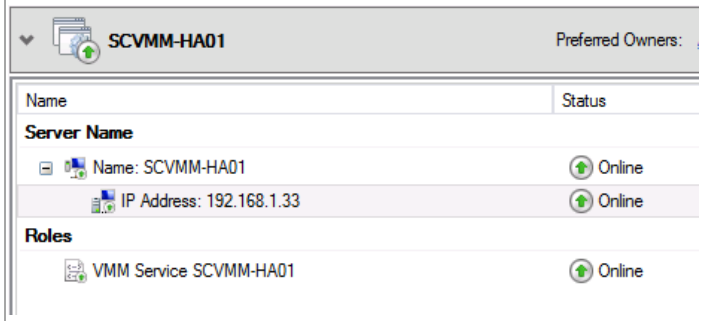
?

The properties were stored, but not all changes will take effect until IP Address: Address on MF-Public is taken offline and then online again. Would you like to do this now?

→ Yes

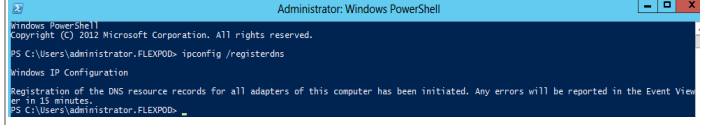
→ No

The highly available Virtual Machine Manager cluster resource IP address is now configured on the MF-Public network.

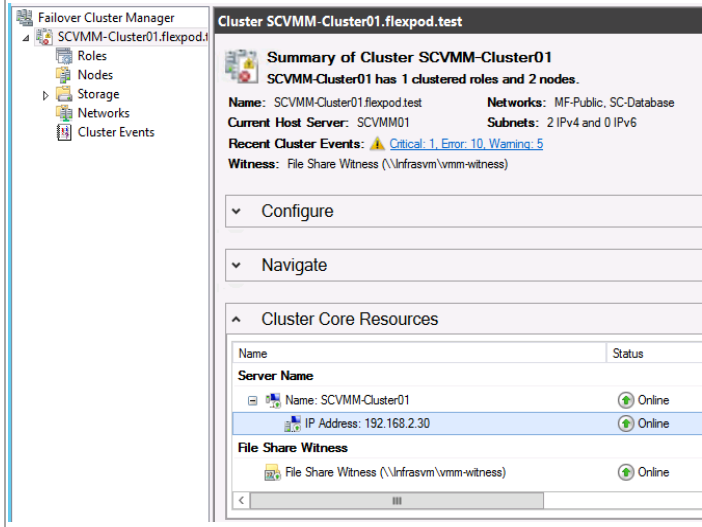


Open a command prompt. Run the following command.

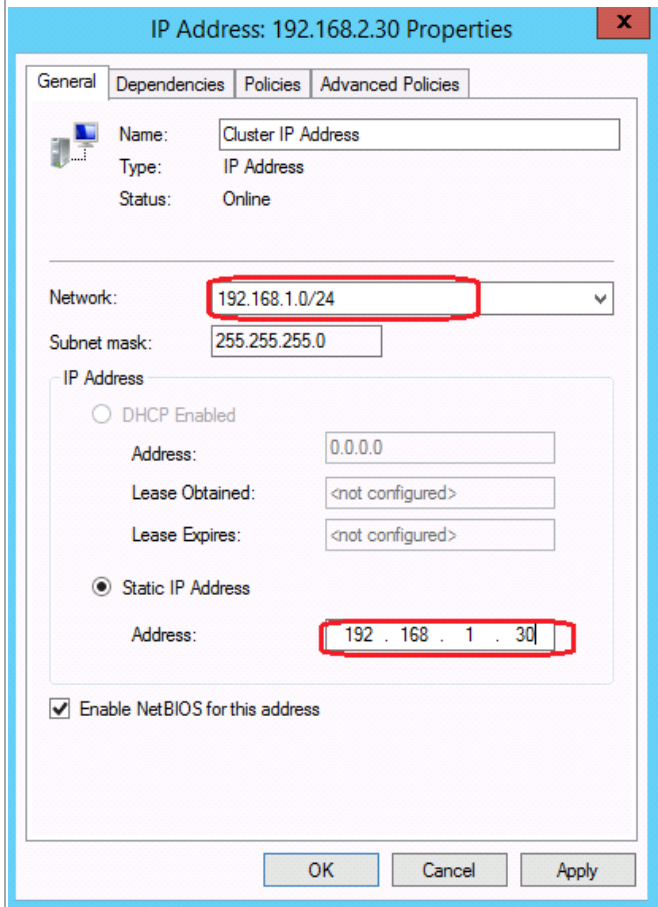
ipconfig /registerdns



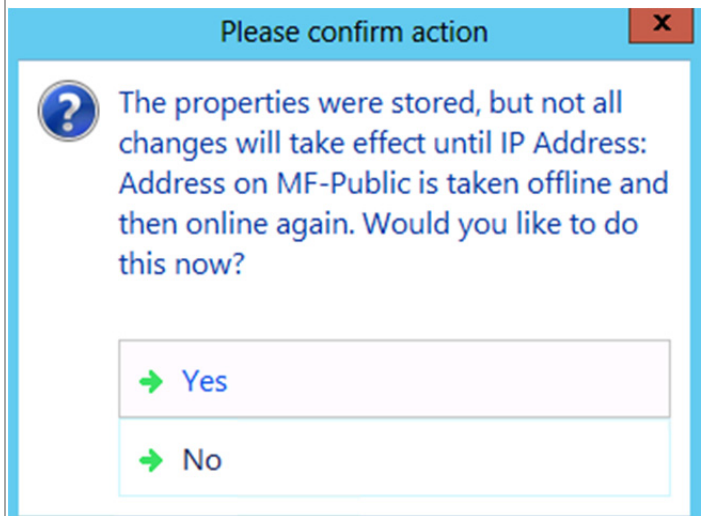
Select the Virtual Machine Manager cluster in the top left pane and double click the cluster core resource IP Address to open its property page.



Update the Network and static IP address to use the MF-Public network.

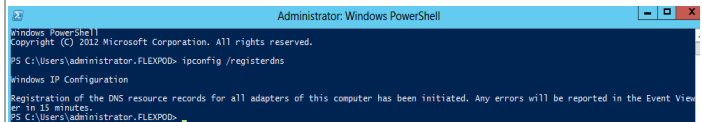


Click **Yes** to take the IP Address resource offline, apply the changes. Click **OK** to bring the IP Address resource back online.



Allow the IP Address resource to be brought offline. Bring the IP Address resource back online.

Open a command prompt. Run the following command.



```
ipconfig /registerdns
```

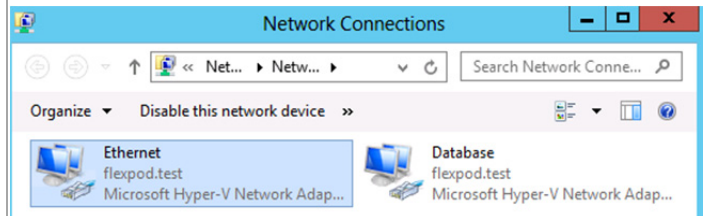


## 19.13 Configure System Center Application Virtual Machine Network Interfaces

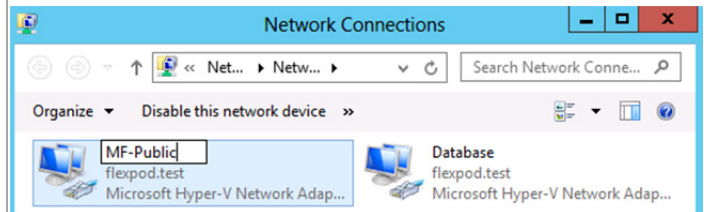
Perform the following operation on the following all System Center virtual machines.

Depending upon how you built your VMs, with or without a virtual NIC to be used by MF-Public, you still need to assign the N1KV MF-Public VM network to each VM. Instructions provided earlier for configuring the SCVMM machines to use this network can be used on each VM to add and/or assign through the SCVMM console. When you have added/assigned the MF-Public network through SCVMM, use these following steps to configure the properties of the VM's NICs.

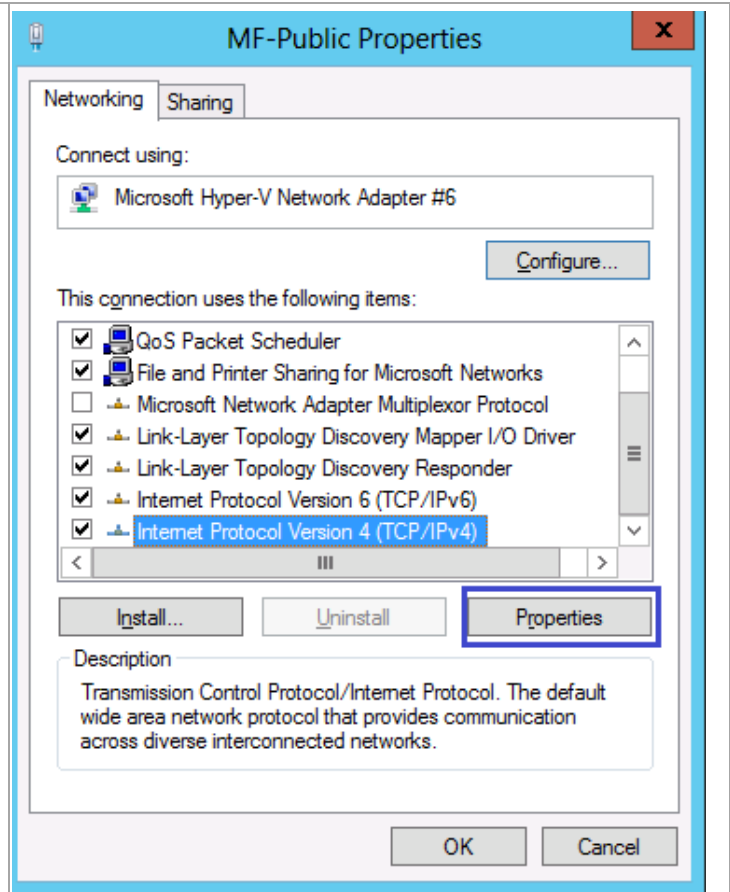
Open Network Connections.



Rename the new network interface to match the network interface connection.



Right click on the new network interface, select **Properties**. Select the TCP/IPv4 item and click **Properties**.



Configure the TCP/IP properties. Specify the IP Address, Subnet mask, Default gateway, and Preferred DNS servers. Click **OK** to save changes.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 2 . 16

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 10 . 10 . 4 . 61

Alternate DNS server: 10 . 10 . 4 . 62

Validate settings upon exit

Advanced...

OK Cancel

Right click on the previously created SC-**Databases** network interface, select properties and click **Advanced...**

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 1 . 16

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 10 . 10 . 4 . 61

Alternate DNS server: 10 . 10 . 4 . 62

Validate settings upon exit

Advanced...

OK Cancel

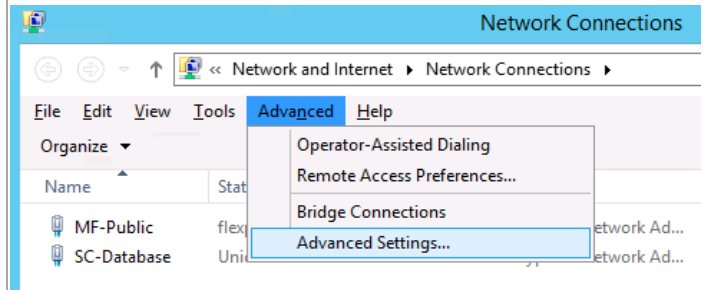
Select the DNS tab. Uncheck **Register this connection's address in DNS**. Click **OK** to save the configuration.

The screenshot shows the 'Advanced TCP/IP Settings' dialog box with the 'DNS' tab selected. The 'DNS server addresses, in order of use:' list is empty. Below it are 'Add...', 'Edit...', and 'Remove' buttons. The section 'The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:' contains three radio button options: 'Append primary and connection specific DNS suffixes' (selected), 'Append parent suffixes of the primary DNS suffix' (checked), and 'Append these DNS suffixes (in order):'. Below this is another empty list with 'Add...', 'Edit...', and 'Remove' buttons. The 'DNS suffix for this connection:' field is empty. The checkbox 'Register this connection's addresses in DNS' is unselected and highlighted with a red box. The checkbox 'Use this connection's DNS suffix in DNS registration' is also unselected. 'OK' and 'Cancel' buttons are at the bottom right.

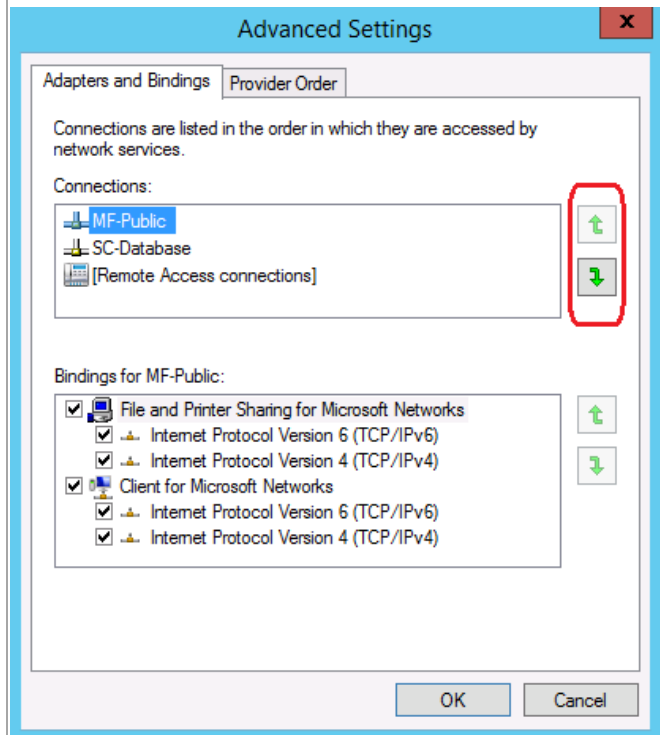
In the general IPv4 TCP/IP properties clear the default gateway and preferred DNS entries. Click **OK** to save the changes.

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'General' tab selected. The 'General' section contains a text box with instructions: 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.' Below this are two radio button options: 'Obtain an IP address automatically' and 'Use the following IP address:' (selected). The 'Use the following IP address:' section has three text boxes: 'IP address:' (192 . 168 . 1 . 16), 'Subnet mask:' (255 . 255 . 255 . 0), and 'Default gateway:' (. . .). Below this are two more radio button options: 'Obtain DNS server address automatically' and 'Use the following DNS server addresses:' (selected). The 'Use the following DNS server addresses:' section has two text boxes: 'Preferred DNS server:' (. . .) and 'Alternate DNS server:' (. . .). At the bottom left is the checkbox 'Validate settings upon exit' (unchecked). At the bottom right is the 'Advanced...' button. 'OK' and 'Cancel' buttons are at the very bottom.

Change the network binding order to ensure the MF-Public network is first. Within Network Connections, press the ALT key and select **Advanced Settings...** from the drop down menu.

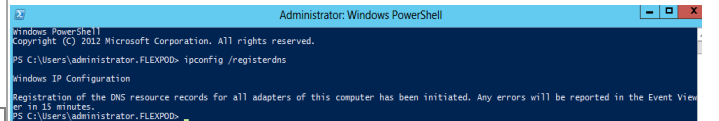


Adjust the order of the NICs by using the up/down arrows to ensure the MF-Public NIC appears first. Click **OK** to continue.



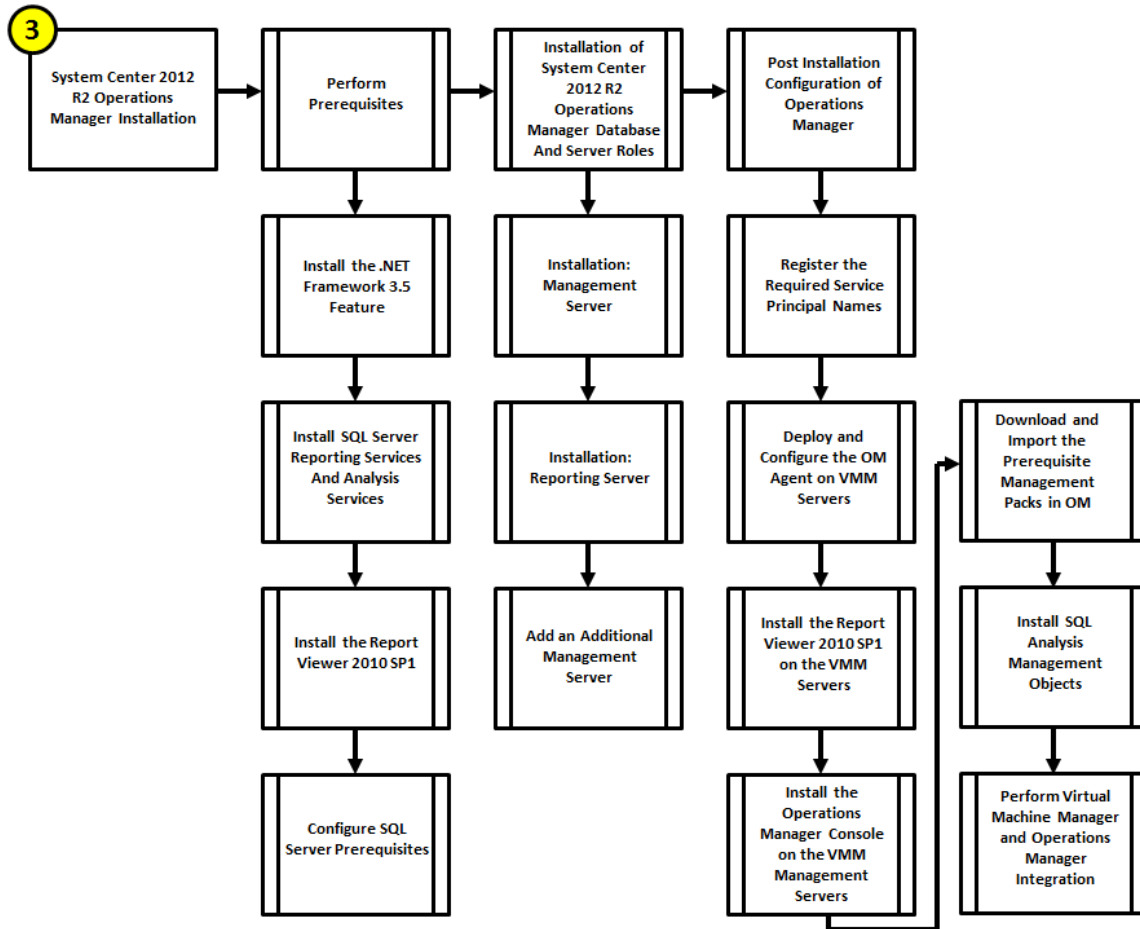
Open a command prompt. Run the following command.

```
ipconfig /registerdns
```



## 20 Operations Manager

The Operations Manager installation process includes the following high-level steps:



### 20.1 Overview

This section provides high-level walkthrough on deploying Operations Manager into the fabric management architecture. The following assumptions are made:

- Three base virtual machines running Windows Server 2012 R2 have been provisioned for Operations Manager
  - Two virtual machines will be configured to run the management service
  - One virtual machine will be configured to run Operations Manager reporting services
- A SQL Server 2012 SP2 cluster with dedicated instances has been established in previous steps:
  - The default SQL Server collation settings are required - Latin1\_General\_100\_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

## 20.2 Prerequisites

The following environment prerequisites must be met before proceeding.

### Accounts

Verify that the following domain accounts have been created:<sup>7</sup>

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.

<sup>7</sup> Specific rights for Operations Manager are outlined in [http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK\\_BeforeYouBegin](http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin).

## 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
<DOMAIN>\FT-SCOM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>\FT-SCOM-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.

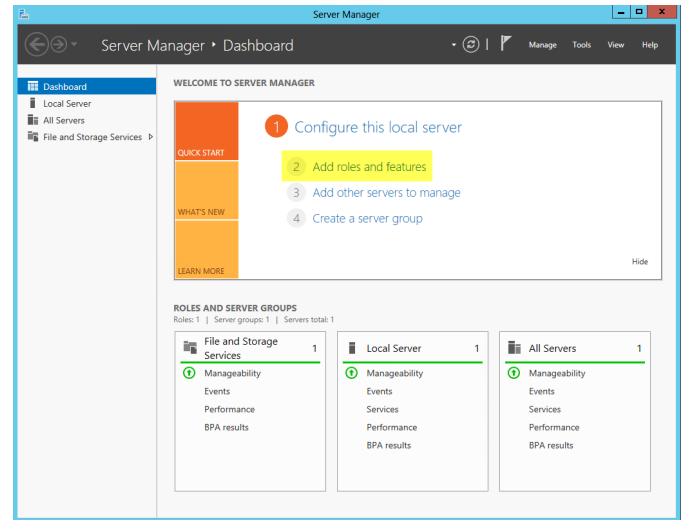
**Perform the following steps on all Operations Manager virtual machines.**

Note that while the following instructions perform the installation through the GUI, it is possible to install the feature with the following PowerShell cmdlet. It assumes the Windows Server 2012 R2 installation media is mounted in drive D:

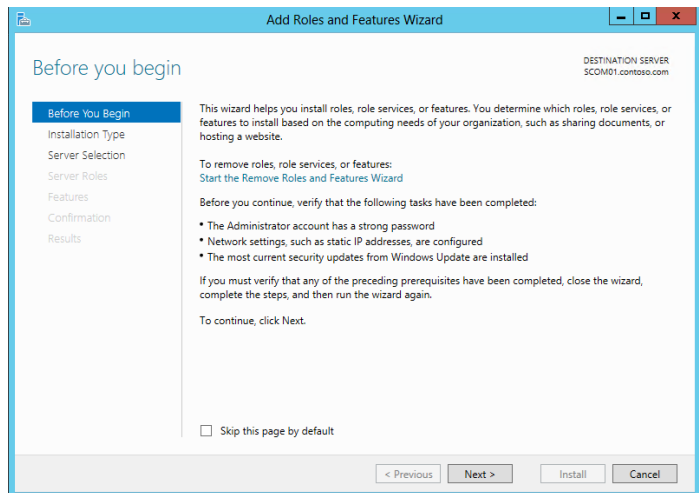
```
Install-WindowsFeature -Name Net-Framework-Core  
-Source D:\sources\sxs
```



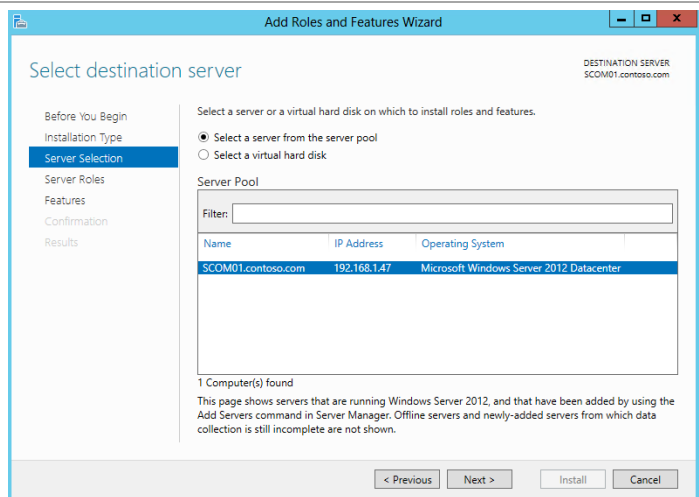
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



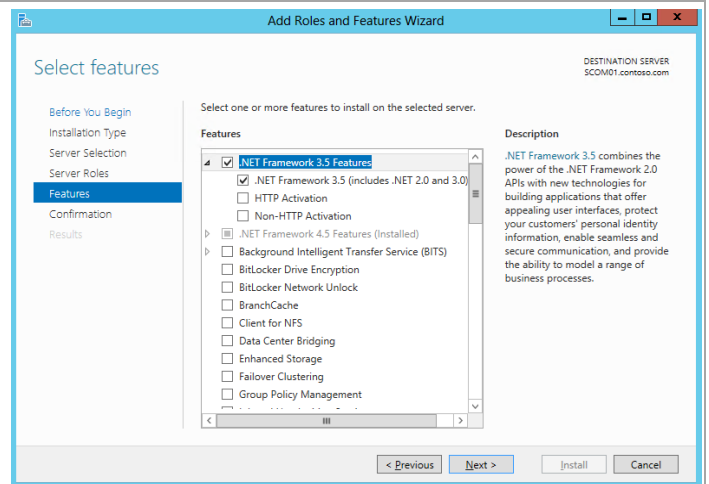
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, –o not click **Next** - for this installation, click the **Server Selection** menu option to continue.



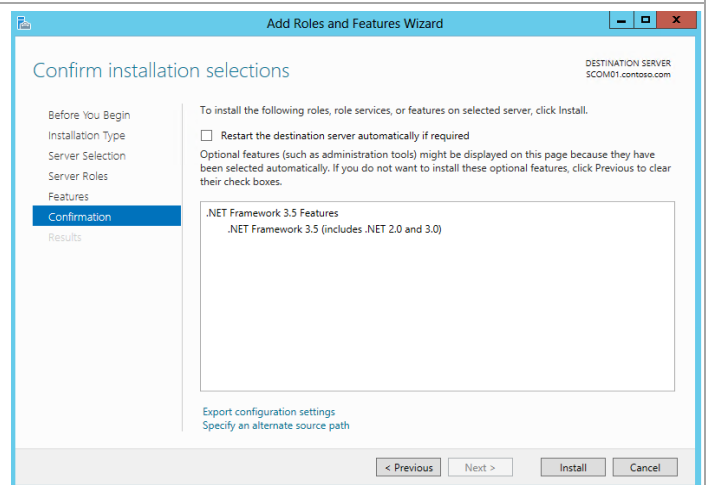
In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and –o not click **Next** - for this installation, click the **Features** menu option to continue.



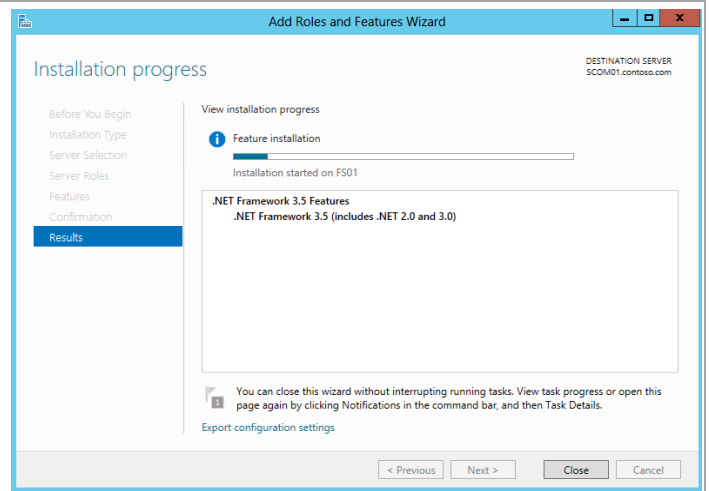
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.  
*Note that 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.*



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



## Install the SQL Server Reporting Services and Analysis Services (Split Configuration)

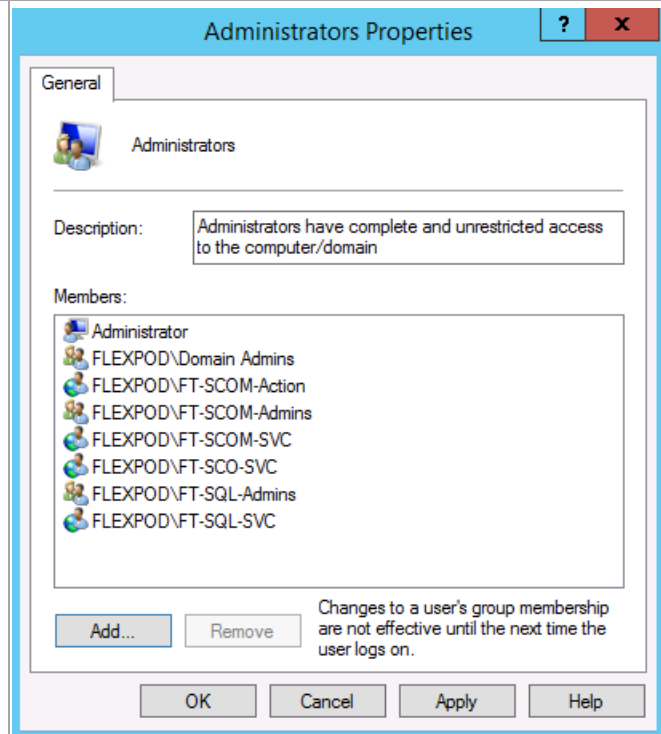
The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the provided steps to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

**Perform the following steps on the **Operations Manager Reporting Server** virtual machine only.**

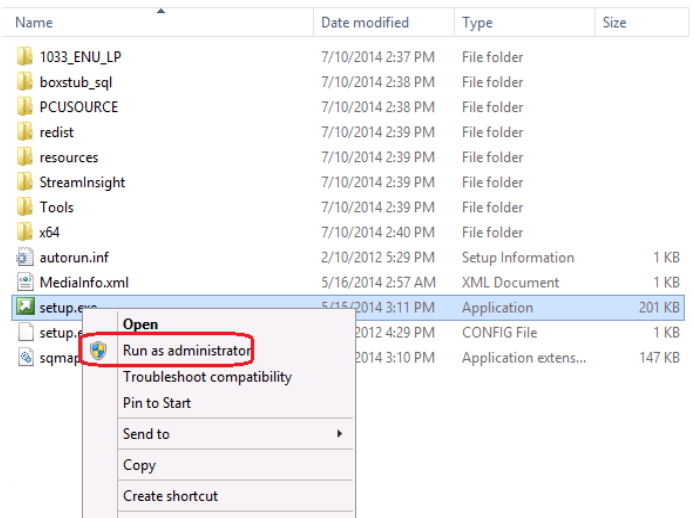
Log on to the Operations Manager Reporting Server virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager reporting server virtual machine:

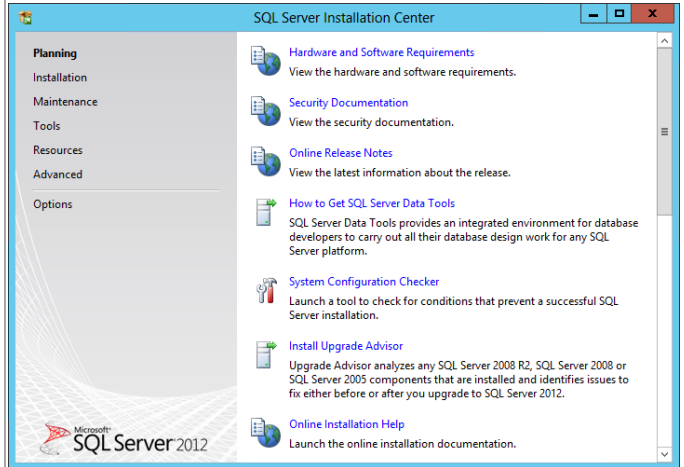
- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.
- SQL Server service account.
- SQL Server Admins group.



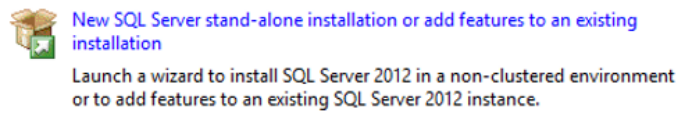
From the SQL Server 2012 SP2 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



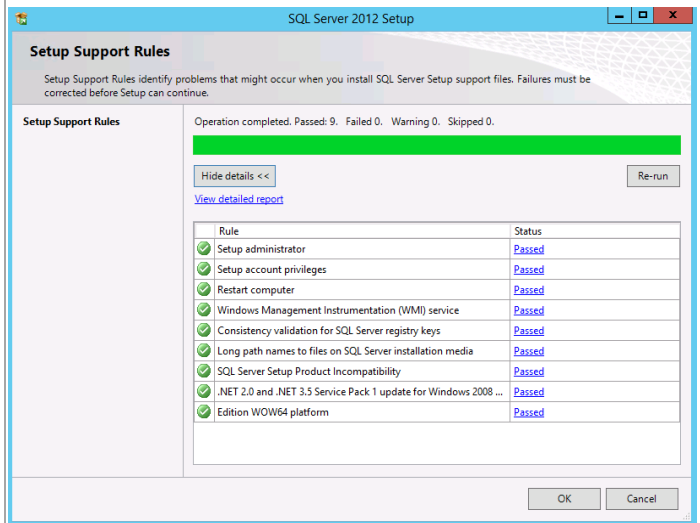
The **SQL Server Installation Center** will appear. Select the **Installation** menu option.



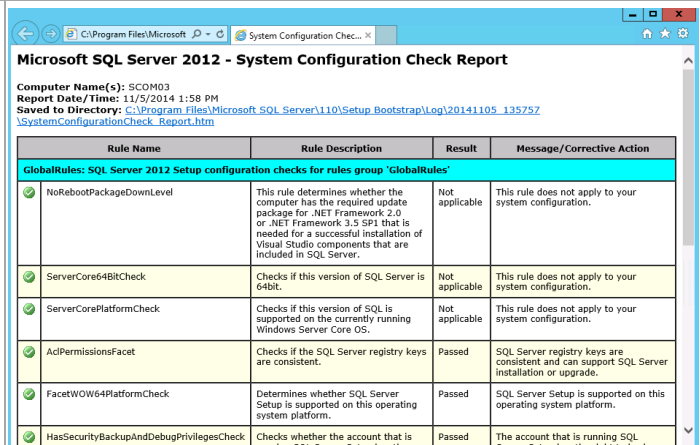
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.



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

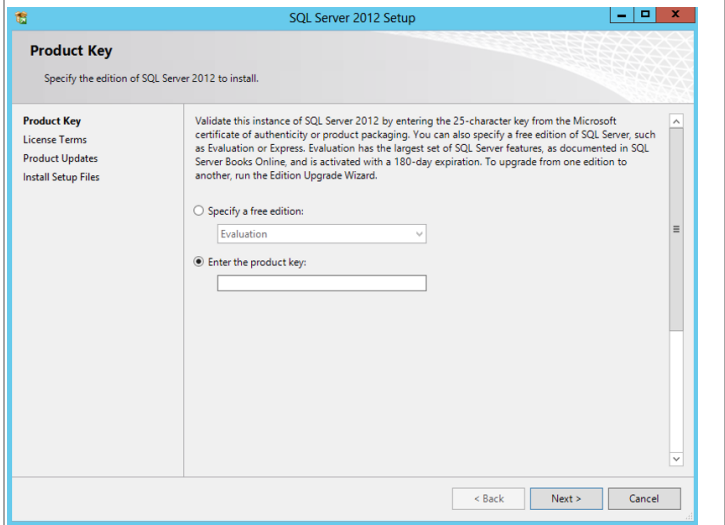


If the **View detailed report** link is selected, the following report is available.

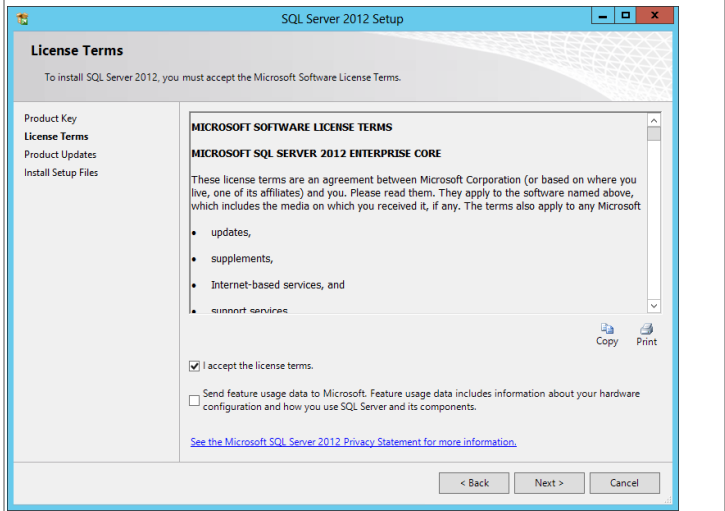


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

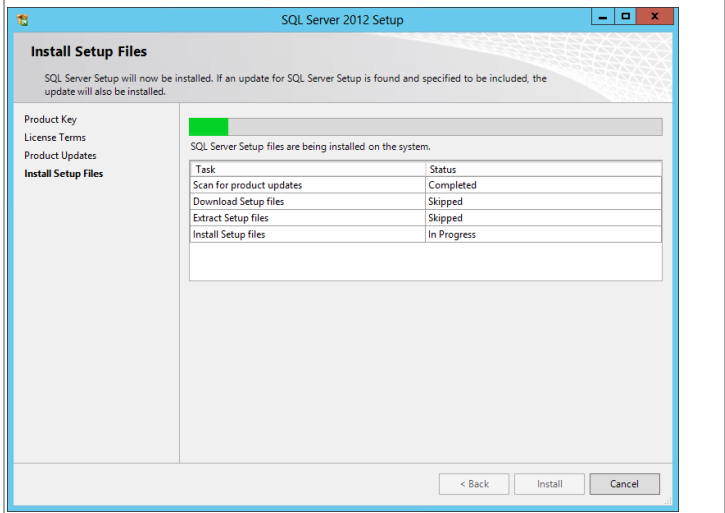
**Note:** If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



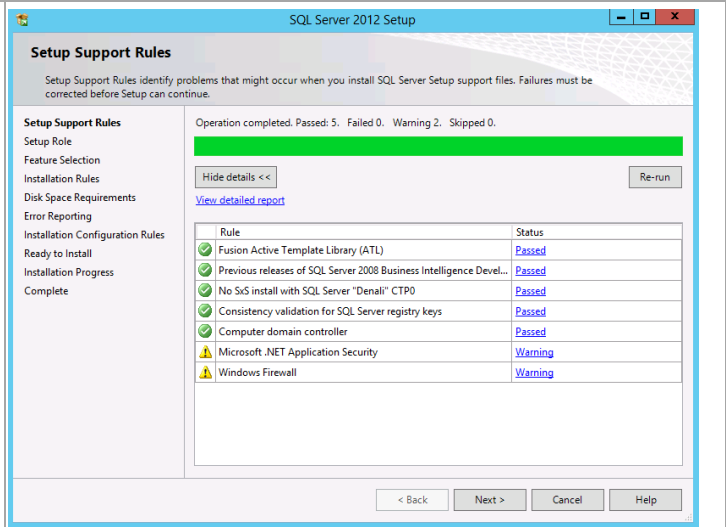
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.



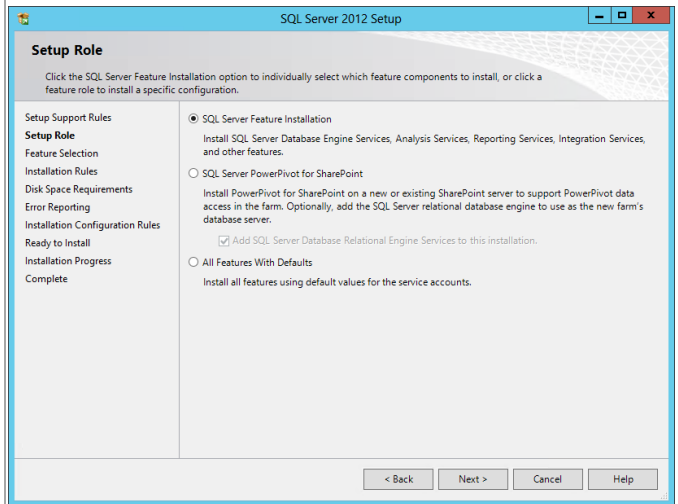
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.



In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP2 environment. Click **Next** to continue.



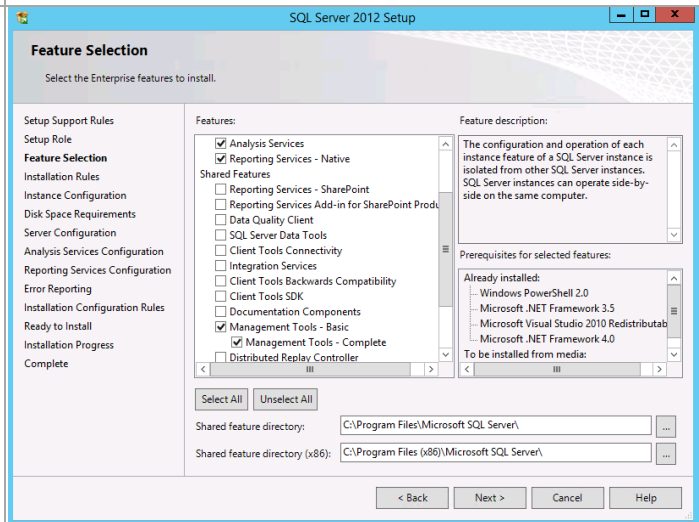
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.



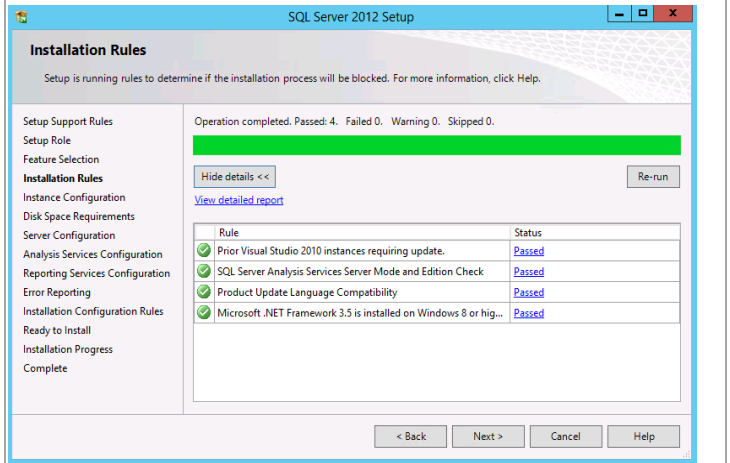
In the **Feature Selection** dialog, select the following features

- Analysis Service**
- Reporting Services – Native**
- Management Tools – Basic**
- Management Tools – Complete**

When all selections are made, click **Next** to continue.



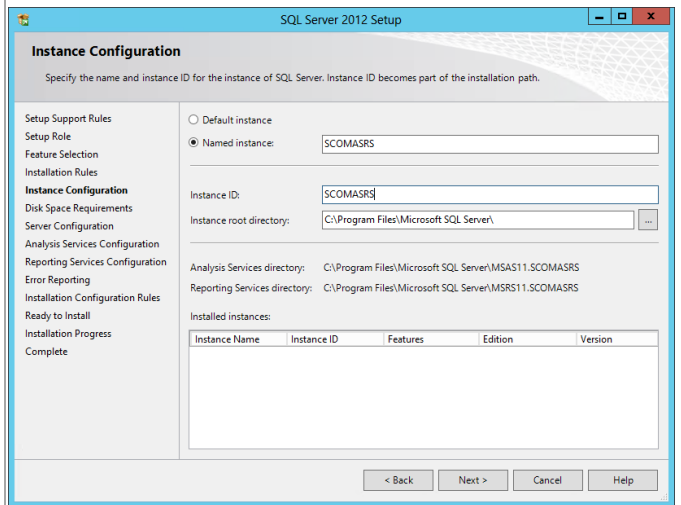
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



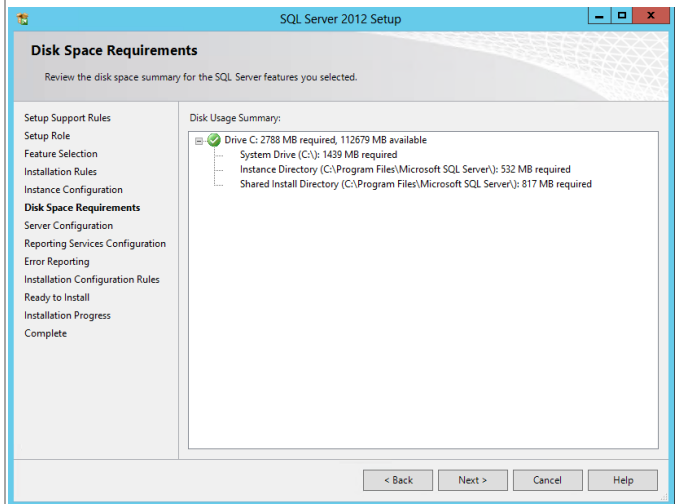
In the **Instance Configuration** dialog, select the **Named instance** option. In the provided text box, specify the instance name being installed.

- **Instance ID** –Select the **Named instance** option and specify **SCOMASRS** in the provided box. Verify the Instance ID is listed as **SCOMASRS** in the associated box. Keep the default Instance root directory values, and then click **Next** to continue.
- **Instance root directory** – accept the default location of `%ProgramFiles%\Microsoft SQL Server`.

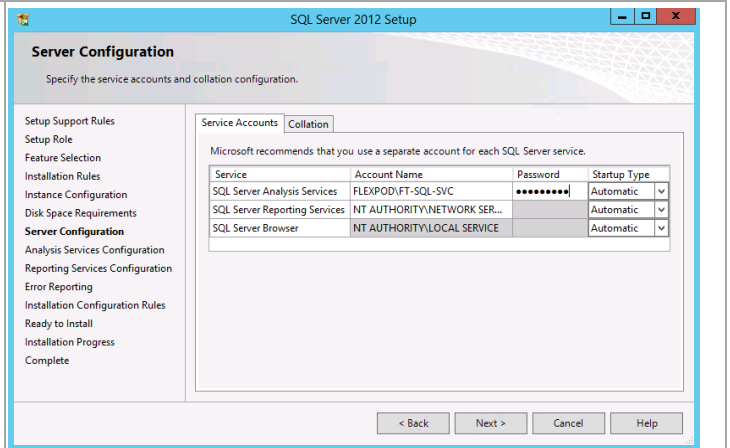
**Note:** A post-installation configuration process will occur to configure the reporting server database within the Operations Manager Data Warehouse SQL Server instance.



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



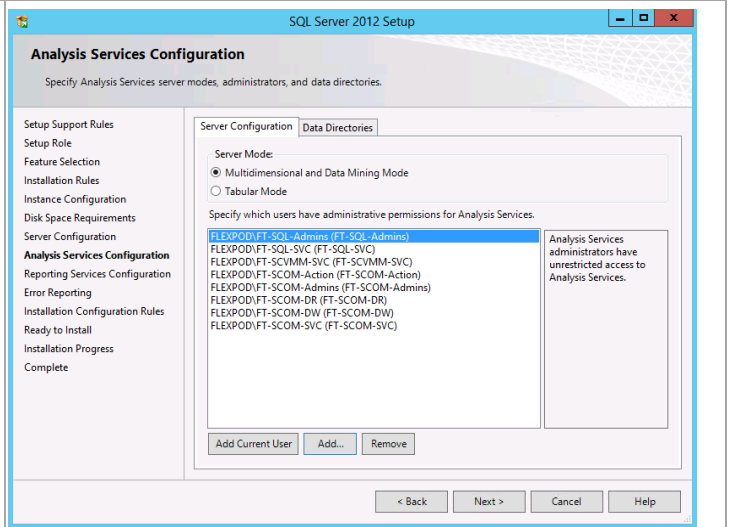
In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **domain SQL service** account for SQL Server Analysis Services and the **NETWORK SERVICE** account for **SQL Server Reporting Services**. Click **Next** to continue.



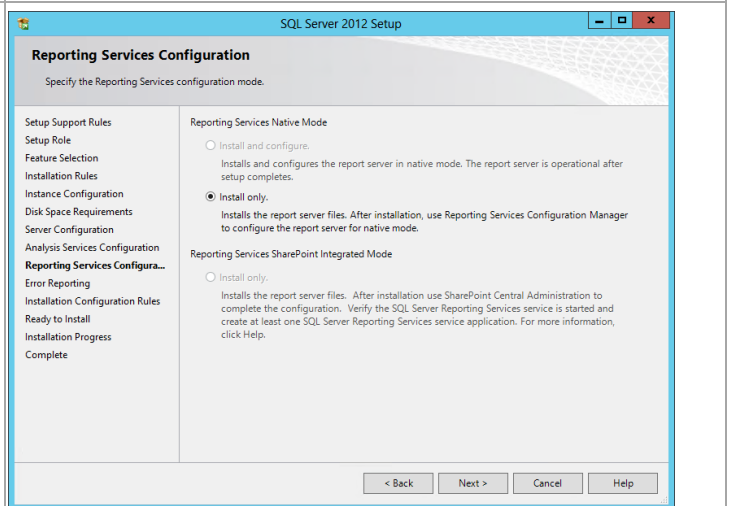
In the **Analysis Services Configuration** dialog, Click **Add**, Verify that the following accounts and/or groups are granted access to the Analysis Services:

- SQL Server Admins group
- SQL Server service account
- Virtual Machine Manager service account
- Operations Manager action account.
- Operations Manager Admins group.
- Operations Manager service account.
- Operations Manager data reader account
- Operations Manager, Data Warehouse write account

Click **Next** to continue.

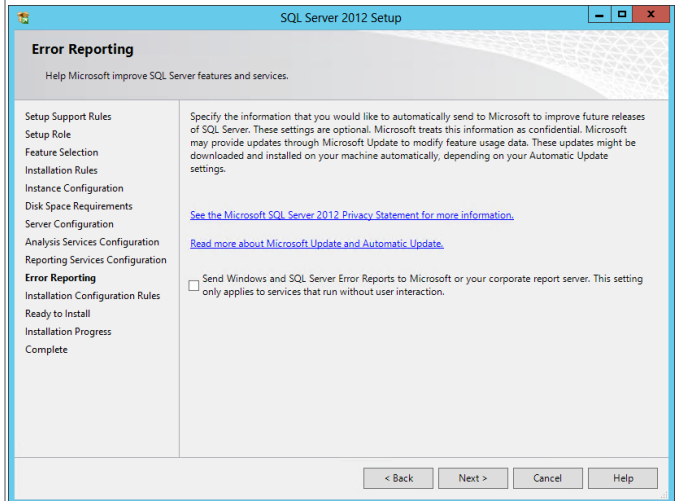


In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.

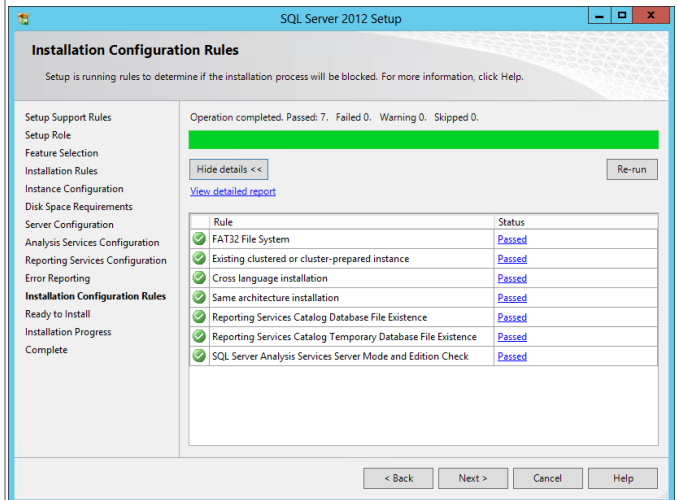




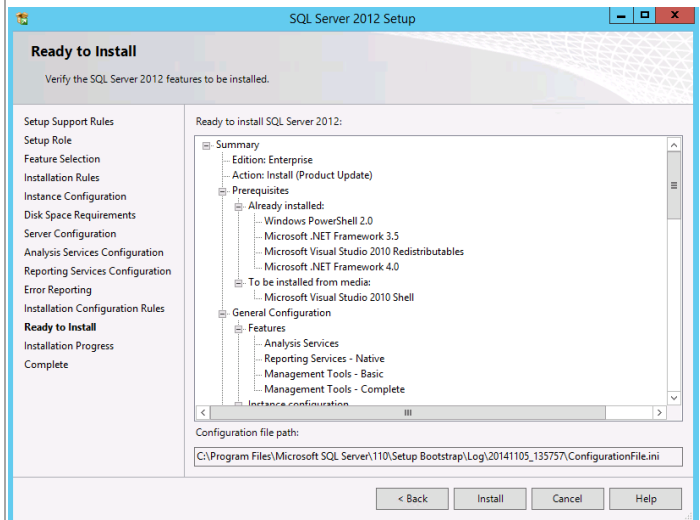
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



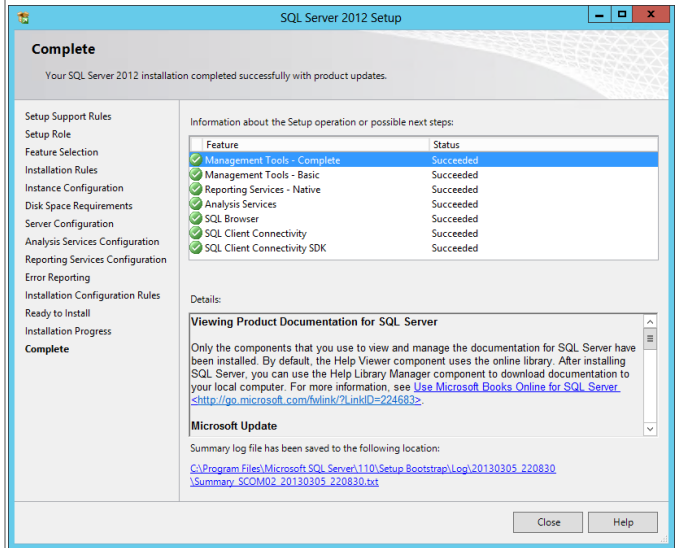
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



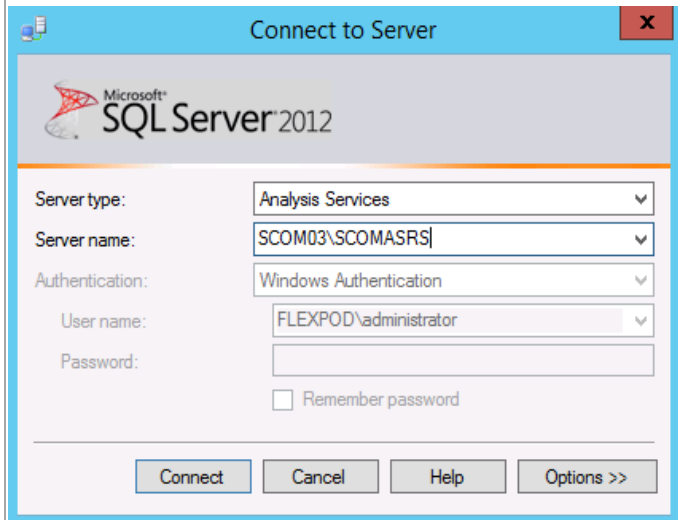
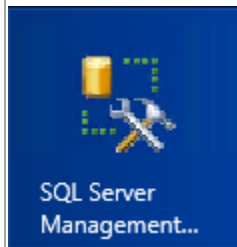
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



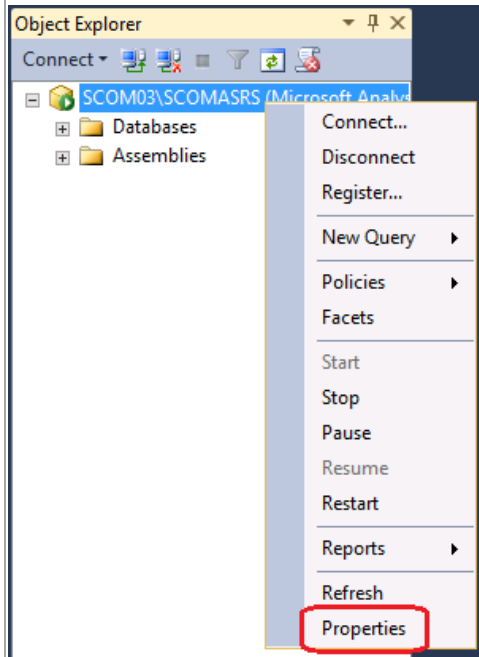
When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



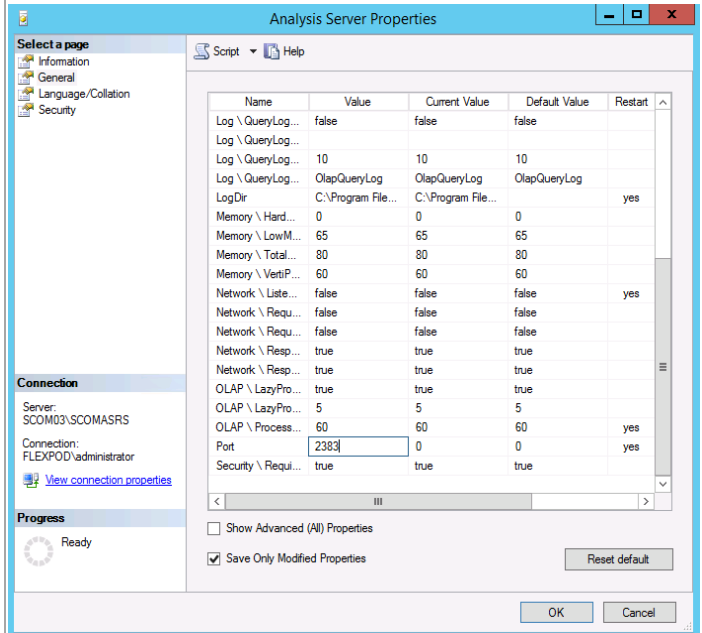
Verify the installation in SSMS prior to moving to the next step of installation. Launch **SQL Server Management Studio** and connect to Analysis Services at **ServerName\InstanceName**.



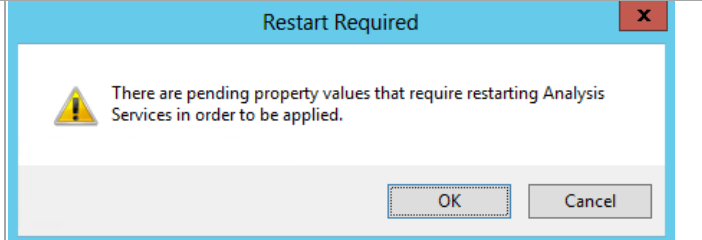
By default, named instances will use dynamic ports. In order to achieve better compatibility with firewalls the instance port should be set to static. Select the SSAS instance. Right-click on the instance and select **Properties**.



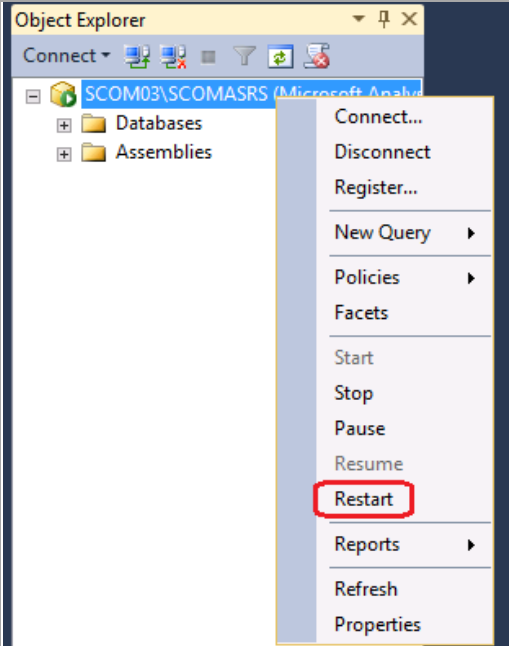
In the **Properties** dialog select the **General** tab. Scroll down to the **Port** value under the **Name** column. Select the value and change the value of 0 (zero) to 2383 or a port value of your choice. When complete, click **OK** to continue.



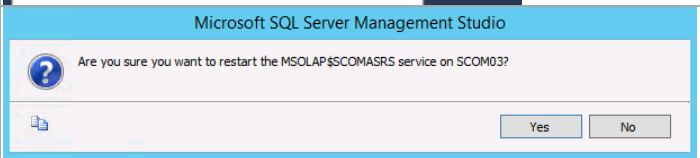
When prompted by the Restart Required dialog, click **OK**.



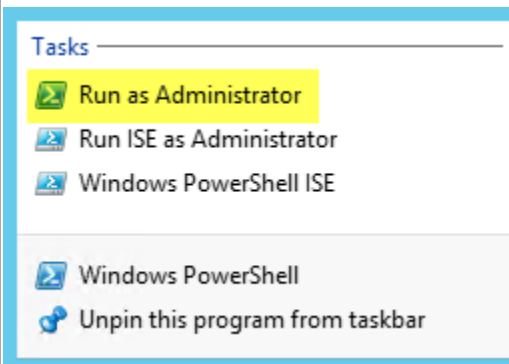
Within **SQL Server Management Studio**, in **Object Explorer**, select the SSAS instance, right-click and select **Restart** from the context menu.



On the confirmation screen, click **Yes**. Close **SQL Server Management Studio**.



By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled. Open an administrative session of PowerShell.



Execute the following commands to create the needed Firewall Rules:

```
New-NetFirewallRule -DisplayName "SQL Analysis Services Browser Service" -Protocol TCP -LocalPort 2382
```

```
New-NetFirewallRule -DisplayName "SQL Analysis Services SCOMASRS Instance" -Protocol TCP -LocalPort 2383
```

```
New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80
```

Adjust the display names and ports based on organizational requirements.

```
PS C:\Windows\system32> 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

Name : {9db92ab5-8ba7-4aed-a5e2-aab368aee05}
DisplayName : SQL Analysis Services Browser Service
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

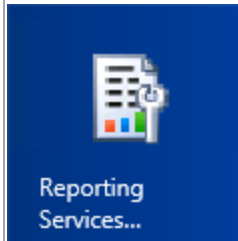
Name : {e713d65-9708-470a-837e-f4265bdf1d68}
DisplayName : SQL Analysis Services SCOMASRS Instance
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

Name : {fae137cf-e4a7-43ce-afbd-79997cae40ce}
DisplayName : SQL Reporting Services
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
```

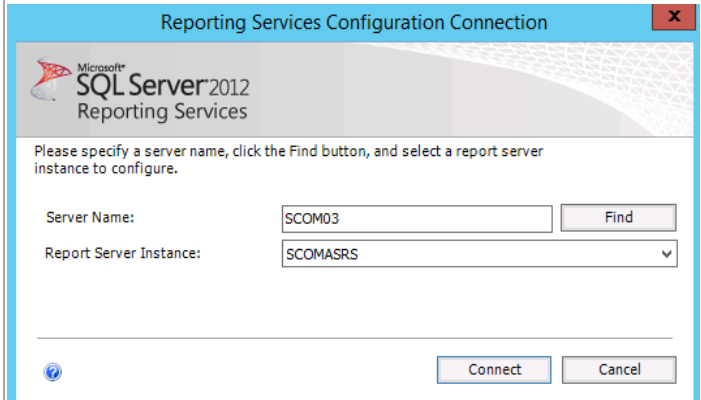
Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.

Name	Group	Profile	Enabled	Action	Override	Pro
SQL Analysis Services Browser Service		All	Yes	Allow	No	Amj
SQL Analysis Services SCOMASRS Instance		All	Yes	Allow	No	Amj
SQL Reporting Services		All	Yes	Allow	No	Amj
BranchCache Content Retrieval (HTTP-In)	BranchCache - Cont...	All	No	Allow	No	SYS
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hoste...	All	No	Allow	No	SYS

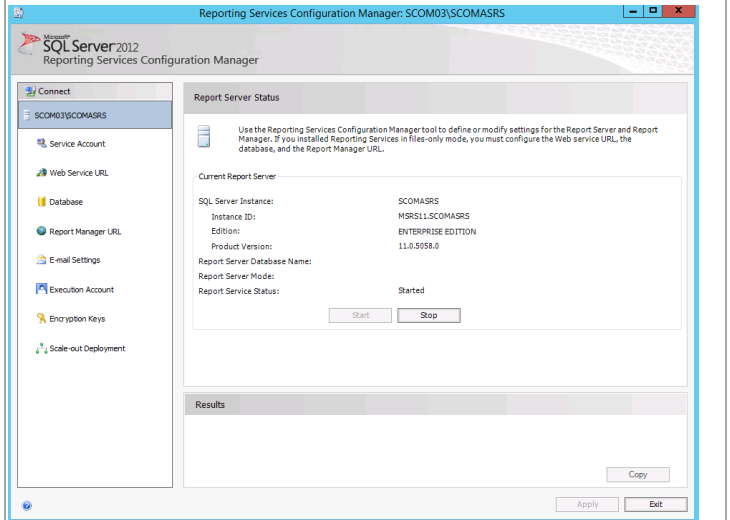
When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start Menu**, navigate and select the **Reporting Services Configuration Manager** tile.



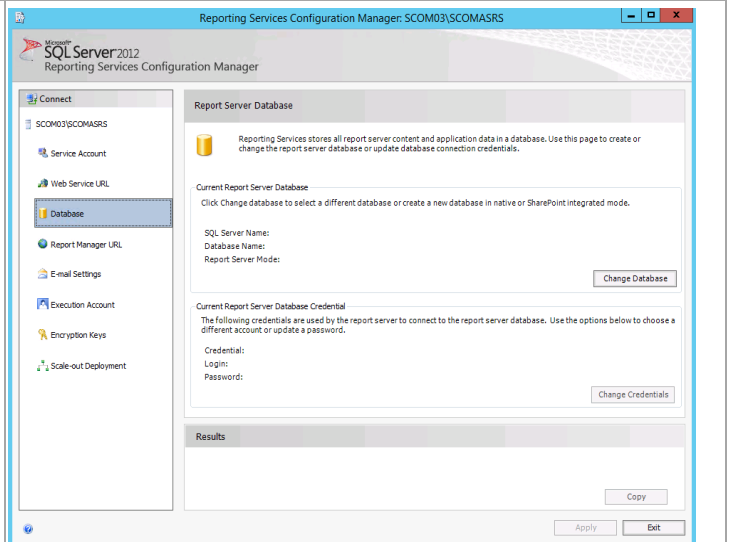
The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Operations Manager server. In the **Report Server Instance** text box, use the default **SCOMASRS** drop-down menu value. Click **Connect**.



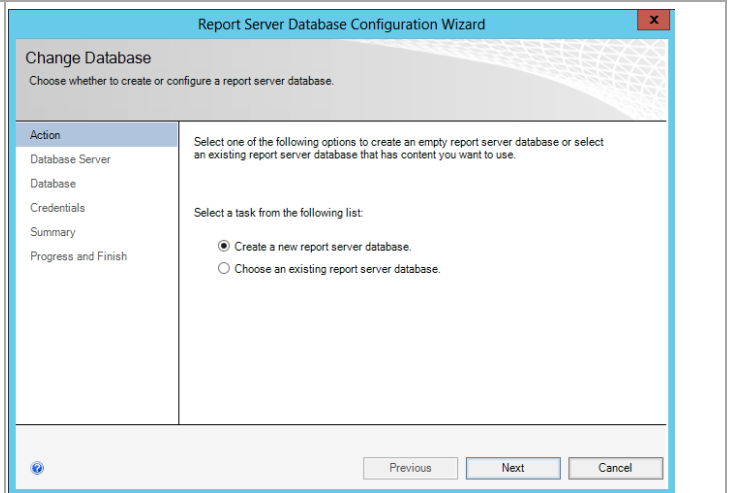
The **Reporting Services Configuration Manager** tool will appear.



In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.



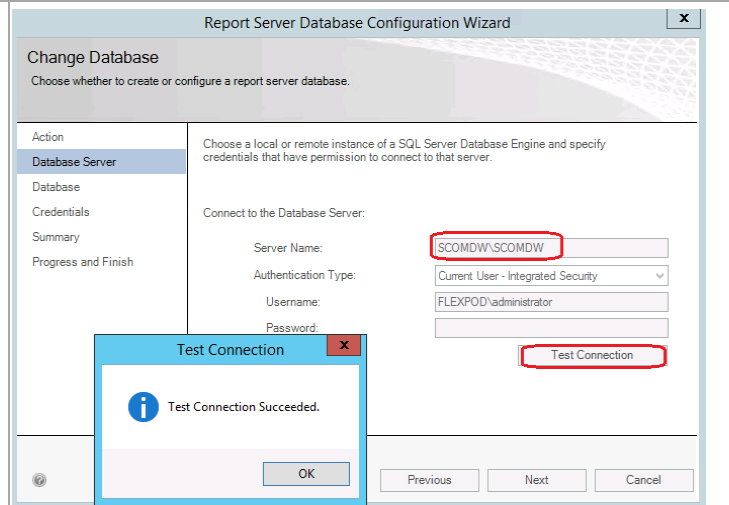
The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – specify the name of the SQL Server CNO and the database instance created for the Operations Manager Data warehouse instance.
- **Authentication Type** – specify **Current User – Integrated Security** from the drop-down menu.

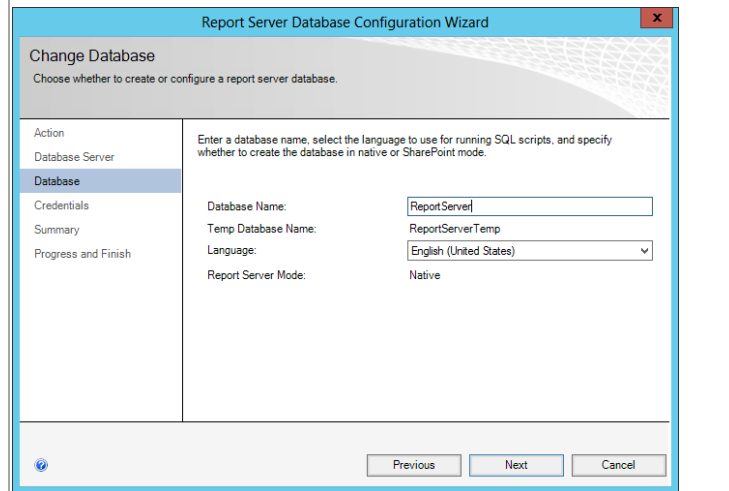
Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



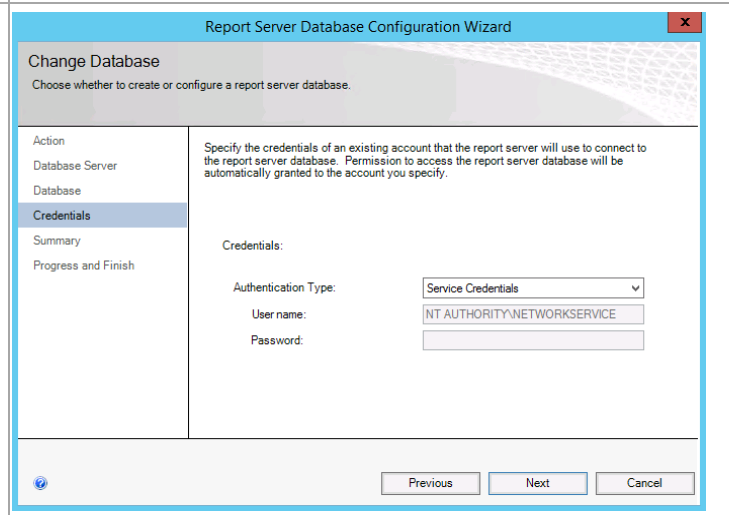
In the **Database** section, specify the following values:

- **Database Name** – accept the default value of ReportServer.
- **Language** – specify the desired language option from the drop-down menu.
- **Report Server Mode** – select the **Native Mode** option.

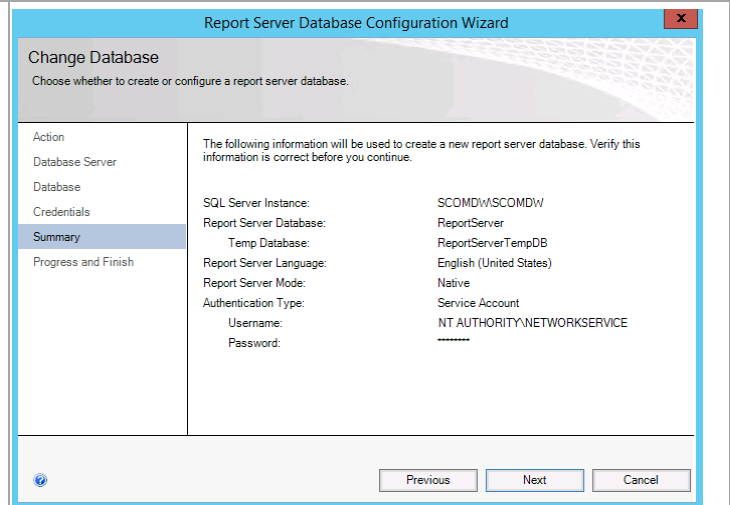
Click **Next** to continue.



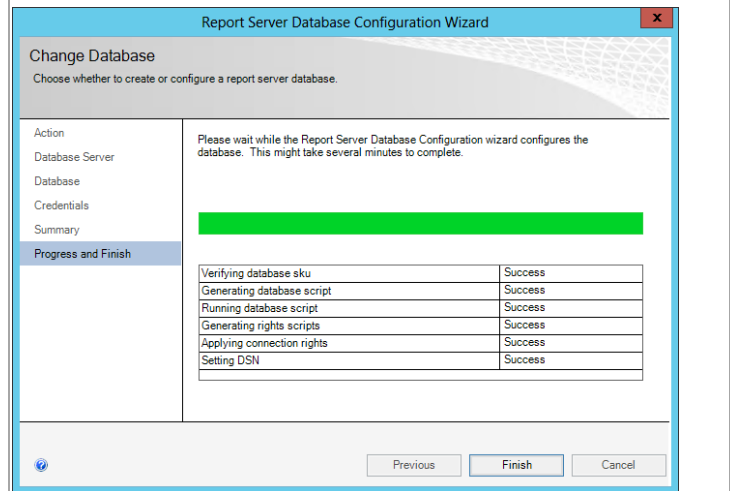
In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.



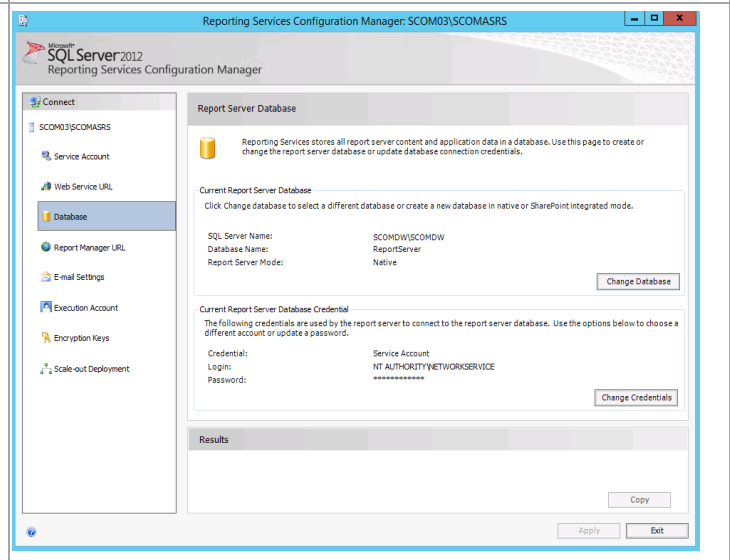
In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.



The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.



In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.

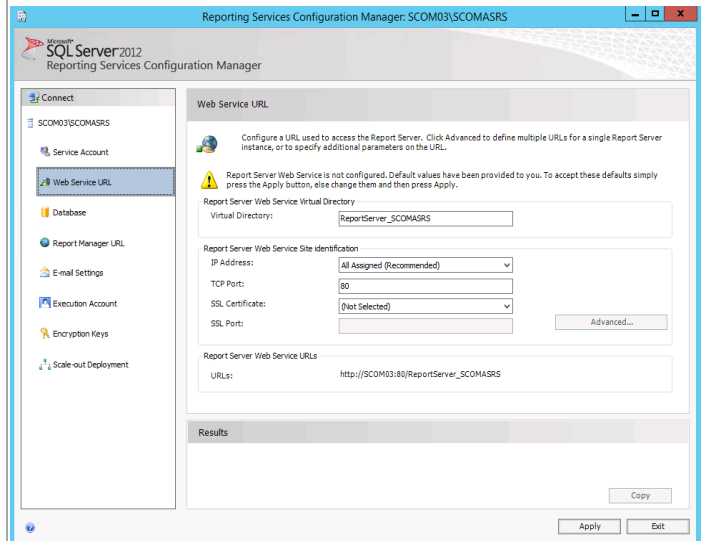




In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer\_SCOMASRS** in the provided text box. **This default value must be used for VMM and SCOM integration to function properly.**
- In the **Report Server Web Service Site Identification** section, set the following values:
  - **IP Address** – set the **All Assigned** drop-down menu value.
  - **TCP Port** – specify the desired TCP Port (default 80).
  - **SSL Certificate** – select the available certificate or choose the default of (Not Selected).

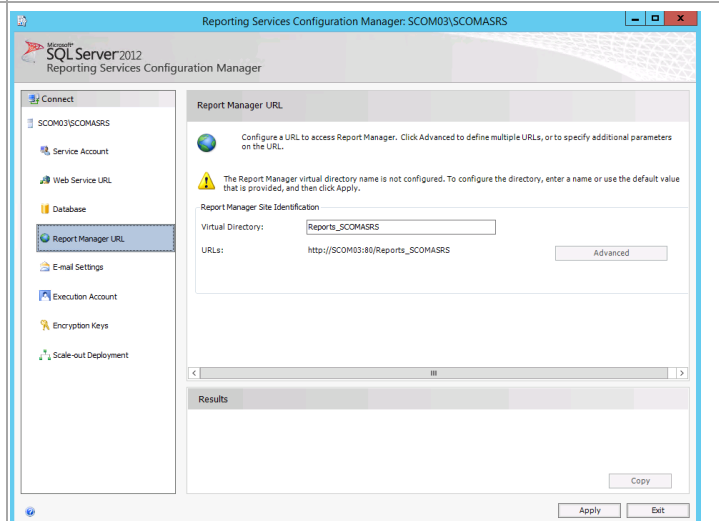
Click the **Apply** button to save the settings and create the Web Service URL.



In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

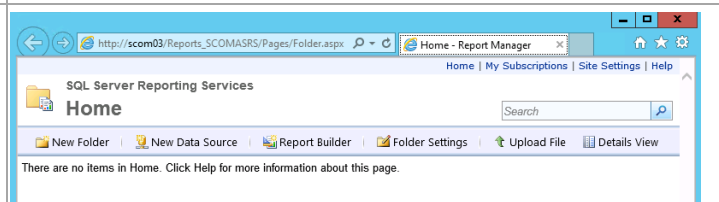
- In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports\_SCOMASRS** in the provided text box. **This default value must be used for VMM and SCOM integration to function properly.**

Click the **Apply** button to save the settings and create the Report Manager URL.

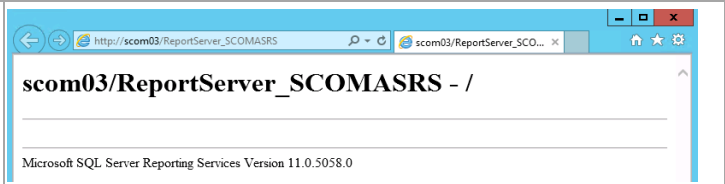


Before performing this and the next step, Internet Explorer Enhanced Security Configuration (ESC) needs to be temporarily disabled.

Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.



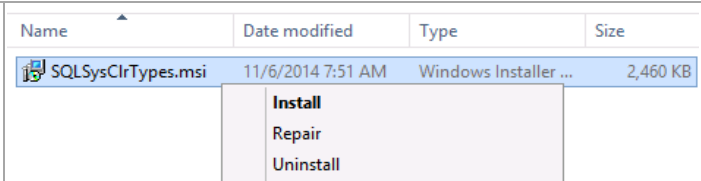
Close the Reporting Server Configuration Manager.

## Install Microsoft Report Viewer 2012

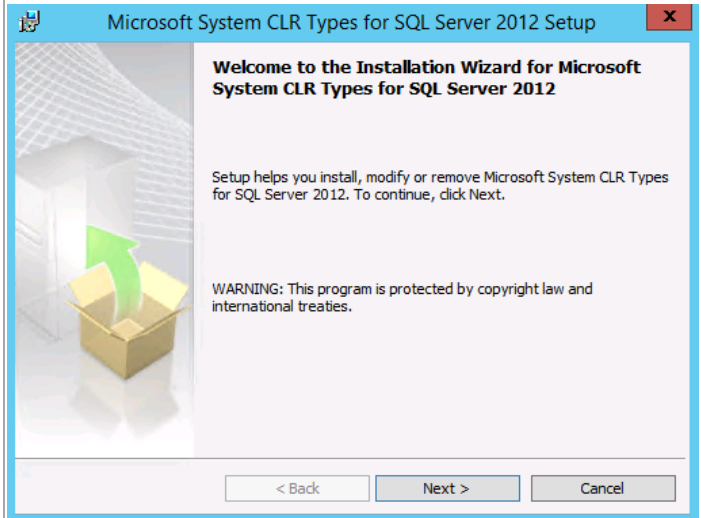
Additionally, the Operations Manager installation also requires the Microsoft System CLR Types for Microsoft SQL Server 2012 and the Microsoft Report Viewer 2012 package to be installed prior to the installation of Operations Manager.<sup>8</sup> Follow the provided steps to install Microsoft Report Viewer 2012.

**Perform the following steps on both Operations Manager management server virtual machines.**

From the installation media source, right-click **SQLSysClrTypes.msi** and select **Install** from the context menu.



On the **Welcome to the Installation...** window click **Next**.

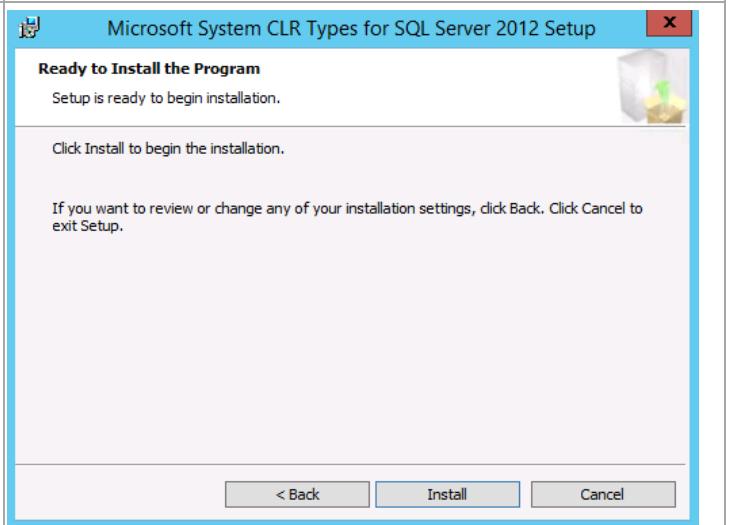


<sup>8</sup> Microsoft System CLR Types for Microsoft SQL Server 2012 - <http://go.microsoft.com/fwlink/?LinkID=239644&clcid=0x409>  
Microsoft Report Viewer 2012 Redistributable Package - <http://www.microsoft.com/en-my/download/confirmation.aspx?id=35747>.

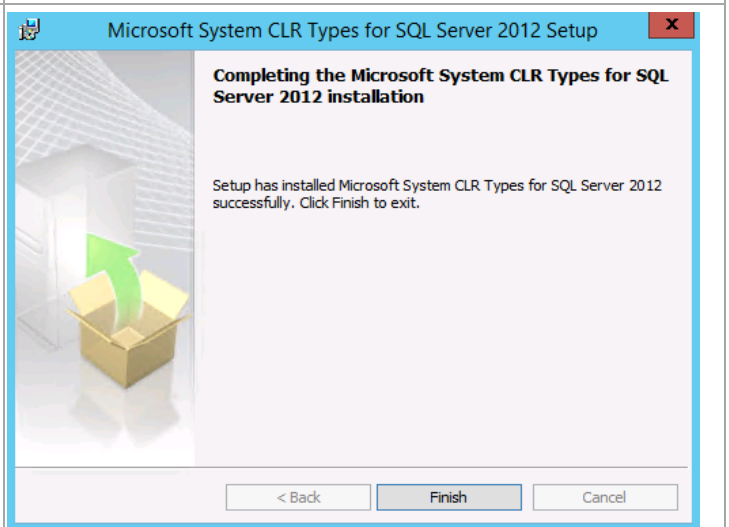
On the License Agreement window, select the **I accept the license terms** check box and click **Next** to continue.



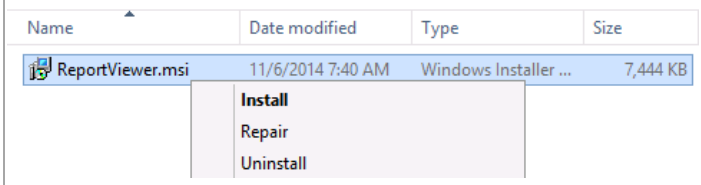
On the **Ready to Install the Program** window click **Install**.



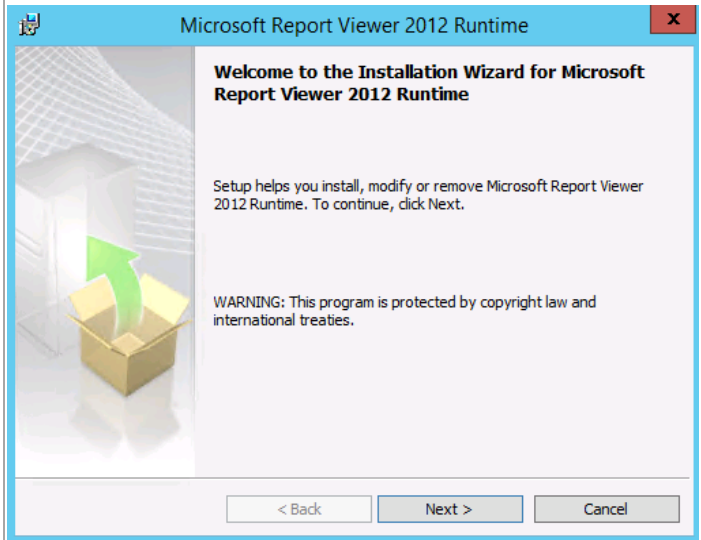
On the **Completing the Microsoft ... Installation** window click **Finish**.



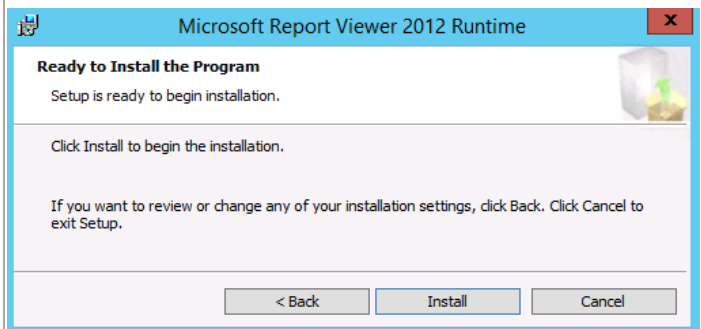
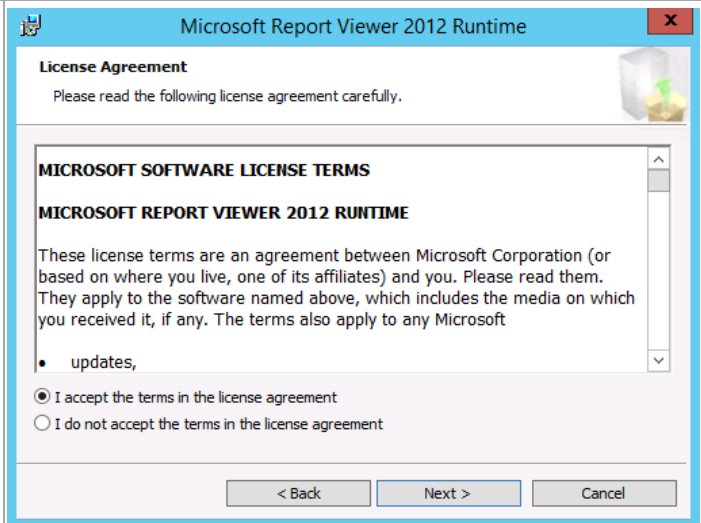
From the installation media source, right-click **ReportViewer.msi** and select **Install** from the context menu to begin setup.



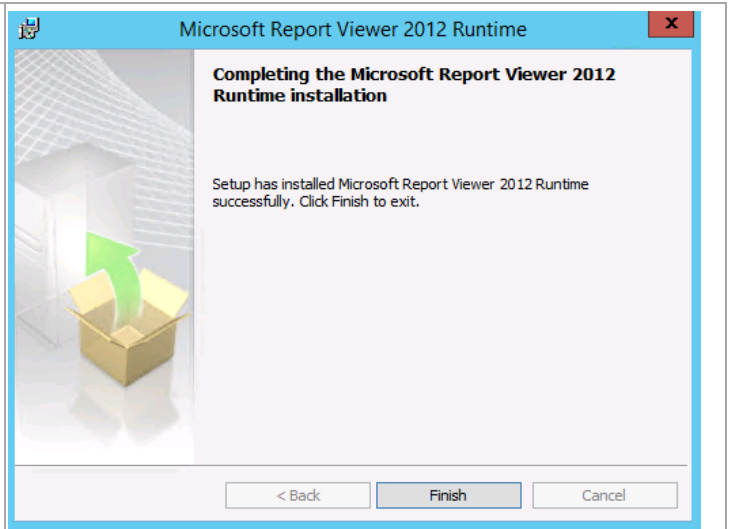
Within the **Microsoft ReportViewer 2012 Redistributable Setup** dialog, select **Next** to begin the installation.



Select the **I have read and accept the license terms** check box and click **Next**.  
On the **Ready to Install the Program** window click **Install**.



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.<sup>9</sup>

---

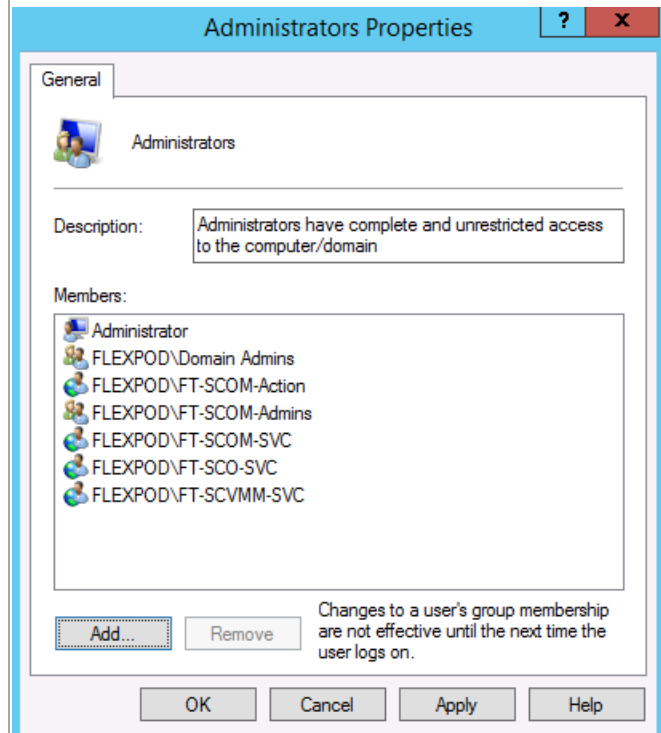
<sup>9</sup> Deploying System Center 2012 - Operations Manager - [http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK\\_BeforeYouBegin](http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin).

Perform the following steps on both **Operations Manager management server** virtual machines.

Log on to the Operations Manager virtual machine as a user with local admin rights.

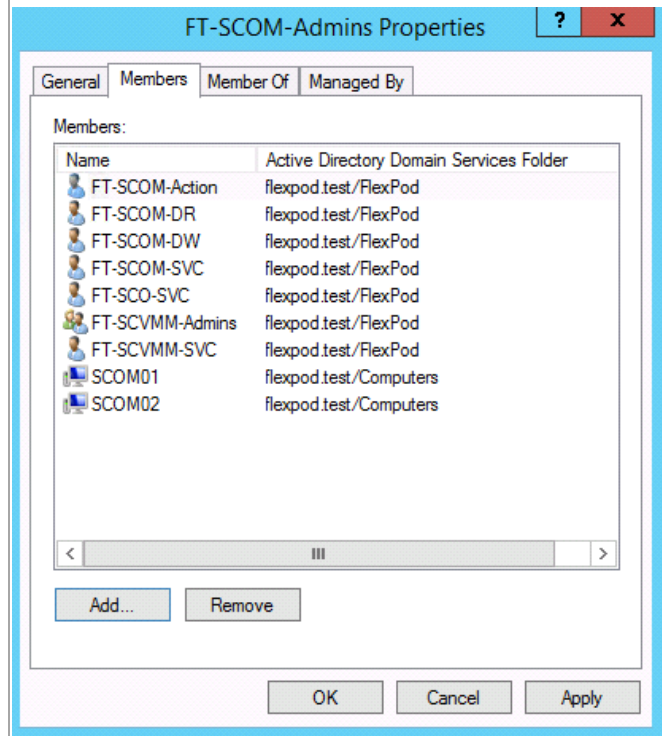
Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager virtual machine:

- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.
- Virtual Machine Manager service account



Perform the following step on an **Active Directory Domain Controller** in the target environment.

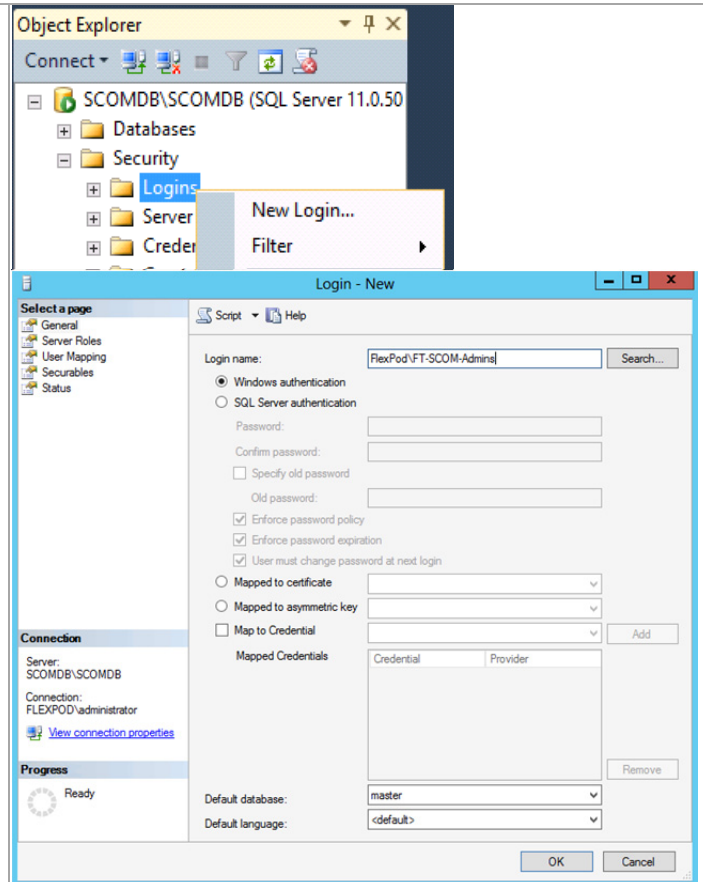
In the domain where Operations Manager will be installed, verify that the Operations Manager computer account and the groups outlined in the table above are members of the OM Admins group created earlier.



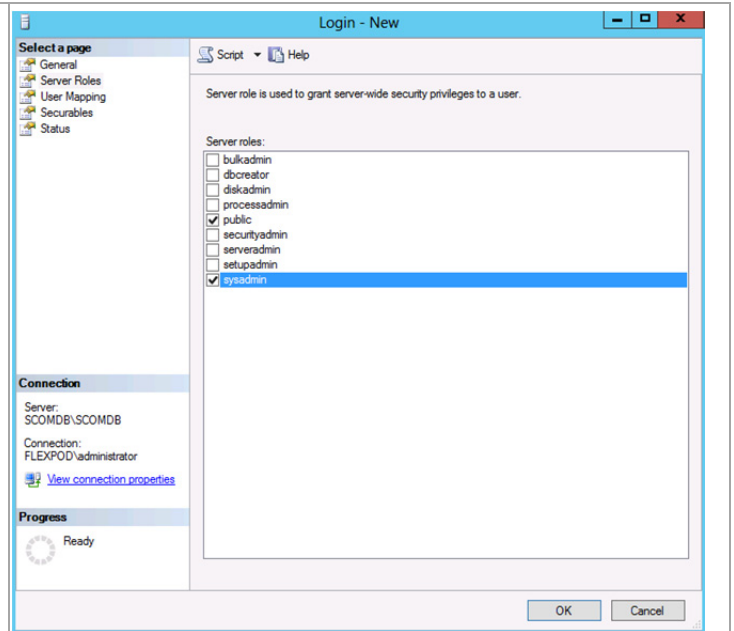
**Perform the following steps on the primary SQL Server cluster node.**

Using Administrative credentials, log on to the first SQL Server and open SSMS. Connect to the Operations Manager SQL Server instance using the values specified earlier. Create a new login by navigating to the **Logins** node under **Security** within SQL Management Studio. Right-click the **Logins** node and select **New Login...** from the context menu.

In the **Login - New** dialog, specify the Operations Manager Admins group created earlier as the new **Login name**.



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.



## 20.3 Installation

### Install the Operations Manager Management Server

The following steps must be completed in order to install and configure the Operations Manager database and server roles.

**Perform the following steps on the first Operations Manager management server virtual machine.**

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

Name	Date modified	Type	Size
acs	9/6/2013 5:55 PM	File folder	
agent	9/6/2013 6:13 PM	File folder	
gateway	9/6/2013 7:10 PM	File folder	
HelperObjects	9/6/2013 5:55 PM	File folder	
Licenses	9/6/2013 5:55 PM	File folder	
ManagementPacks	9/6/2013 5:55 PM	File folder	
msxml	9/6/2013 5:55 PM	File folder	
ProductDocumentation	9/6/2013 5:55 PM	File folder	
ReportModels	9/6/2013 5:55 PM	File folder	
SCXACS	9/6/2013 6:13 PM	File folder	
setup	9/6/2013 6:13 PM	File folder	
SupportTools	9/10/2013 3:11 PM	File folder	
autorun.inf	8/12/2013 5:30 PM	Setup Information	1 KB
Setup.exe	9/6/2013 4:19 PM	Application	1,463 KB

Context menu for Setup.exe:

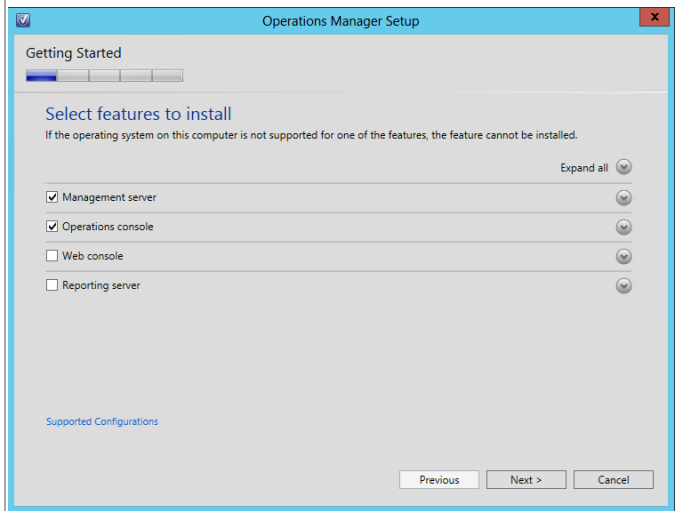
- Open
  - Run as administrator
  - Troubleshoot compatibility



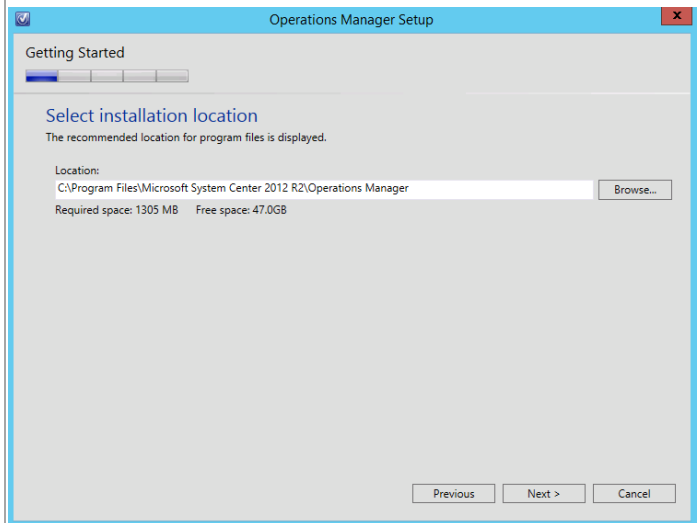
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.



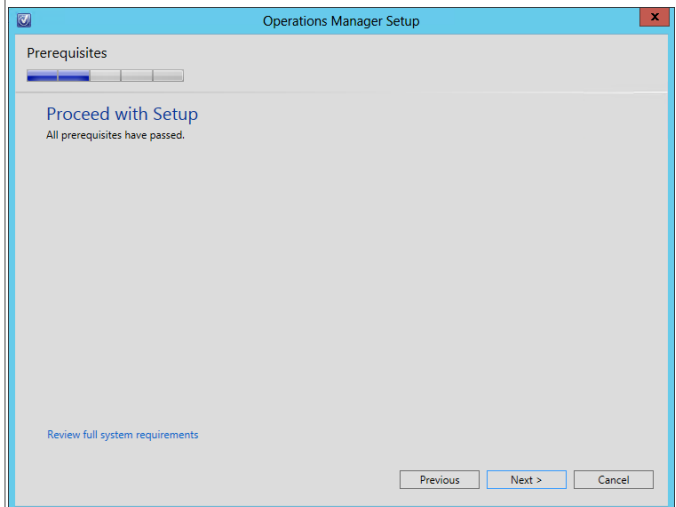
In the **Select features to install** dialog, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012 R2\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system pre-requisites are met in the **Proceed with Setup** dialog. If any pre-requisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.

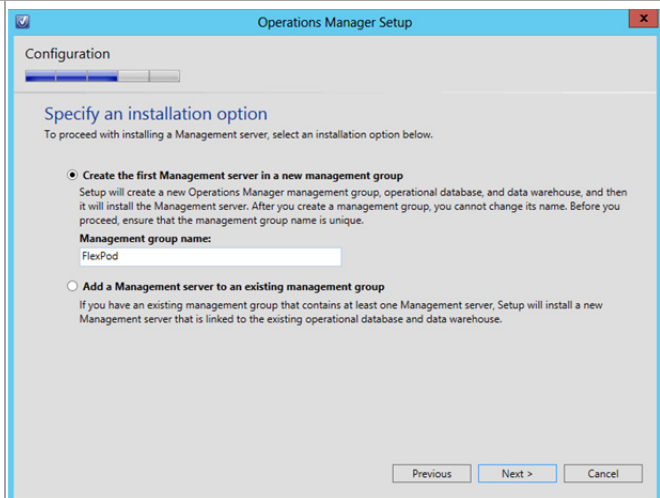


In the **Specify an installation option** dialog, two installation options are provided:

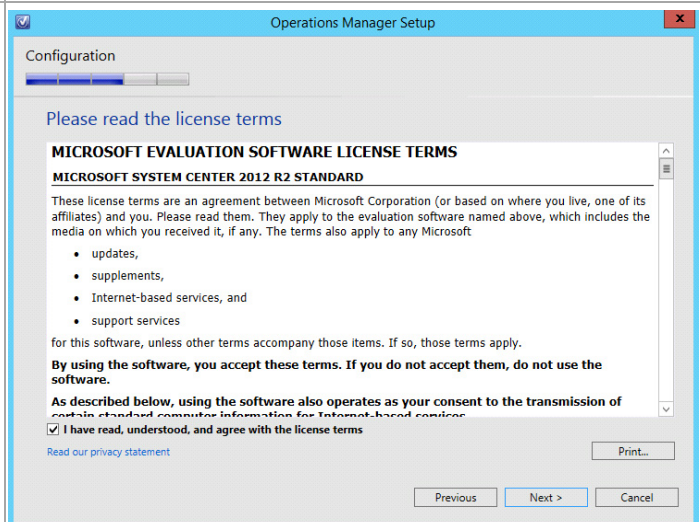
- Create the first management server in a new management group.
- Add a Management server to an existing management group.

Select the **Create the first Management server in a new management group** option and supply a unique name in the **Management group name** text box. Note that this name must be unique across System Center products.

Click **Next** to continue.



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



In the **Configure the operational database** dialog, Specify the following information in the provided text boxes:

- **Server name and instance name** – specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.
- **SQL Server port** – specify the TCP port used for SQL Server connectivity (1433 is the default, however this may be different based on instance requirements outlined earlier).
- **Database name** – specify the name of the Operations Manager database. In most cases the default value of OperationsManager should be used.
- **Database size (MB)** – specify the initial database size. <sup>10</sup> The following values can be used as a general guideline:
  - Up to 500 agents: 12 GB.
  - Up to 1000 agents: 24 GB.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the log files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

The screenshot shows the 'Operations Manager Setup' dialog box, specifically the 'Configure the operational database' step. The dialog has a title bar with 'Operations Manager Setup' and a close button. Below the title bar is a 'Configuration' section with a progress indicator. The main area is titled 'Configure the operational database' and includes a warning: 'Before you click Next, verify the database name, the instance name, and the port. Ensure that you have sufficient permissions on the database instance.' The fields are as follows: 'Server name and instance name' is 'SCOMDB\SCOMDB', 'SQL Server port' is '10476', 'Database name' is 'OperationsManager', 'Database size (MB)' is '6000', 'Data file folder' is '\\Infrasvm\SCOMDB\MSSQL11.SCOMDB\MSSQL\DATA', and 'Log file folder' is '\\Infrasvm\SCOMDBLOG\MSSQL11.SCOMDB\MSSQL\Data'. There are 'Browse...' buttons next to the folder fields. At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

<sup>10</sup> System Center 2012 - Operations Manager Component Add – On - <http://www.microsoft.com/en-us/download/details.aspx?id=29270> provides general guidance for database sizing.

In the **Configure the data warehouse database** dialog, specify the following information in the provided text boxes:

- **Server name and instance name** – specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.
- **SQL Server port** – specify the TCP port used for SQL Server connectivity (1433 by default, however this may be different based on instance requirements outlined earlier).
- **Database name** – specify the name of the Operations Manager Data Warehouse database. In most cases the default value of OperationsManagerDW should be used.
- **Database size (MB)** – specify the initial database size.<sup>11</sup> The following values can be used as a general guideline:
  - Up to 500 agents: 356 GB.
  - Up to 1000 agents: 720 GB.
- **Data file folder** – specify the drive letter associated in the SQL Service cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

The screenshot shows the 'Configure the data warehouse database' dialog box. The 'Server name and instance name' field contains 'SCOMDW\SCOMDW' and the 'SQL Server port' field contains '10477'. The 'Database name' field contains 'OperationsManagerDW' and the 'Database size (MB)' field contains '140000'. The 'Data file folder' field contains '\\Infrasvm\SCOMDW\MSSQL11.SCOMDW\MSSQL\DATA\' and the 'Log file folder' field contains '\\Infrasvm\SCOMDW\LOG\MSSQL11.SCOMDW\MSSQL\Data'. The 'Create a new data warehouse database' radio button is selected. The 'Previous', 'Next >', and 'Cancel' buttons are visible at the bottom.

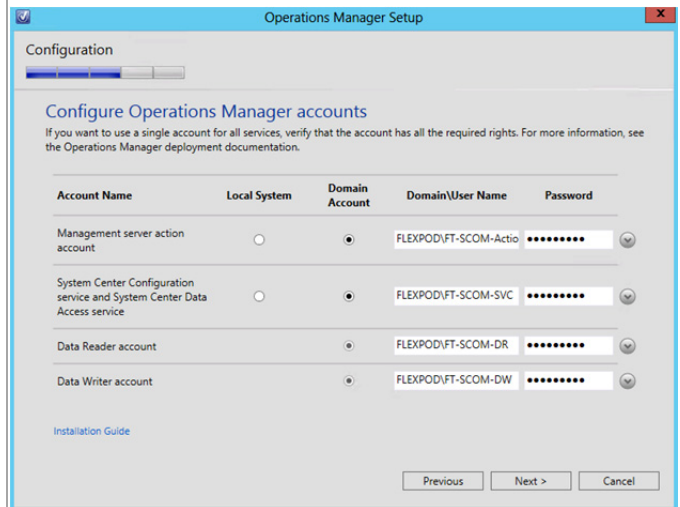
<sup>11</sup> System Center 2012 - Operations Manager Component Add – On - <http://www.microsoft.com/en-us/download/details.aspx?id=29270> provides general guidance for database sizing.

In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- Management server action account
- System Center Configuration service and System Center Data Access service
- Data Reader account
- Data Writer account

If the use of a Domain Account is specified, enter the user account information as `<DOMAIN>\<USERNAME>` and enter the appropriate password.

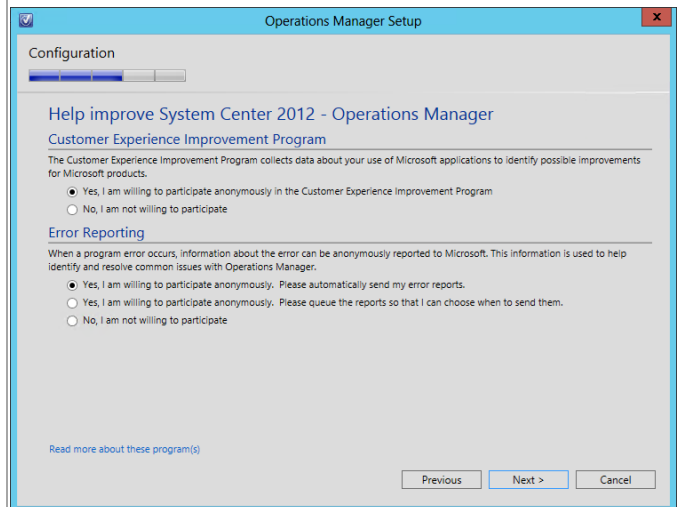
When completed, click **Next** to continue.



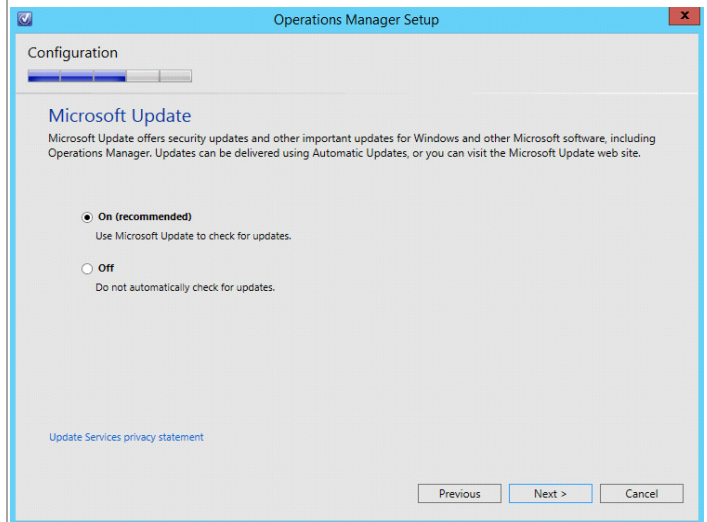
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- Customer Experience Improvement Program
- Error Reporting

Select the appropriate option based on your organization's policies and click **Next** to continue.

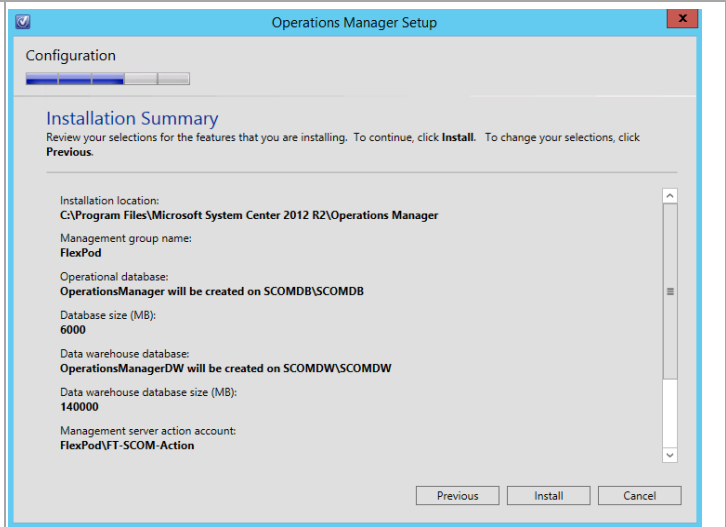


If you want to check for updates automatically, select **On** radio button. Click **Next** to continue.

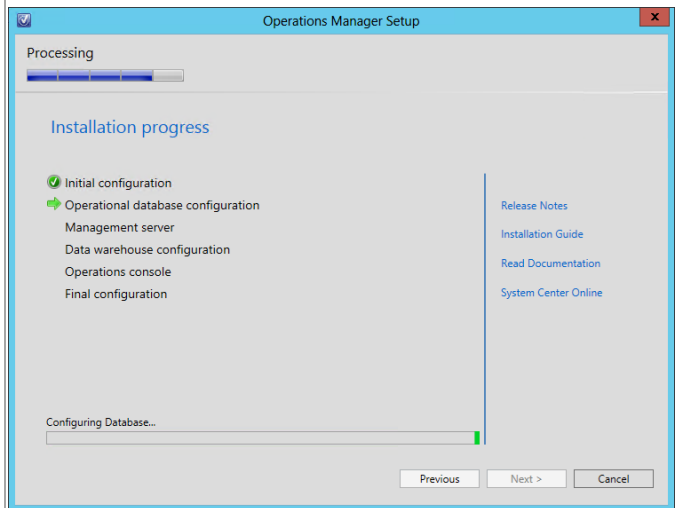


The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

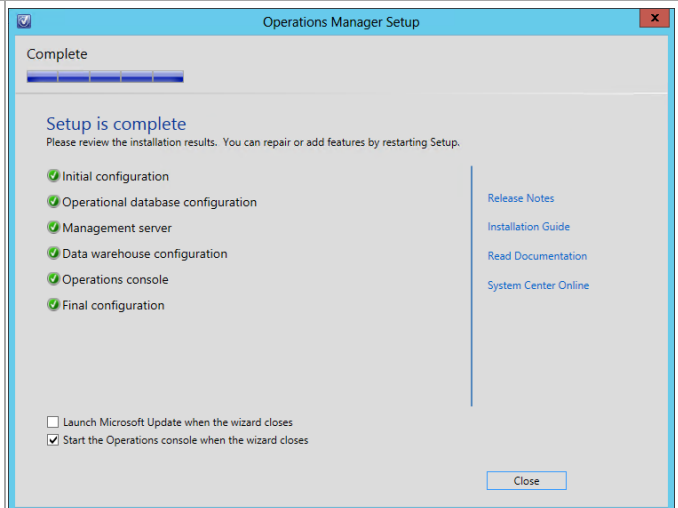
**Note:** Make sure you set the database sizes appropriately for your particular deployment.



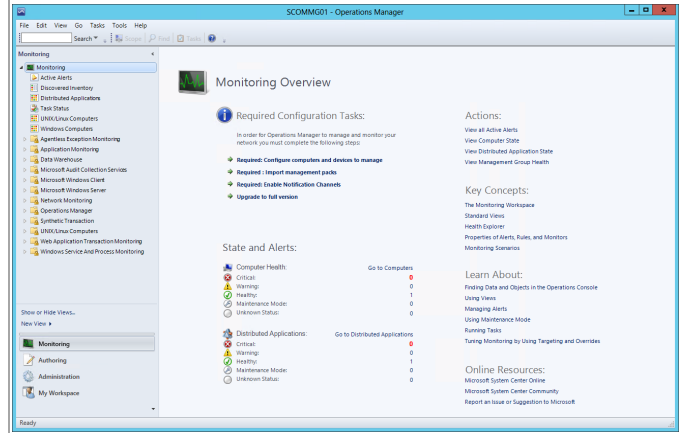
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.



When completed, the **Operations Manager** console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.

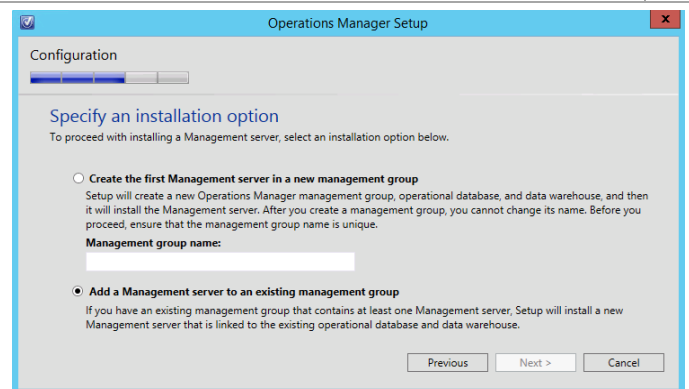


## Install Second Operations Manager Server

Installation of the second Operations Manager management server is almost identical to installing the first server. The following steps show which setup entries differ during installation.

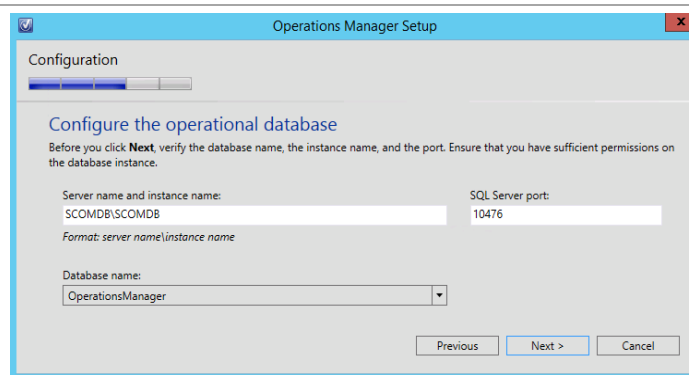
Perform the following altered steps on the **second Operations Manager management server virtual machine**.

On the **Configuration/Specify and installation option** screen of setup, select the **Add a Management server to an existing management group** radio button. Click **Next** to continue.



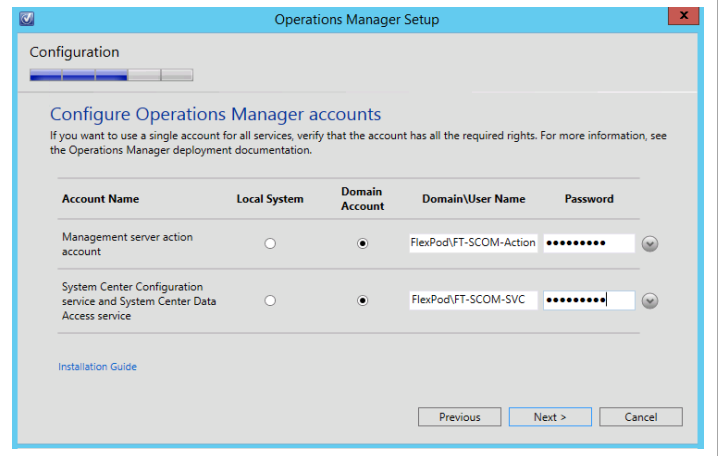
On the **Configuration/Configure the operational database** screen of setup, specify the CNO and database instance name of the Operations Manager database. Specify the **port number** that you assigned to this instance. From the dropdown list of the Database name field, select the **OperationsManager** database.

Click **Next** to continue.



On the **Configuration/Configure Operations Manager accounts** screen of setup, specify the Management server action account and Configuration service and data access accounts with the appropriate passwords.

Click **Next** to continue.

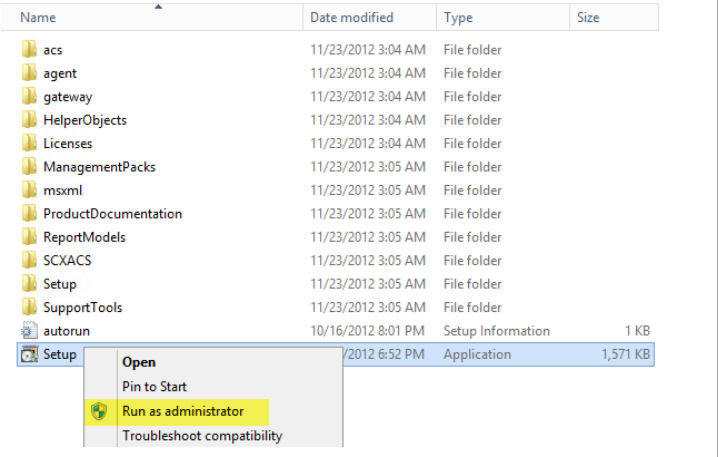


## Install the Operations Manager Reporting Server

The following steps must be completed in order to install and configure the Operations Manager reporting server role.

**Perform the following steps on the Operations Manager reporting server virtual machine.**

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

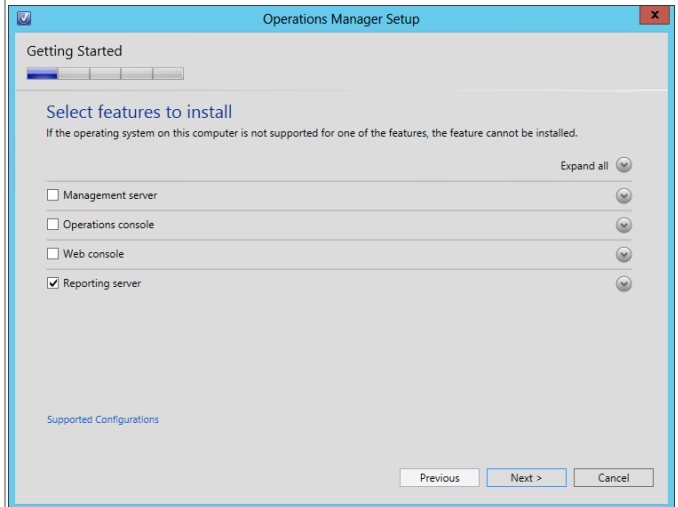


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.

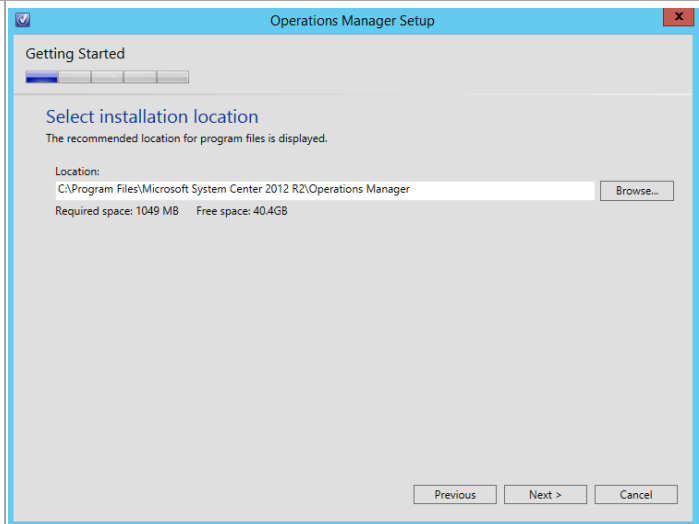




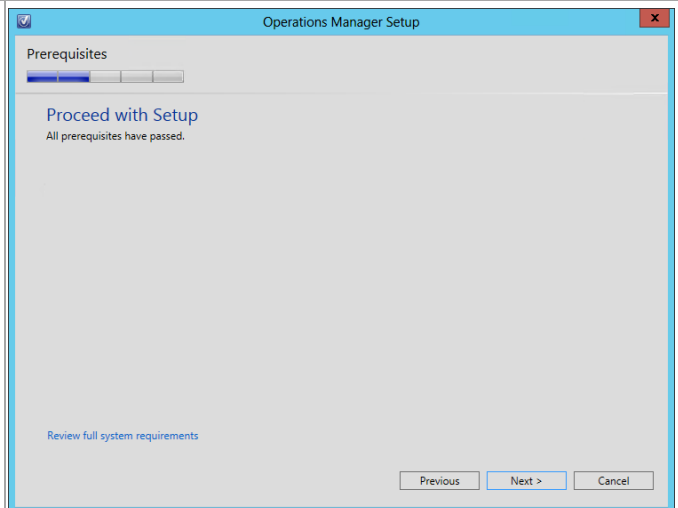
In the **Select features to install** dialog, verify that the **Reporting server** check boxes are selected. Click **Next** to continue.



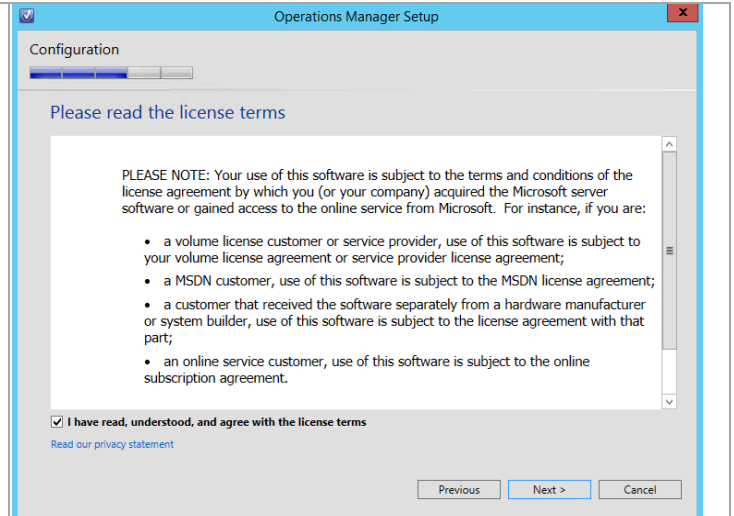
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.



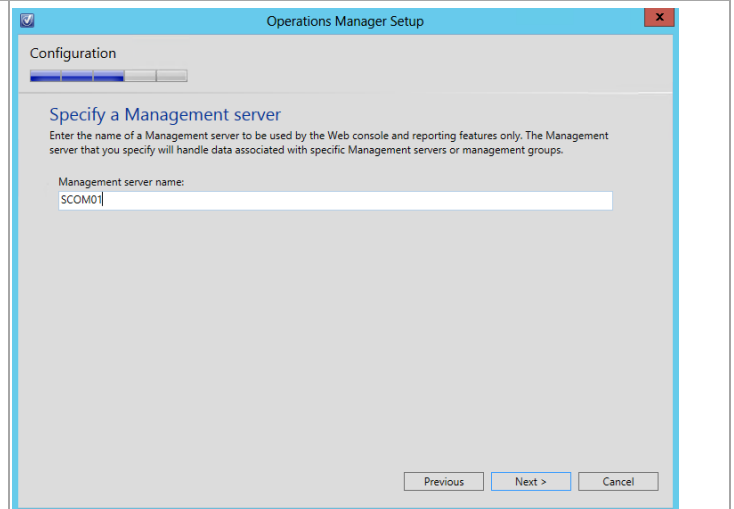
The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



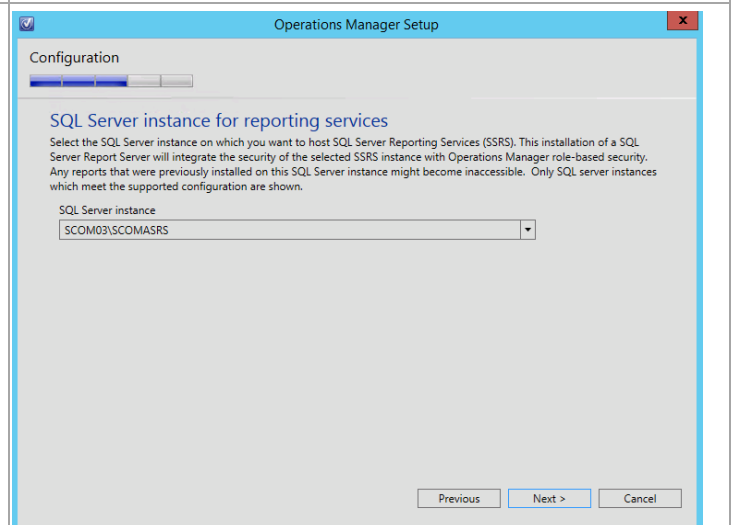
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.



In the **Specify a Management server** dialog, type the name of the previously installed management server in the **Management server name** text box. Click **Next** to continue.



In the **SQL Server instance for reporting services** dialog, select the SQL Server instance hosting the local SQL Server Reporting Services and SQL Server Analysis Services from the drop-down menu created during earlier steps. Click **Next** to continue.

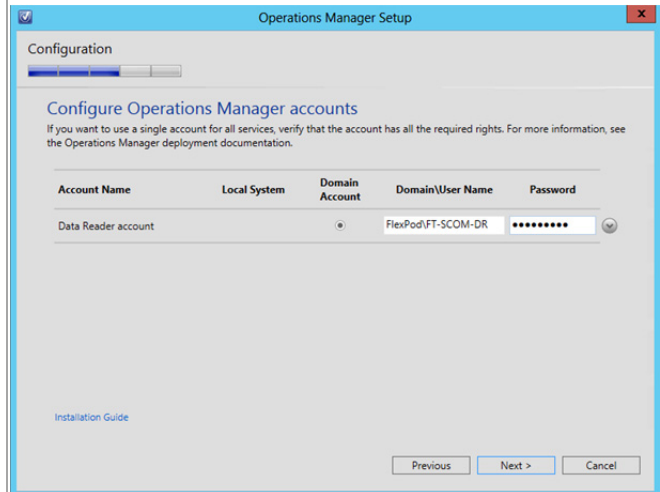


In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- **Data Reader account.**

If the use of a Domain Account is specified, enter the user account information as `<DOMAIN>\<USERNAME>` and enter the appropriate password.

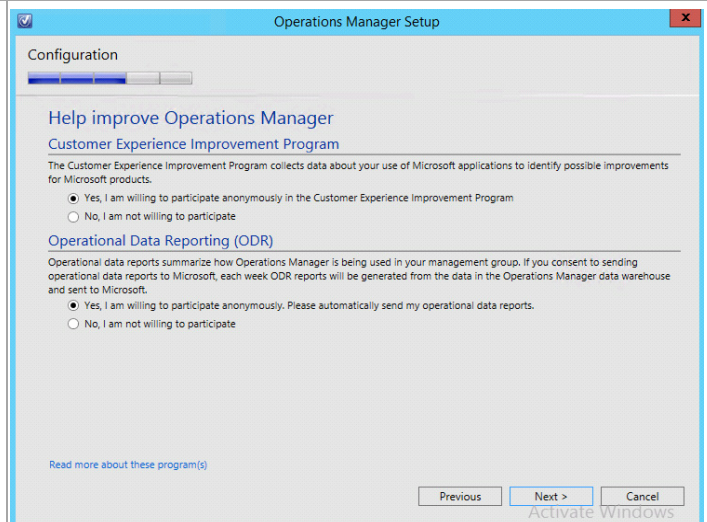
When completed, click **Next** to continue.



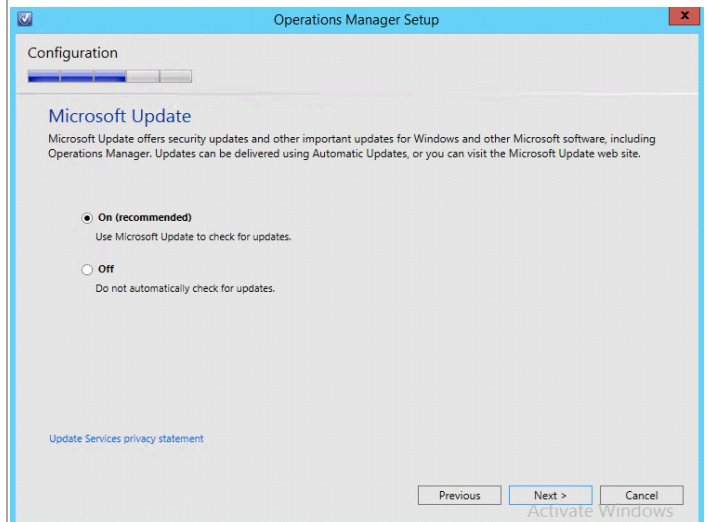
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. This includes:

- **Operational Data Reporting (ODR).**

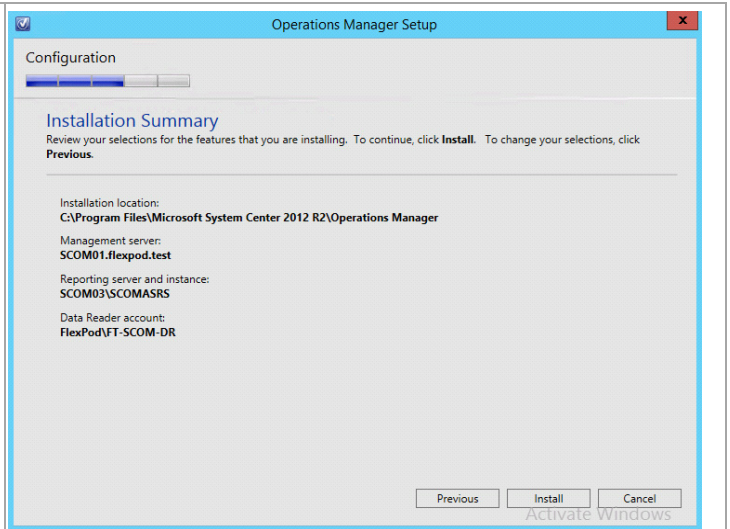
Select the appropriate option based on your organization's policies and click **Next** to continue.



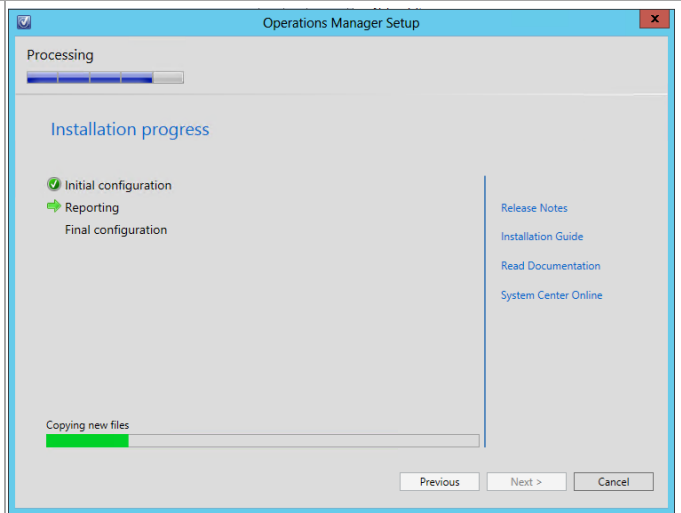
If you wish to use Microsoft Update select the radio button by **On**.



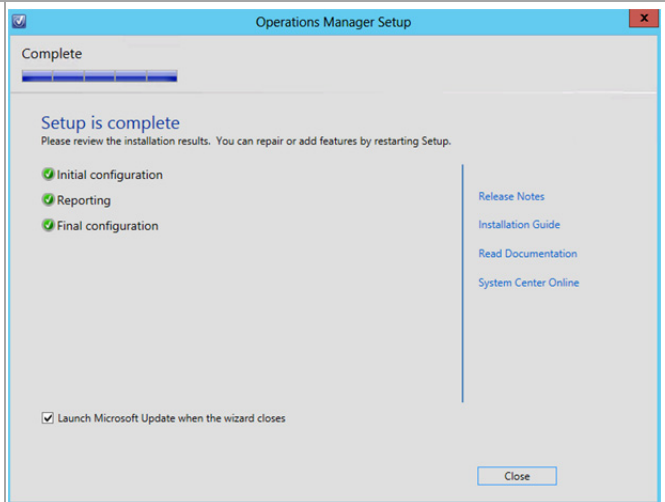
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



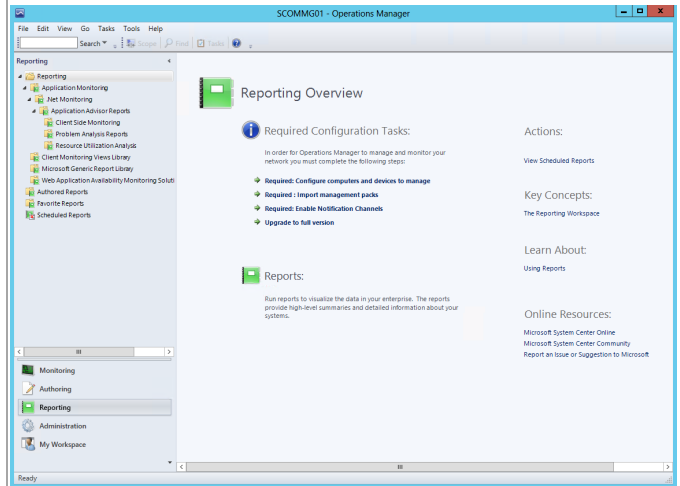
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch Microsoft Update when the wizard closes** check box is selected and click **Close** to complete the installation.



When completed, open the Operations Manager console from the first management server. From this console, the installation can be validated by noting that the **Reporting** node is now visible in the console.



## 20.4 Post-Installation Tasks

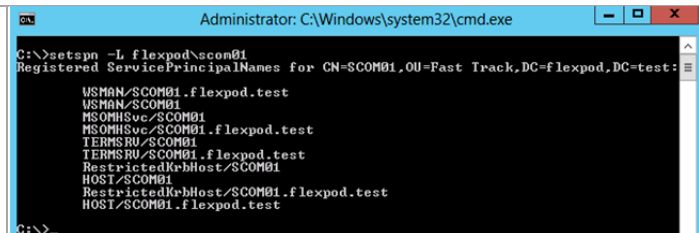
When the installation is complete, the following tasks must be performed to complete Operations Manager and Virtual Machine Manager integration.

### Register the Required Service Principal Names for the Operations Manager Management Servers

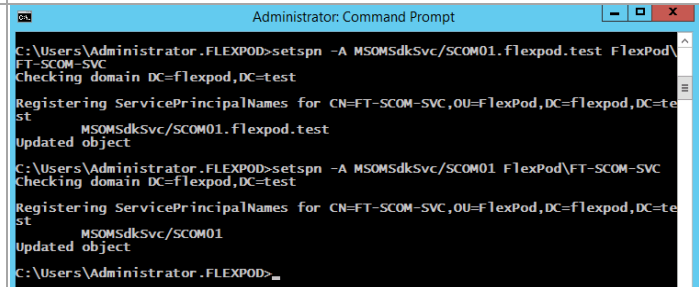
The following steps must be performed on a Domain Controller or one of the Operations Manager servers using a domain admin account or an account with permissions to create SPNs.

**Perform the following steps on a Domain Controller in the domain where Operations Manager is installed.**

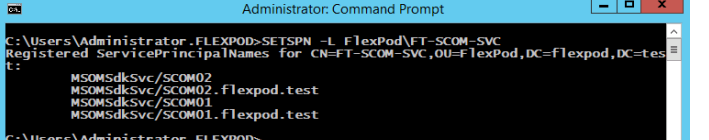
The Operations Manager Health Service SPN's should be set automatically by the Management Server's computer account. To confirm the SPN's set correctly open an administrative command prompt and execute the following command:  
**SETSPN -L <DOMAIN>\<SERVERNAME>**  
 Where <DOMAIN> is the Active Directory domain name where the Operations Manager management server is installed and <SERVERNAME> is the name of the Operations Manager Management Server.



The Data Access Service account runs under a domain user account context and is not able to create the appropriate SPNs in Active Directory. The following command must be executed by a domain admin account or an account with delegated permissions to user objects.



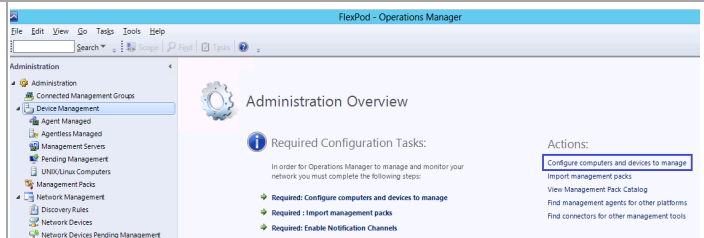
To set the SPN run the following commands from an administrative command prompt:  
**SETSPN.exe -A**

<p>MSOMSdkSvc/&lt;ManagementServerFQDN&gt; &lt;domain&gt;\&lt;SDKServiceAccount&gt;</p> <p>SETSPN.exe -A MSOMSdkSvc/&lt;ManagementServerNetBIOS&gt; &lt;domain&gt;\&lt;SDKServiceAccount&gt;</p> <p>Where &lt;ManagementServerFQDN&gt; is the name of the Operations Manager management server and &lt;SDKServiceAccount&gt; is the name of the Operations Manager Service Account.</p> <p>If there is more than one Management Server being deployed then these commands <b>must be run for each</b> Management Server.</p>	<pre>SETSPN -A MSOMSdkSvc/SCOM01.FlexPod.test FlexPod\FT-SCOM-SVC</pre> <pre>SETSPN -A MSOMSdkSvc/SCOM01 FlexPod\FT-SCOM-SVC</pre> <pre>SETSPN -A MSOMSdkSvc/SCOM02.FlexPod.test FlexPod\FT-SCOM-SVC</pre> <pre>SETSPN -A MSOMSdkSvc/SCOM02 FlexPod\FT-SCOM-SVC</pre>
<p>When complete the SPNs can be confirmed with the following command: SETSPN -L &lt;DOMAIN&gt;\&lt;SDKServiceAccount&gt;</p>	

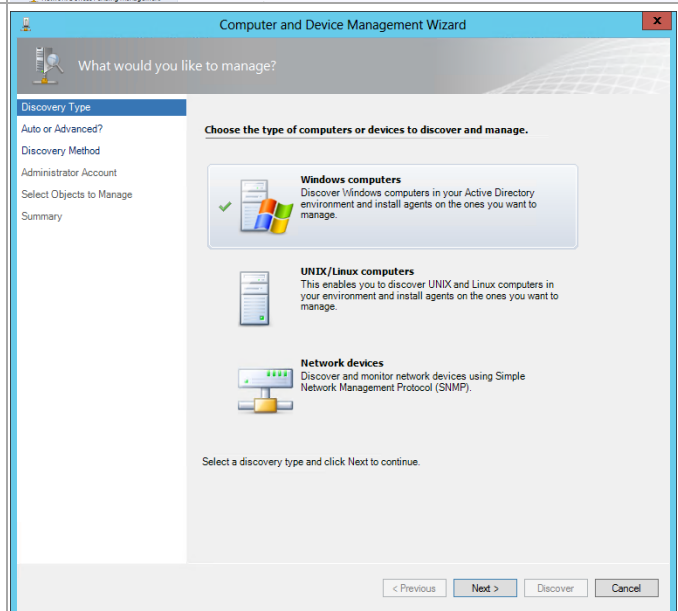
## Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Server Nodes

Perform the following steps on the **Operations Manager management server virtual machine**.

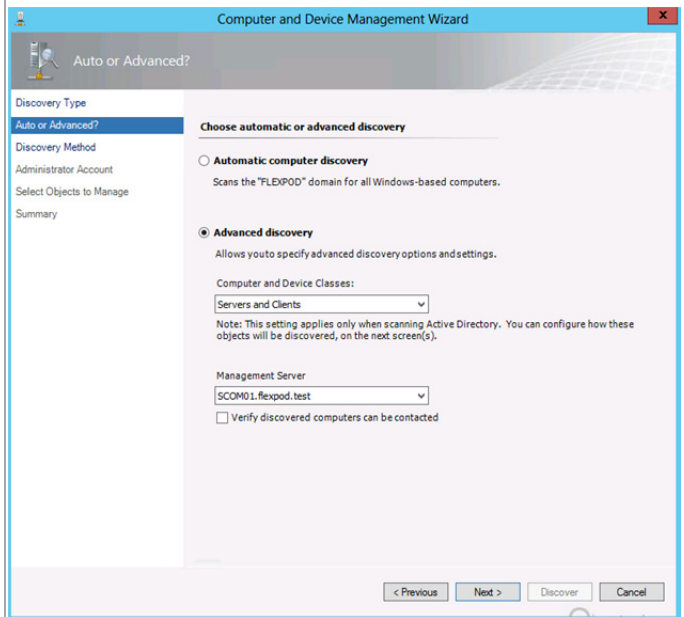
In **Operations Manager** console, navigate to the **Administration** workspace. Under **Actions**, select **Configure computers and devices to manage**.



The **Computer and Device Management Wizard** will appear. In the **Discovery Type** dialog, select **Windows computers** from the available options and click **Next** to continue.

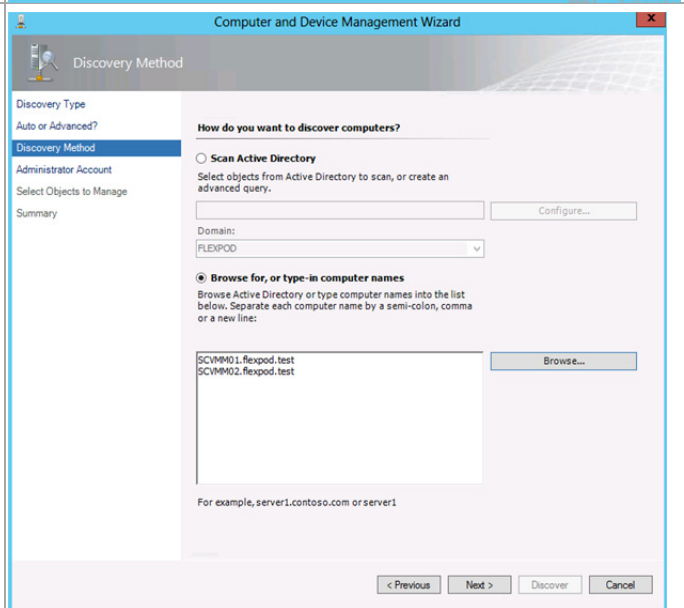


In the **Auto or Advanced?** dialog, select the **Automatic computer discovery** option and click **Next** to continue.

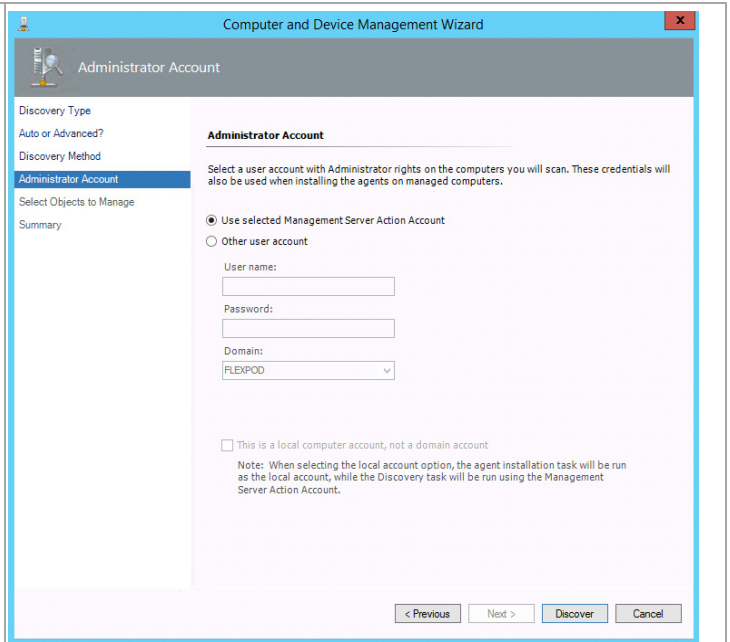


In the **Discovery Method** dialog box, under **Browse for, or type-in computer names**, input the names of both VMM servers. Click **Next** to continue.

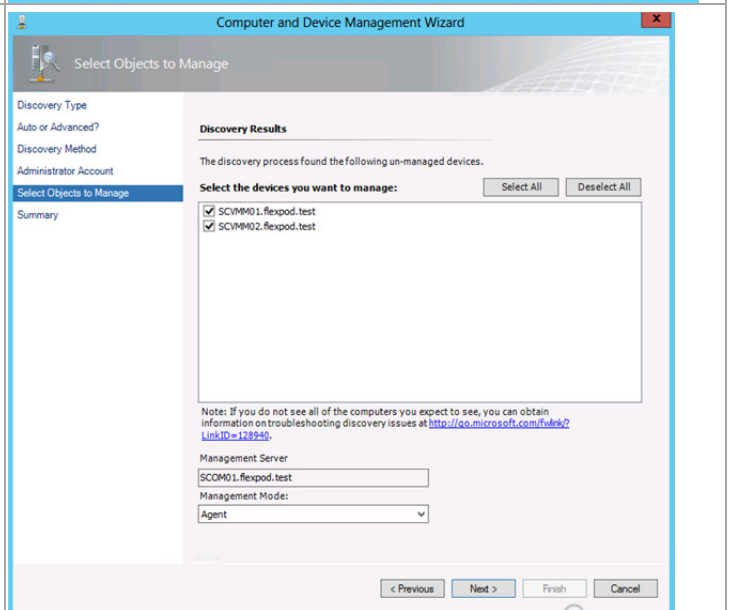
**Note:** You may also want to include the Hyper-V hosts as servers to be discovered. Remember that the Operations Manager Action account needs to be a member of the local administrators group.



In the **Administrator Account** dialog, if the account you are logged in with is a local administrator on the VMM servers then leave the default selection in place, if not then select the **Other user account** option and provide the credentials required to access Active Directory and perform discovery in your environment. Verify that the **This is a local computer account, not a domain account check box** is clear and click **Discover** to continue.

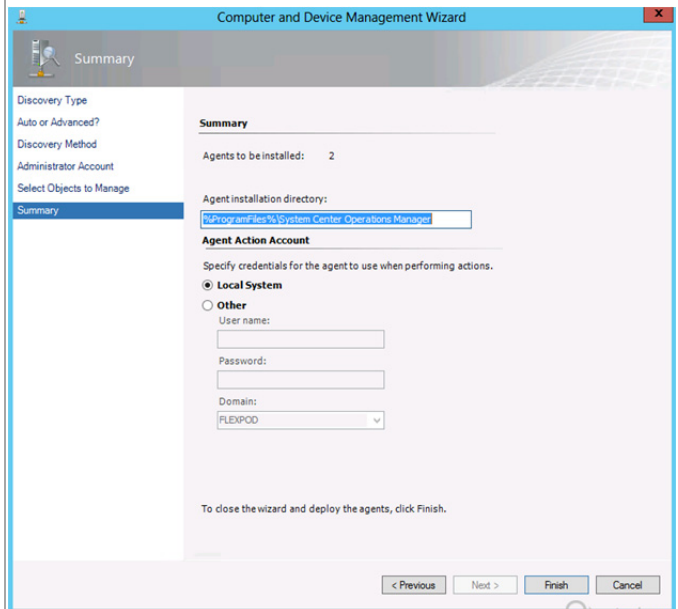


In the **Select Objects to Manage** dialog, review the Discovery Results and select the VMM server. From the **Management Mode** drop-down menu, select **Agent** and click **Next** to continue.

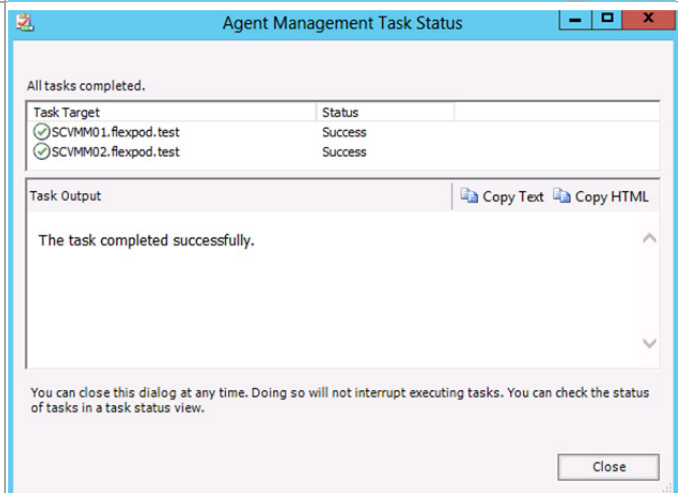




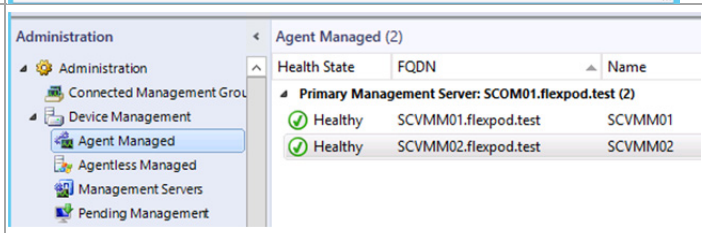
In the **Summary** dialog, accept the default **Agent installation directory** as `%ProgramFiles%\System Center Operations Manager`. In the **Agent Action Account** section, select the **Local System** option. When complete, click **Finish** to perform the agent installation.



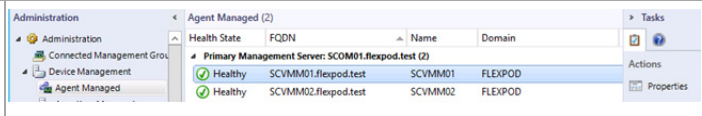
In the **Agent Management Task Status** dialog, verify that the agent installation completes successfully. When successful, click **Close** to complete the operation.



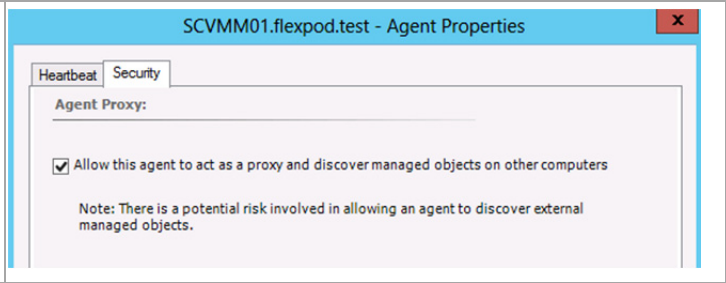
The next step is to enable the Operations Manager agent deployed to the Virtual Machine Manager management server to be a proxy agent. In **Operations Manager** console, navigate to the **Administration** workspace, expand the **Device Management** node and select the **Agent Managed** view.  
*Note: It can take a few minutes for the Health State to transition from Not Monitored to Healthy.*



In the **Agent Managed** pane, select the agent associated with the VMM Management Server and click **Properties** in the task pane.



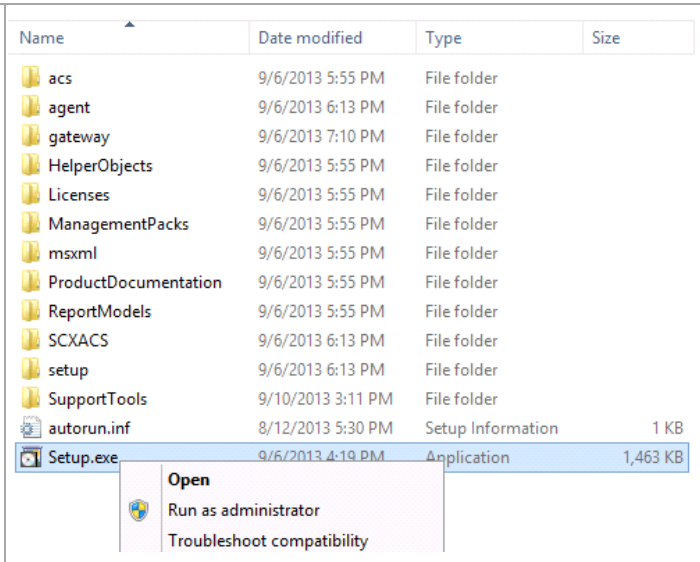
In the **Agent Properties** dialog, select the **Security** tab. Verify that the **Allow this agent to act as a proxy and discover managed objects on other computers** check box is selected then click **OK** to save the changes.  
Repeat for the other SCVMM server.



## Install Operations Manager Console on the Virtual Machine Manager Management Server

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

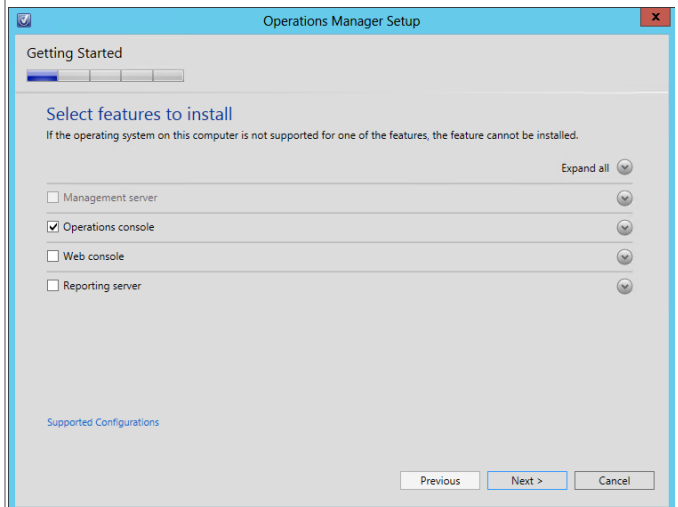
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



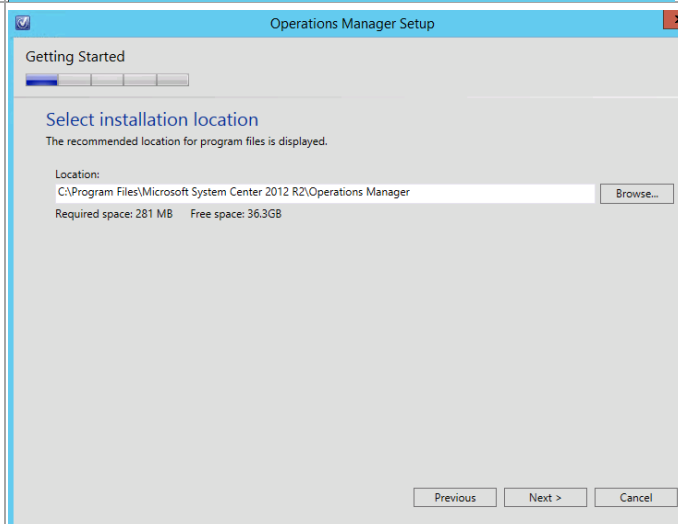
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



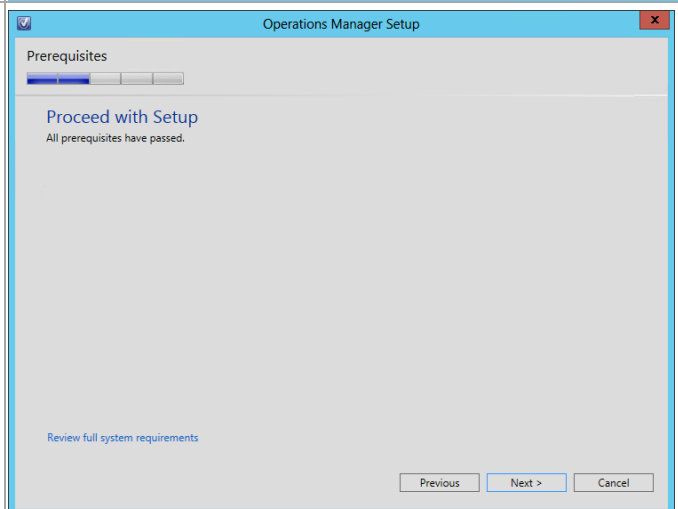
In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.



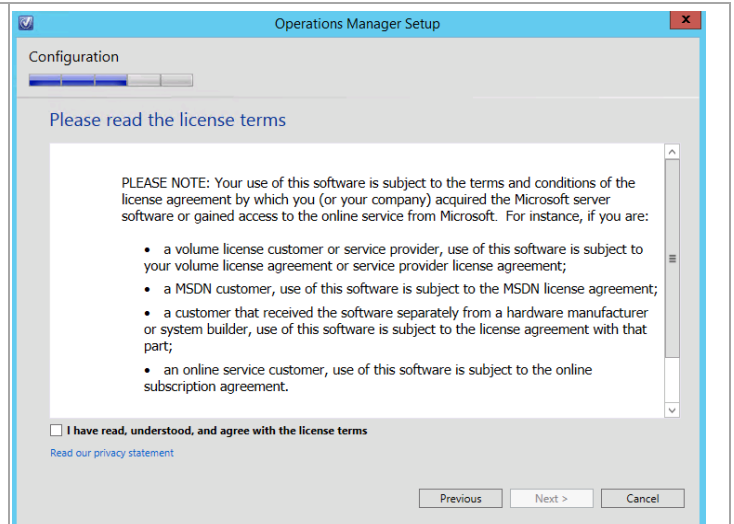
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012 R2\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



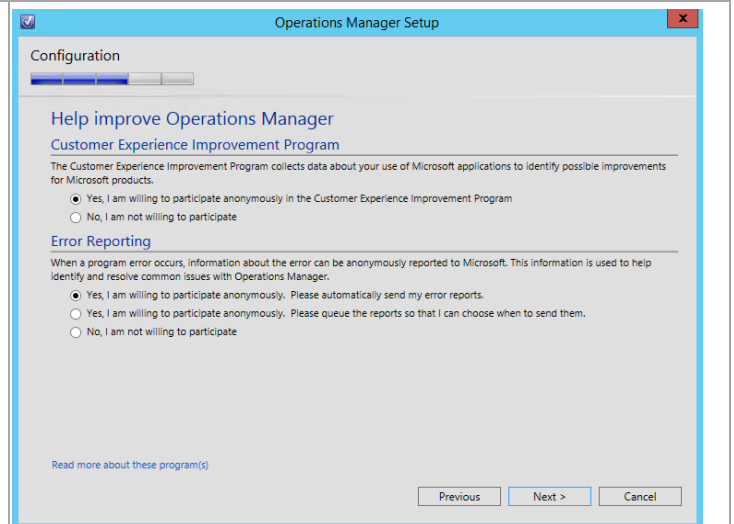
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.



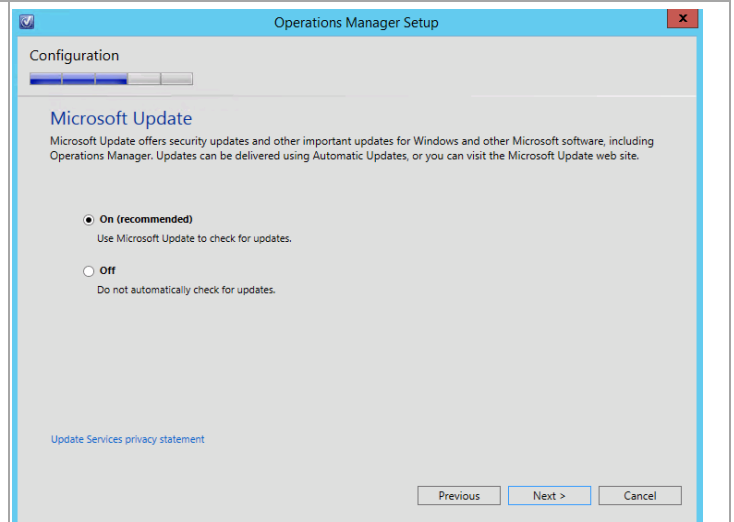
The **Help Improve System Center 2012 – Operations Manager** dialog provides options for participating in various product feedback mechanisms. These include:

- Customer Experience Improvement Program
- Error Reporting

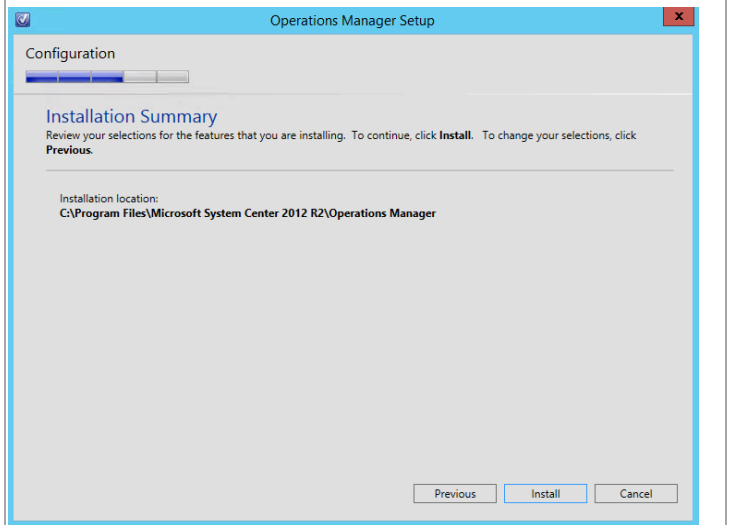
Select the appropriate option based on your organization's policies and click **Next** to continue.



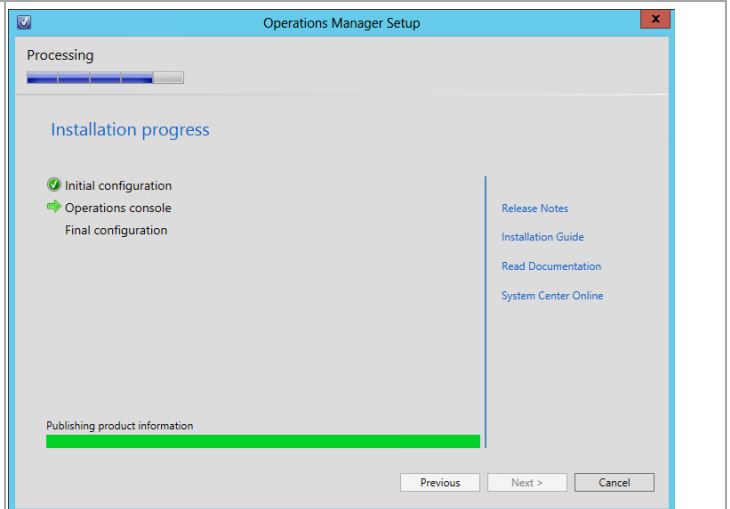
To use Microsoft Update to check for updates, select the radio button by **On**. Click **Next** to continue.



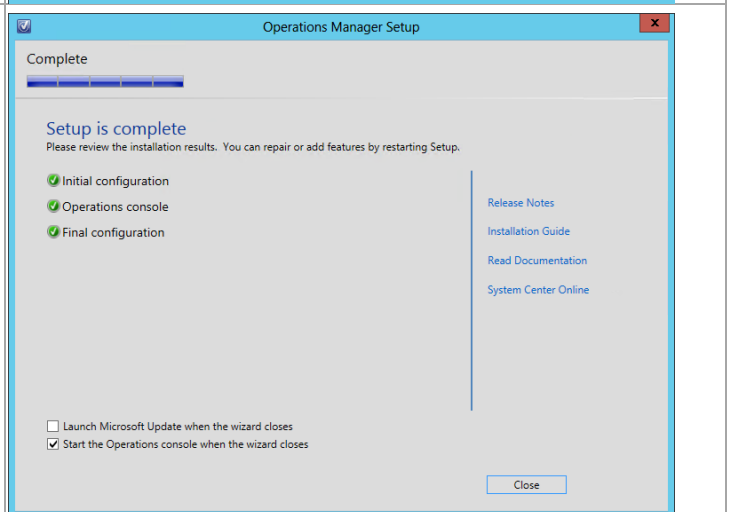
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



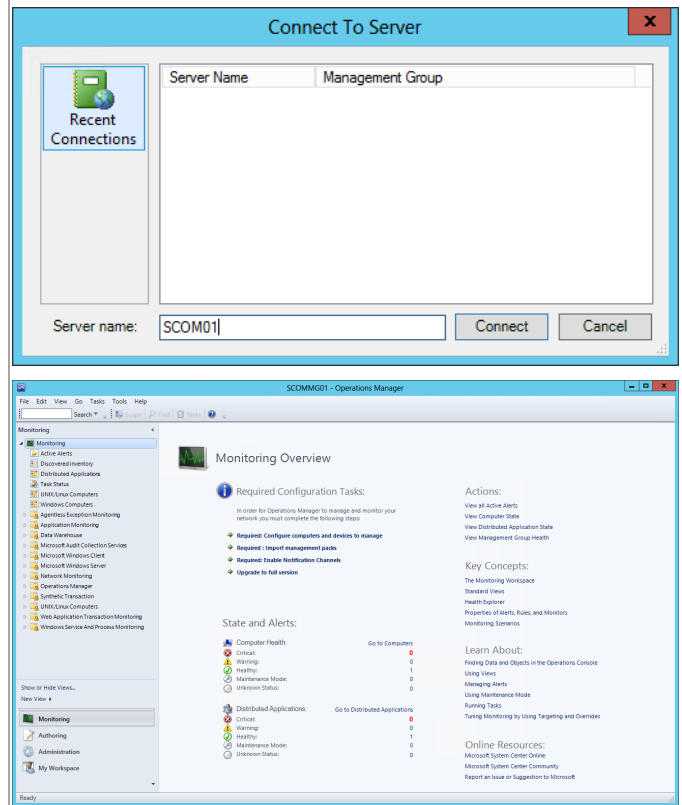
The wizard will display the progress while performing the installation.



When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Management console when the wizard closes** check box is selected and click **Close** to complete the installation.



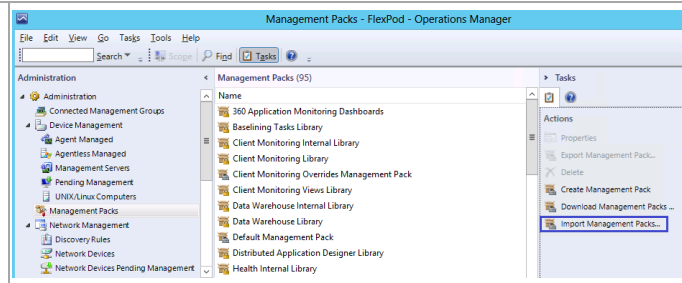
When completed, the **Operations Manager console** will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



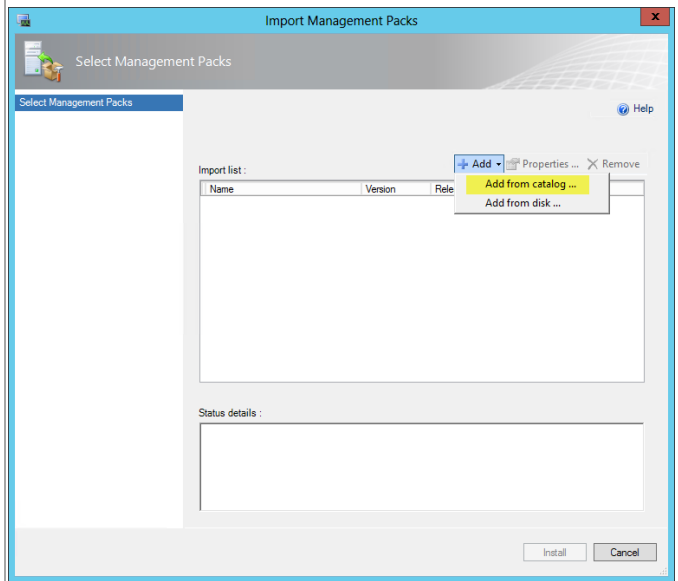
## Download and Import the Required Prerequisite Management Packs in Operations Manager

Perform the following steps on the **Operations Manager** virtual machine.

In the **Operations Manager** console, navigate to the **Administration** pane and select the **Management Packs** node. In the **Actions** pane, click **Import Management Packs...**



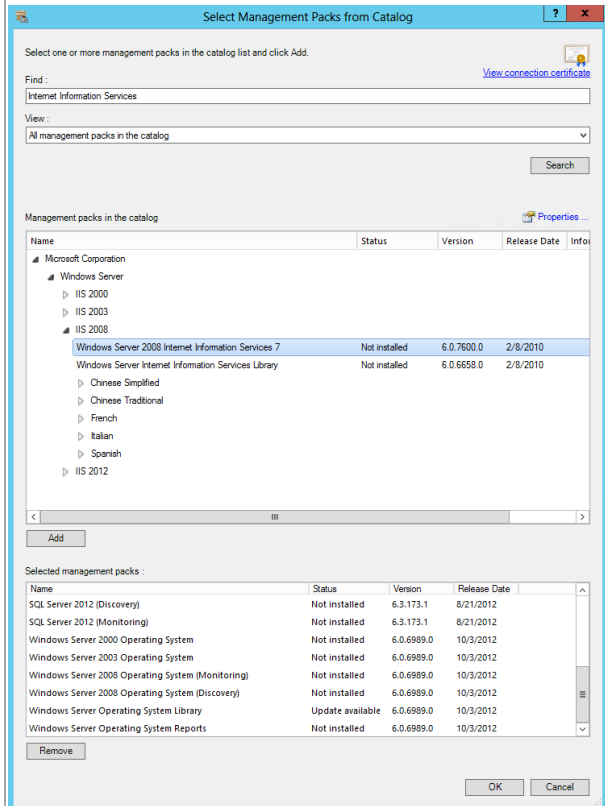
In the **Select Management Packs** dialog, click the **Add** button and select **Add from catalog...** in the drop-down menu.



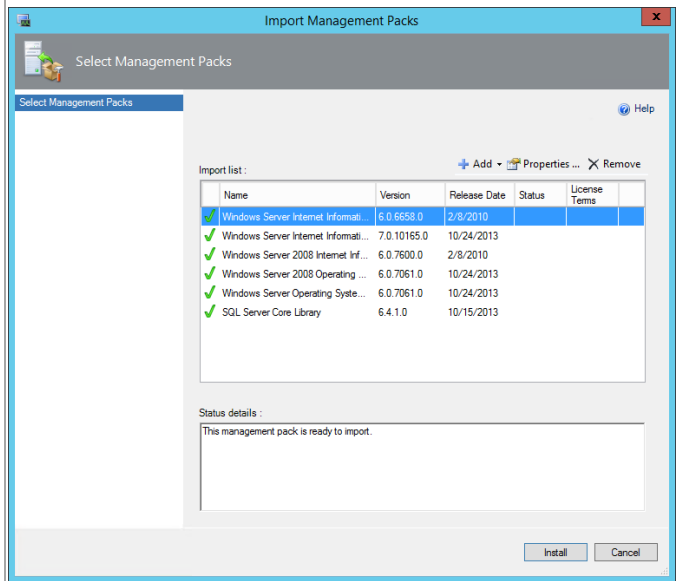
In the **Select Management Packs from Catalog** dialog, find and add the following management packs (in this order):

- Windows Server Internet Information Services Library
- Windows Server Internet Information Services 2003
- Windows Server 2008 Internet Information Services 7
- Windows Server 2008 Operating System (Discovery)
- Windows Server Operating System Library
- SQL Server Core Library
- 

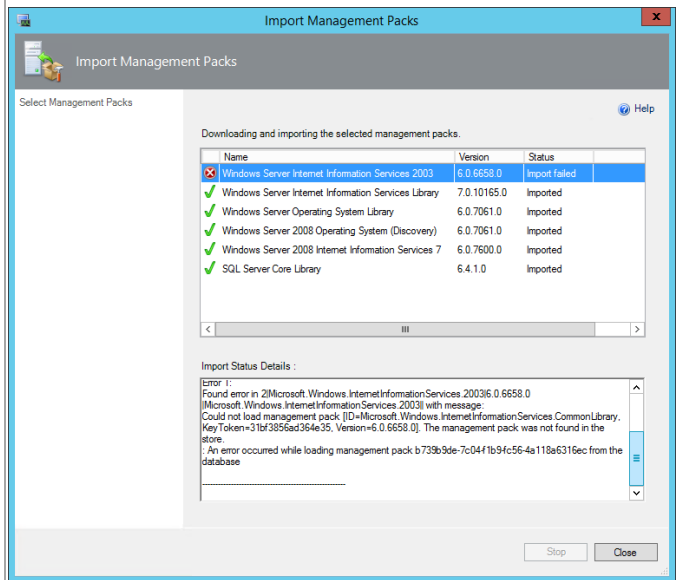
When added, click **OK** to continue.



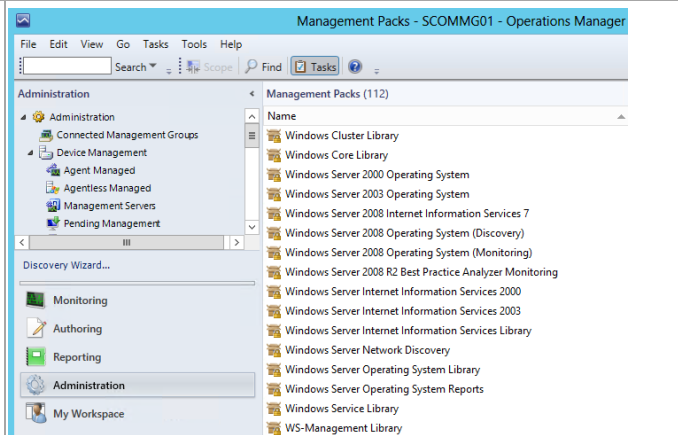
At the **Select Management Packs** dialog, click **Install** to import the selected management packs.



The management packs will download and import into Operations Manager. When complete, verify that the imports were successful and click **Close** to exit the Import Management Packs wizard.



In the **Operations Manager** console, go to the **Administration** workspace and verify the previously selected management packs are now installed.



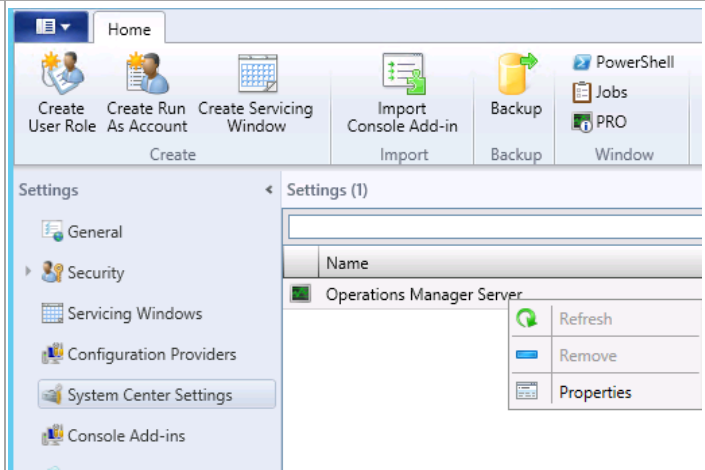


## Perform Virtual Machine Manager and Operations Manager Integration

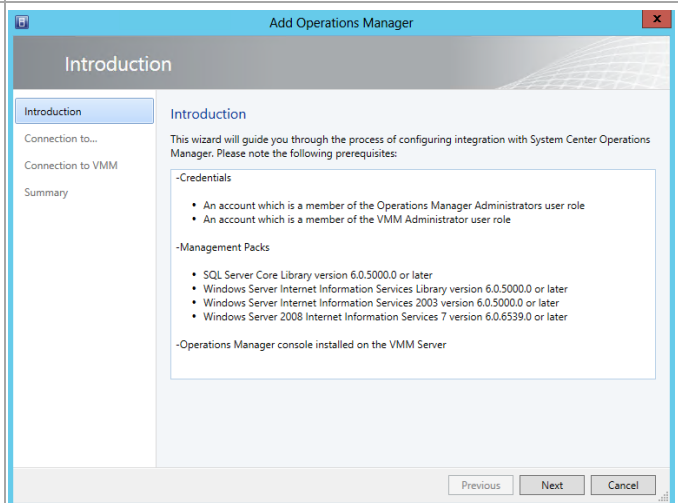
When all pre-requisite configurations and installations are performed, the integration of Virtual Machine Manager and Operations Manager can be completed.

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

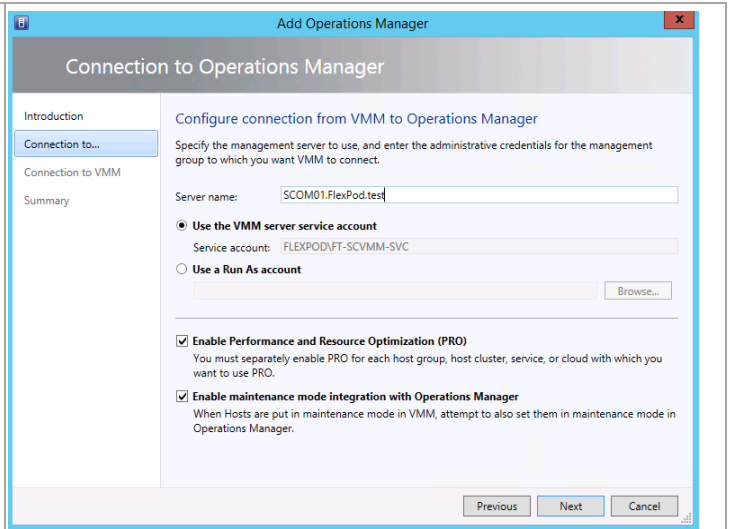
In the **Virtual Machine Manager** console, navigate to **Settings** pane and select **System Center Settings**, right-click **Operations Manager Server** and select **Properties** from the context menu.



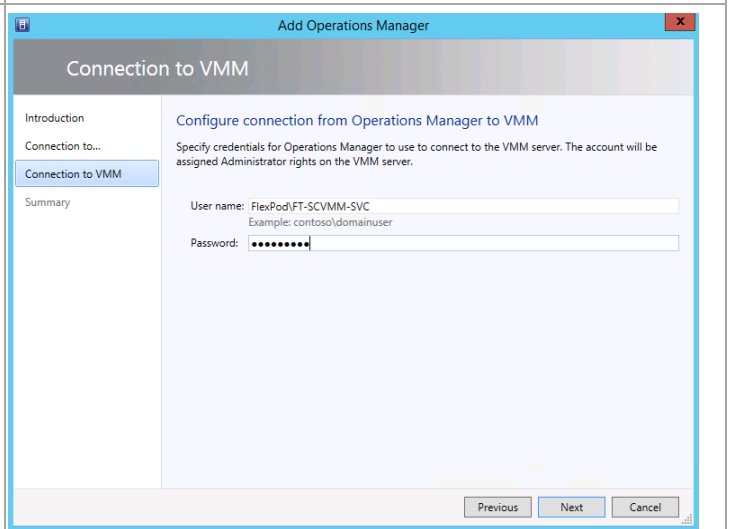
The **Add Operations Manager** dialog will appear. In the **Introduction** dialog, verify the prerequisites have been met and click **Next** to continue.



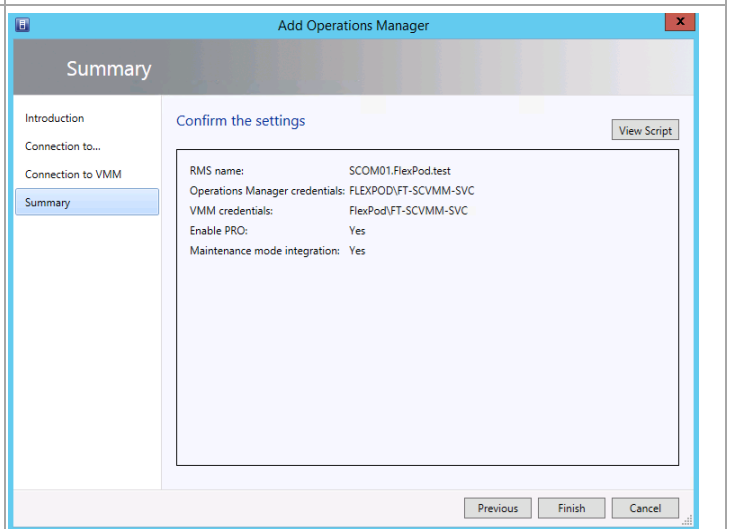
In the **Connection to Operations Manager** dialog, type the FQDN of the Operations Manager server in the **Server name** text box. Select the **Use the VMM server service account** option. Select the **Enable Performance and Resource Optimization (PRO)** and **Enable maintenance mode integration with Operations Manager** check boxes. When complete, click **Next** to continue.



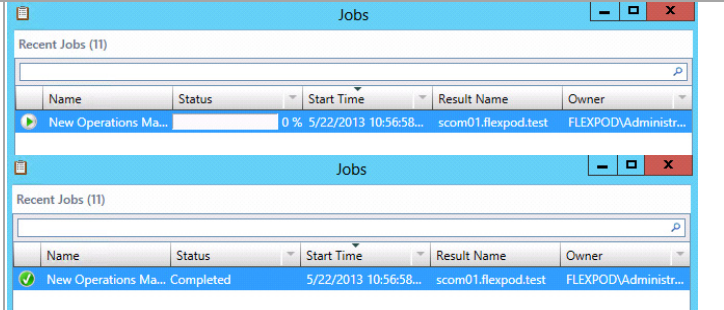
In the **Connection to VMM** dialog, specify the VMM service account credentials in the **User name** and **Password** text boxes and click **Next** to continue.



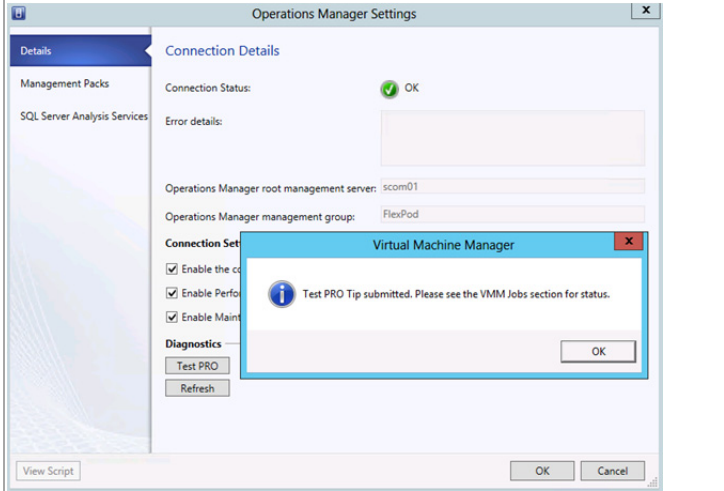
In the **Summary** dialog, verify the options selected click **Finish** to begin the Operations Manager integration process.



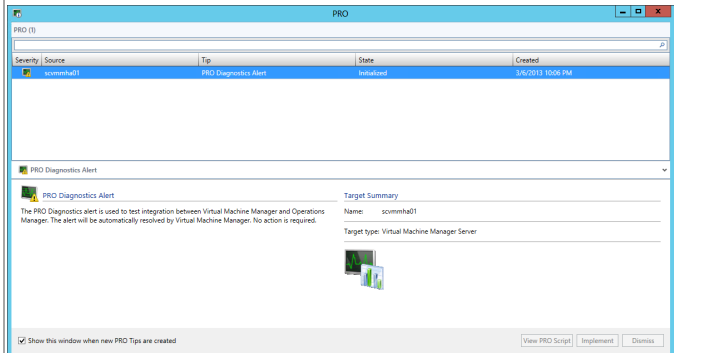
The **Jobs** pane will appear. Before moving forward, wait for the job to complete successfully.



In the Virtual Machine Manager console, navigate back to **Settings** then select **System Center Settings** and double-click **Operations Manager Server**. The Operations Manager Settings dialog will appear. In the **Details** pane, click the **Test PRO** button.



As part of the test, PRO will generate a diagnostics alert.



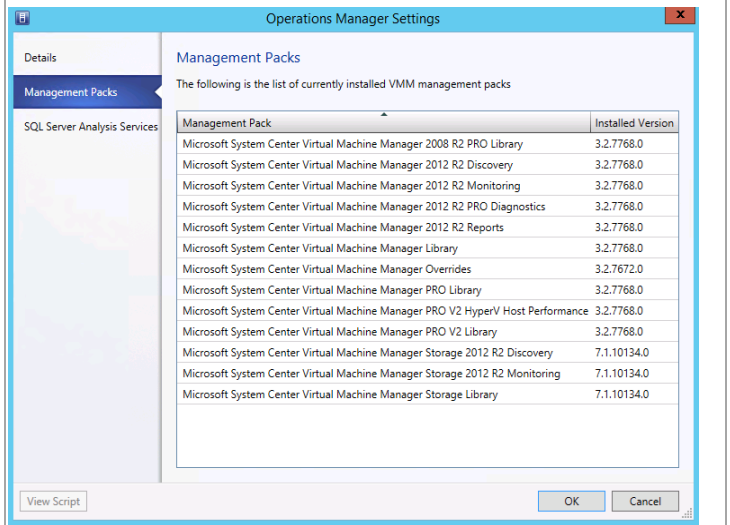
After a few minutes, verify that the PRO test is successful. Navigate to the Jobs pane and verify the PRO jobs completed successfully.

Name	Status	Start Time	Result Name
Set state of a PRO tip	Completed	11/6/2014 12:45:52 PM	PRO Diagnostics Alert
Set state of a PRO tip	Completed	11/6/2014 12:45:51 PM	PRO Diagnostics Alert
PRO diagnostics	Completed	11/6/2014 12:45:38 PM	PRO Diagnostics Alert

Step	Name	Status	Start Time
1	PRO diagnostics	Completed	11/6/2014 12:45:38 PM
1.1	Create new PRO tip	Completed	11/6/2014 12:45:39 PM
1.2	Implement the fix for a PRO tip	Completed	11/6/2014 12:45:43 PM
1.2.1	Invoke remediation	Completed	11/6/2014 12:45:43 PM
1.2.2	Wait for remediation	Completed	11/6/2014 12:45:44 PM

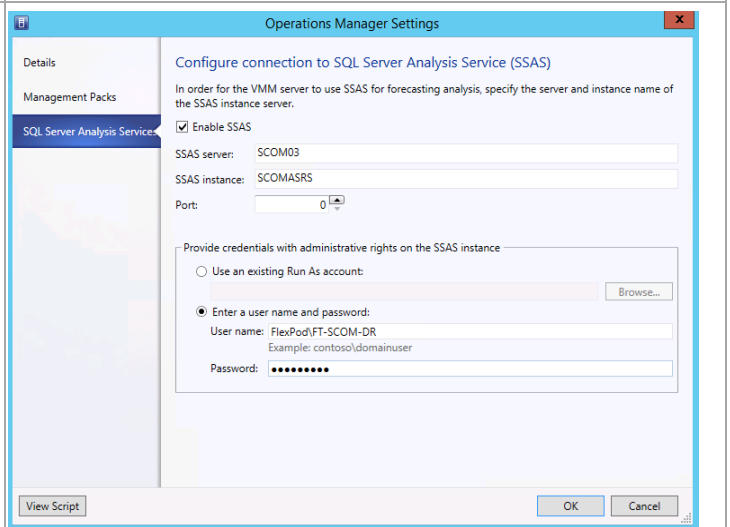
In the **Management Packs** dialog, verify all Virtual Machine Manager Management Packs were successfully installed.



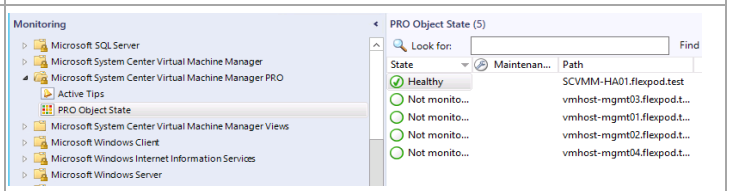
In the **Configure connection to SQL Server Analysis Services (SSAS)** dialog, provide the following information. Select the **Enable SSAS** check box. Provide the following information on the text boxes provided:

- **SSAS server** – *Specify the Operations Manager database server instance.*
- **SSAS Instance** – *Specify the SSAS instance name created earlier.*
- **Port** - *Leave the default value of 0.*

In the **Provide credentials with administrative rights on the SSAS instance**, select the **Enter a user name and password** option and provide the supplied credentials for the Operations Manager Data Reader account. Click **OK** to save these settings.



On the **Operations Manager** console, go to **Monitoring** workspace, navigate to the **Microsoft System Center Virtual Machine Manager PRO** node and select **PRO Object State**. Verify the VMM server is listed with a health state other than “*Not Monitored*.”



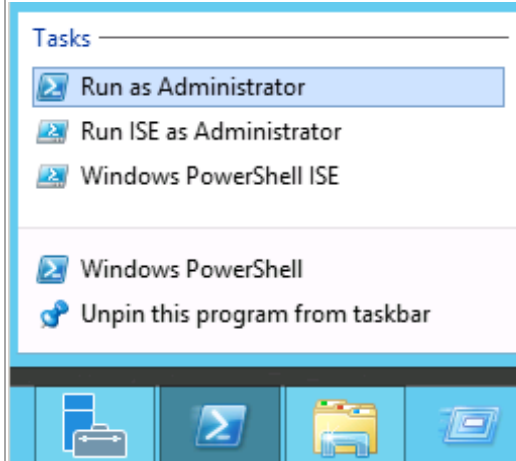
## 20.5 Install NetApp Management Pack

The following steps must be completed in order to install and configure the NetApp OnCommand SCOM Management Pack.

## Install and Configure SNMP

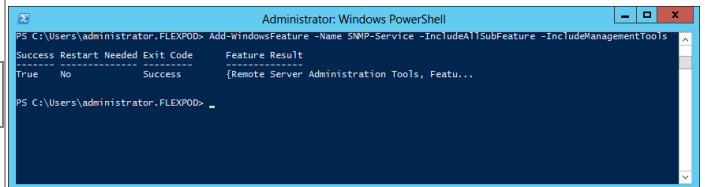
Perform the following steps on each **Operations Manager management server** virtual machine.

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

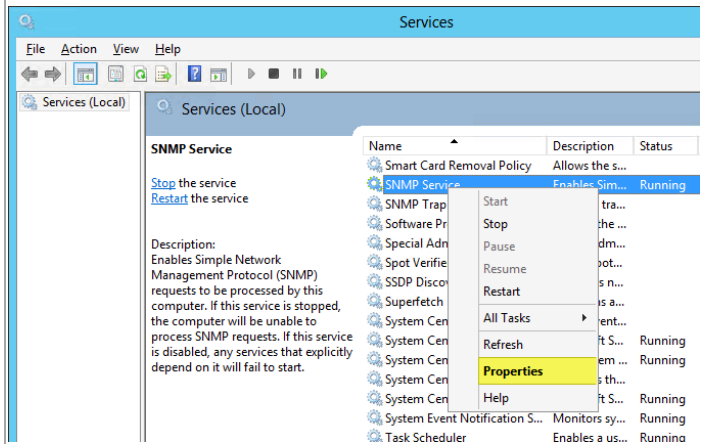


Add the SNMP feature by entering the following command:

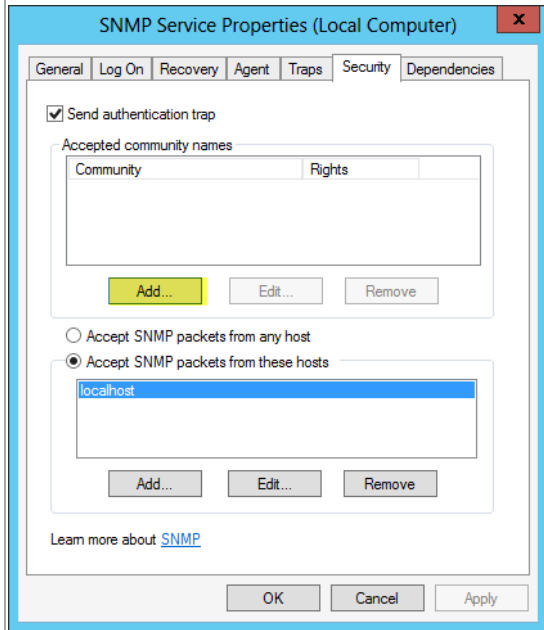
```
Add-WindowsFeature -Name SNMP-Service -IncludeAllSubFeatures -IncludeManagementTools
```



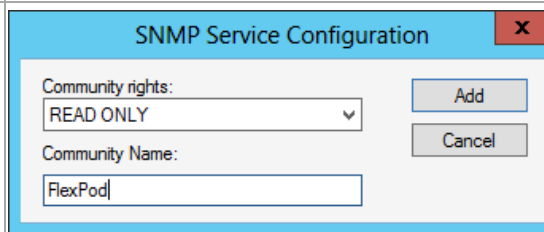
Open the Services management console, right-click **SNMP Service**, and select **Properties**



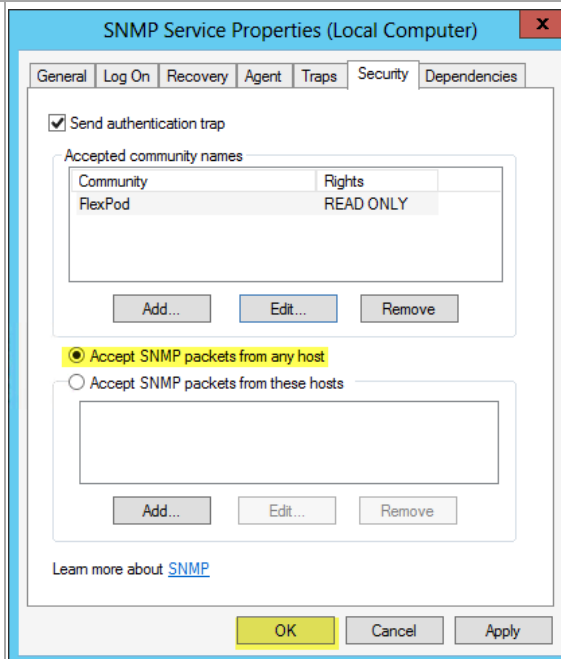
On the SNMP Service Properties page, select the **Security** tab, and under Accepted Community Names, click **Add**.



In the SNMP Service Configuration dialog box, set the following values and then click **Add**:



On the Security tab, select **Accept SNMP Packets from any Host**. Click **OK** to complete the configuration.



## Install NetApp OnCommand Plugin Management Pack

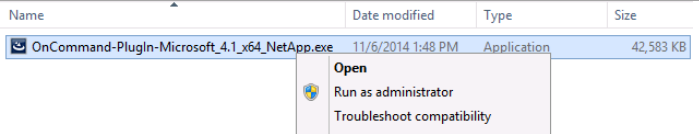
Perform the following steps on each **Operations Manager management server** virtual machine.

On a domain controller create this domain account <DOMAIN>\FT-OCPM-SVC. Add it to the local administrator group on the servers shown to the right.

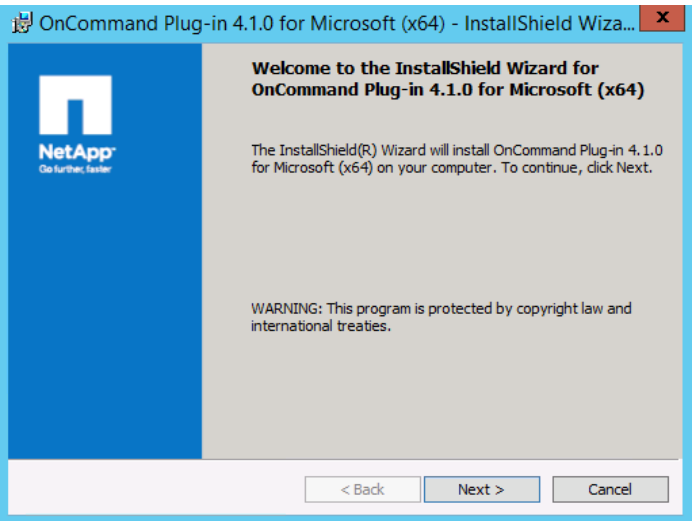
This account will need:

- Full admin permissions on all Hyper-V hosts to be managed.
- Full admin on the Operation Management servers.

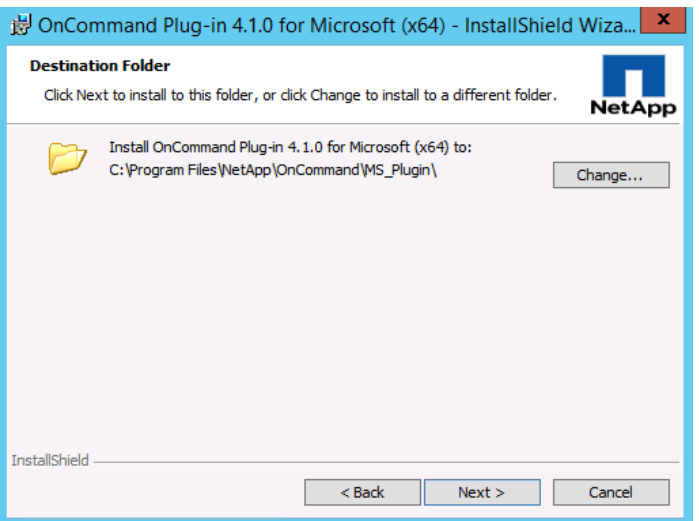
Log in to the SCOM management server, right-click the **OCPM 4.1 installation package**, and select **Run as Administrator** to start the OCPM installation wizard.



On the Welcome Page click **Next**.

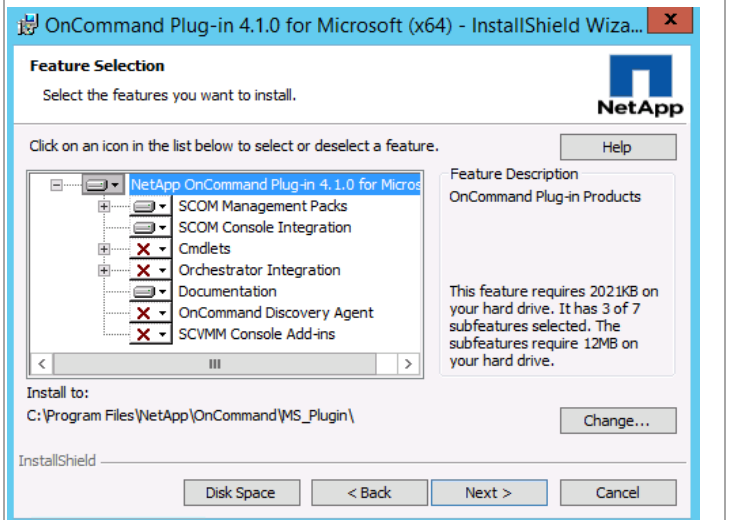


On the Destination Folder page, click **Next** to keep the default installation folder



On the Feature Selection page, select the following features and click Next:

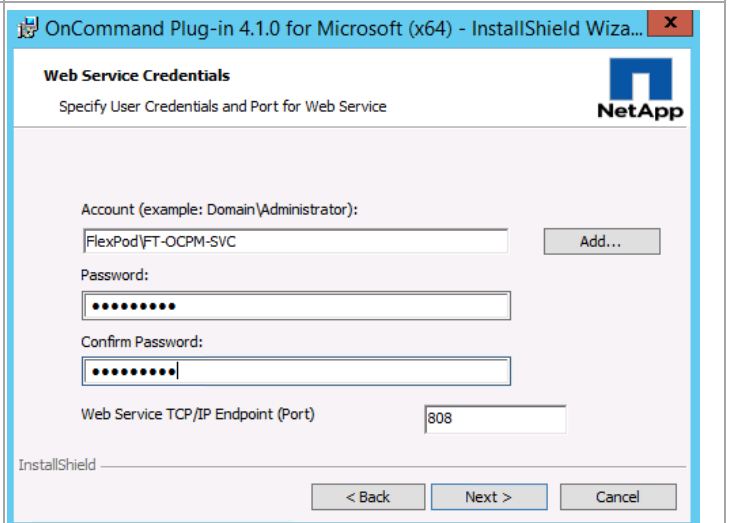
- SCOM Management Packs
- SCOM Console Integration
- Documentation



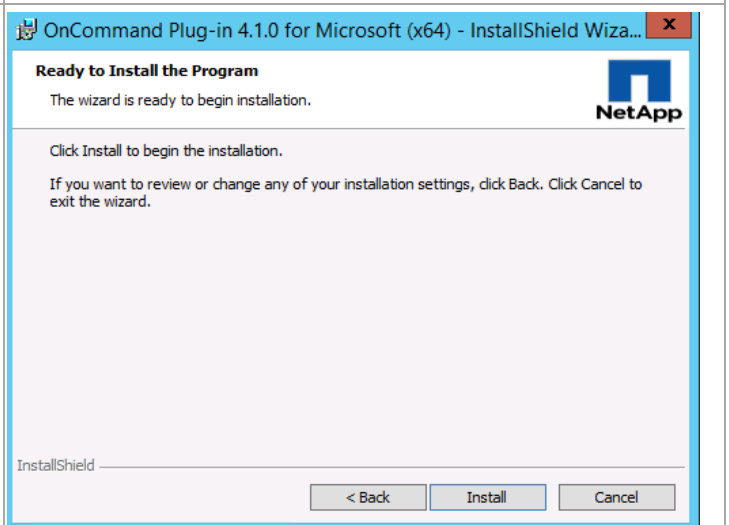
On the Web Service Credentials page, enter the following credentials and click Next:

- Account: Active Directory domain user account to be used for web service communication
- Password: Password of the domain user account
- 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

**Note:** All System Center servers running the OCPM web service must use the same port for communication.



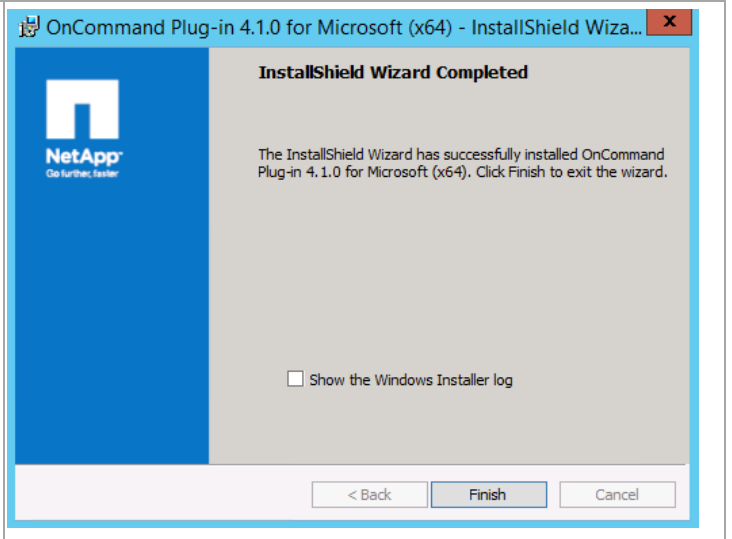
Click **Install** to continue the installation.





On the InstallShield Wizard Completed page, click **Finish** to complete the installation.

Restart the server.

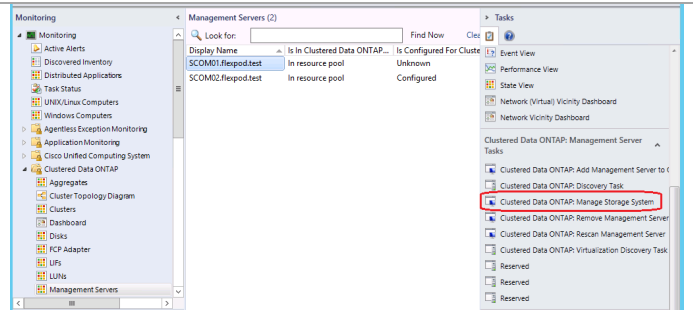


## Configure NetApp OnCommand Plugin Management Pack

Perform the following steps on one of the **Operations Manager** virtual machine.

In the **Operations Manager** console, navigate to the **Monitoring** pane and select the **Clustered Data ONTAP -> Management Server**

On the tasks pane select **Clustered Data ONTAP: Manage Storage System**

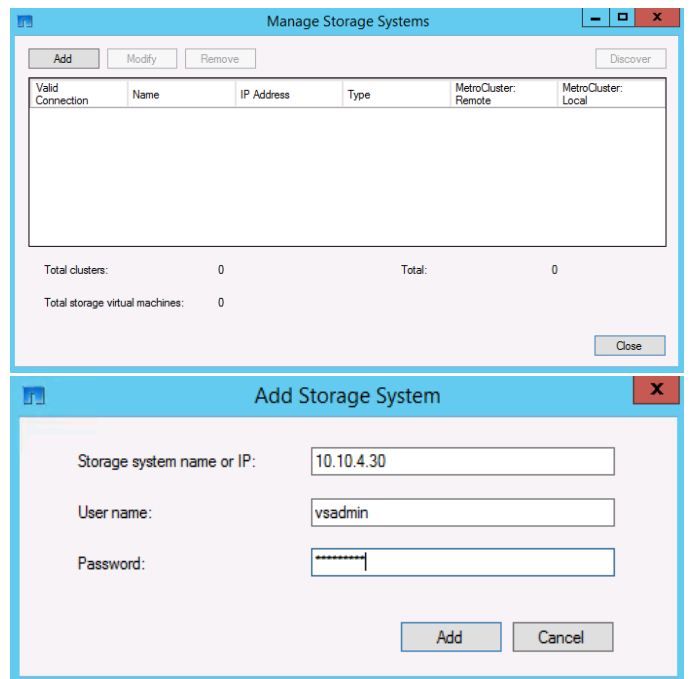


Click the **Add** button on the Manage Storage Systems.

In the resulting pop-up enter the following

- Enter the **Storage system name or IP**
- Enter the **User name**
- Enter the **Password**
- Click **Add**.

**Note:** It can take 15 Minutes to an hour to complete discovery once the credentials are saved.



## 20.6 Install the Cisco UCS Management Pack

Verify the following Components are installed in the virtual machine where management pack will be installed

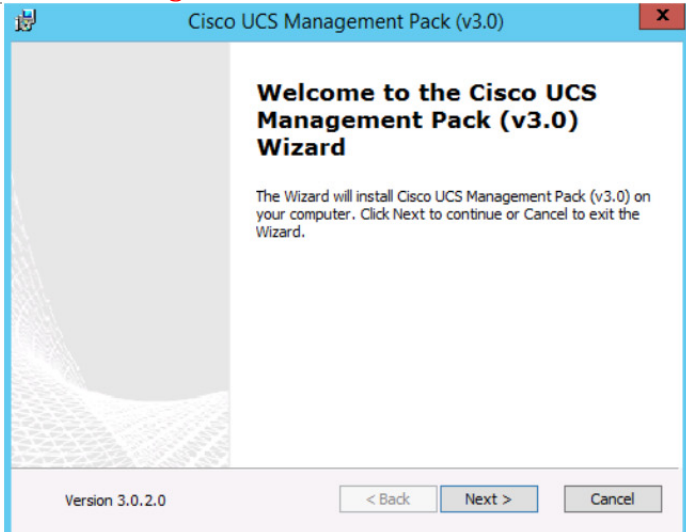
- Windows PowerShell 2.0
- .NET Framework 4
- System Center 2012 R2 Operations Manager

Cisco UCS Manager Management Pack for Microsoft System Center Operations Manager can be downloaded at the following link:

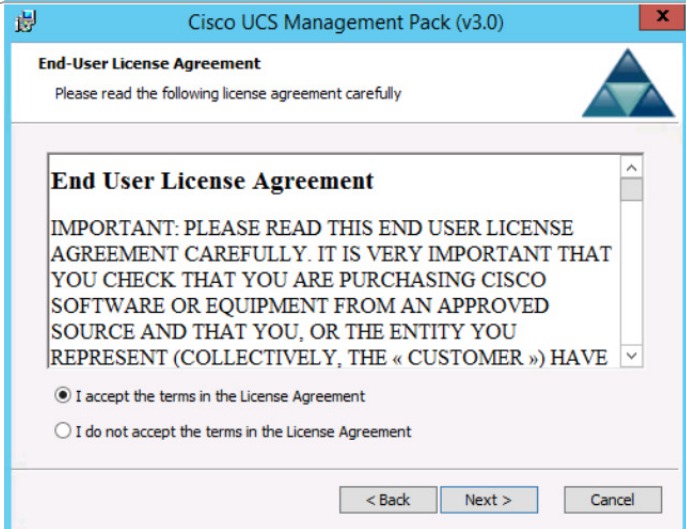
<http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=283034298&release=3.0.2&reind=AVAILABLE&rellifecycle=&reltype=latest>

**Perform the following steps on the first Operations Manager virtual machine.**

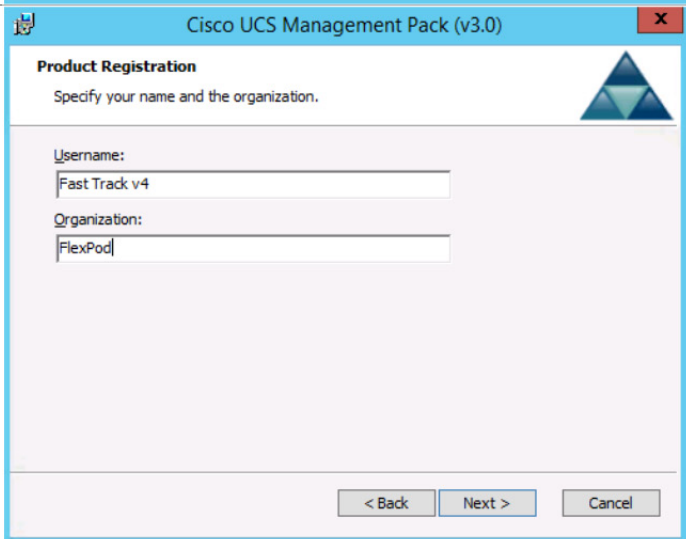
Make sure the Operations Manager console is not running.  
Launch the Management Pack Installer. The **Setup Wizard** screen appears.



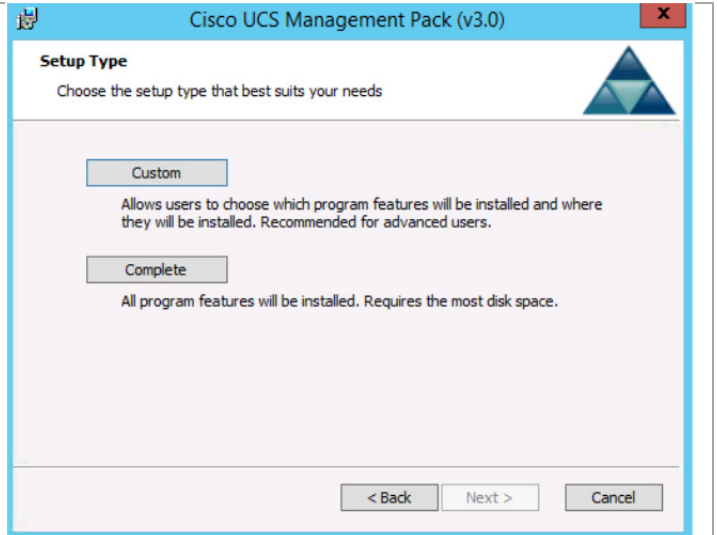
Click the **Next** button. The **License Agreement** screen appears. Select **I agree** radio button and click the **Next** button.



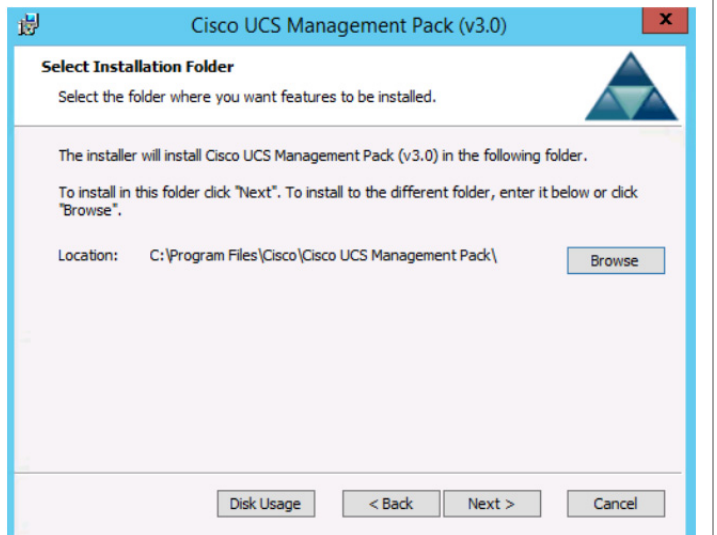
Enter **Username** and **Organization** and click **Next**. Username is a required field.



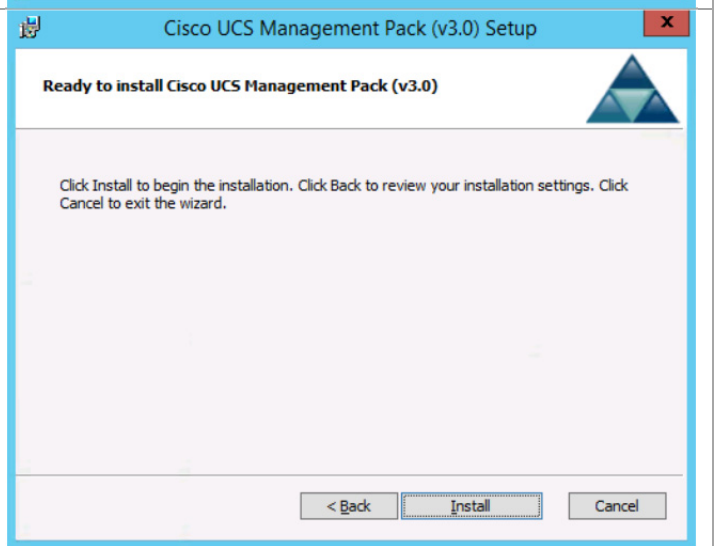
Select the **Complete** installation option.



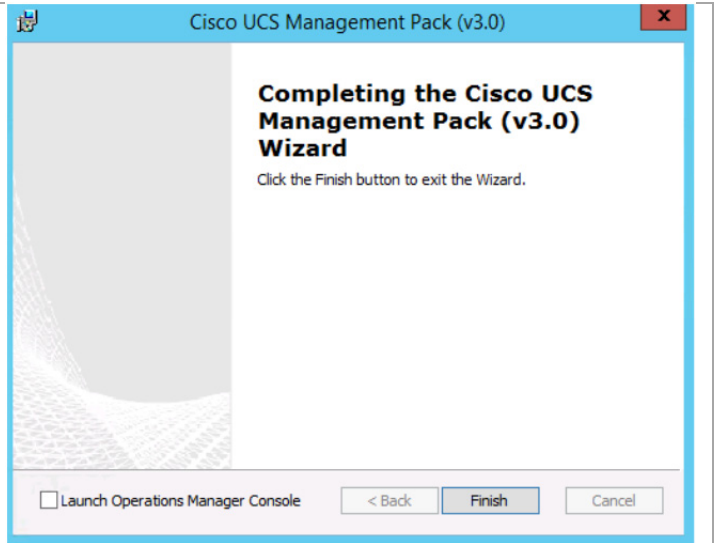
The **Select Installation Folder** Screen appears. Specify the folder location to install the Management Pack, in the **Location** field and click the **Next** button.



Click the **Install** button to start the installation.



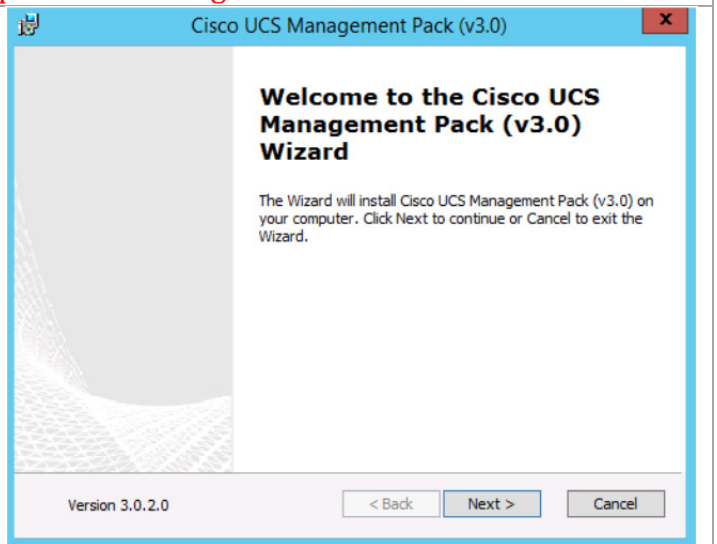
After successful installation of Cisco UCS Management Pack the **Installation Complete** screen appears. Click the **Finish** button to exit and launch the Operations Manager Console.



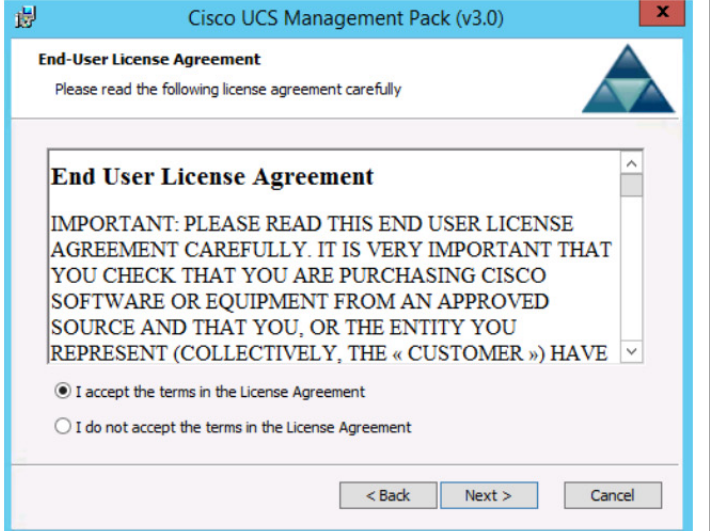
## Install on Second Operations Manager Virtual Machine

**Perform the following steps on the second Operations Manager virtual machine**

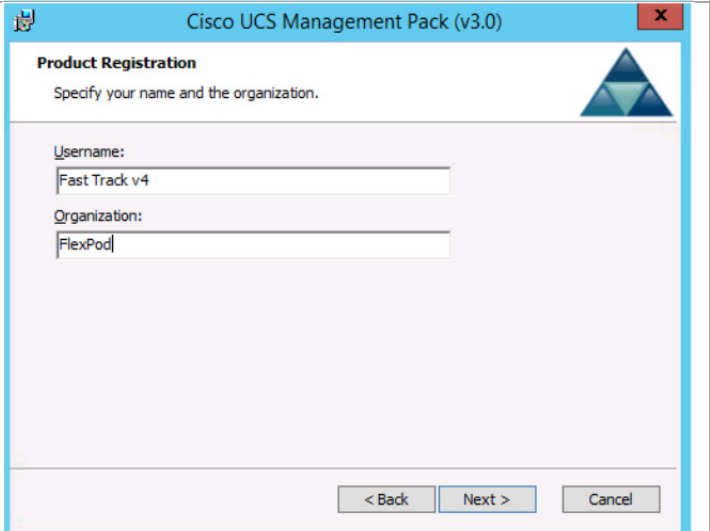
Make sure the Operations Manager console is not running.  
Launch the Management Pack Installer. The **Setup Wizard** screen appears.



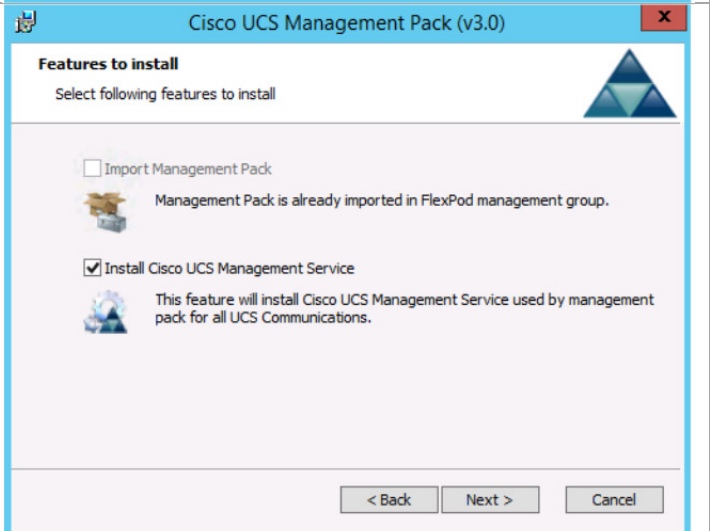
Click the **Next** button. The **License Agreement** screen appears. Select **I agree** radio button and click the **Next** button.



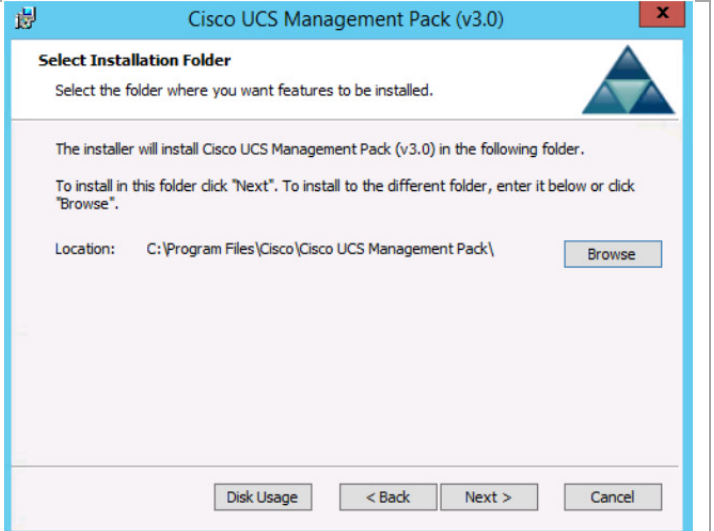
Enter **Username** and **Organization** and click **Next**. Username is a required field.



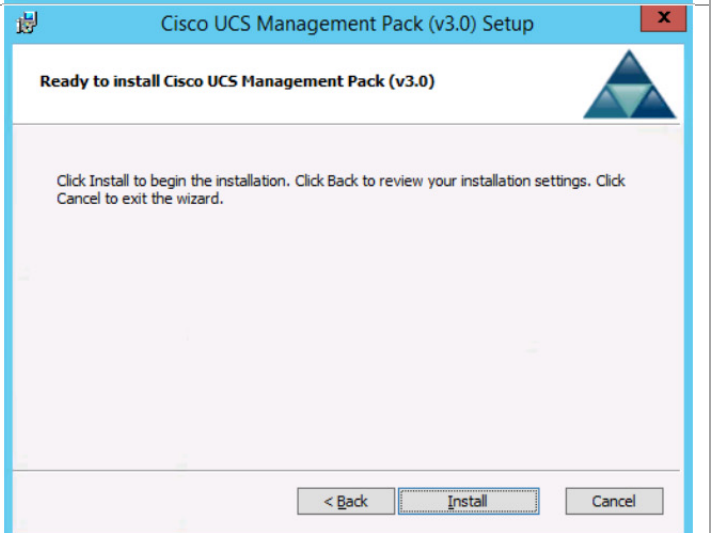
Select the **Install Cisco UCS Management Service** installation option. Click **Next** to continue.



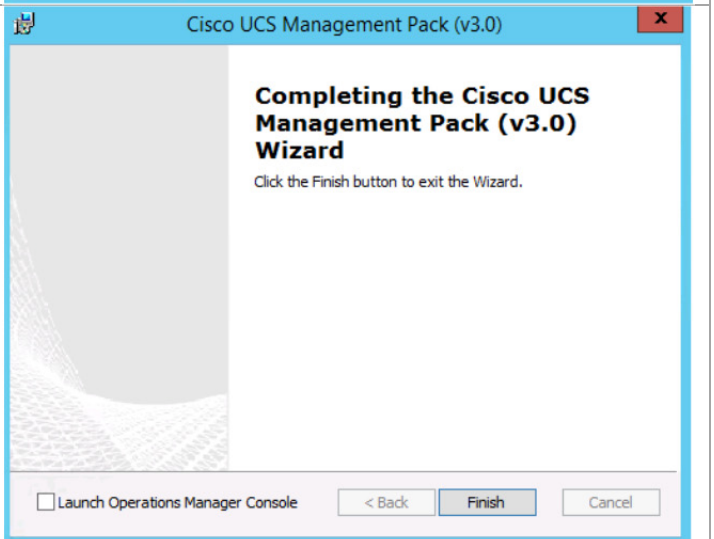
The **Select Installation Folder** Screen appears. Specify the folder location to install the Management Pack, in the **Location** field and click the **Next** button.



Click the **Install** button to start the installation.



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.



## Add Firewall Exceptions to the Cisco UCS Management Service

After you have installed the Cisco UCS management pack, you ensure certain firewall rules are enabled on every management server hosting the Cisco UCS Management Service. Issue the following PowerShell commands to create the inbound and outbound rules. These rules must be created on each Operations Manager server.

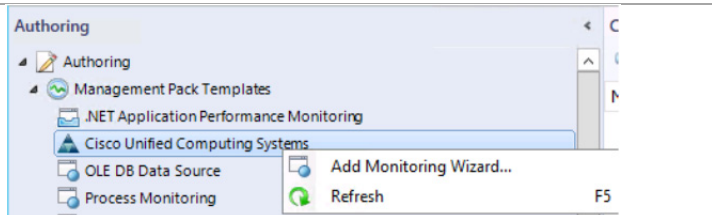
```
Set-NetFirewallRule -Name "FPS-ICMP4-ERQ--n" -Enabled True -Profile Any
Set-NetFirewallRule -Name "FPS-ICMP6-ERQ--n" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteSvcAdmin-In-T-P" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteSvcAdmin-RPCSS-In-T-P" -Enabled True -Profile Any
```

## Configuring SCOM to Monitor Cisco Unified Computing System

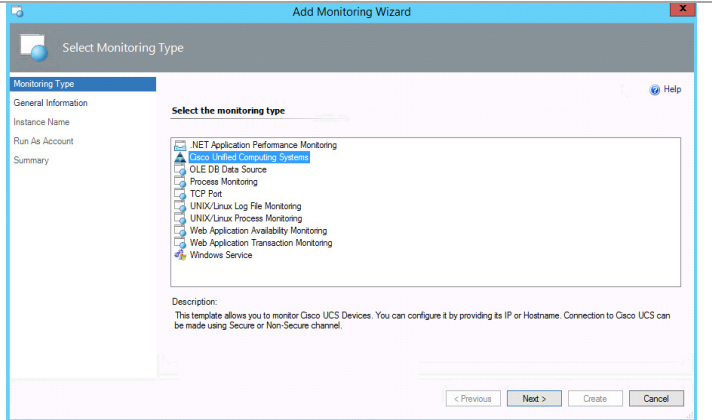
After the Cisco UCS Management Pack is successfully installed on the Operation Manager virtual machine it must be configured for accessing configuration and event data on the Cisco Unified Computing System. The following procedures provide guidance for this process.

Perform the following steps on the first Operations Manager virtual machine

In the **Authoring** column, expand **Management Pack Templates** and select **Cisco Unified Computing Systems**. Right-click and select the **Add Monitoring Wizard**.



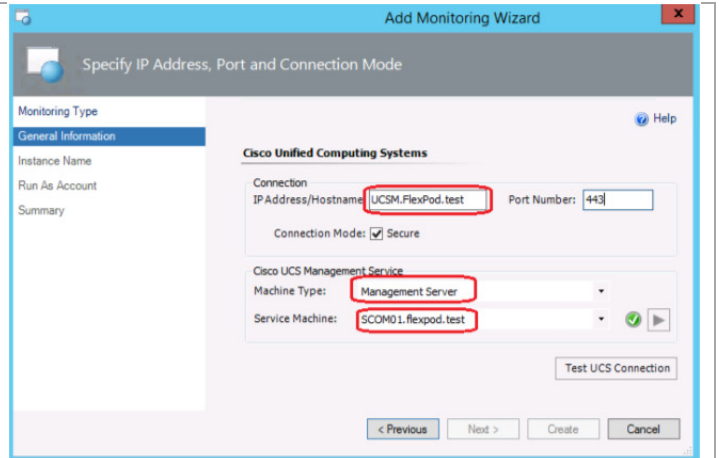
The **Select Monitoring Type** screen appears. Select **Cisco Unified Computing Systems** as the monitoring type and click the **Next** button.



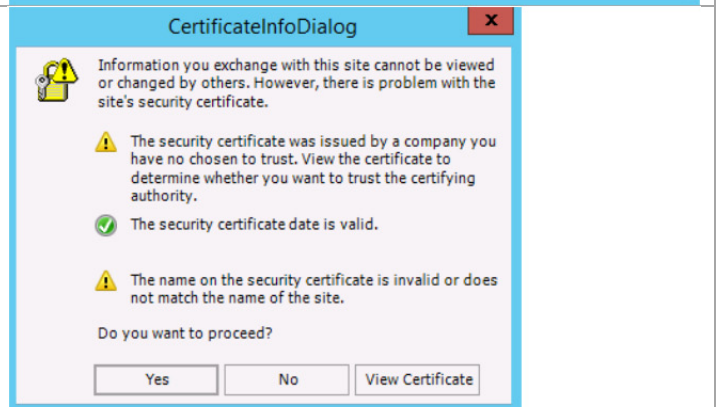


The **General Information** screen appears. Specify **IP Address/Hostname** of the UCS domain, **Port Number**, and **Connection Mode**. For **Machine Type** select **Management Server** from the drop-down list. For **Service Machine** select the server on which you are installing this.

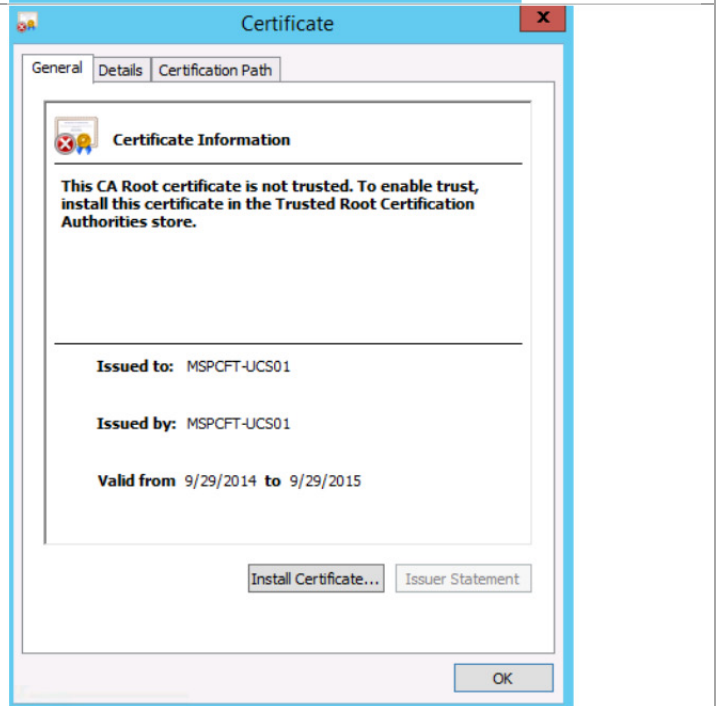
Click the **Test connection** button.



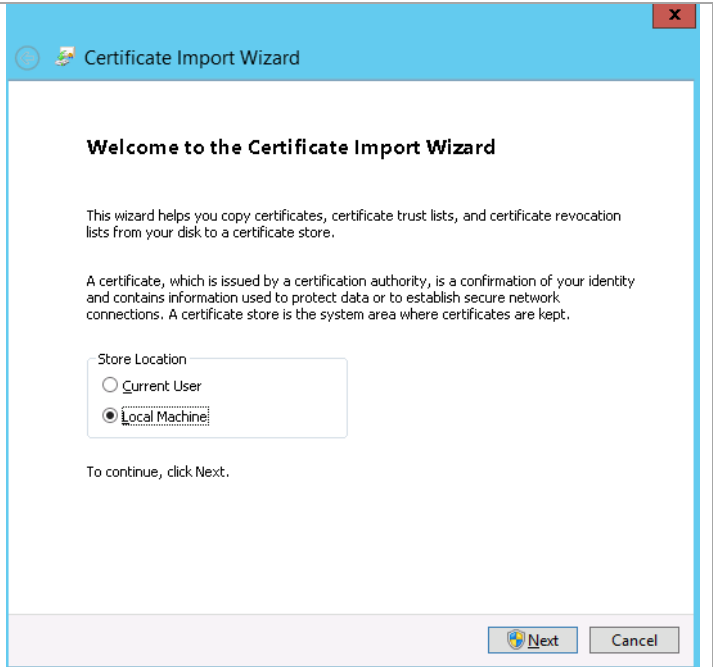
You will receive a security alert due to an unrecognized certificate. Click **View Certificate**.



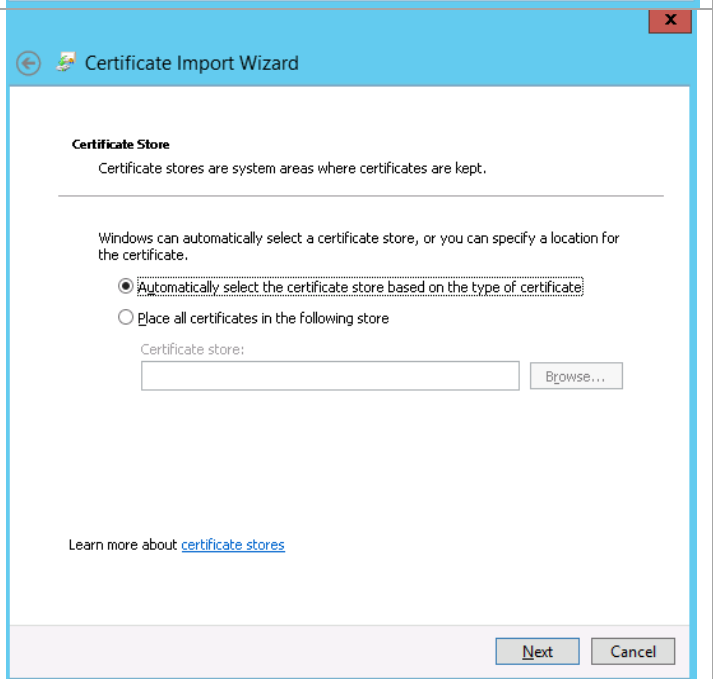
Click **Install Certificate**.



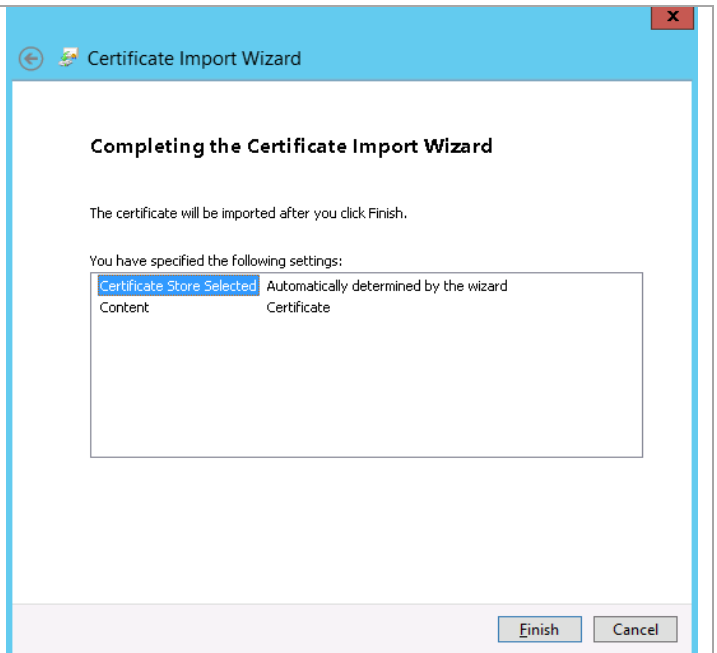
Select **Local Machine** and click **Next**.



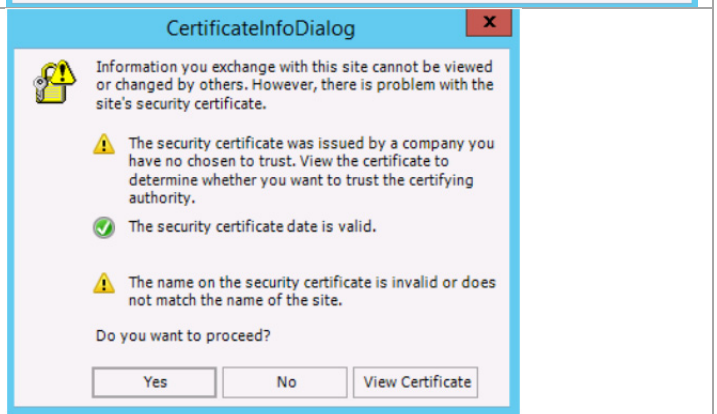
Select the option **Automatically select the certificate store based on the type of certificate** and click **Next**.



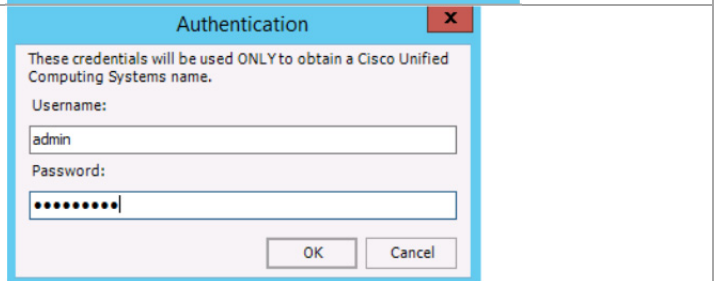
Select the default location and click **Finish**.



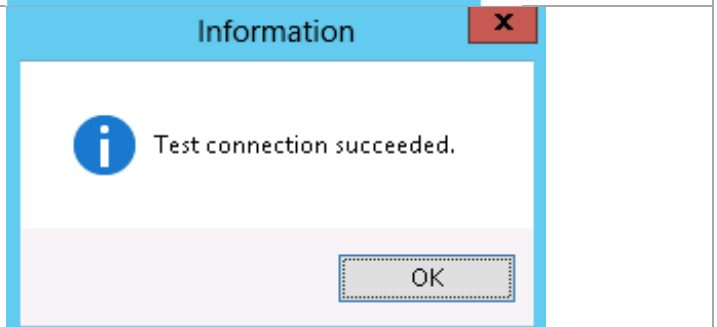
Click **Yes** to proceed.



Enter the **Cisco UCS Manager account and password**, then click **OK**.



Click **OK** to close the information window.



Click **Next** to proceed.

The screenshot shows the 'Add Monitoring Wizard' window with the title 'Specify IP Address, Port and Connection Mode'. On the left, a navigation pane lists 'Monitoring Type', 'General Information', 'Instance Name', 'Run As Account', and 'Summary'. The 'General Information' section is active. The main area is titled 'Cisco Unified Computing Systems' and contains the following fields: 'Connection' with 'IP Address/Hostname' set to 'UCSM.FlexPod.test' and 'Port Number' set to '443'; 'Connection Mode' with 'Secure' checked; 'Cisco UCS Management Service' with 'Machine Type' set to 'Management Server' and 'Service Machine' set to 'SCOM01.flexpod.test'. A 'Test UCS Connection' button is at the bottom right. Navigation buttons '< Previous', 'Next >', 'Create', and 'Cancel' are at the bottom.

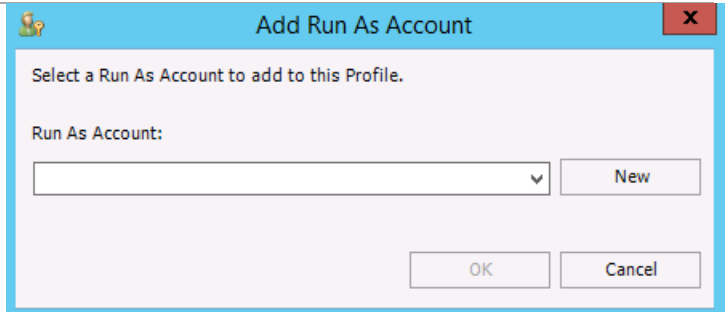
Leave the displayed **Cisco UCS Manager instance name** and click **Next**.

The screenshot shows the 'Add Monitoring Wizard' window with the title 'Cisco UCS Instance Name'. The navigation pane on the left has 'Instance Name' selected. The main area is titled 'Enter UCS name and description' and contains a 'Name' field with 'MSPOFT-UCS01' and a larger 'Description' text area. Below this is the 'Management Pack' section, which includes a 'Create destination management pack:' field with 'MSPOFT-UCS01', a checkbox for 'Use existing management pack or create new', and a 'Default Management Pack' dropdown menu. Navigation buttons '< Previous', 'Next >', 'Create', and 'Cancel' are at the bottom.

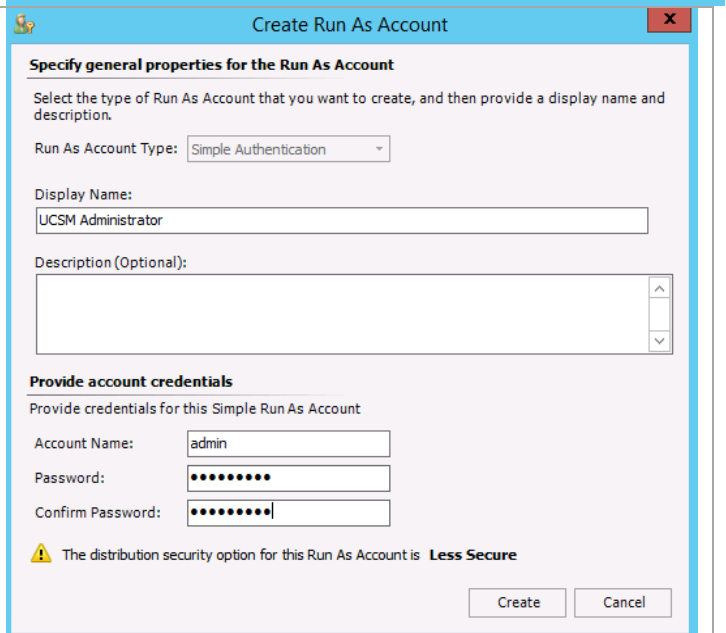
On the **Run As Account Summary** window check the box by **Associate Run As Account**. Click the **Add...** icon.

The screenshot shows the 'Add Monitoring Wizard' window with the title 'Run As Account Summary'. The navigation pane on the left has 'Run As Account' selected. The main area is titled 'Add Run As Accounts' and contains a checkbox for 'Associate Run As Account' which is checked. Below it is a table for 'Run As Accounts' with columns 'Account Name', 'Account Type', and 'Description'. An 'Add...' icon with a green plus sign is to the right of the table. Below the table is the 'Authentication' section with a note: 'You must associate a "Run As" Account with a corresponding Cisco UCS Instance "Run As" Profile.' Navigation buttons '< Previous', 'Next >', 'Create', and 'Cancel' are at the bottom.

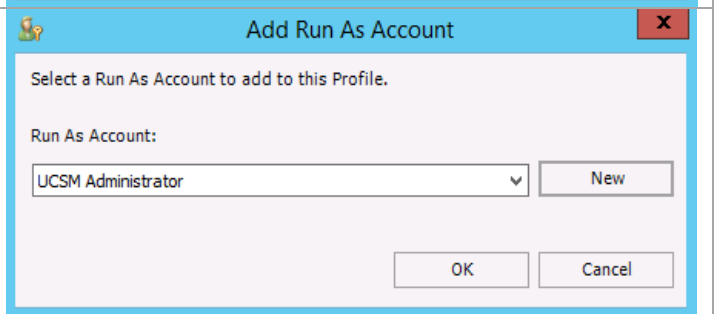
On the **Add Run As Account** pop-up click **New**.



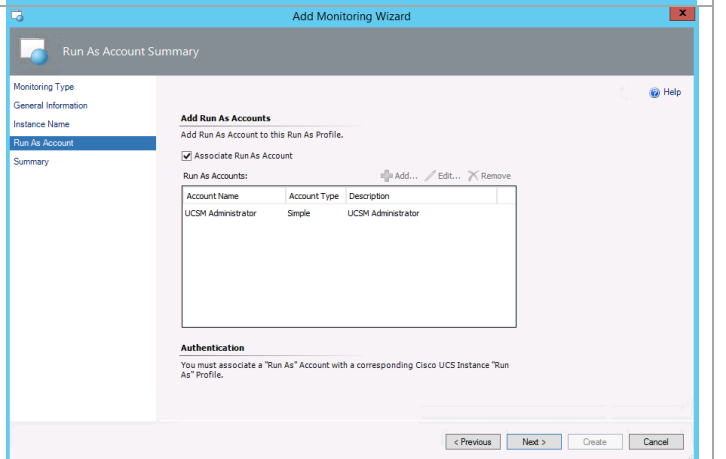
On the **Create Run As Account** window enter a **Display Name** for this run as account. Under **Provide account credentials** enter the credentials for the UCSM admin account. Click **Create**.



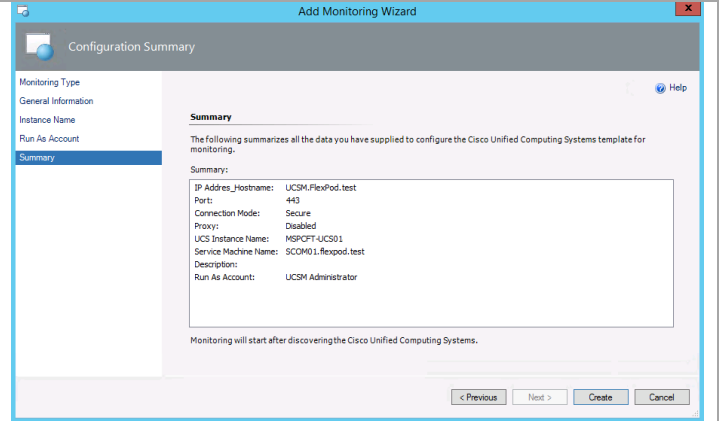
On the **Add Run As Account** window, ensure the newly created run as account is selected and click **OK**.



On the **Run As Account Summary** window click **Next** to continue.



Review the configuration summary and click the **Create** button to complete the Add Monitoring wizard.

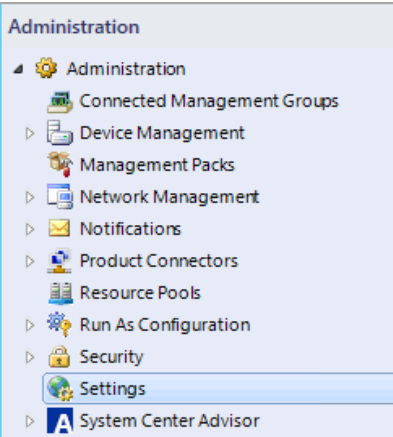


## Create a Resolution State

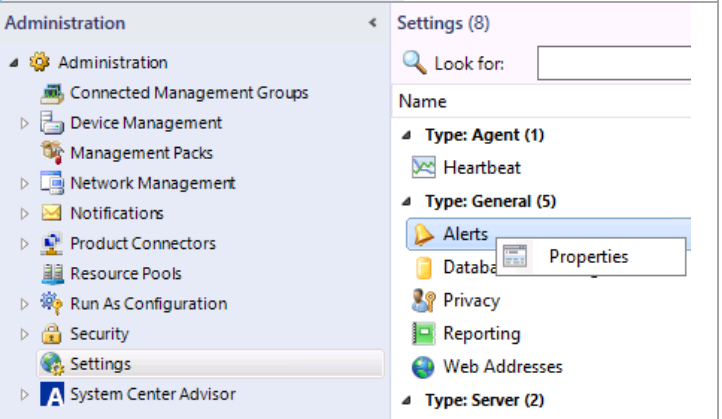
A resolution state can be assigned to and is visible on all faults. However, you can only acknowledge Cisco UCS faults. The following steps guide you on creating a resolution state for use with Cisco Unified Computing System.

**Perform the following steps on the first Operations Manager virtual machine.**

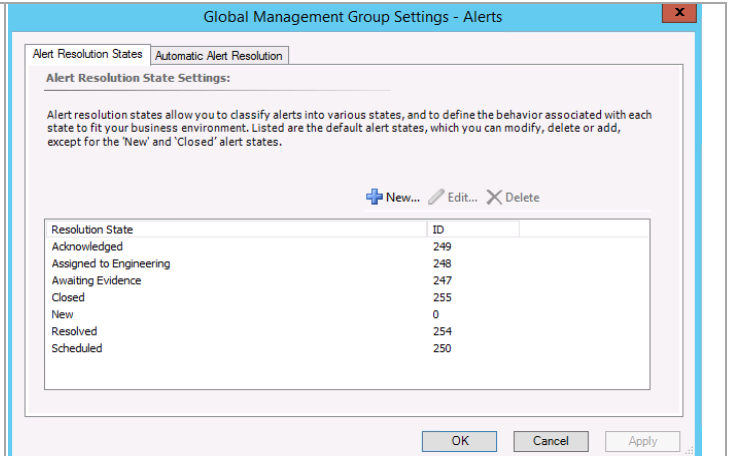
Navigate to **Administration > Settings**.



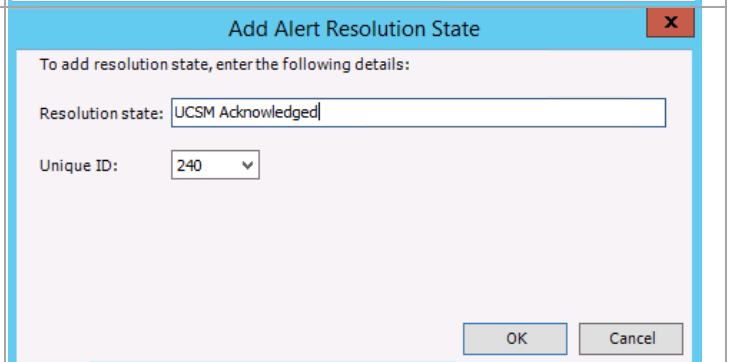
Under **Settings** right-click **Alerts** and select **Properties**.



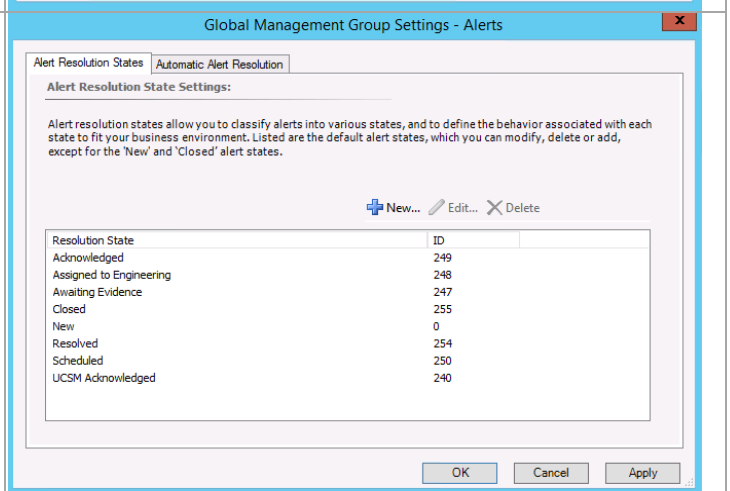
On the **Global Management Group Settings - Alerts** window click **New...**



On the **Add Alert Resolution State** pop-up enter a Resolution State name that identifies this as a UCSM state. From the Unique ID drop-down select and available number. Click **OK**.



On the **Global Management Group Settings - Alerts** window click **OK**.



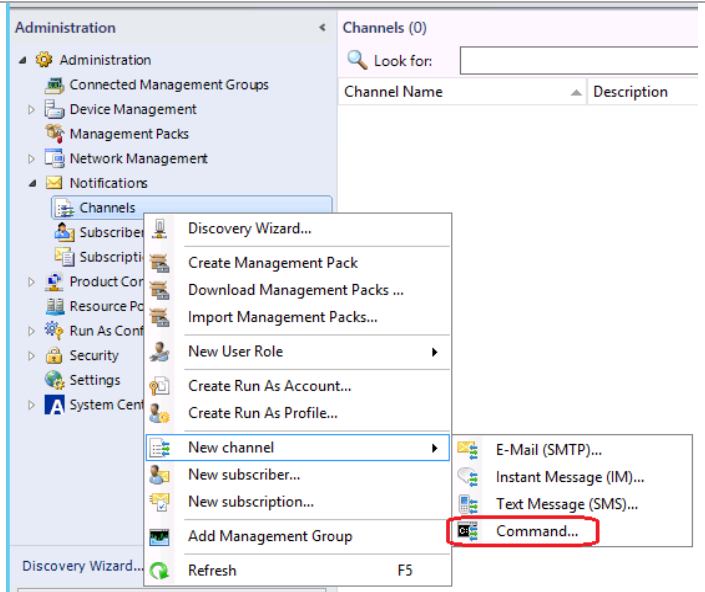
## Configuring Bidirectional Communication

The following procedure describes the required configuration to communicate with Cisco UCS for acknowledging alerts from the Operations Manager Console.

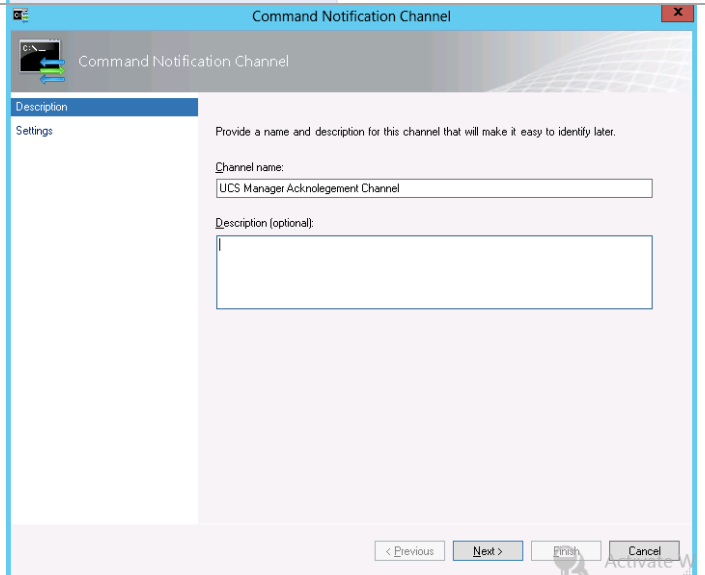
**Note:** The Bidirectional feature is currently limited to Management Servers on which SCOM 2012 R2 Console and Cisco UCS MP are both installed.

Perform the following steps on the first Operations Manager virtual machine.

Navigate to **Administration > Notifications > Channels**. Right-click on **Channels**. Select **New Channel** from the menu and select the **Command** option.



The **Command Notification Channel** opens. Specify **Channel Name** and **Description**. Click the **Next** button.





The **Settings** page of the Command Notification Channel opens.

Specify **Full path of the command file** as

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Specify **Command Line parameters**

```
-Command "&
'C:\ProgramData\Cisco\UCSM\Script\AcknowledgeFault.ps1' " -getDescription
'$Data [Default='Not
Present'] /Context/DataItem/AlertDescription$'
'$Data [Default='Not
Present'] /Context/DataItem/ManagedEntityPath$\$Data [Default='Not
Present'] /Context/DataItem/ManagedEntityDisplayName$'
```

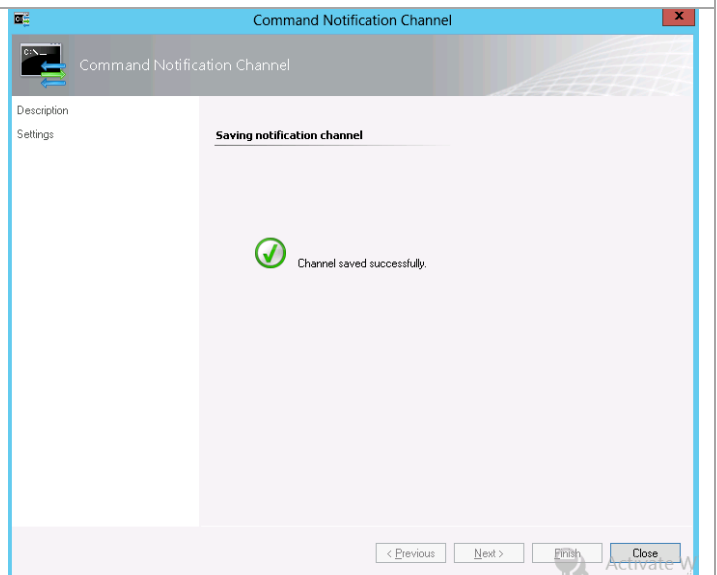
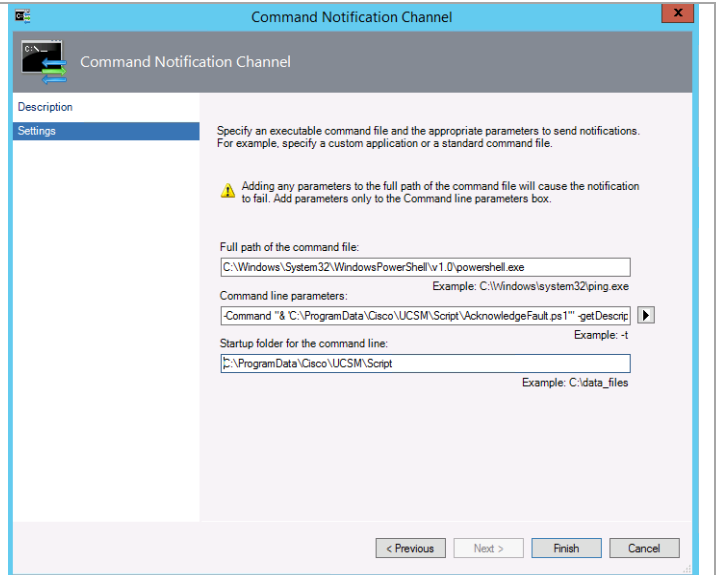
Specify **Start up folder for the command line** as

```
C:\ProgramData\Cisco\UCSM\Script
```

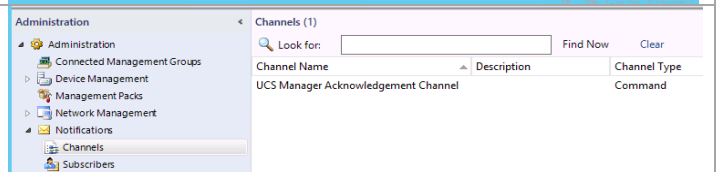
**Note:** Verify the path for script is valid.

Click the **Finish** button.

The new Channel is saved successfully. Click **Close** to close the wizard.

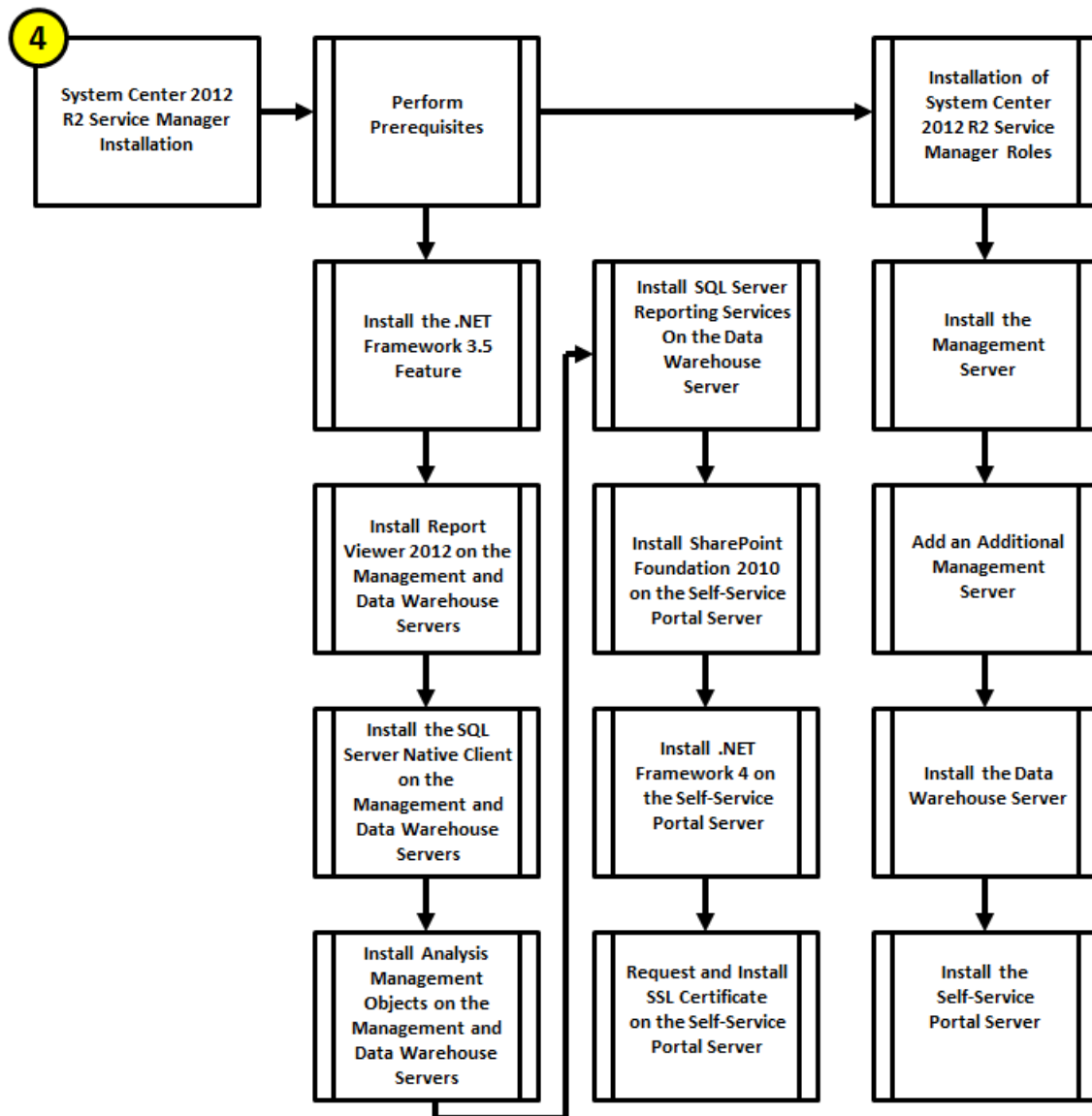


The new channel appears in the **Channel view**.



## 21 Service Manager

The Service Manager installation process includes the following high-level steps:



## 21.1 Overview

This section provides a high-level walkthrough on deploying Service Manager into the Fast Track fabric management architecture. The following requirements are necessary to deploy the management, data warehouse, and self-service portal servers:

### Management Server

- A base virtual machine running Windows Server 2012 R2 has been provisioned for the Service Manager Management server role.
- A multi-node, SQL Server 2012 SP2 cluster with dedicated a Service Manager instance 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 SP1 Redistributable 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 R2 has been provisioned for the Service Manager data warehouse server role.
- A multi-node, SQL Server 2012 SP2 cluster with dedicated instance that has been established in previous steps for Service Manager.
  - SCSMAS – instance for SQL Server 2012 SP2 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 SP1 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 SP1 is installed

- The .NET Framework 4 Redistributable is installed.
- SharePoint Foundation 2010 SP2 is installed.
- SharePoint Foundation 2010 SP2 has a number of prerequisites. If the self-service portal server has internet connectivity, the instructions for installing SharePoint Foundation 2010 SP2 shows how to automatically install them. If the server does not have internet connectivity, the following components must be manually downloaded and installed in this order.
  - **SQL Server 2008 Native Client** - <http://go.microsoft.com/fwlink/?LinkId=123718&clcid=0x409>
  - **WCF fix for Win2008 R2 (KB976462)** - <http://go.microsoft.com/fwlink/?LinkId=166231>
  - **Windows Identity Framework (KB974405)** - <http://go.microsoft.com/fwlink/?LinkId=166363>
  - **Microsoft Sync Framework Runtime v1.0 (x64)** - <http://go.microsoft.com/fwlink/?LinkId=141237&clcid=0x409>
  - **Microsoft Chart Controls for the Microsoft .NET Framework 3.5** - <http://go.microsoft.com/fwlink/?LinkId=141512>
  - **Microsoft Filter Pack 2.0** - <http://www.microsoft.com/en-us/download/details.aspx?id=17062>
  - **Microsoft SQL Server 2008 Analysis Services ADOMD.NET** - <http://go.microsoft.com/fwlink/?LinkId=160390&clcid=0x409>
  - **Microsoft Server Speech Platform Runtime** - <http://go.microsoft.com/fwlink/?LinkId=166378>
  - **Microsoft Server Speech Recognition Language - TELE(en-US)** - <http://go.microsoft.com/fwlink/?LinkId=166371>
  - **SQL 2008 R2 Reporting Services SharePoint 2010 Add-in** - <http://go.microsoft.com/fwlink/?LinkId=166379>

## 21.2 Prerequisites

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.
<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

User name	Purpose	Permissions
		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.

## Configuration of Service Manager Environmental Prerequisites

The following steps must to be completed in order to install the Service Manager roles correctly.

**Perform the following steps on all Service Manager Servers virtual machines.**

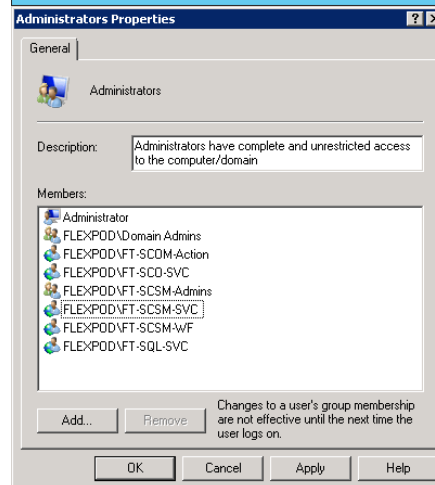
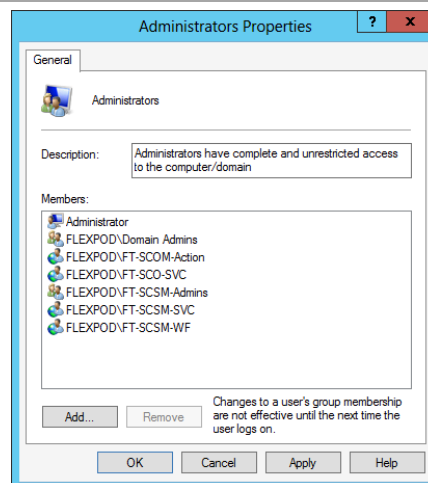
Log on to each Service Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the local Administrators group on each Service Manager virtual machine:

- Operations Manager action account.
- Service Manager workflow account.
- Service Manager service account.
- Service Manager Admins group.
- Orchestrator service account.

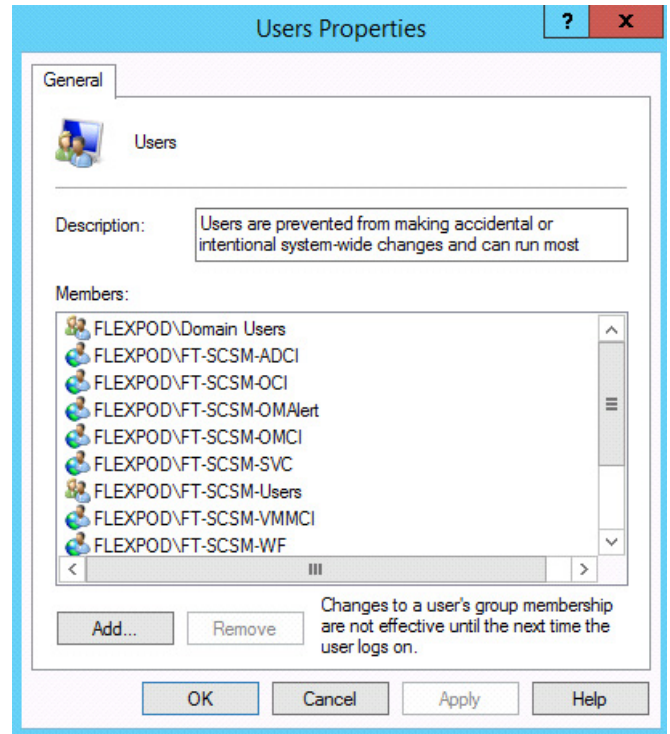
On the self-service portal server, also add the following account:

- SQL service account



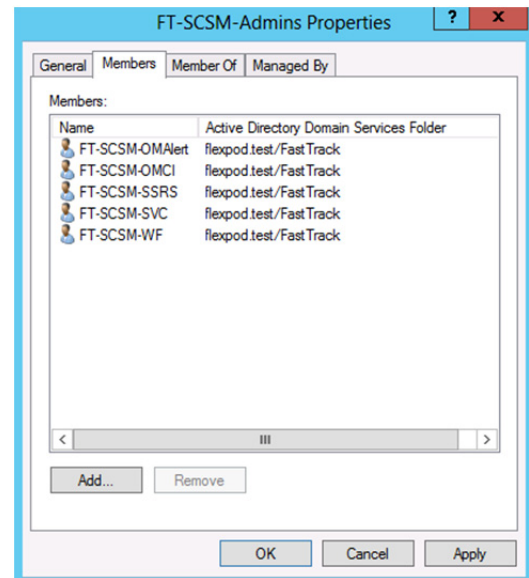
Verify that the following accounts and/or groups are members of the local Users group on each Service Manager virtual machine:

- Service Manager Active Directory CI connection account.
- Service Manager Orchestrator CI connection account.
- Service Manager Operations Manager alert connection account.
- Service Manager Operations Manager CI connection account.
- Service Manager service account.
- Service Manager users group.
- Service Manager Virtual Machine Manager CI connection account.
- Service Manager workflow account.

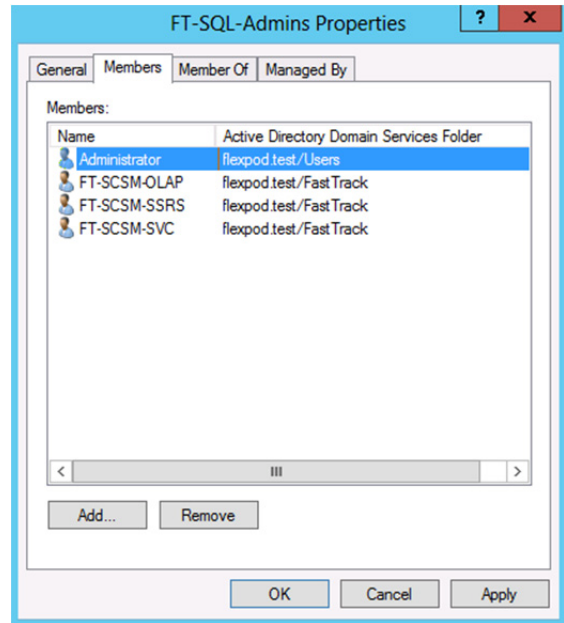


Perform the following step on an **Active Directory Domain Controller** in the target environment.

In the domain where Service Manager will be installed, verify that the SM Operations Manager alert connectors and the Service Manager service accounts are members of the SM Admins group created earlier.

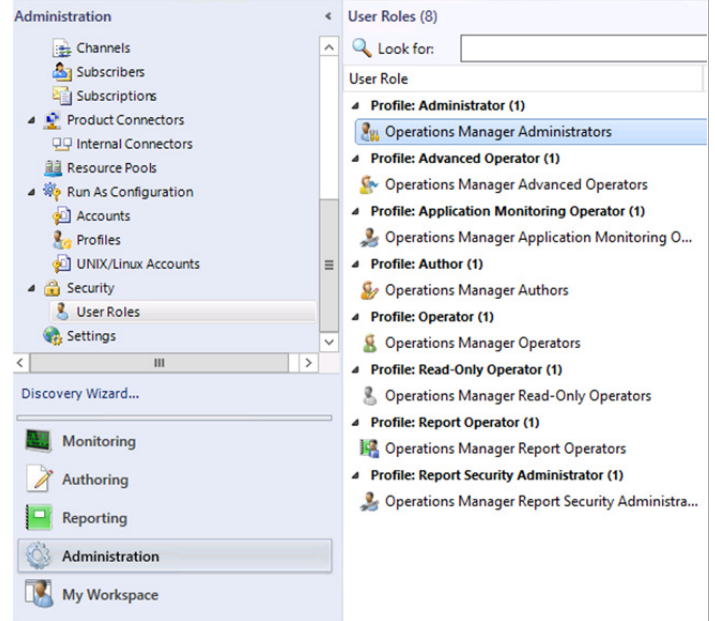


In the domain where Service Manager will be installed, verify that the SM OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group created earlier.



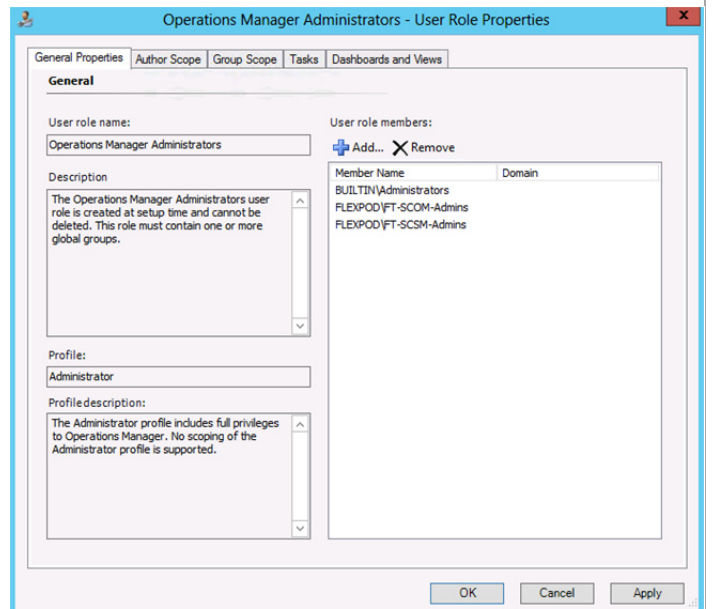
Perform the following steps on the **Operations Manager** virtual machine.

Log on to the Operations Manager server as an Administrator. In the **Operations Manager console**, navigate to **Administration > Security > User Roles > Operations Manager Administrators**.

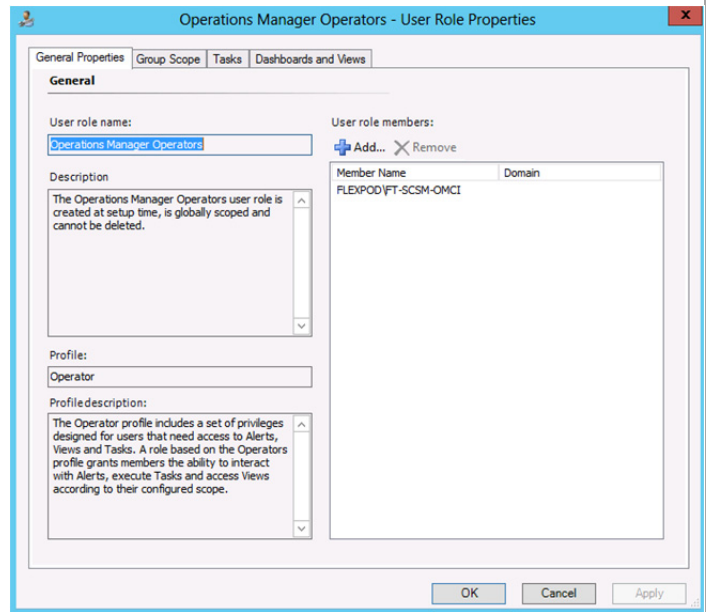




Right-click and select **Properties**, then add the **SCSM Admins** group and **SCOM Admins** group to the role. Click **OK** to save the changes.



While still in the **Security** node under **User Roles**, locate the **Operations Manager Operators** role and add the **SCSM OMCI** user to the role. Click **OK** to save the changes.

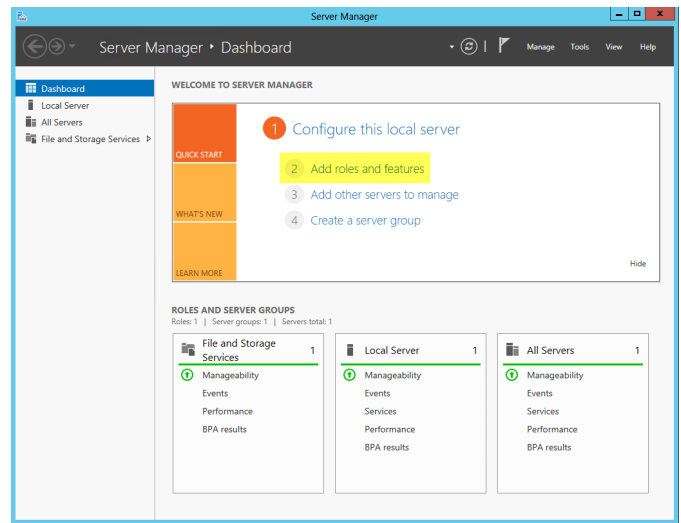


## Add the .NET Framework 3.5 Feature on all Server Manager Servers

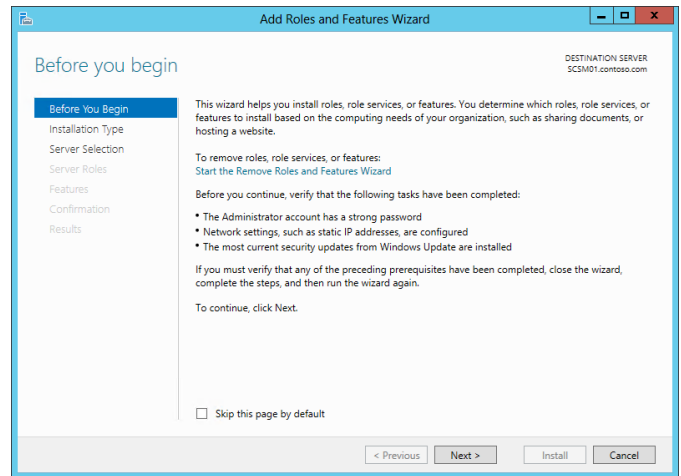
The Service Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5 Feature.

Perform the following steps on the **Service Manager management server (SCSM01)** and **data warehouse (SCSM02)** virtual machines.

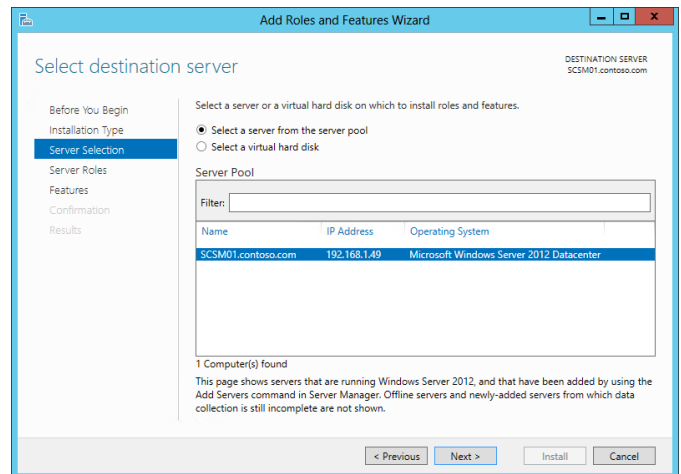
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



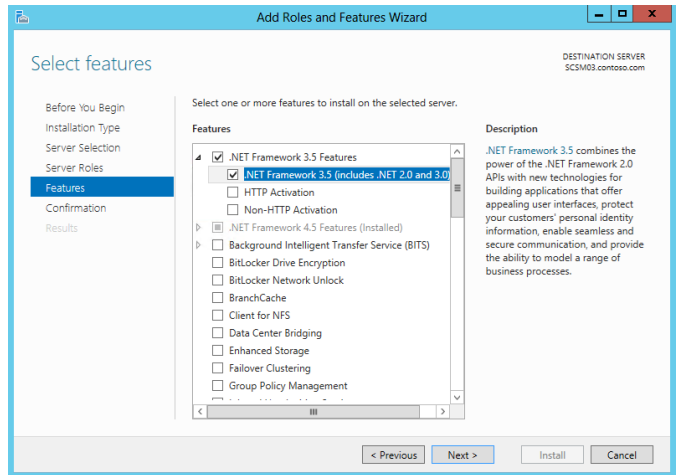
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, –o not click **Next** - for this installation, click the **Server Selection** menu option to continue.



In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and –o not click **Next** - for this installation, click the **Features** menu option to continue.

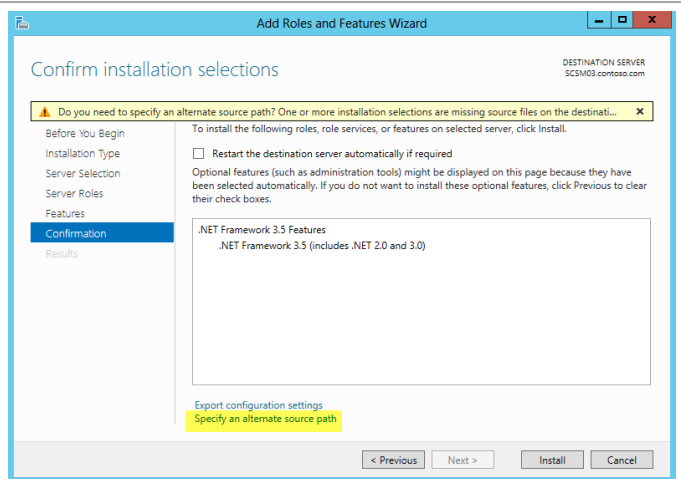


To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.

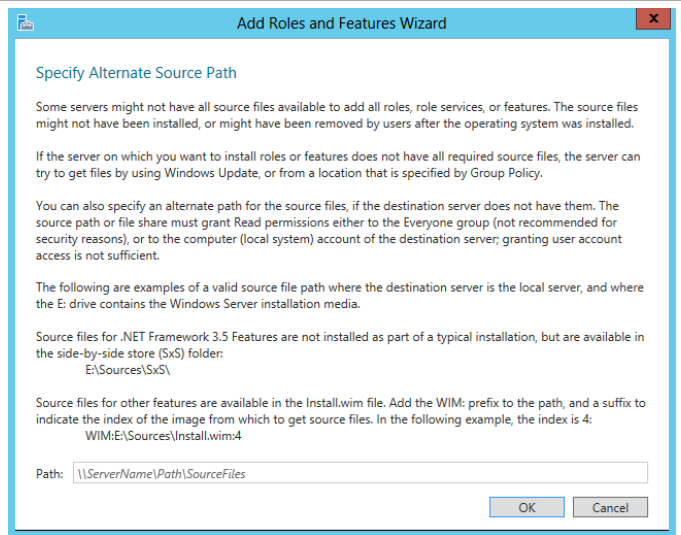


In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

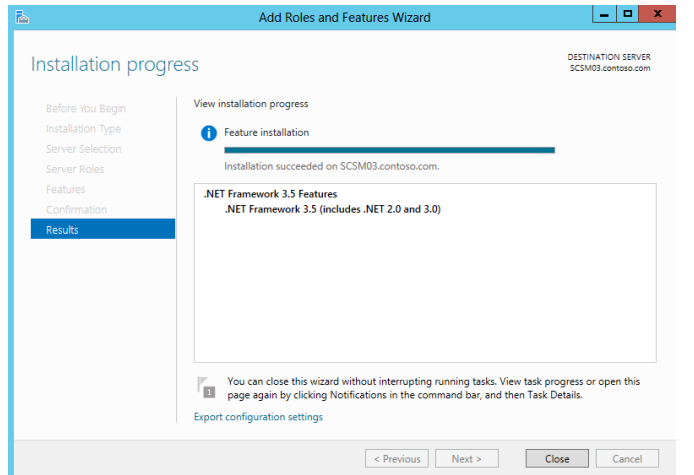
*Note that the **Export Configuration Settings** option is available as a link on this dialog to export the options selected to XML. When exported, this can be used in conjunction with the **Server Manager PowerShell** module to automate the installation of roles and features. Also, if the server does not have internet access an alternate source path can be specified by clicking the **Specify and alternate source patch link**.*



*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.*



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

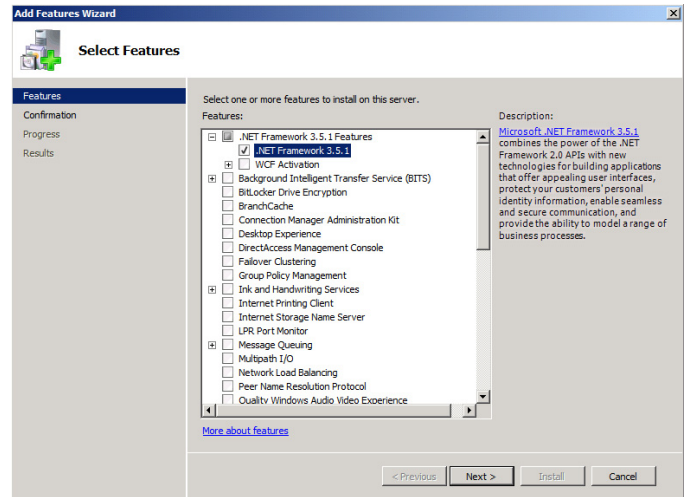


The above steps make use of the provided GUI to add the feature. It can also be added with the shown PowerShell command. This assumes the Windows Server distribution media is mounted to driver D:

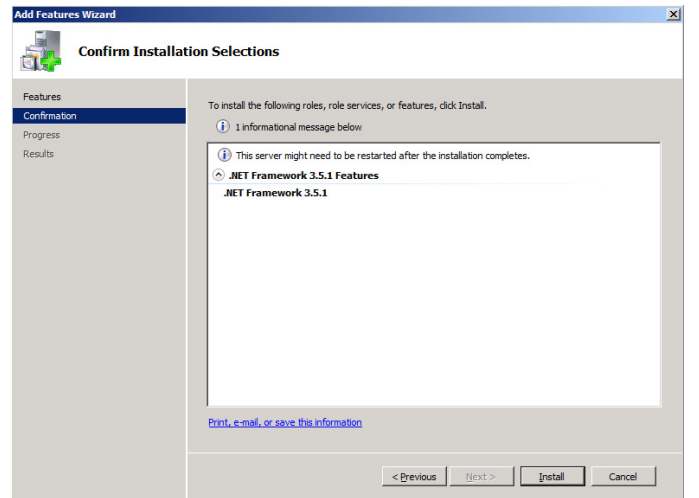
Install-WindowsFeature -Name Net-Framework-Core -Source D:\sources\sxs

**Perform the following steps on the Service Manager Self-Service Portal virtual machine running Windows Server 2008 R2.**

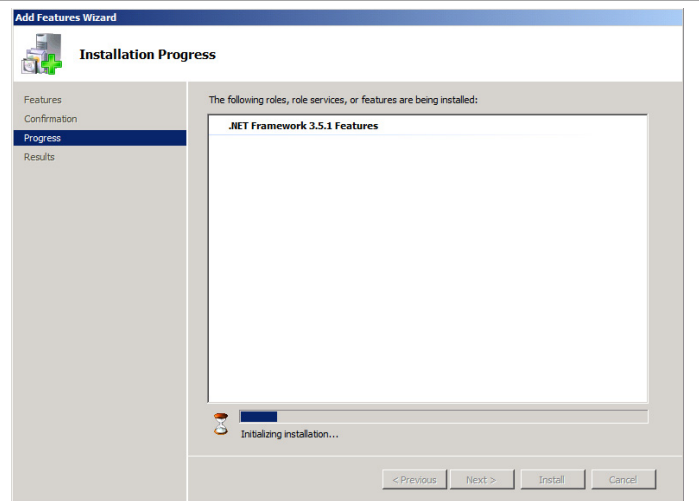
To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features**, and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.



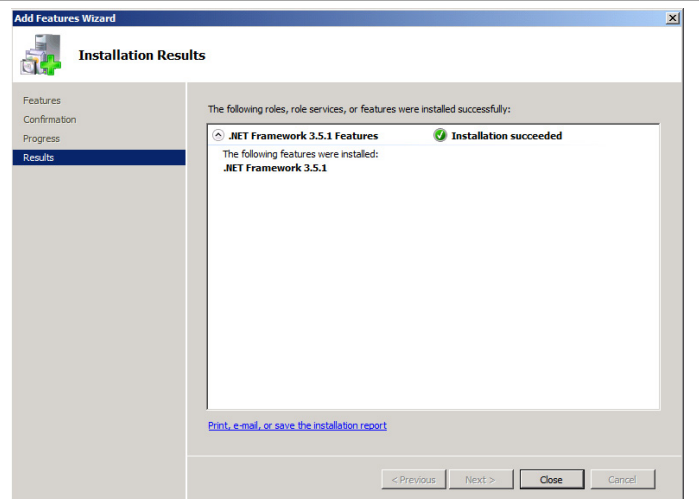
In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.



The **Installation Progress** dialog will show the progress of the feature install.



When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.

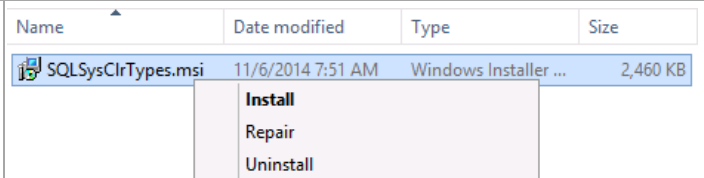


## Install Microsoft Report Viewer 2012 Redistributable

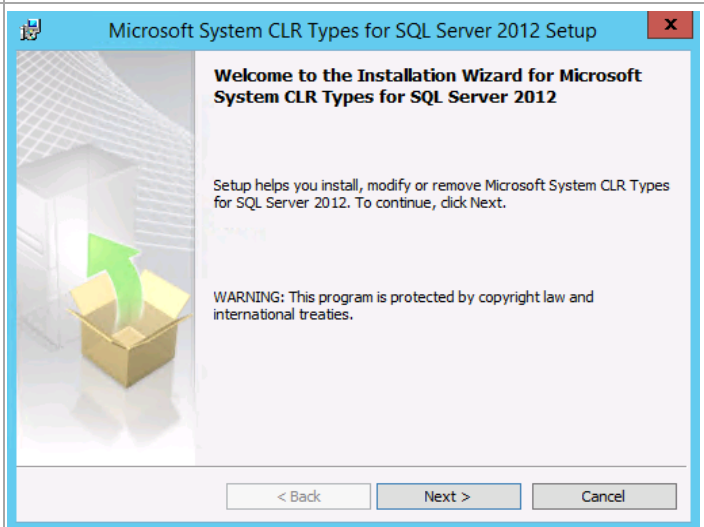
The Server Manager management and Data Warehouse server installations also require the **Microsoft Report Viewer 2012 Redistributable** be installed prior to installation. A prerequisite to that installation is the Microsoft System CLR Types for SQL Server 2012. The following steps are provided to help install these components.

**Perform the following steps on the **Server Manager management (SCSM01) and Data Warehouse server (SCSM02) virtual machines.****

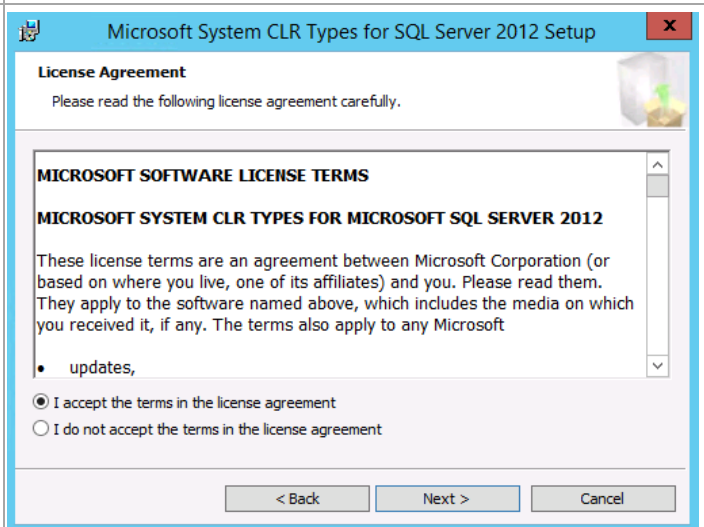
From the installation media for the Microsoft System CLR Types for SQL Server 2012, right-click **SQLSysClrTypes.msi** and select **Install**.



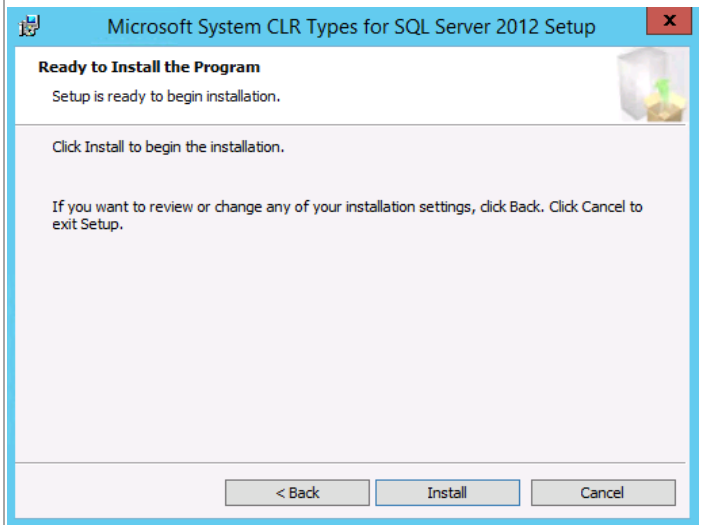
On the Welcome window, click **Next** to continue.



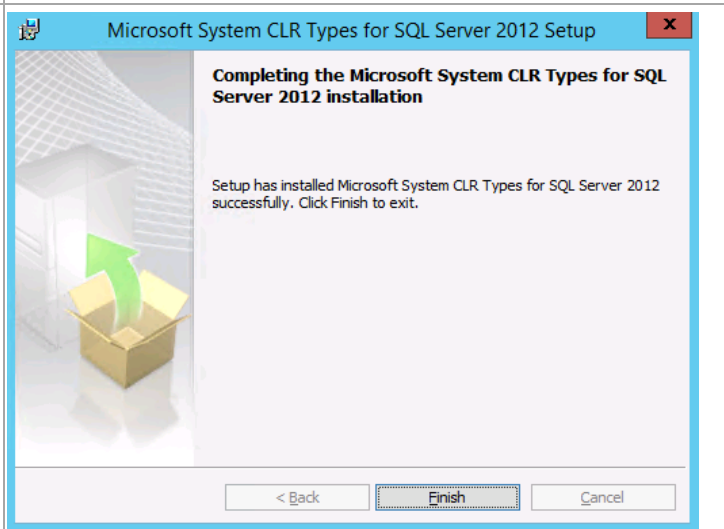
Click the radio button by **I accept the terms in the license agreement** and click **Next** to continue.



On the Ready to install the Program window click **Install** to start the installation.

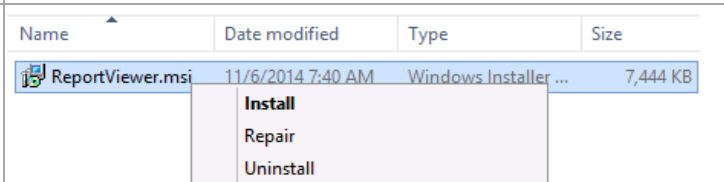


When the installation completes, click **Finish**.

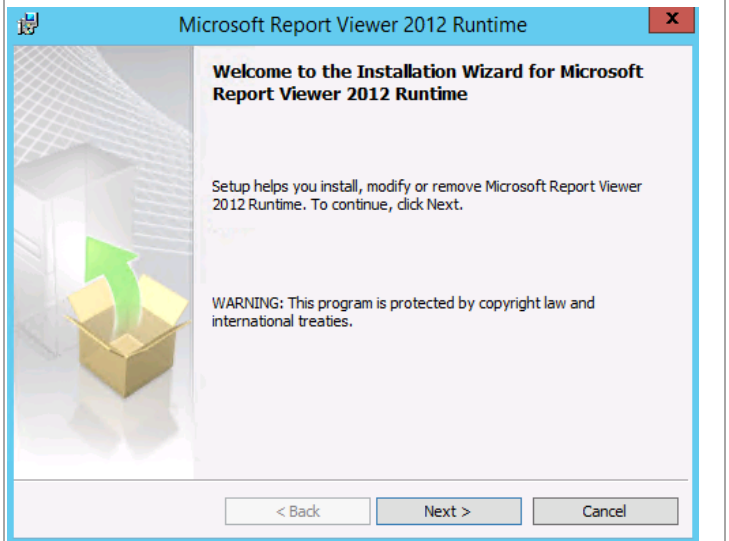


From the installation media source for the Report Viewer, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

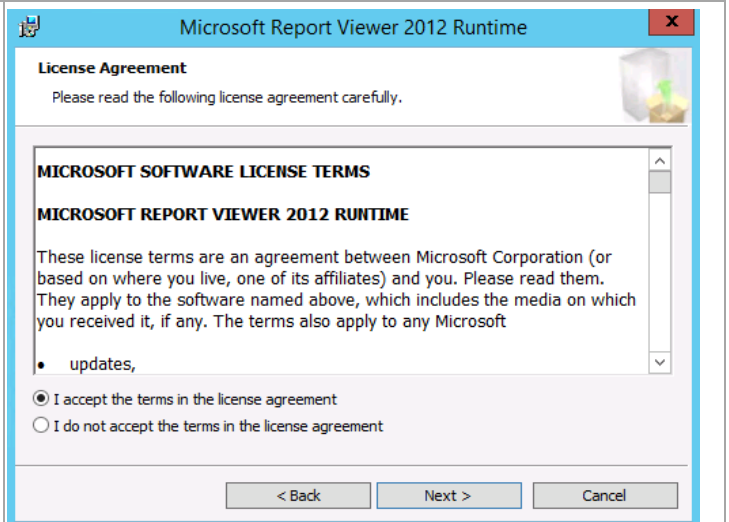
*Note: Report Viewer can be found in the prerequisites folder of the Service Manager 2012 SP1 installation media or it can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=3203>*



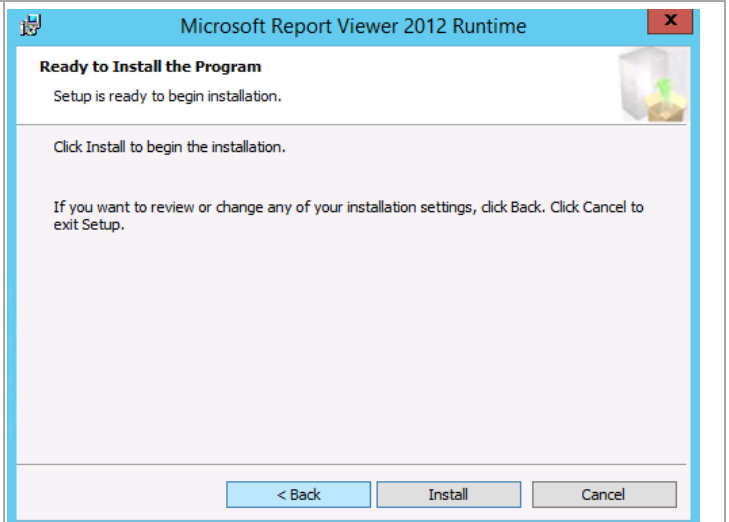
On the welcome window click **Next** to continue.



Within the **License Agreement** window, select the radio button by **I have read and accept the license terms**. Click **Install** to continue.

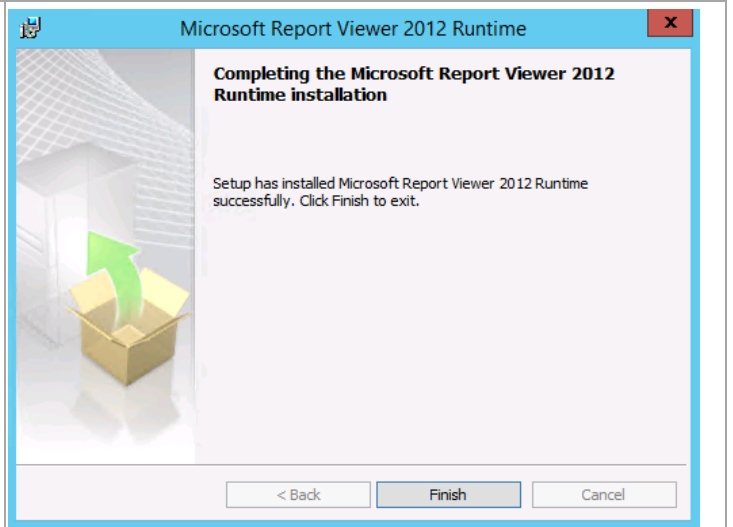


On the Ready to Install the Program window click **Install** to start the installation.





When completed, click **Finish** to exit the installation.



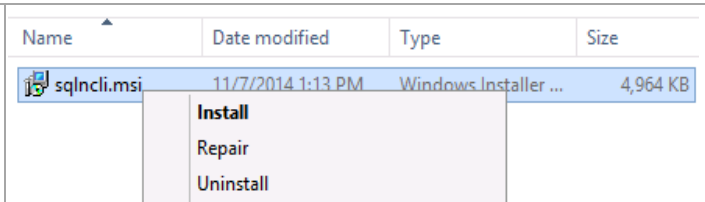
## Install SQL Server 2012 Native Client

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.

From the installation media source, right-click **SQLNCLI.MSI** and select **Install** from the context menu to begin setup.

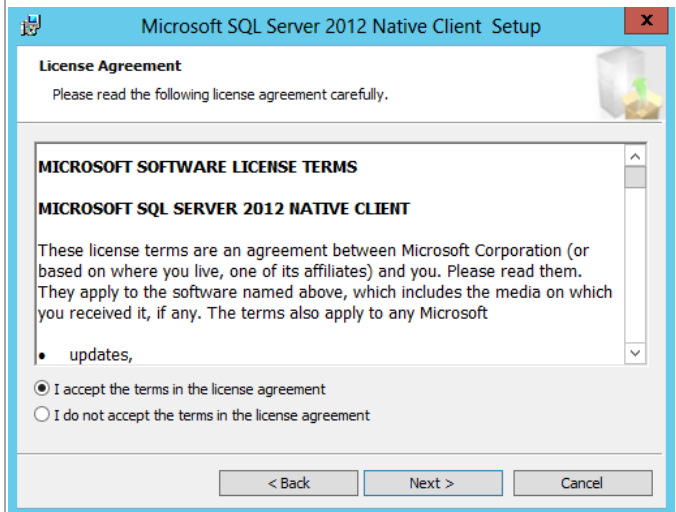
**Note:** the SQL Server 2012 SP1 Native Client installer, **1033\x64\sqlncli.msi**, can be downloaded from <http://download.microsoft.com/download/4/B/1/4B1E9B0E-A4F3-4715-B417-31C82302A70A/ENU/x64/sqlncli.msi>.



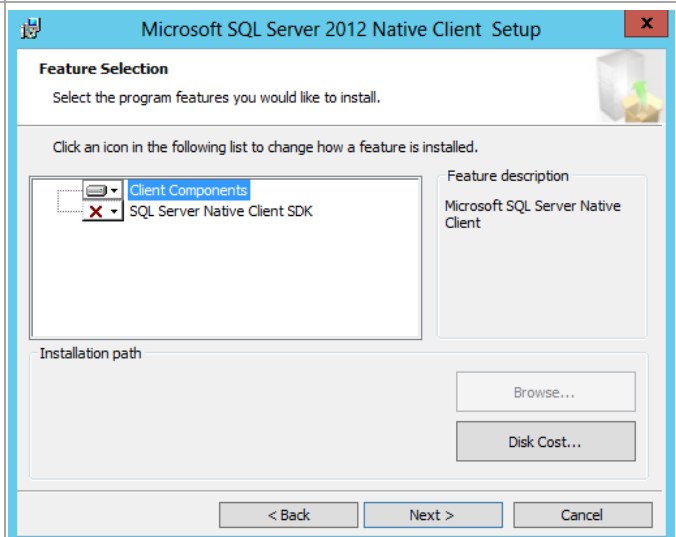
The setup wizard will appear. Click **Next** to continue.



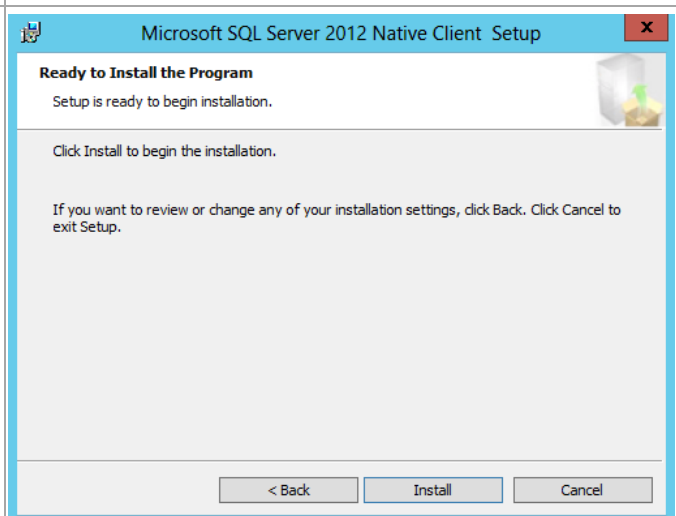
Within the **License Terms** dialog, select the **I accept the terms in the license agreement** check box. Click **Next** to continue.



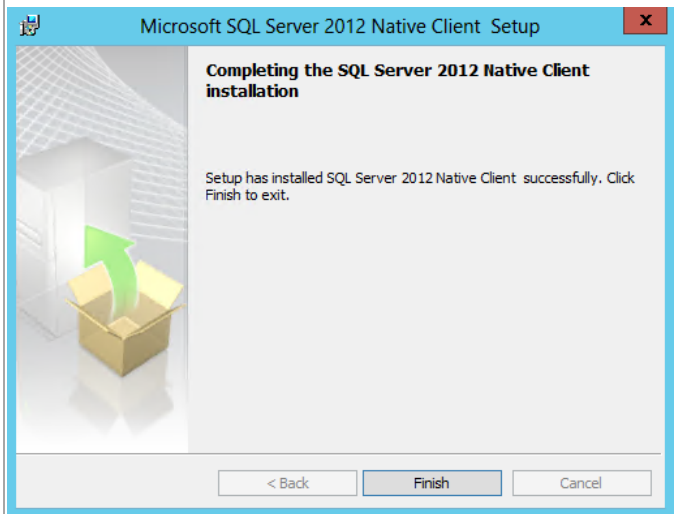
In the **Feature Selection** dialog, verify that the **Client Components** feature is selected for installation. Click **Next** to continue.



In the **Ready to Install the Program** dialog, click **Install** to begin the installation.



When completed, click **Finish** to exit the installation.



## Install SQL Server 2012 SP1 Analysis Management Objects

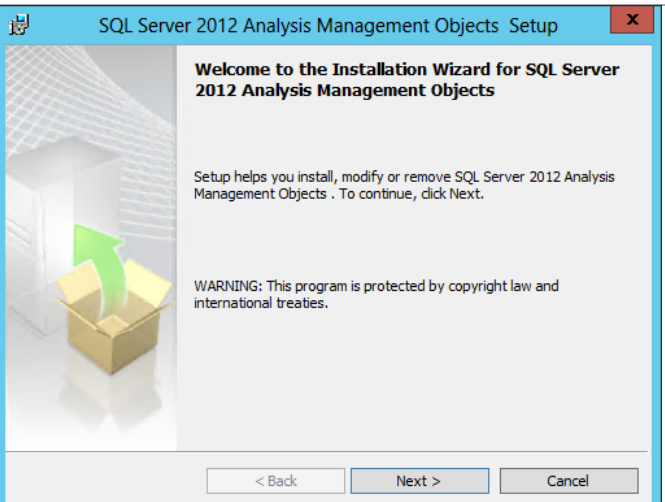
The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 SP1 Analysis Management Object be installed prior to installation. Follow the provided steps to install the SQL Server 2012 SP1 Analysis Management Objects.

Perform the following steps on the **Server Manager Management (SCSM01)** and **Data Warehouse server (SCSM02)** virtual machines.

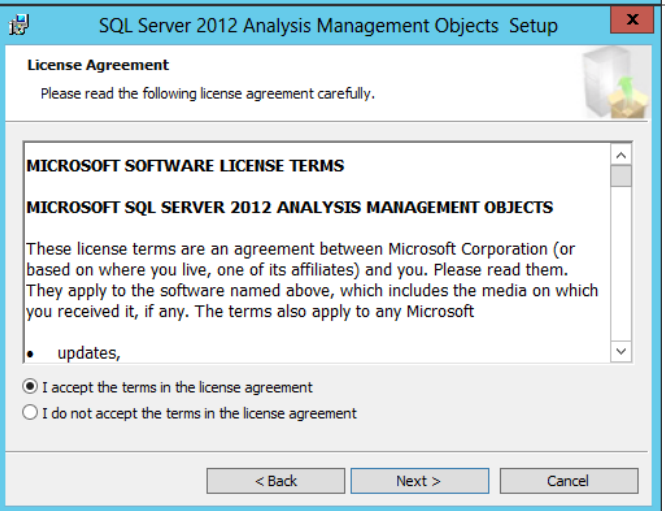
From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL\_AS\_AMO.MSI** to begin setup.  
**Note:** The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL\_AS\_AMO.MSI**, can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=35580>.

Name	Date modified	Type	Size
SQL_AS_AMO	3/7/2013 11:04 AM	Windows Installer Package	3,604 KB

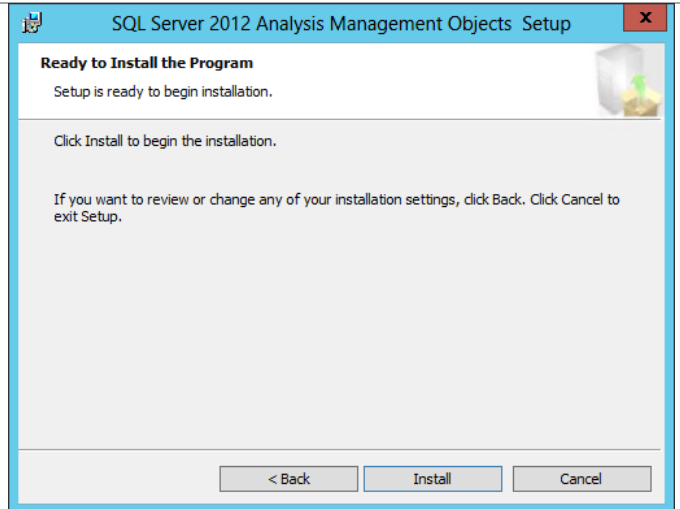
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



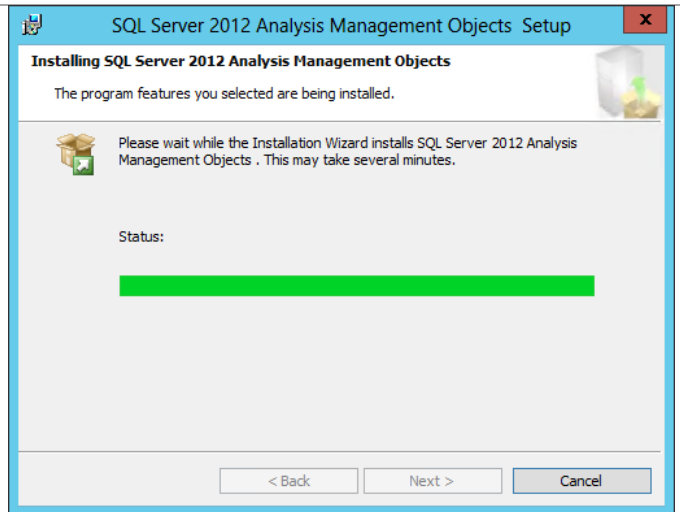
In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.



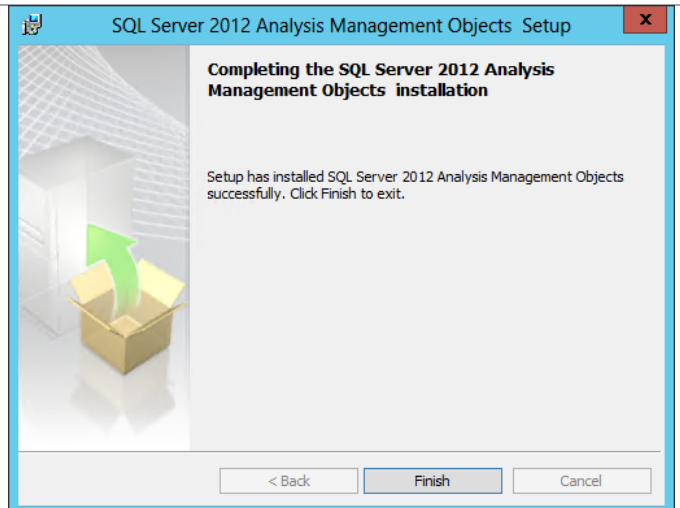
In the **Ready to Install the Program** dialog, click **Install** to begin the installation.



The installation process may take several minutes to complete. The progress is displayed on the status dialog.



In the **Completing the SQL Server 2012 Analysis Management Objects installation** dialog, click **Finish** to exit the installation.

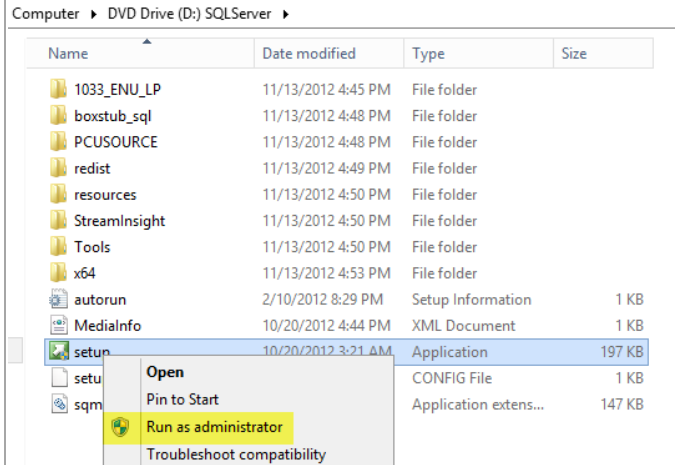


## Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

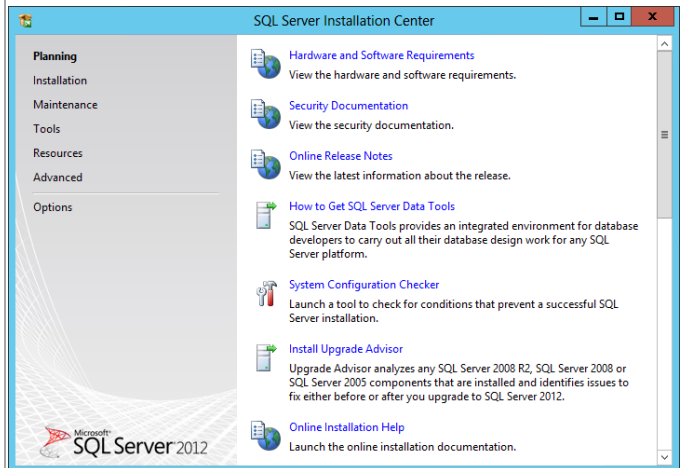
The Service Manager Data Warehouse installation requires SQL Server Reporting Services to be installed to support the Service Manager reporting features. Follow the provided steps to install SQL Server Reporting Services.

Perform the following steps on the **Service Manager Data Warehouse (SCSM02)** virtual machine.


From the SQL Server 2012 SP2 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



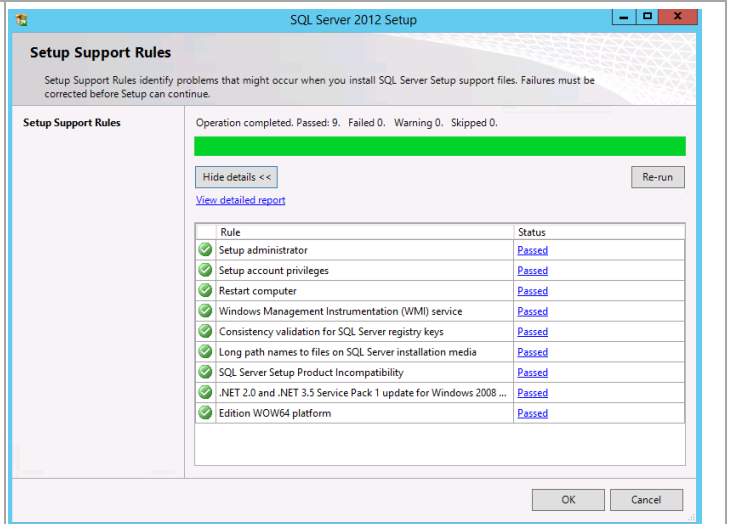
The **SQL Server Installation Center** will appear. Select the **Installation** menu option.



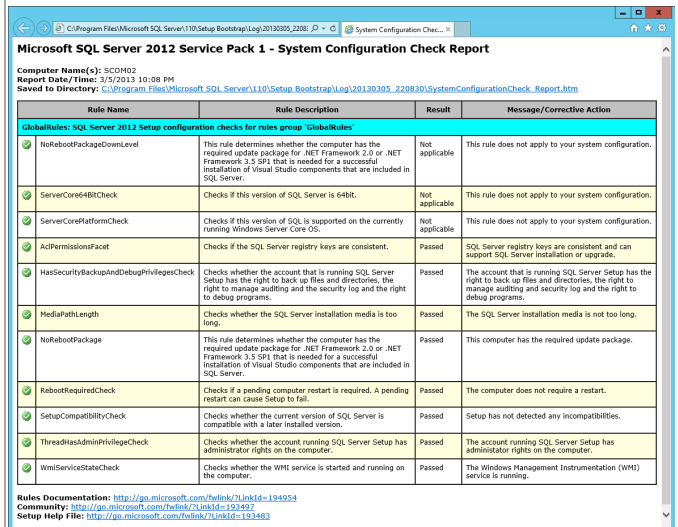
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.

 **New SQL Server stand-alone installation or add features to an existing installation**  
 Launch a wizard to install SQL Server 2012 in a non-clustered environment or to add features to an existing SQL Server 2012 instance.

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

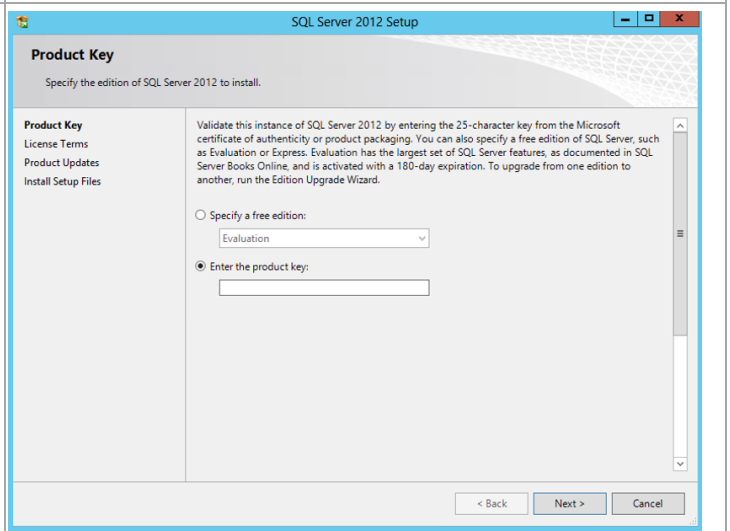


If the **View detailed report** link is selected, the following report is available.

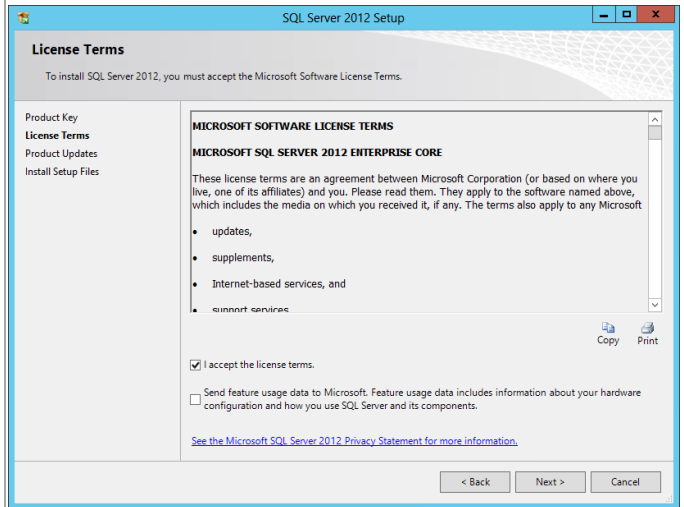


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

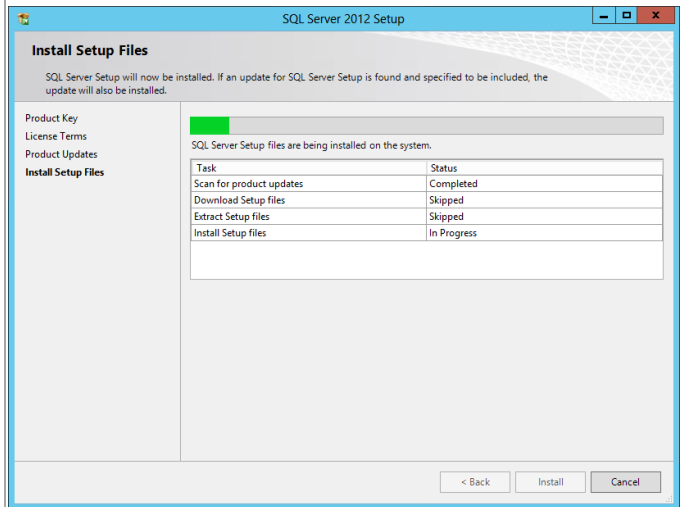
**Note:** If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



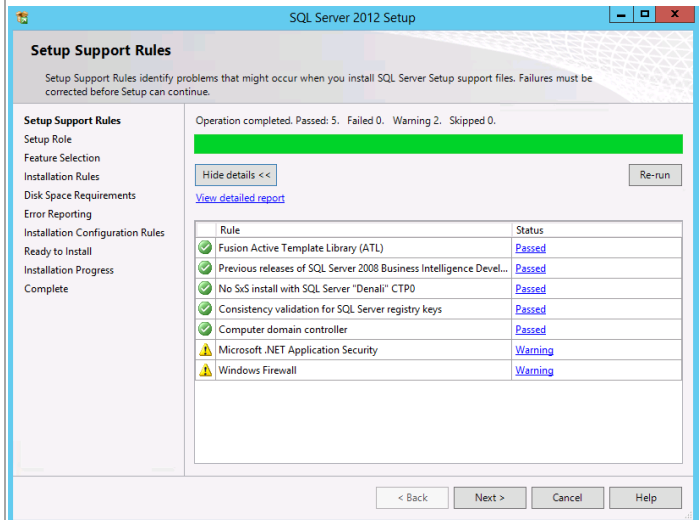
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.



In the **Install Setup Files** dialog, the process shows the status of the setup file installation.

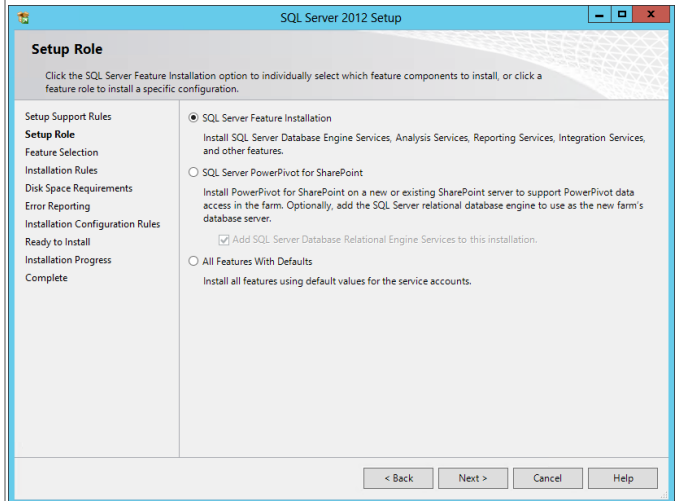


In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include .NET Application Security and Windows Firewall warnings that are generally acceptable. Click **Next**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

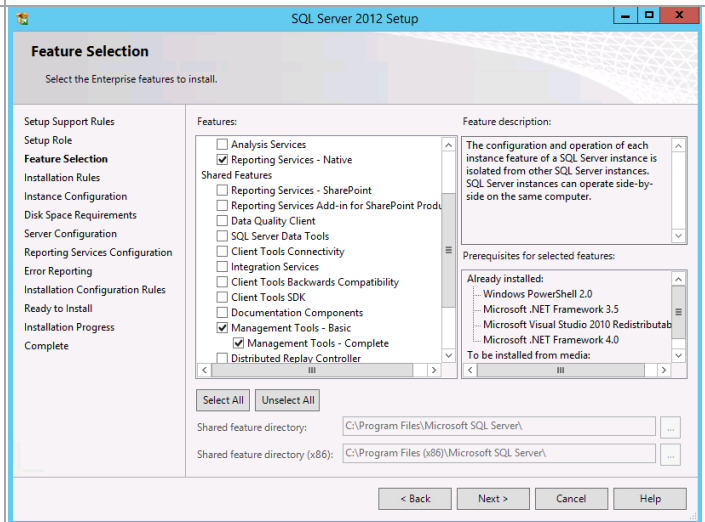




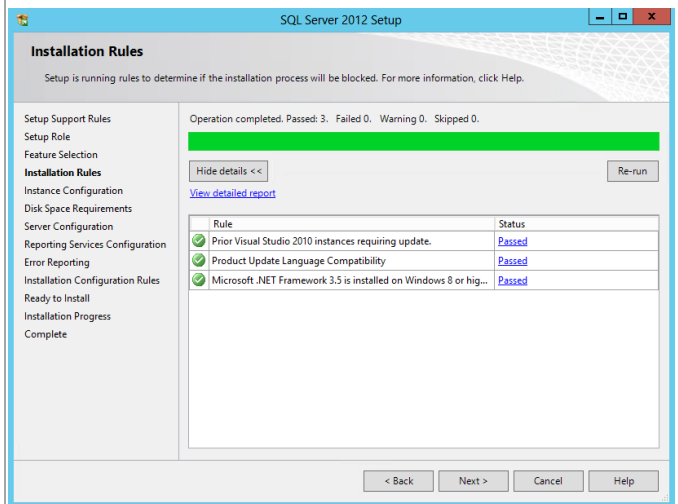
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.



In the **Feature Selection** dialog, select the **Reporting Services - Native**, **Management Tools - Basic**, and **Management Tools - Complete** check boxes. When all selections are made, click **Next** to continue.

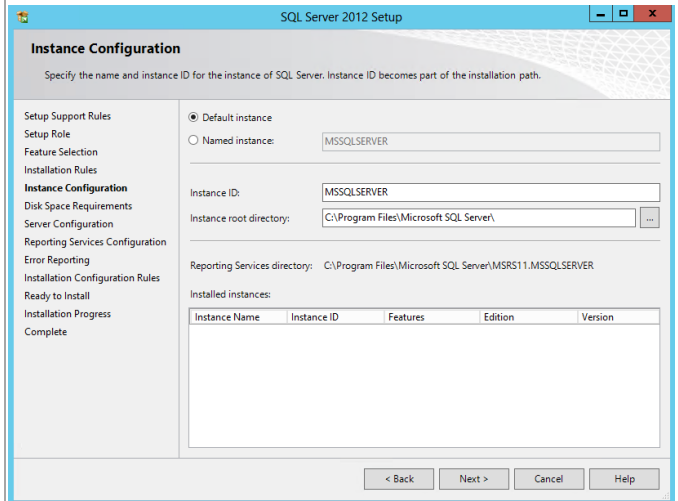


In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

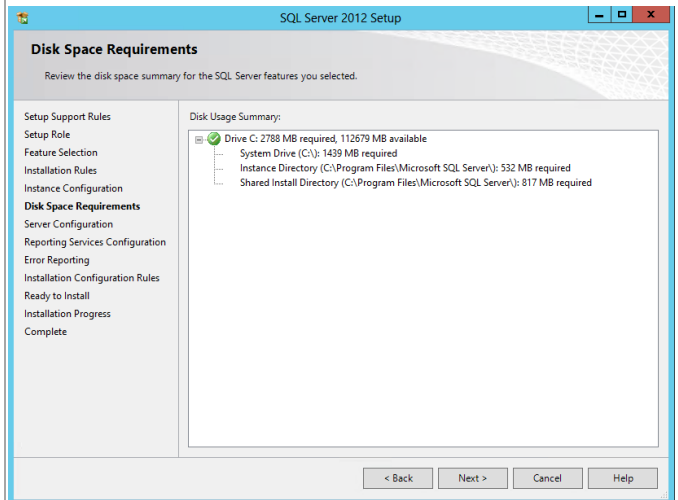


In the **Instance Configuration** dialog, select the **Default instance** option and accept the default options for **Instance ID** and **Instance root directory** values. Click **Next** to continue.

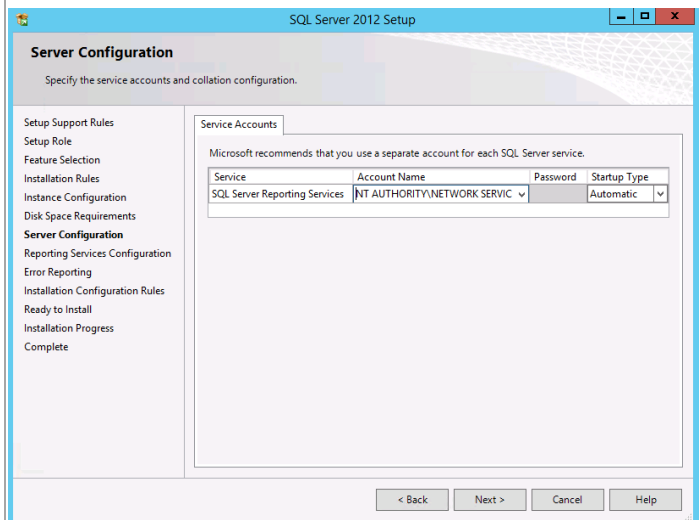
**Note:** A post-installation configuration process will occur to configure the reporting server database within the Service Manager Data Warehouse SQL Server instance.



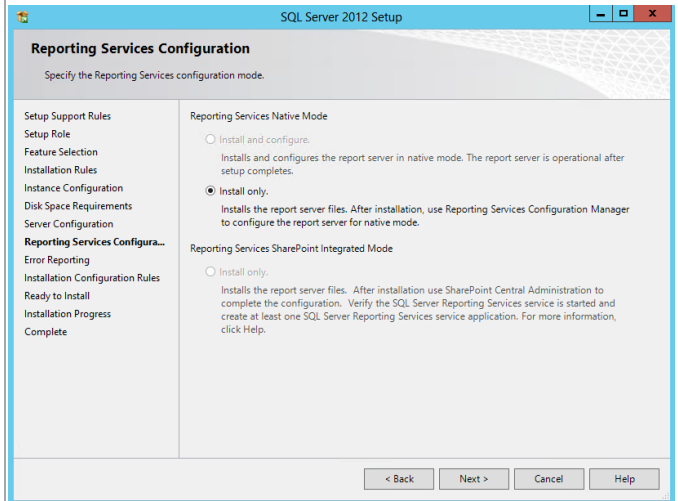
In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.



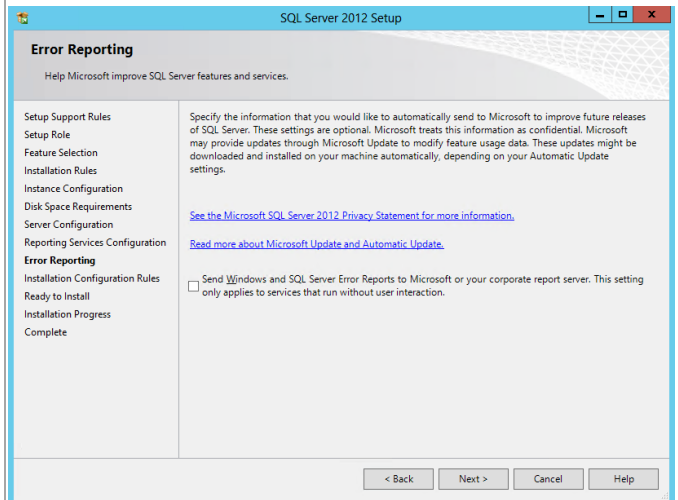
In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NETWORK SERVICE** account for the SQL Server Reporting Services service. Click **Next** to continue.



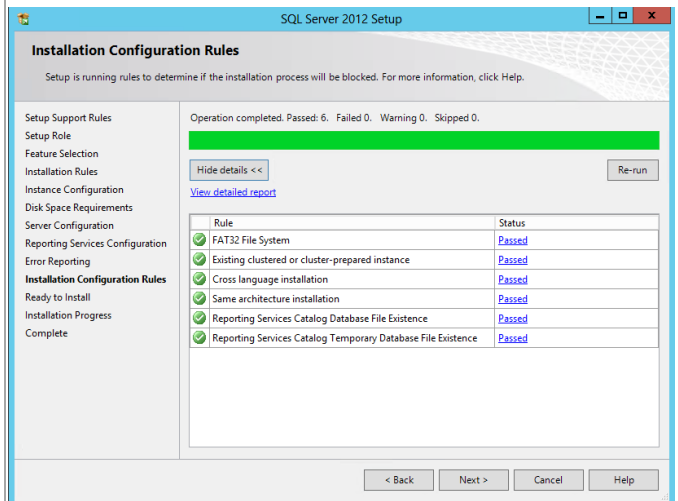
In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.



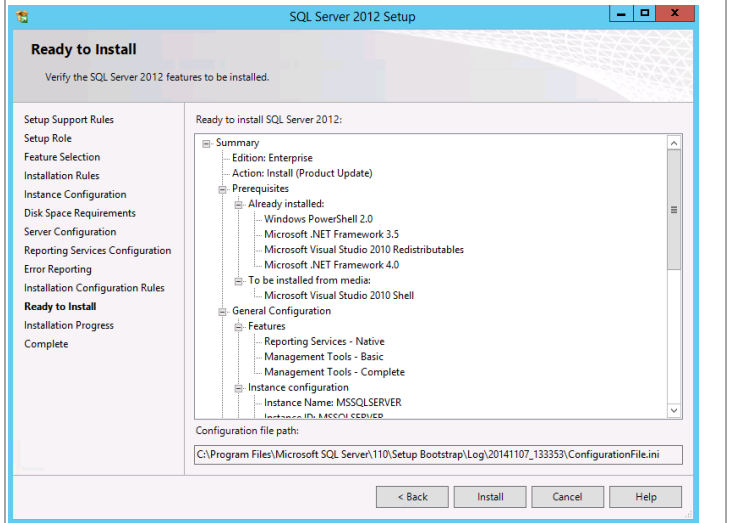
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



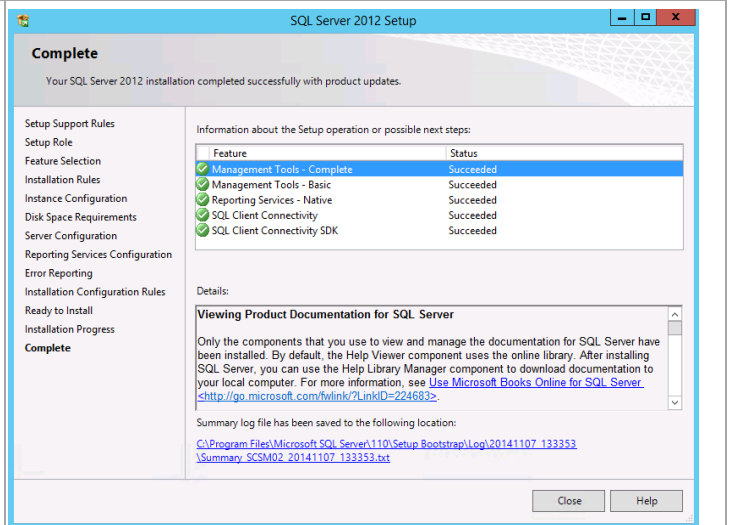
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



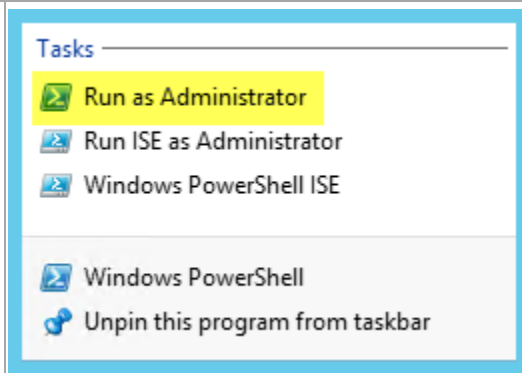
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



When complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



By default the Windows Firewall will not allow traffic in for and SQL services or for the SSRS Web Service. Firewall exceptions will need to be created if the Windows Firewall is enabled. Open an administrative session of PowerShell.



Execute the following commands to create the needed Firewall Rules:

```
New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80
```

Adjust the display names and ports based on organizational requirements.

```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80

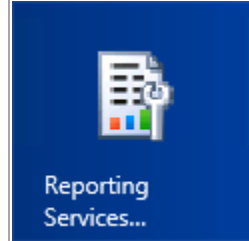
Name                : (26898efb-90e5-4c43-825b-3e36404b9258)
DisplayName          : SQL Reporting Services
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Any
Platform             :
Direction            : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```

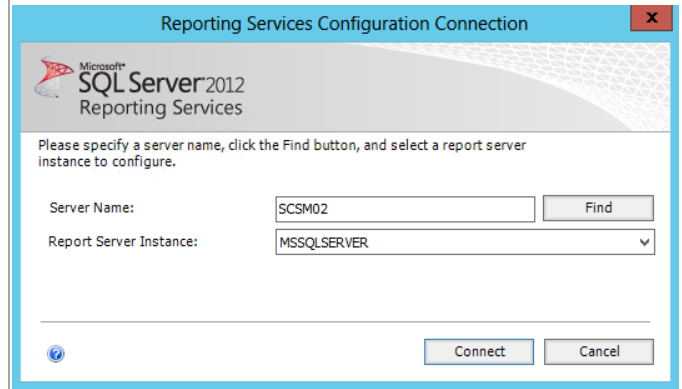
Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.

Name	Group	Profile	Enabled	Action	Override
SQL Reporting Services		All	Yes	Allow	No
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow	No

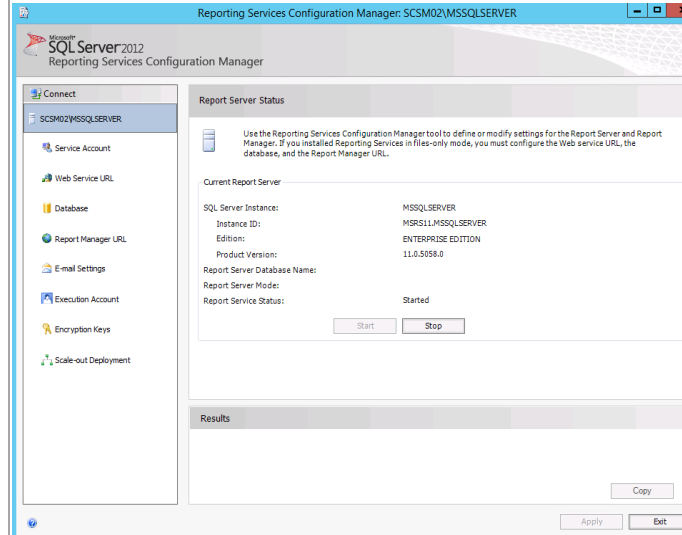
When installed, verify that SQL Server Reporting Services installed properly by opening the console. From the **Start** screen, navigate and select the **Reporting Services Configuration Manager** tile.



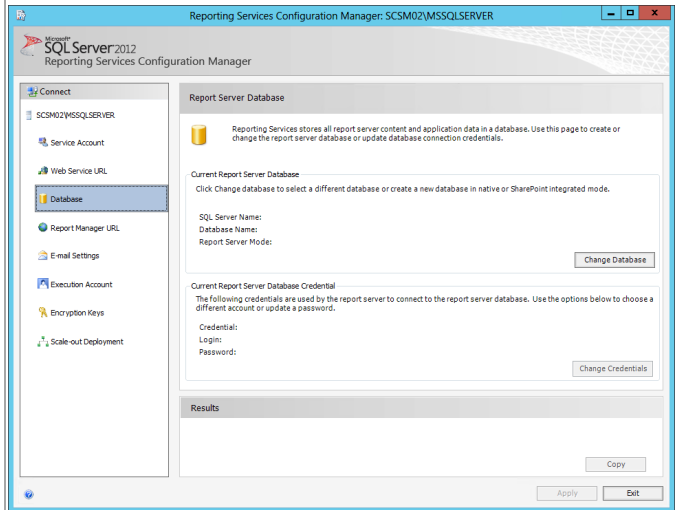
The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Service Manager server. In the **Report Server Instance** text box, use the default **MSSQLSERVER** drop-down menu value. Click **Connect**.



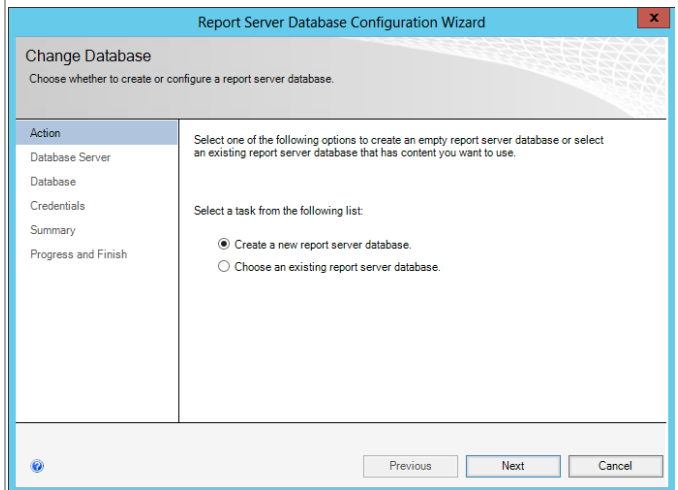
The **Reporting Services Configuration Manager** tool will appear.



In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.



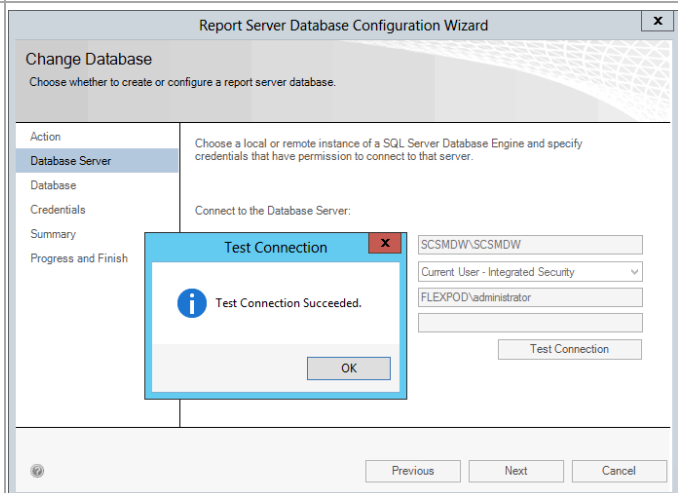
The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – specify the name of the SQL Server Cluster *SCSMDW Instance CNO* and the database instance created for the Service Manager Data Warehouse installation.
- **Authentication Type** – specify **Current User – Integrated Security** from the drop-down menu.

Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



In the **Database** section, specify the following values:

- **Database Name** – *accept the default value of ReportServer.*
- **Language** – *specify the desired language option from the drop-down menu.*
- **Report Server Mode** – *select the Native Mode option.*

Click **Next** to continue.

**Report Server Database Configuration Wizard**

**Change Database**  
Choose whether to create or configure a report server database.

Action  
Database Server  
**Database**  
Credentials  
Summary  
Progress and Finish

Enter a database name, select the language to use for running SQL scripts, and specify whether to create the database in native or SharePoint mode.

Database Name: ReportServer  
Temp Database Name: ReportServerTemp  
Language: English (United States)  
Report Server Mode: Native

Previous Next Cancel

In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.

**Report Server Database Configuration Wizard**

**Change Database**  
Choose whether to create or configure a report server database.

Action  
Database Server  
Database  
**Credentials**  
Summary  
Progress and Finish

Specify the credentials of an existing account that the report server will use to connect to the report server database. Permission to access the report server database will be automatically granted to the account you specify.

Credentials:  
Authentication Type: Service Credentials  
User name: NT AUTHORITY\NETWORKSERVICE  
Password:

Previous Next Cancel

In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.

**Report Server Database Configuration Wizard**

**Change Database**  
Choose whether to create or configure a report server database.

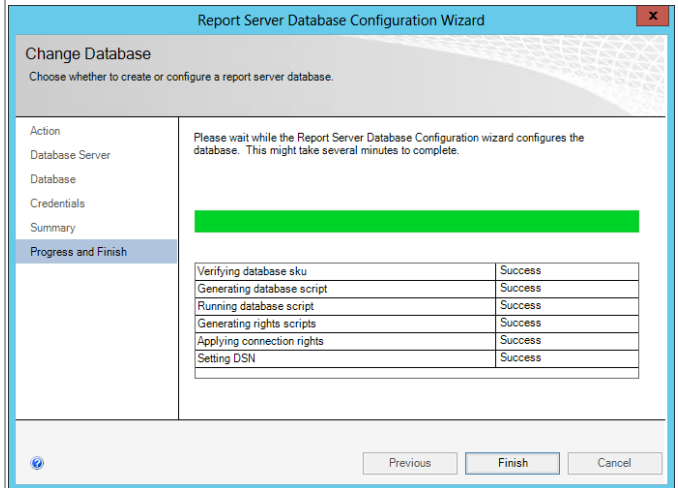
Action  
Database Server  
Database  
Credentials  
**Summary**  
Progress and Finish

The following information will be used to create a new report server database. Verify this information is correct before you continue.

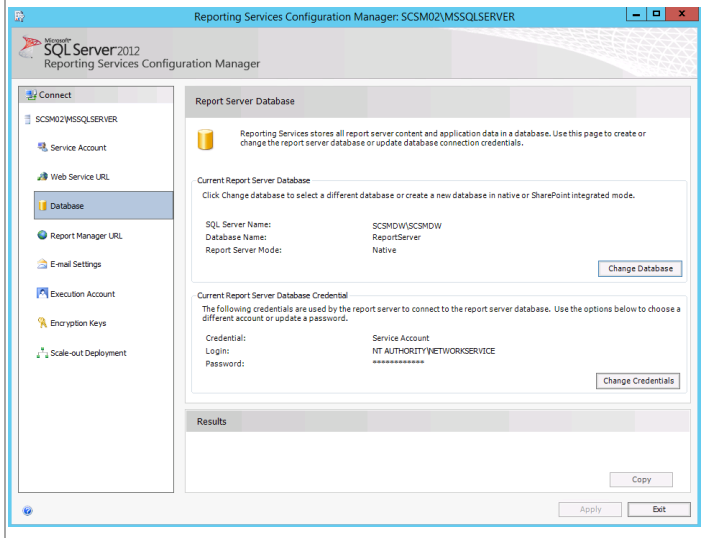
SQL Server Instance: SCSMDW/SCSMDW  
Report Server Database: ReportServer  
Temp Database: ReportServerTempDB  
Report Server Language: English (United States)  
Report Server Mode: Native  
Authentication Type: Service Account  
Username: NT AUTHORITY\NETWORKSERVICE  
Password: \*\*\*\*\*

Previous Next Cancel

The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.



In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.

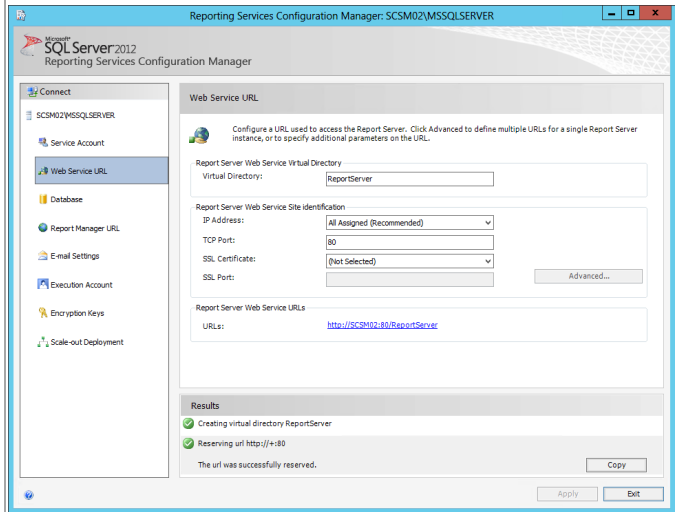




In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer** in the provided text box.
- In the **Report Server Web Service Site Identification** section, set the following values:
  - **IP Address** – set the **All Assigned** drop-down menu value.
  - **TCP Port** – specify the desired **TCP Port** (default 80).
  - **SSL Certificate** – select the available certificate or choose the default of **(Not Selected)**.

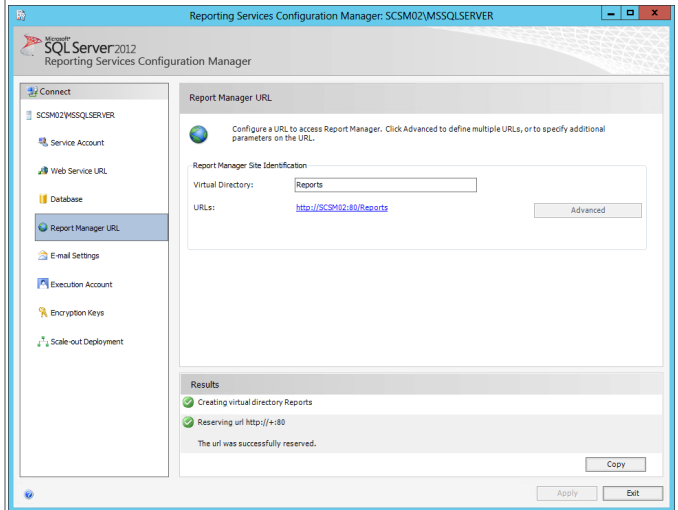
Click the **Apply** button to save the settings and create the Web Service URL.



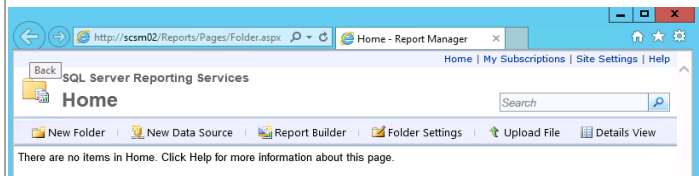
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

- In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports** (default) in the provided text box.

Click the **Apply** button to save the settings and create the Report Manager URL.



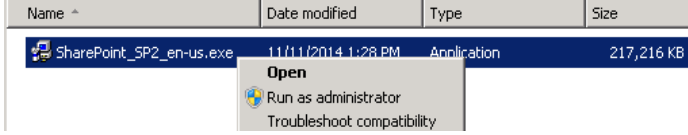
Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



<p>Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.</p> <p><i>Note that in order to test the URL directory from the Service Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.</i></p>	
<p>Close the Reporting Server Configuration Manager.</p>	

## Install SharePoint Foundation 2010 SP2 on the Self-Service Portal Server

SharePoint Foundation 2010 SP2 must be installed to allow for configuration of SharePoint with the SQL Server 2012 installation. The following steps must be completed in order to install SharePoint Foundation 2010 SP2 on the Service Manager self-service portal server only.

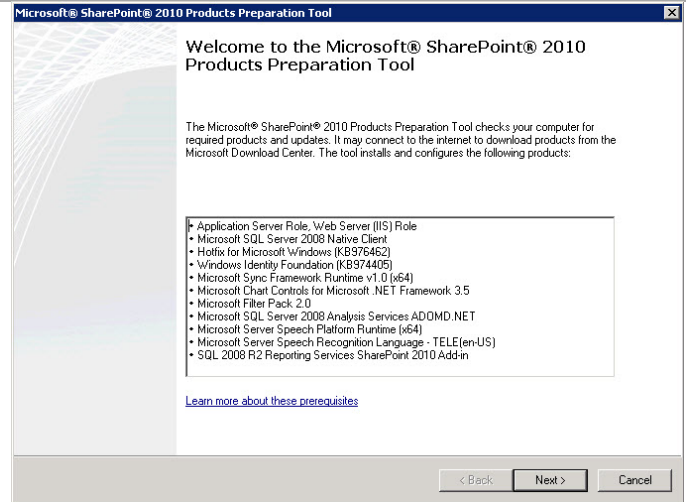
<p><b>Perform the following steps on the <b>Service Manager self-service portal (SCSM03) virtual machine.</b></b></p> <p>This procedure assumes internet connectivity for this virtual machine. If the virtual machine does not have internet connectivity see the list of files in the Overview section that will need to be downloaded and installed manually before running these steps.</p>									
<p>Log on to Service Manager self-service portal server (<b>NOT</b> a Service Manager management server or the Data Warehouse server). Locate the SharePoint Foundation 2010 installation file. Right-click <b>SharePointFoundation.exe</b> and select <b>Run as administrator</b> from the context menu to begin setup.<sup>12</sup></p>	 <table border="1" data-bbox="857 1045 1541 1081"> <thead> <tr> <th>Name</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>SharePoint_SP2_en-us.exe</td> <td>11/11/2014 1:28 PM</td> <td>Application</td> <td>217,216 KB</td> </tr> </tbody> </table>	Name	Date modified	Type	Size	SharePoint_SP2_en-us.exe	11/11/2014 1:28 PM	Application	217,216 KB
Name	Date modified	Type	Size						
SharePoint_SP2_en-us.exe	11/11/2014 1:28 PM	Application	217,216 KB						

<sup>12</sup> Microsoft SharePoint Foundation 2010 - <http://www.microsoft.com/en-us/download/details.aspx?id=24983>.

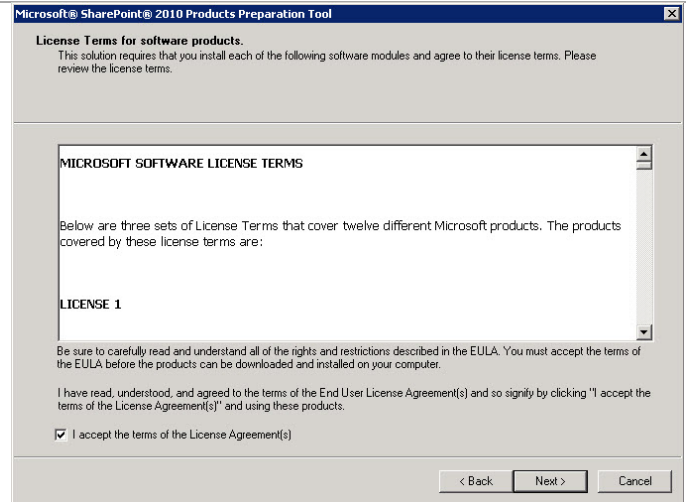
The **SharePoint Foundation 2010** setup dialog will appear. In the **Install** section, select **Install software prerequisites**.



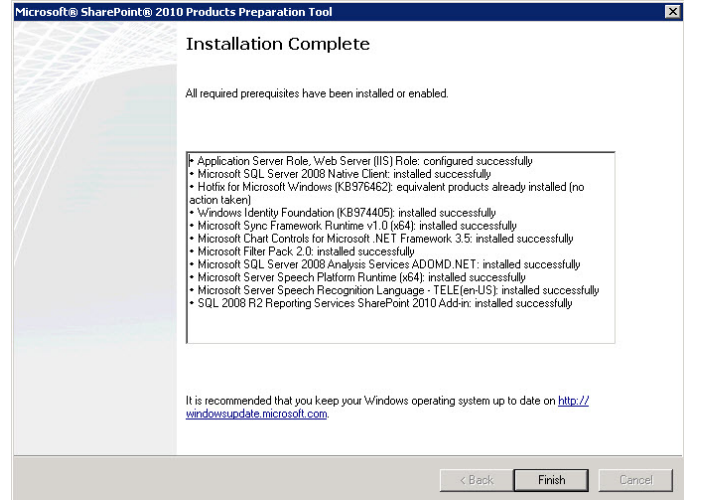
The **Microsoft SharePoint 2010 Products Preparation Tool** will open. Click **Next** to continue.



In the **License Terms for software products** dialog, verify that the **I accept the terms of the License Agreement** installation option check box is selected and click **Next** to continue.



After the prerequisites install, the **Installation Complete** dialog will appear. Click **Finish** to complete the installation then **restart** the system.

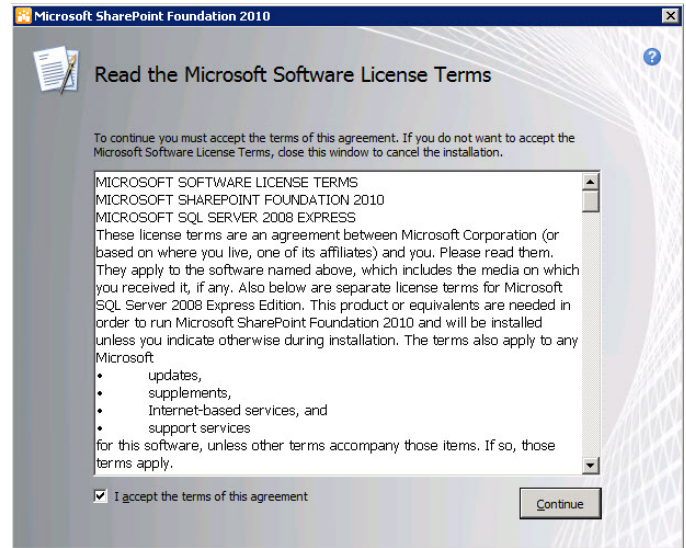


Perform the following steps on the **Service Manager self-service portal (SCSM03) virtual machine**.

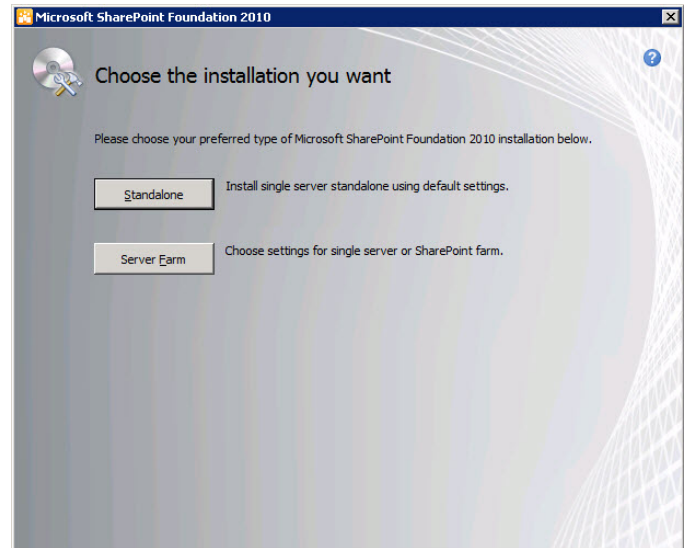
After the system restart, log back on with an account with administrative privileges. Re-launch the SharePoint Foundation 2010 installation. In the **SharePoint Foundation 2010** setup dialog, navigate to the **Install** section and select **Install SharePoint Foundation**.



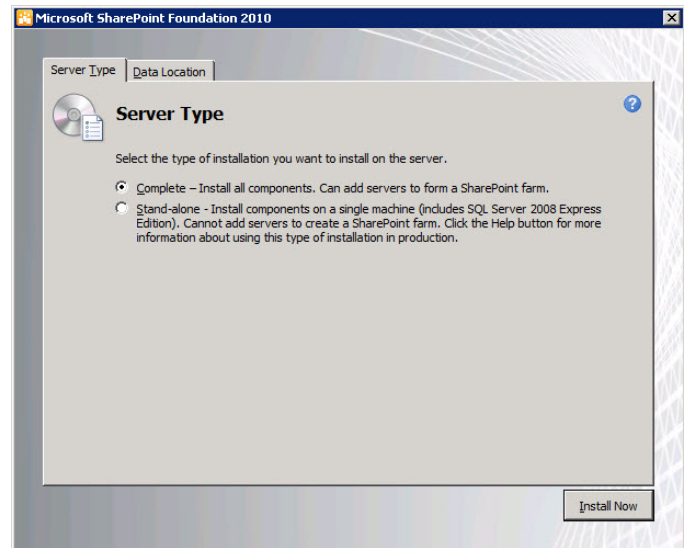
In the **Read the Microsoft Software License Terms** dialog, verify that the **I accept the terms of this Agreement** installation option check box is selected and click **Continue**.



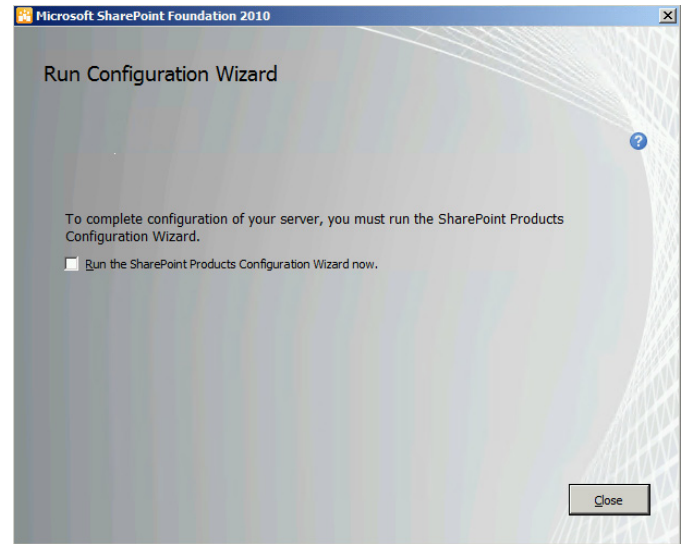
In the **Choose the installation you want** dialog, click the **Server Farm** button.



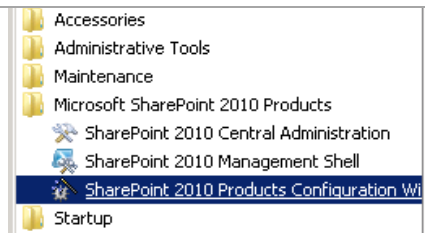
In the **Server Type** dialog, select the **Complete** option and click **Install Now**.



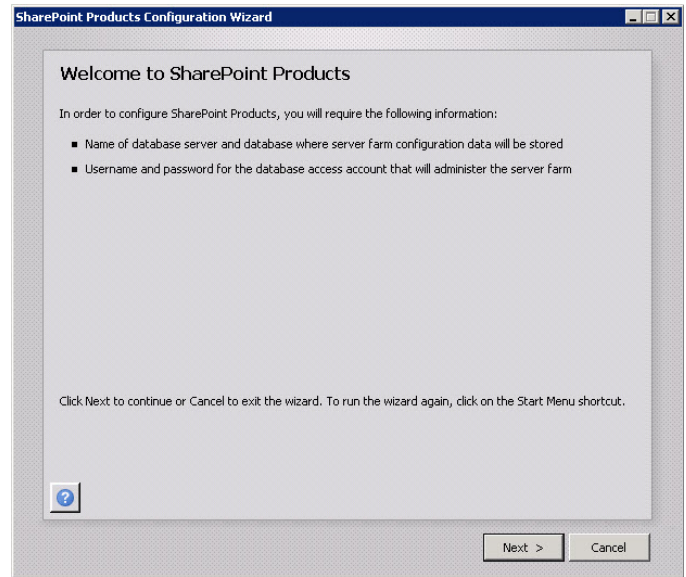
After installation, the **Run Configuration Wizard** dialog will appear. Verify that the **Run the SharePoint Products Configuration Wizard now** check box is not selected and click **Close**. Restart the system.



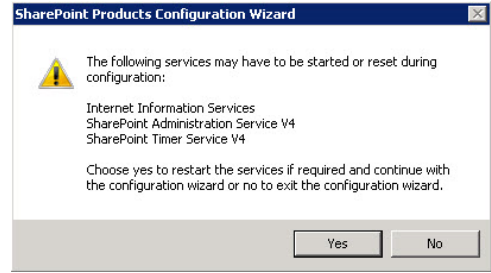
From the **Start** menu, expand the **Microsoft SharePoint 2010 Products** program folder and select **SharePoint 2010 Products Configuration Wizard**.



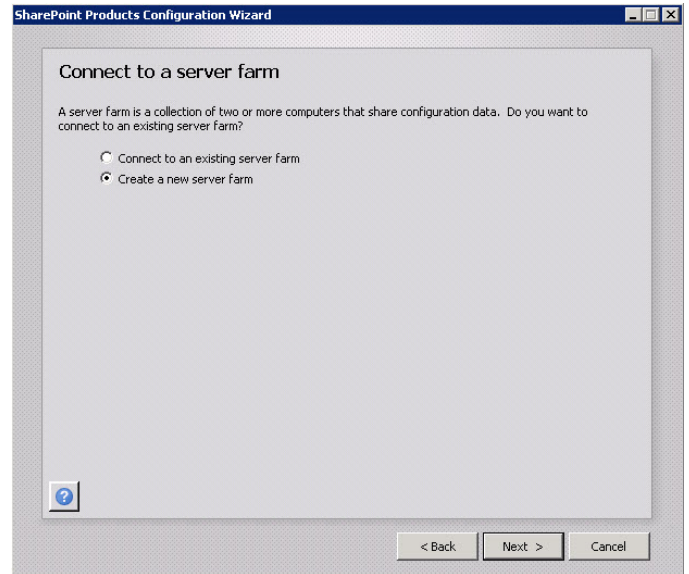
The **SharePoint Products Configuration Wizard** will appear. Click **Next** to continue with the wizard.



A dialog will appear that states that some services require restart as part of the installation. Click **Yes** to perform the services restart.



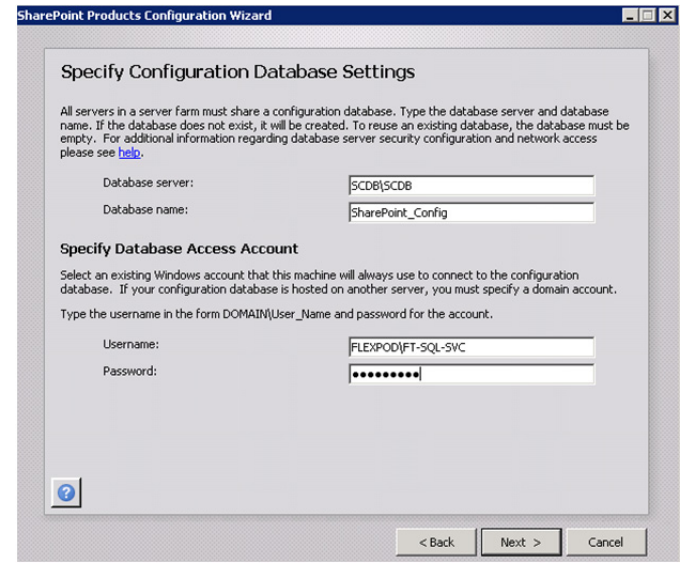
The **Connect to a server farm** dialog will appear. Select the **Create a new server farm** option and click **Next** to continue.



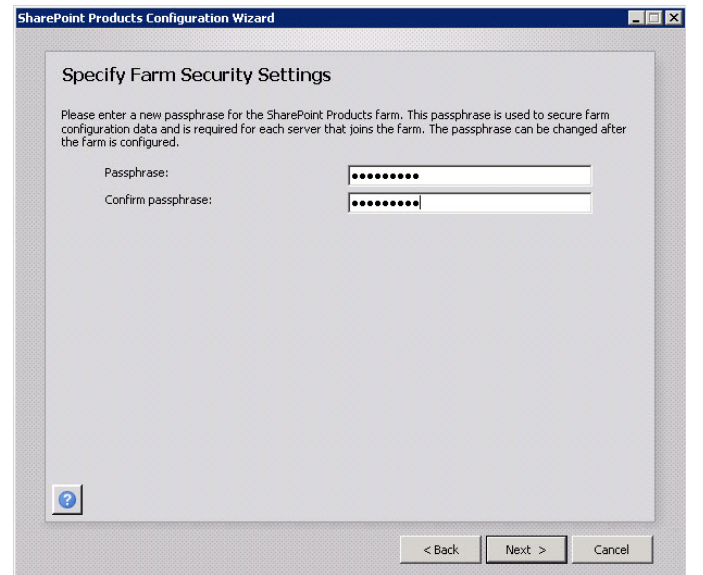
In the **Specify Configuration Database Settings** dialog, specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server CNO and the database instance created for the Service Manager installation.
- **Database name** – specify the name of the SharePoint database. In most cases the default value of *SharePoint\_Config* should be used.

In the **Specify Database Access Account** section, specify the Username (<DOMAIN>\<USERNAME>) and associated password for the SQL Server service account. When complete, click **Next** to continue.



In the **Specify Farm Security Settings** dialog, enter a unique passphrase in the **Passphrase** text box. Re-type the passphrase in the **Confirm passphrase** text box and click **Next** to continue.



In the **Configure SharePoint Central Administration Web Application** dialog specify a TCP port by selecting the **Specify port number** check box and providing a port number in the supplied text box.

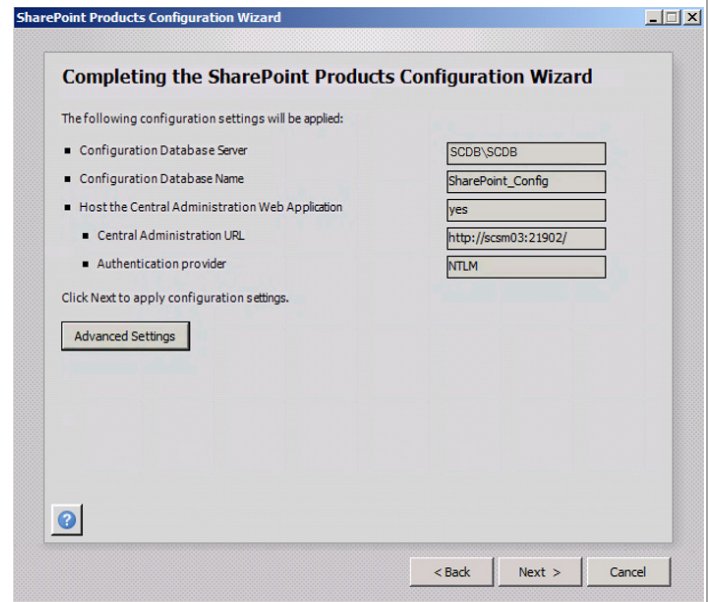


In the **Configure Security Settings** section, select the **NTLM** option.

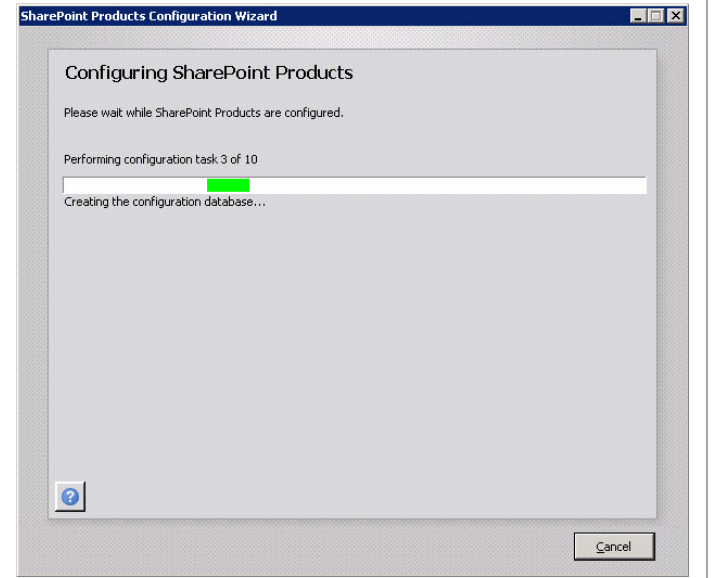
When completed, click **Next** to continue.



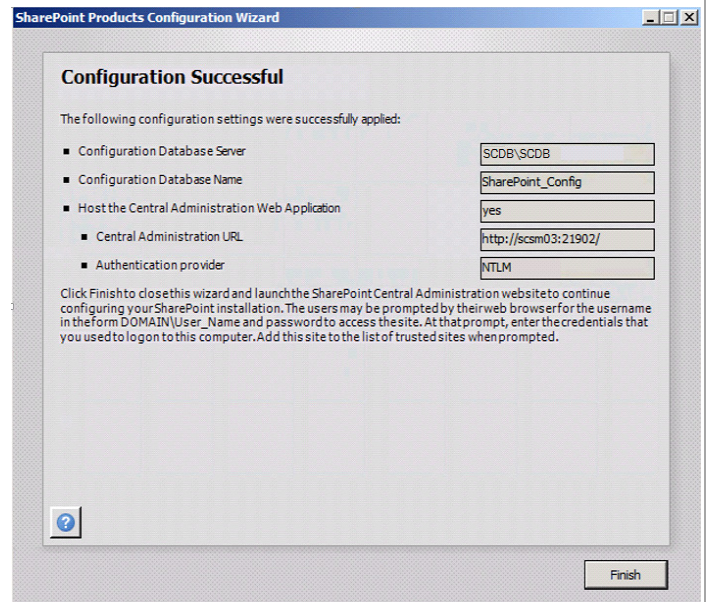
The **Completing the SharePoint Products Configuration Wizard** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Next** to continue.



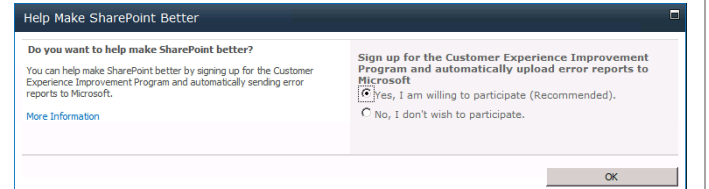
The wizard will display the progress while performing the SharePoint configuration.



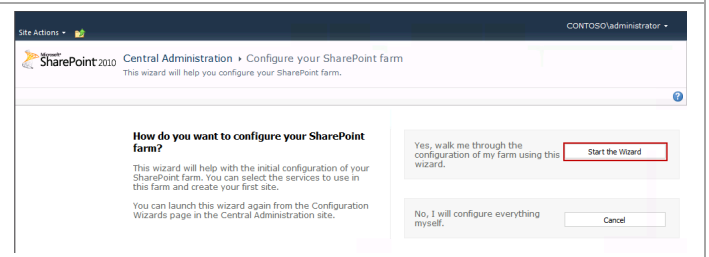
When successful, the **Configuration Successful** dialog will appear. Click **Finish** to complete the configuration of SharePoint Foundation 2010 Service Pack 2.



When prompted in the **Help Make SharePoint Better** page, select the appropriate option based on your organization's policies and click **OK** to save this setting.



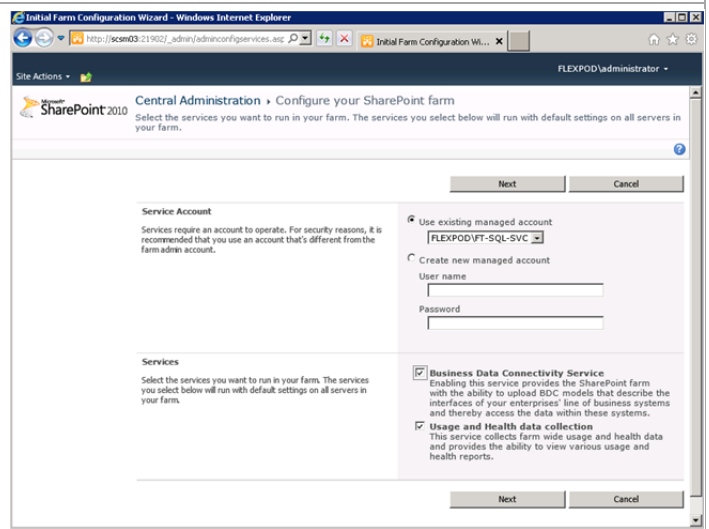
In the **Central Administration - Configure your SharePoint farm** page; click the **Start the Wizard** button to begin the SharePoint configuration.



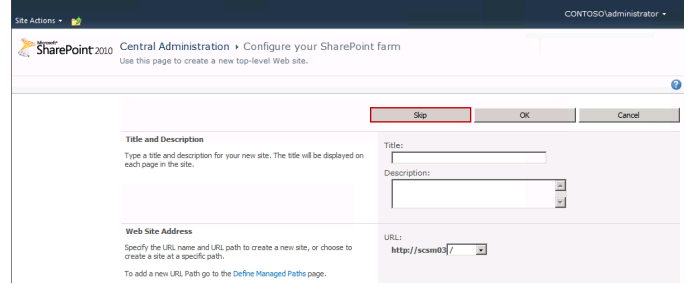
In the **Service Account** section, select the **Use existing managed account** and select the Service Manager Service Account from the drop-down menu.

In the **Services** section, select the **Business Data Connectivity Services** and **Usage and Health data collection** check boxes.

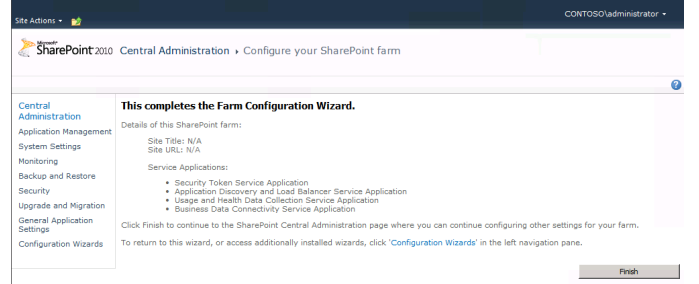
Click **Next** to continue.



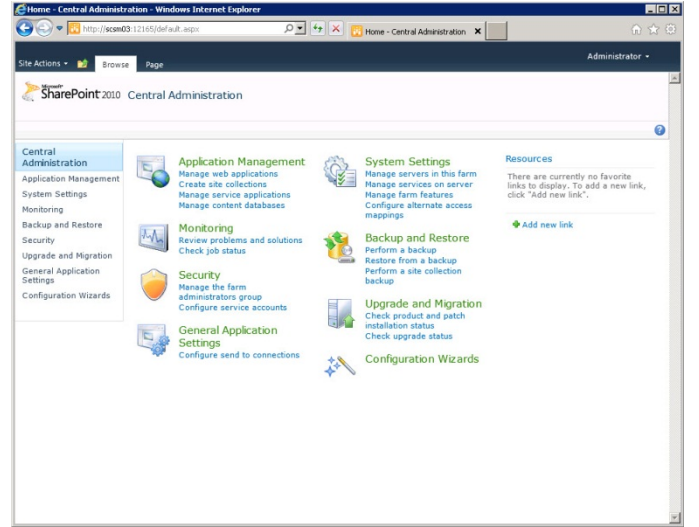
In the Web Site configuration page, click the **Skip** button to continue without configuring these settings.



The SharePoint farm configuration is now complete. Click the **Finish** button to exit.



The **SharePoint Central Administration** portal will open. Verify that SharePoint is operating properly by launching the Central Administration portal prior to proceeding to the Service Manager self-service portal installation.

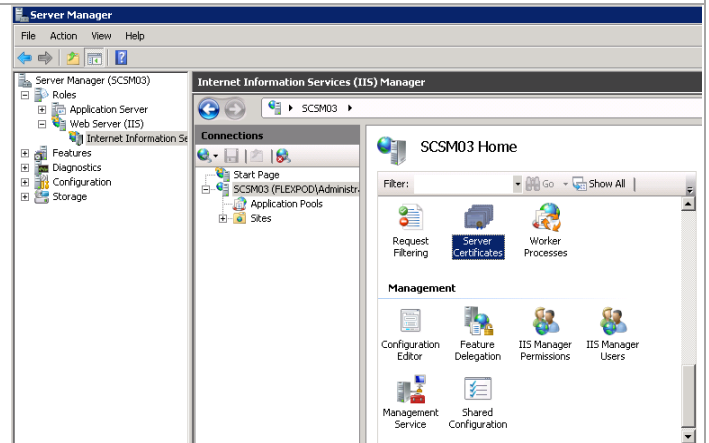


## Request and Install SSL Certificate on the Self-Service Portal Server

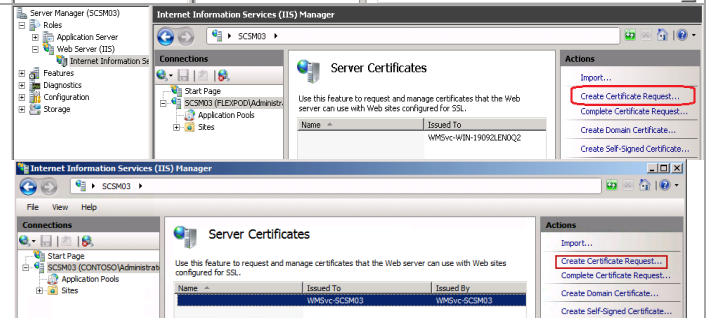
Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website.<sup>13</sup> If the self-service portal is to be installed without SSL this section can be skipped. There are several ways to request an SSL 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.**

Log on to the Service Manager virtual machine with a user with local admin rights. In the **Server Manager** console navigate to **Roles > Web Server (IIS) > Internet Information Services (IIS) > Server Certificates**. Under Connections click on the server node and double-click **Server Certificates**.

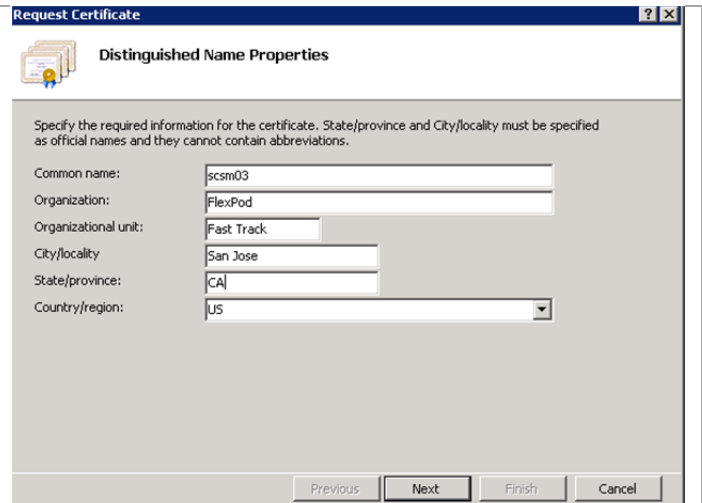


The **Server Certificates** pane will expand. Under actions, click **Create Certificate Request...**

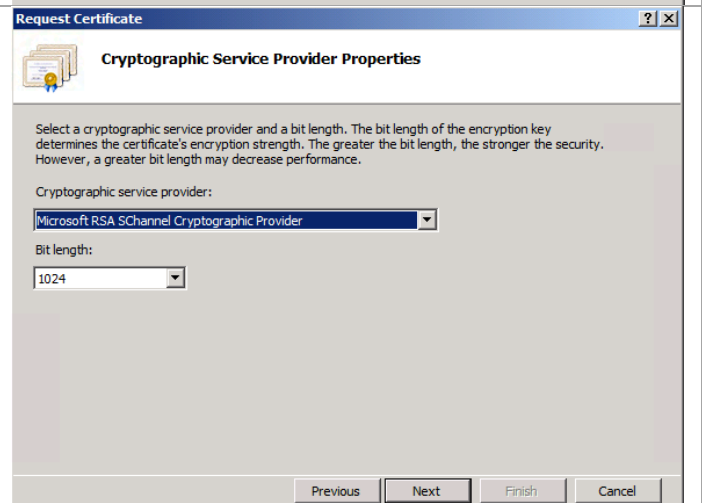


<sup>13</sup> SSL Certificates for the self-service portal - <http://technet.microsoft.com/en-us/library/hh667343.aspx>.

The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name that the server will be accessed in the web browser. Click **Next** to continue.

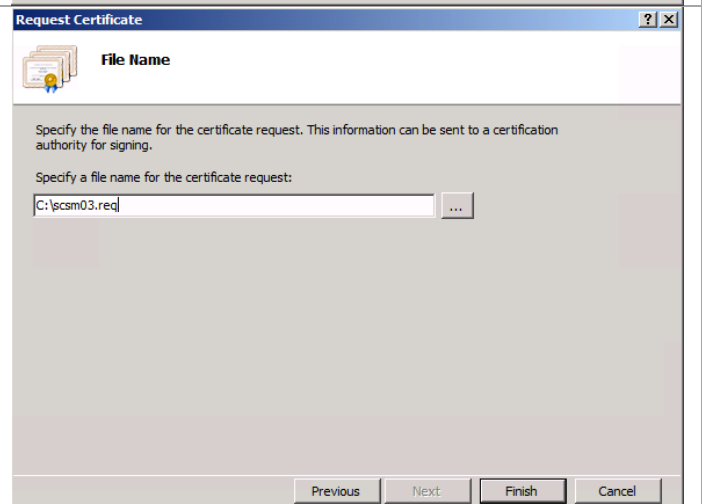


In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing certification authority (CA). In most cases, selecting the default CSP and default bit length is satisfactory. Click **Next** to continue.

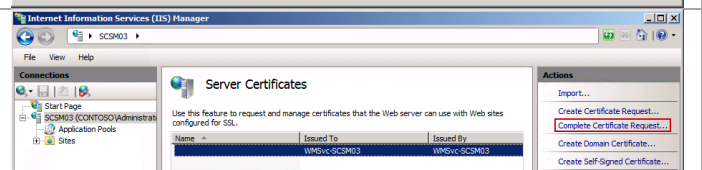


In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

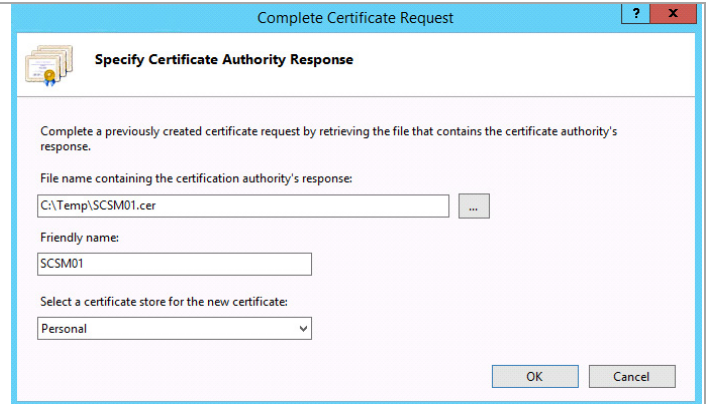
When completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.



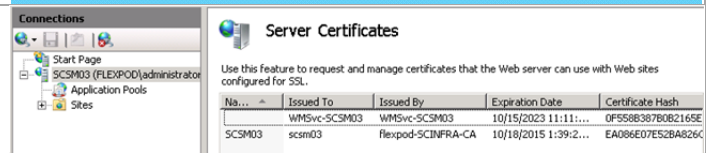
After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** once again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Accept the default certificate store of Personal. Click **OK** to complete the operation.



In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.



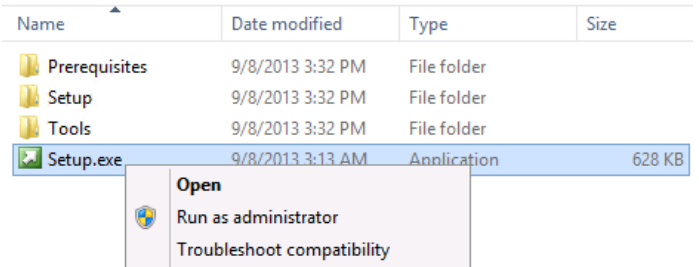
## 21.3 Installation

### Install the Service Manager Management Server

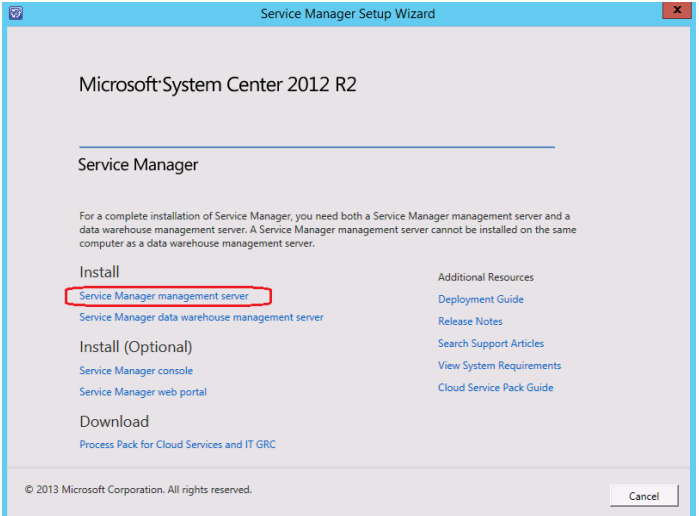
The following steps must to be completed in order to install the Service Manager Management server role.

Perform the following steps on the **first Service Manager Management server (scsm01) virtual machine.**

Log on to Service Manager management server (**NOT** the Service Manager Data Warehouse server nor the self-service portal server).  
From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



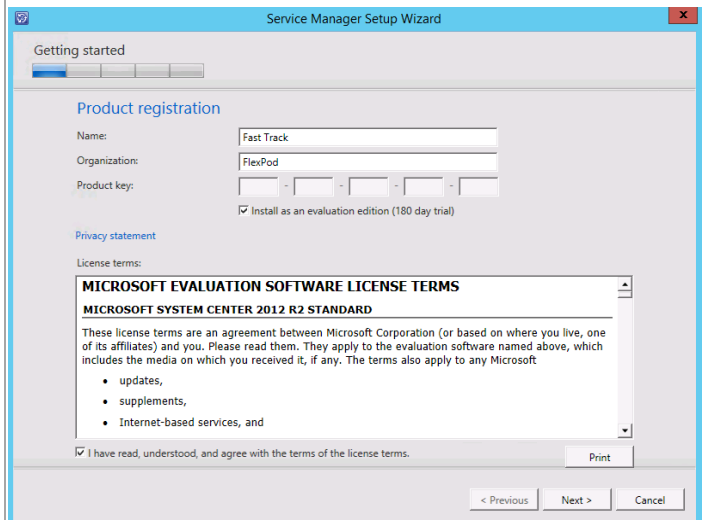
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager management server** to begin the Service Manager server installation.



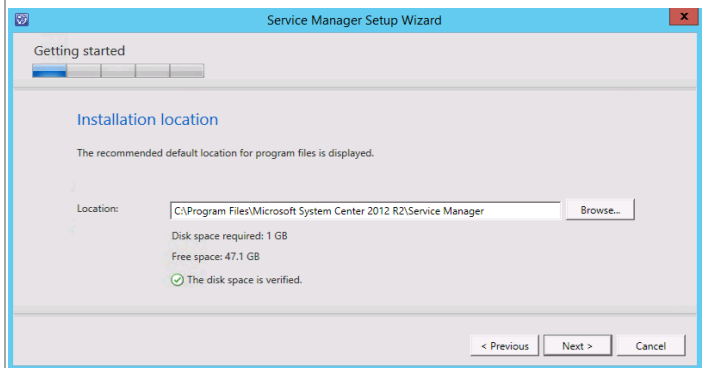
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name** – specify the name of the primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.
- **Product key** – provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.

In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.

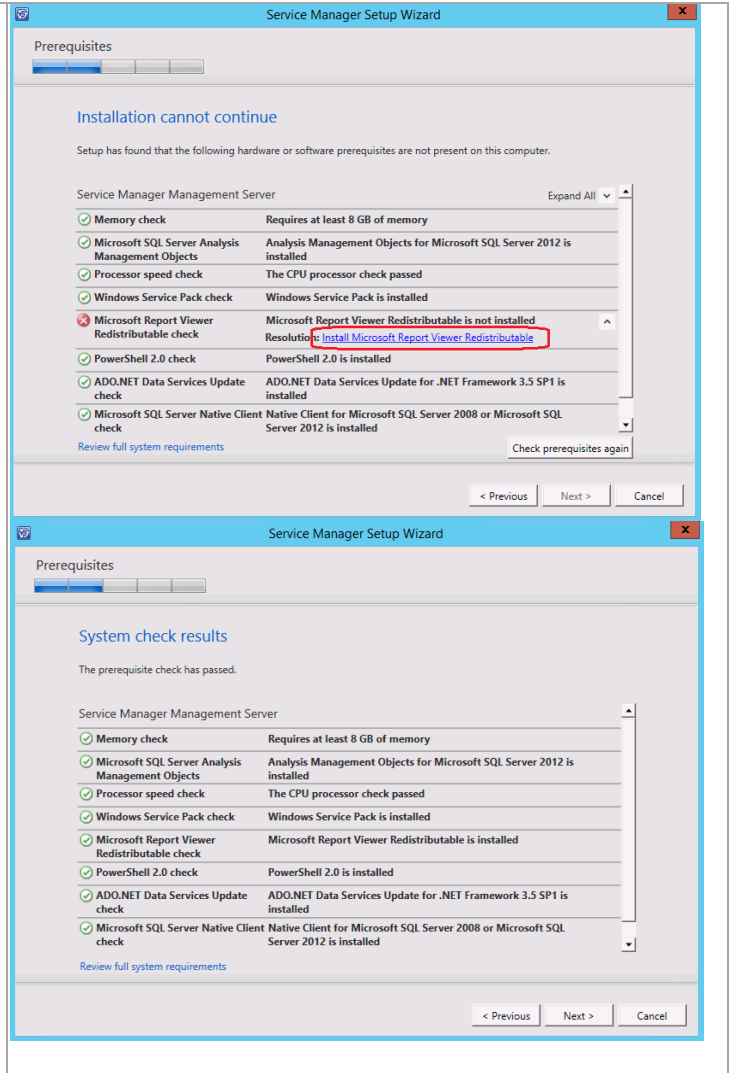


In the **Installation location** dialog, specify a location or accept the default location of `%ProgramFiles%\Microsoft System Center 2012 R2\Service Manager` for the installation. Click **Next** to continue.





The setup will verify that all system prerequisites are met in the **System check results** dialog. Even though the Report Viewer has been previously installed, this installation requires installation of the bits included with this installation. Click on the link to **Install Microsoft Report Viewer Redistributable** and click through the installation. When the Report Viewer installation completes, check the prerequisites again. If any prerequisites other are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



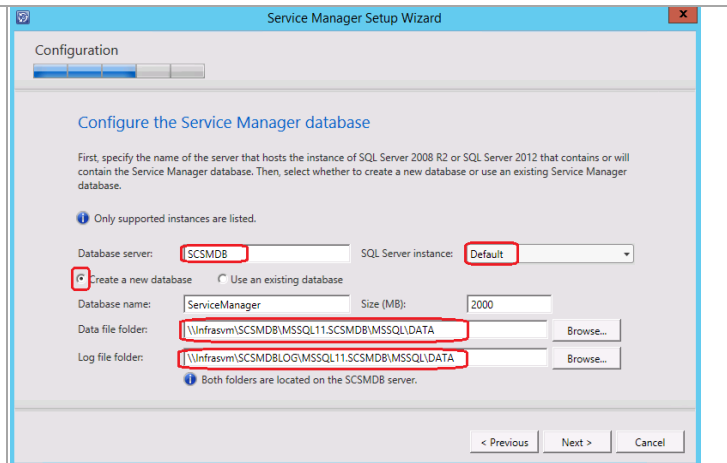
In the **Configure the Service Manager database** dialog, specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation.
- **SQL Server instance** – specify Default as the name of the SQL Server database instance created for the Service Manager installation.

Select the **Create a new database** option and specify the following information in the provided text boxes:

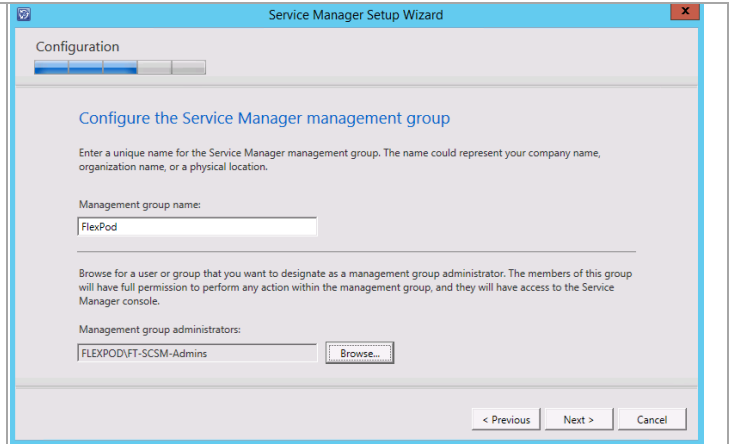
- **Database name** – specify the name of the Service Manager database. In most cases the default value of ServiceManager should be used.
- **Size (MB)** – specify the initial database size<sup>14</sup>. The default value can be used for Fast Track validation.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager database. This should be cross-checked with the worksheet identified earlier. Ensure the proper SMB share location is specified.
- **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. Ensure the proper SMB share location is specified.

Click **Next** to continue.

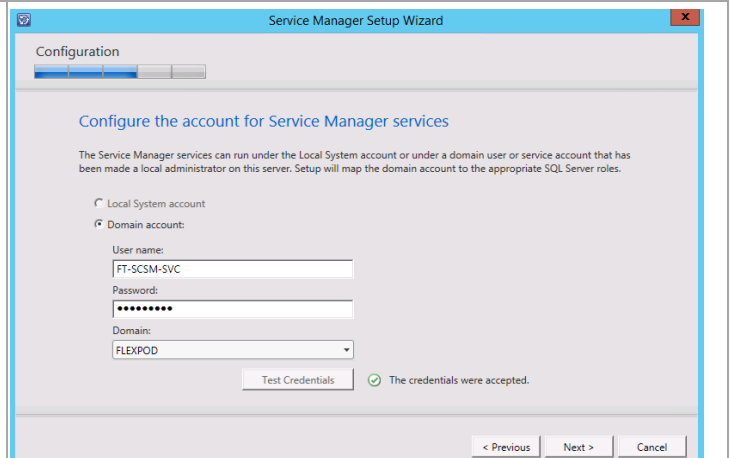


<sup>14</sup> Planning for Performance and Scalability in System Center 2012 - Service Manager - <http://technet.microsoft.com/en-us/library/hh495684.aspx> contains a link to the Service Manager job aids and provides general guidance for database sizing

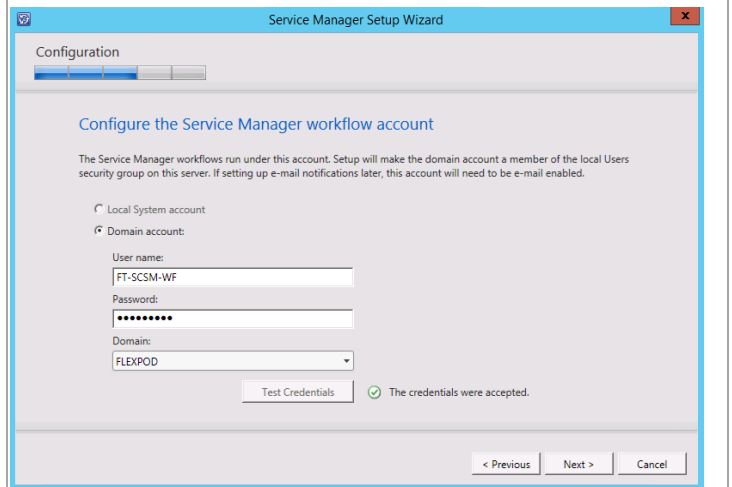
In the **Configure the Service Manager management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager Data Warehouse and Operations Manager installations. Specify the Service Manager Administrators group in the **Management group administrators** object picker section. Click **Next** to continue.



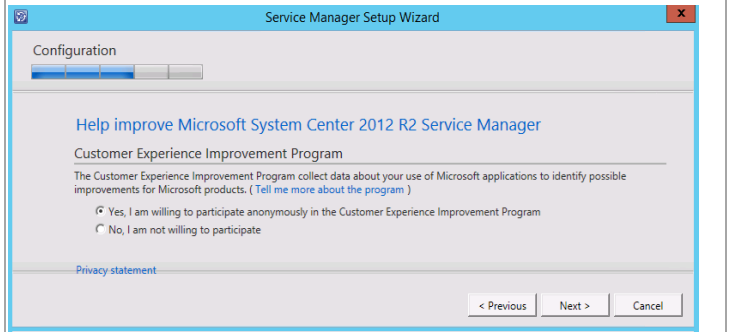
In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.



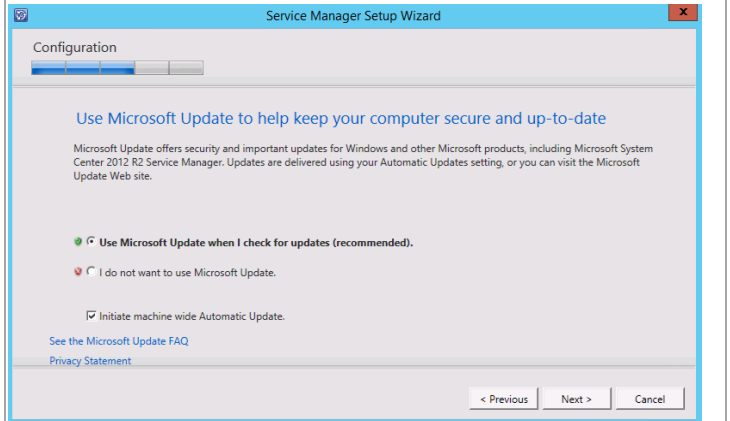
In the **Configure the account for Service Manager workflow account** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.



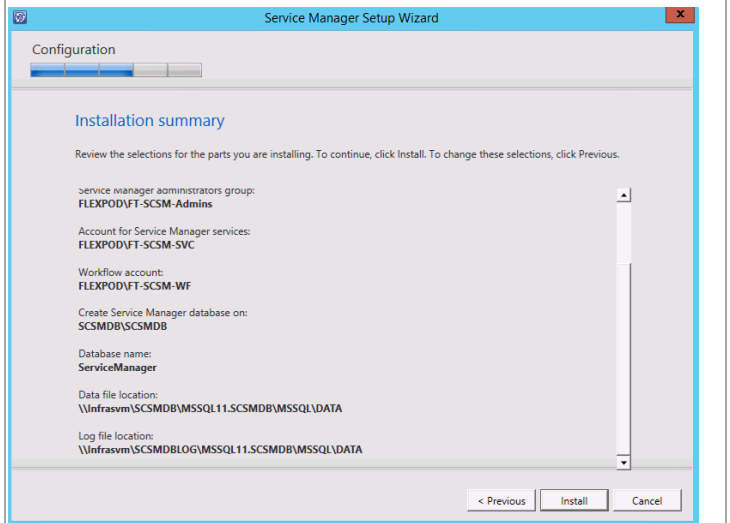
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



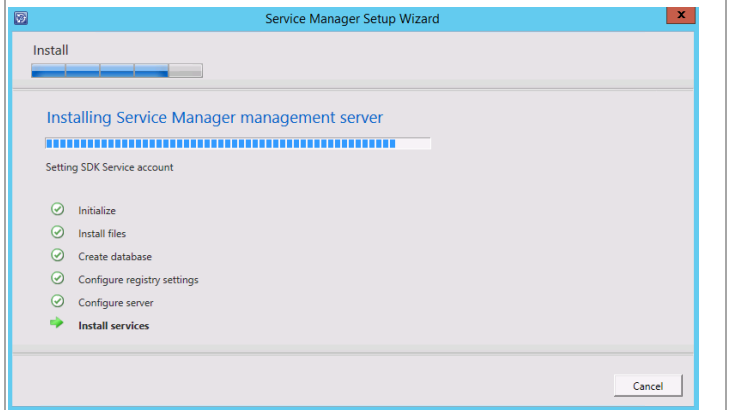
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



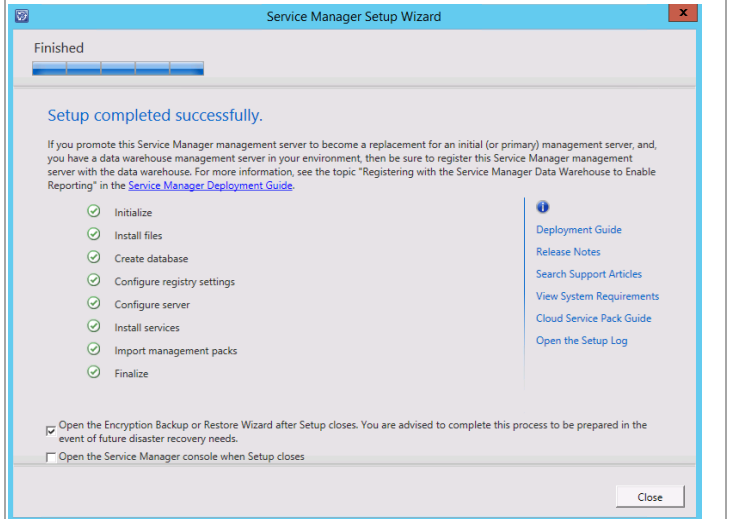
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** dialog.

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.

Click **Close** to complete the installation.



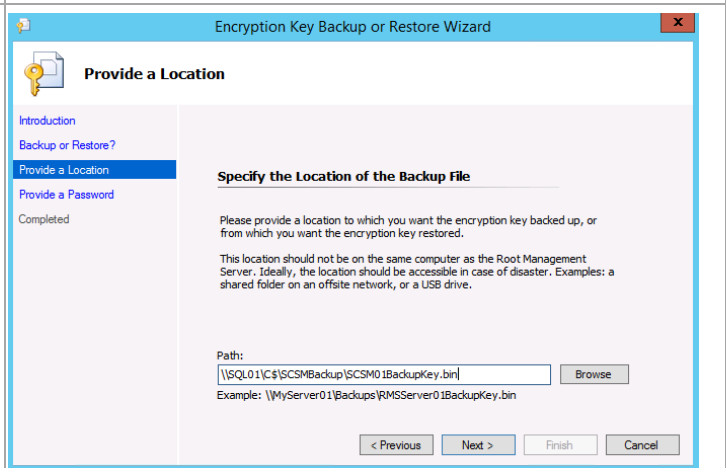
When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



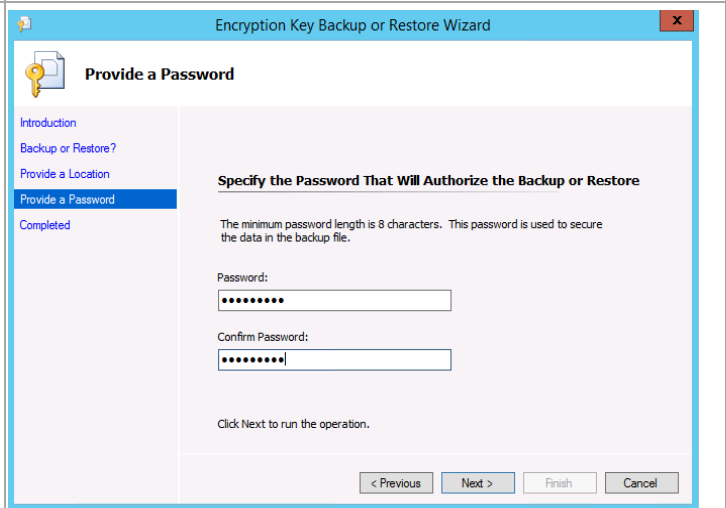
In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.



In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** text box and object picker. The path must be an existing path. Click **Next** to continue.



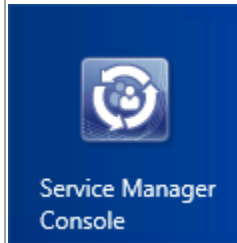
In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.



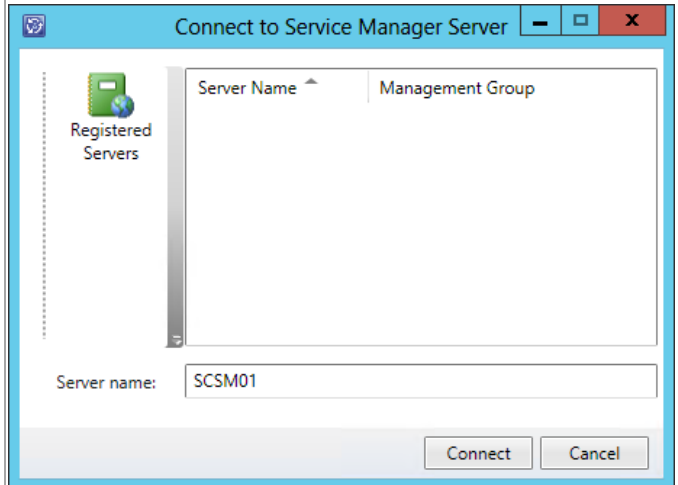
When complete, click **Finish** to exit the wizard.



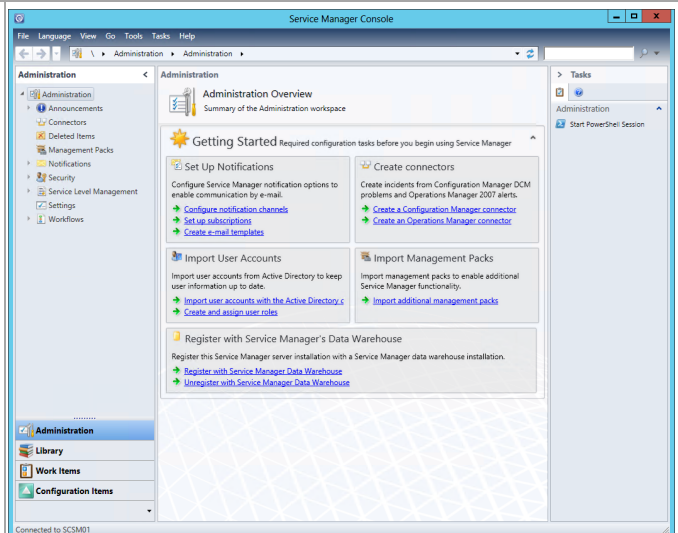
When installed, verify that the Service Manager management server installed properly by opening the console. From the **Start** screen, click the **Service Manager Console** tile.



In the **Connect to Service Manager Server** dialog, specify the Service Manager management server name in the **Server name** text box and click **Connect** to start the console.



The Service Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



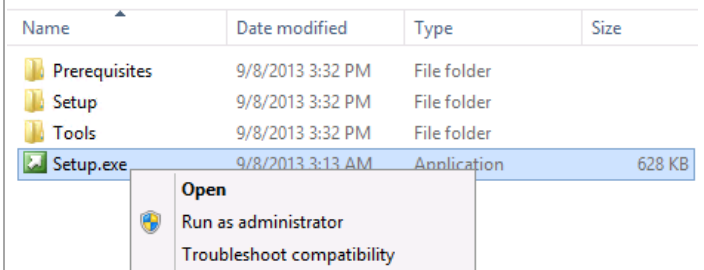
## Install the Service Manager Data Warehouse Server

The following steps must to be completed in order to install the Service Manager Data Warehouse server role.

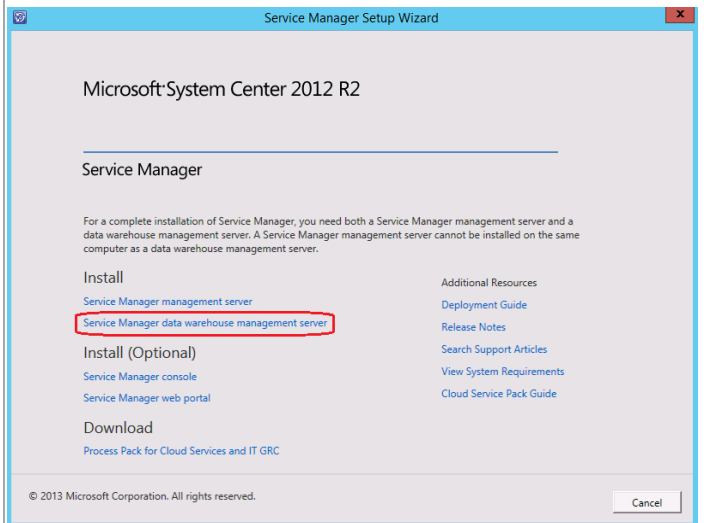
**Perform the following steps on the Service Manager Data Warehouse server (scsm02) virtual machine.**

Log on to Service Manager Data Warehouse server (**NOT** the Service Manager management server or the self-service portal server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



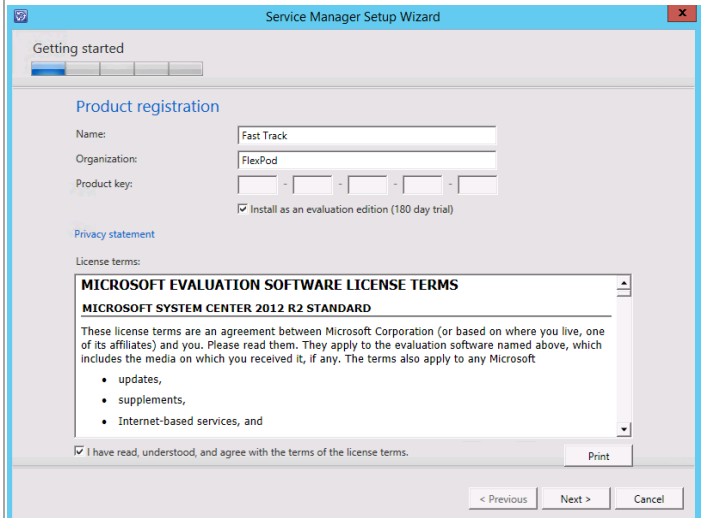
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager data warehouse management server** to begin the Service Manager server installation.



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

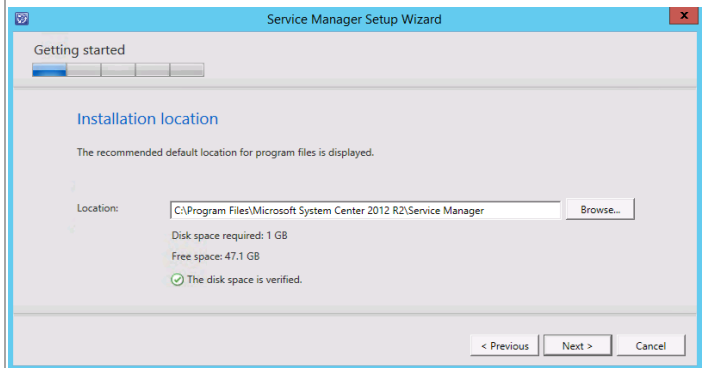
- **Name** – specify the name of the primary user or responsible party within your organization.
- **Organization** - specify the name of the licensed organization.
- **Product key** – provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.

In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.

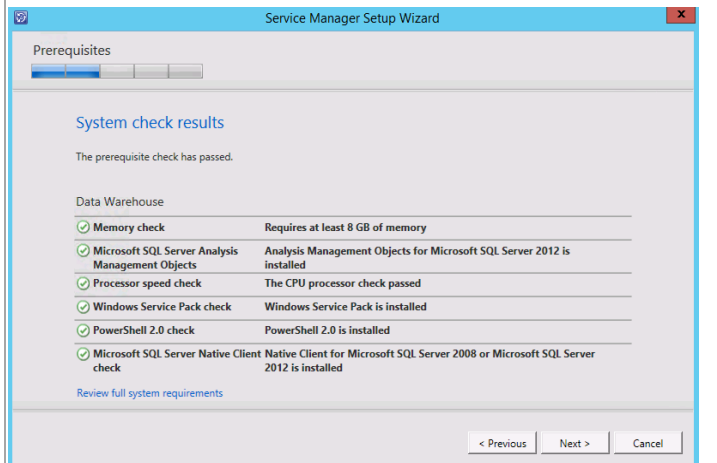




In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012 R2\Service Manager* for the installation. Click **Next** to continue.

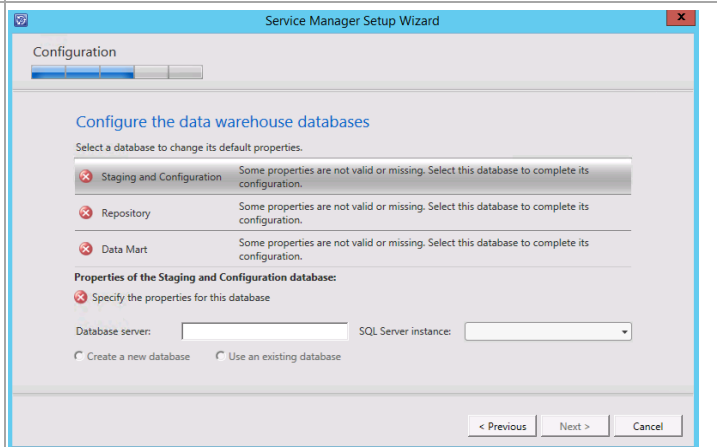


The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



When the **Configure the data warehouse databases** dialog launches each subcategory will appear with an error message until each of the following sections are configured:

- Staging and Configuration
- Repository
- Data Mart



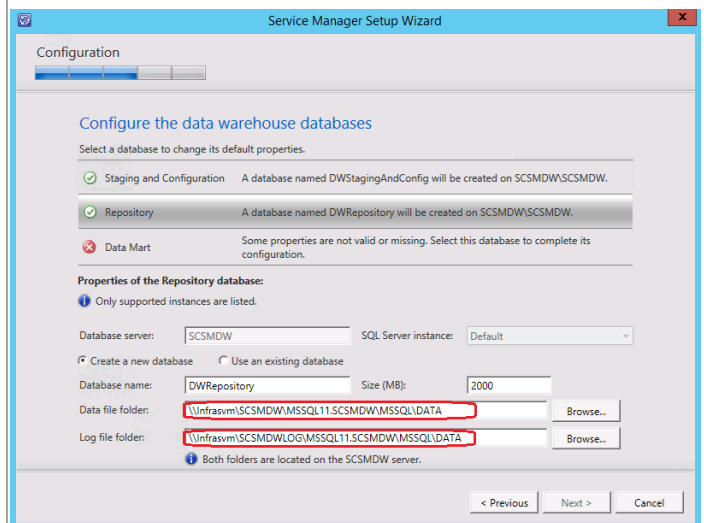
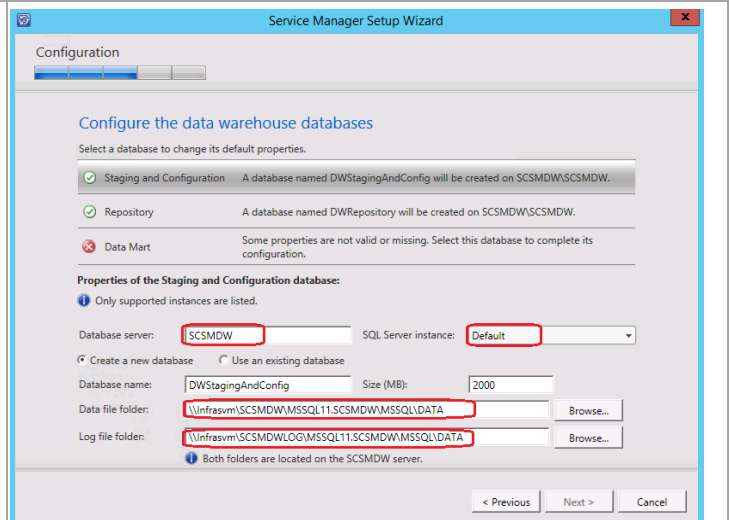
In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.
- **SQL Server instance** – specify Default as the name of the SQL Server database instance created for the Service Manager installation Data Warehouse.

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the SM Data Warehouse database. In most cases the default value of DWStagingAndConfig should be used for the Staging and Configuration section and DWRepository should be used for the Repository section.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. Set the correct value on the Staging and Configuration section as well as the Repository section. Ensure the proper SMB share location is specified.
- **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. Ensure the proper SMB share location is specified.
- Set the correct value on the Staging and Configuration section as well as the Repository section

Click **Data Mart** to continue.



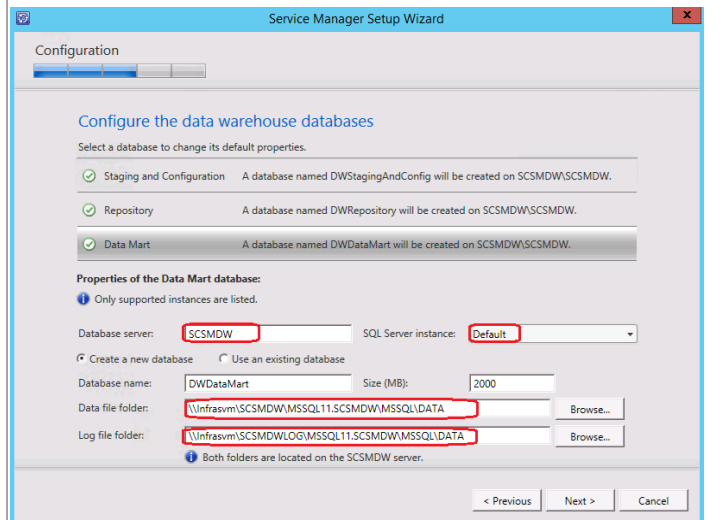
In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).
- **SQL Server instance** – specify Default as the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).

Select the **Create a new database** option and specify the following information in the provided text boxes:

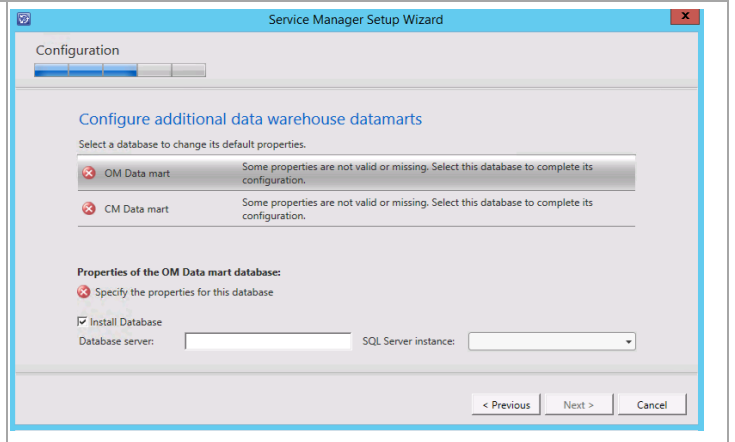
- **Database name** – specify the name of the Service Manager Data Warehouse database. In most cases the default value of DWDDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above) Ensure the proper SMB share location is specified.
- **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) Ensure the proper SMB share location is specified.

Click **Next** to continue.



When the **Configure additional data warehouse datamarts** dialog launches, each subcategory will appear with an error message until each of the following sections are configured:

- OM Data mart
- CM Data mart

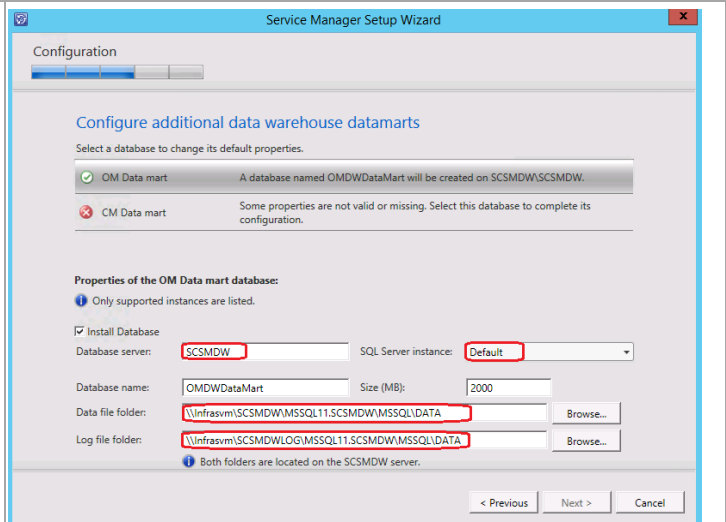


In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **OM Data Mart** section:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)
- **SQL Server instance** – specify **Default** as the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the Service Manager OM Data mart database. In most cases the default value of *OMDWDDataMart* should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager OM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above) Ensure the proper SMB share location is specified.
- **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) Ensure the proper SMB share location is specified.



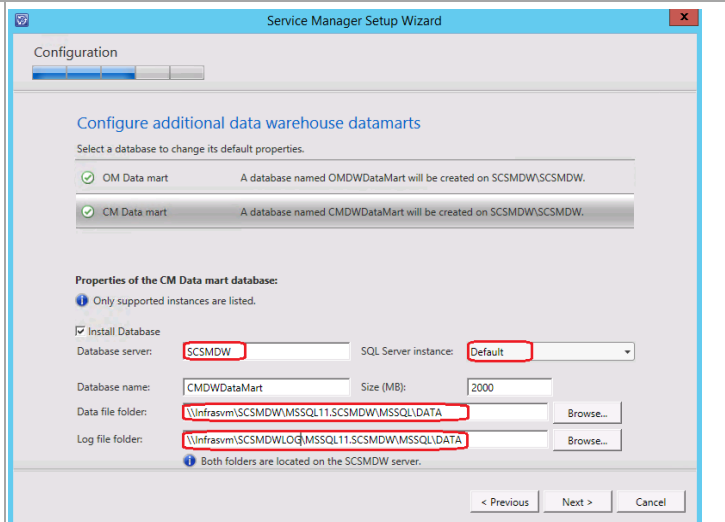
Optionally, a CM Data mart can be created for Configuration manager integration. To complete this, in the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **CM Data Mart** section:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)
- **SQL Server instance** – specify **Default** as the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the Service Manager CM Data mart database. In most cases the default value of CMDWDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager CM Data mart database. This should be cross-checked with the worksheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above) Ensure the proper SMB share location is specified.
- **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)

Ensure the proper SMB share location is specified

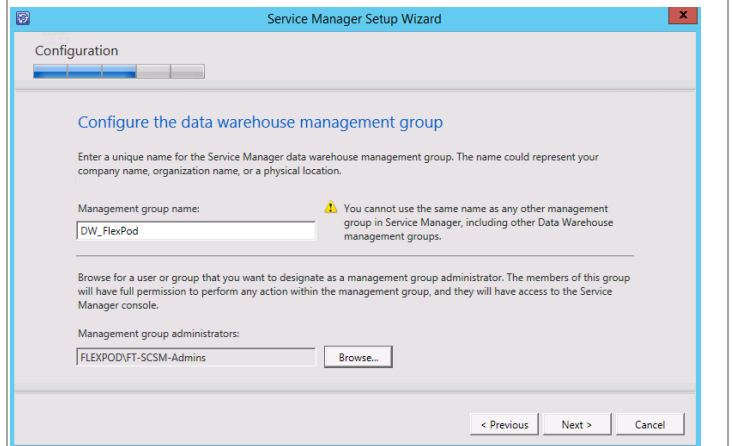


Click **Next** to continue.

In the **Configure the data warehouse management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager management server and Service Manager Operations Manager installations.

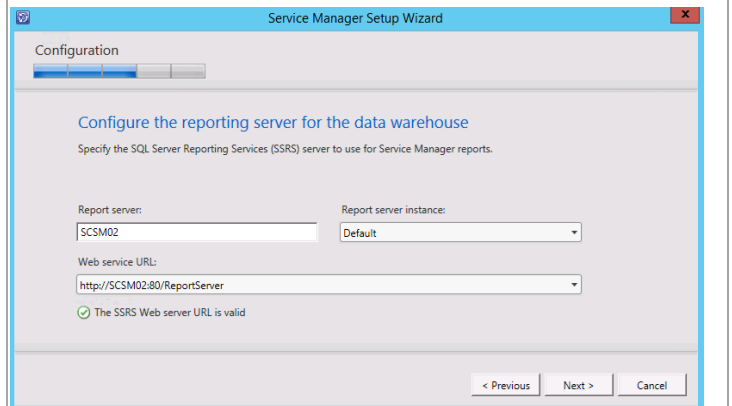
Specify the SM Administrators group in the **Management group administrators** object picker section.

Click **Next** to continue.



In the **Configure the reporting server for the data warehouse** dialog, the default values from this and the web server installations will be displayed and validated. If anything reports incorrectly, resolve the issue before continuing.

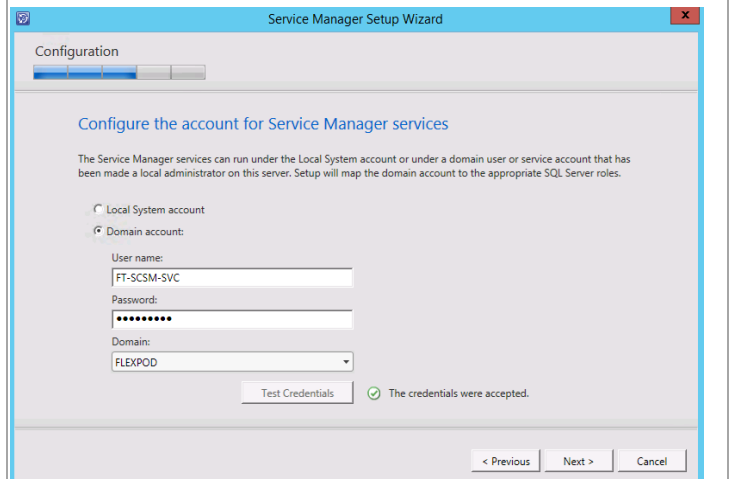
Click **Next** to continue.



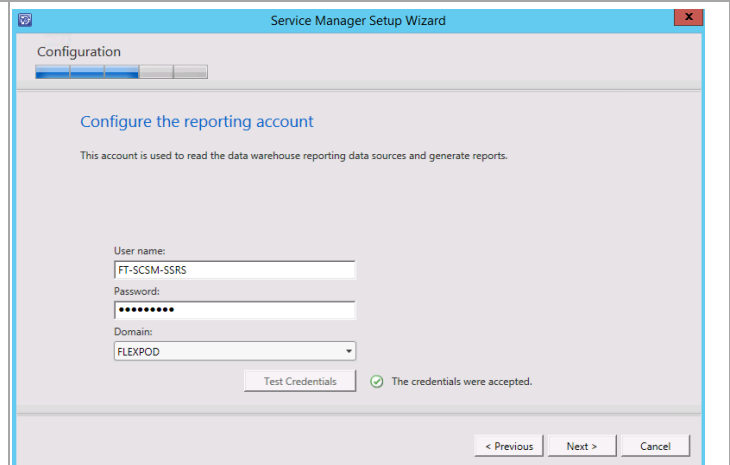
In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

When successful, click **Next** to continue.

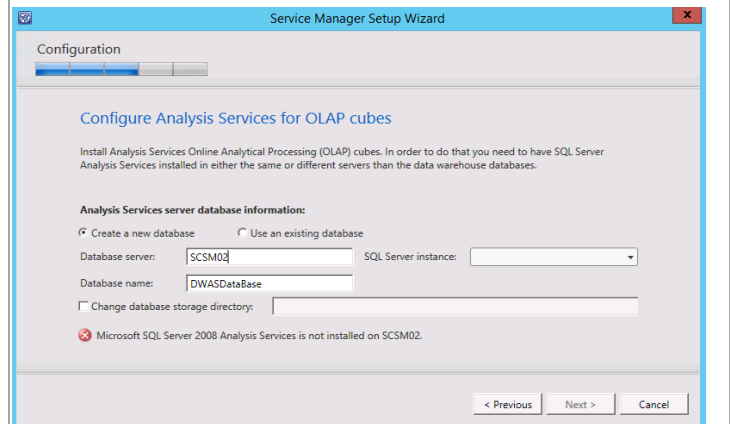


In the **Configure the reporting account** dialog, specify the SCSM SQL Server Reporting Services Account in the **User name** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. When successful, click **Next** to continue.

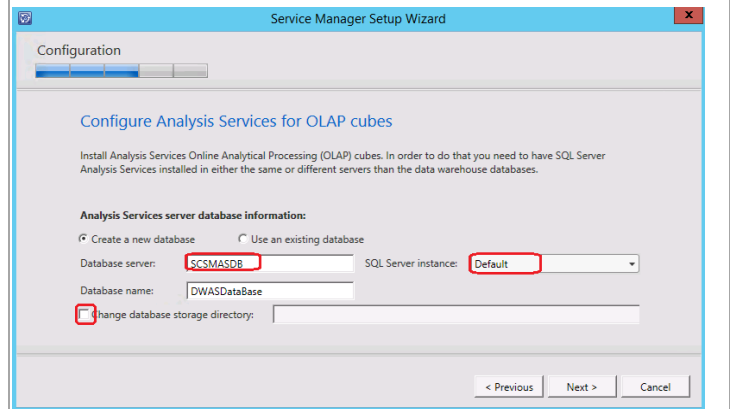


In the **Configure Analysis Services for OLAP cubes** dialog, select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server cluster CNO created for the Service Manager installation SQL Server Analysis Services.
- **SQL Server instance** – specify **Default** as the name of the SQL Server database instance created for the Service Manager installation SQL Server Analysis Services.
- **Database name** – specify the name of the SQL Server Analysis Services database. In most cases the default value of **DWASDataBase** should be used.



Confirm that the **Change database storage directory** check box is clear and click **Next** to continue.

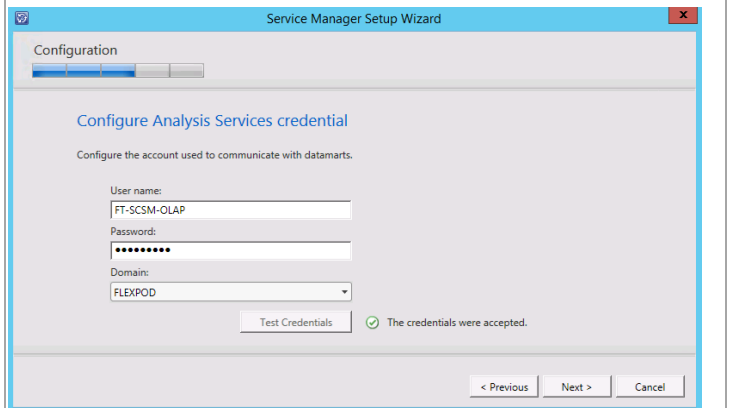




In the **Configure Analysis Services Credential** dialog, specify the SM OLAP Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

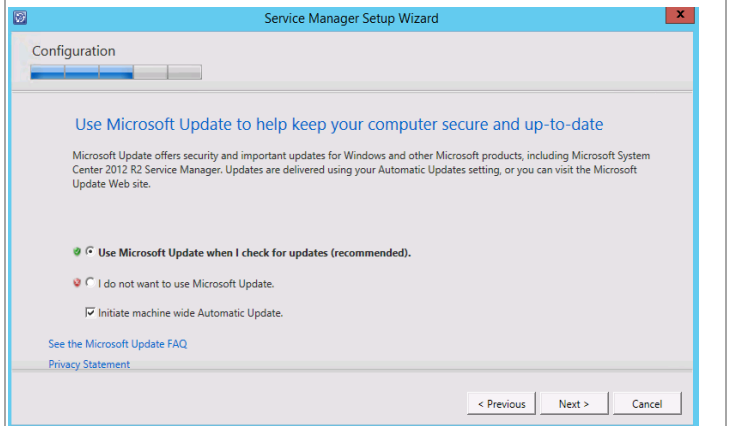
When successful, click **Next** to continue.



In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.

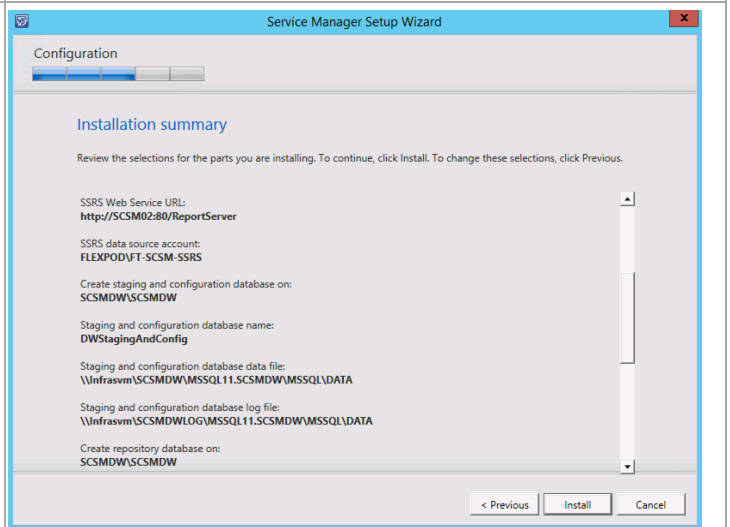


Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.

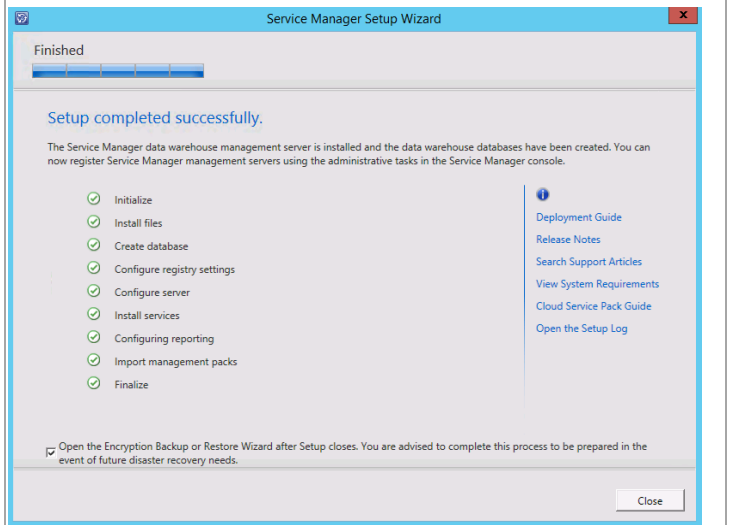


The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

The wizard will display the progress while installing features.



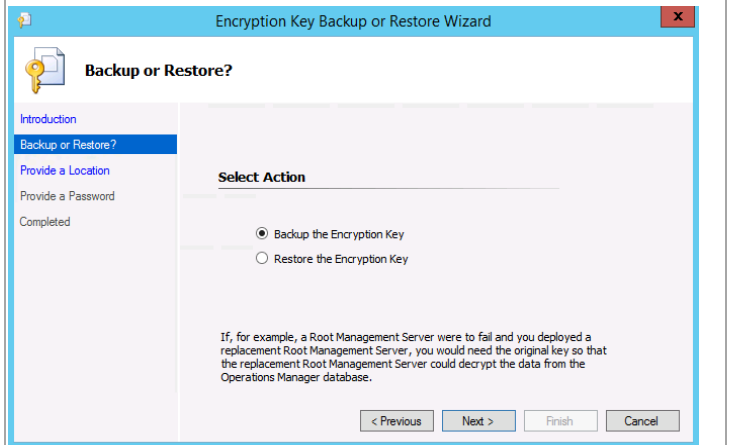
When the installation completes, the wizard will display the **Setup completed successfully** dialog. Ensure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to launch the wizard after setup. Click **Close** to complete the installation.



When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.



In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** text box and object picker. Click **Next** to continue.



In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.

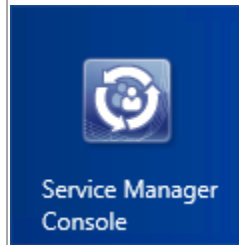


When complete, click **Finish** to exit the wizard.



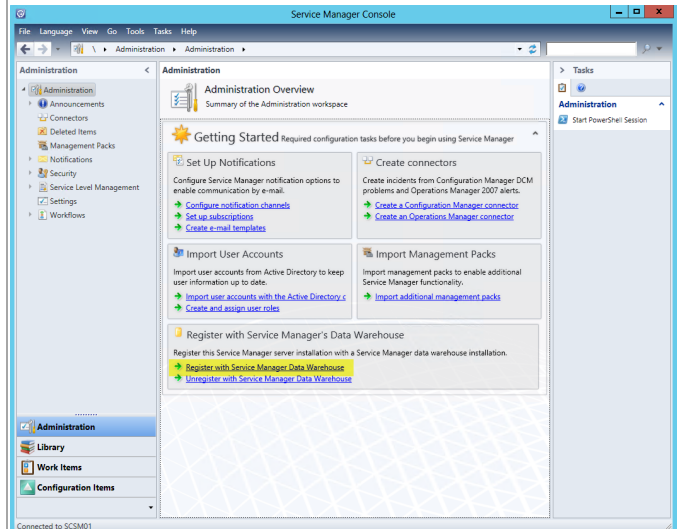
Perform the following steps on the **Service Manager Management server (SCSM01)** virtual machine to register the Service Manager Data Warehouse and enable reporting in the Service Manager instance.

Log in to the Service Manager management server using an account with administrator permissions. From the Windows **Start** screen, select the **Service Manager Console** tile.

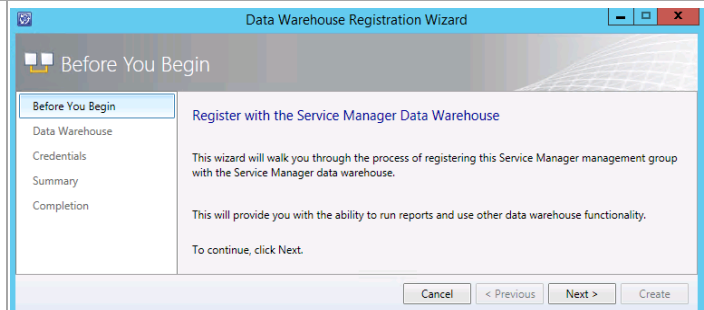


Within the **Service Manager Console**, select the **Administration** node and navigate to the **Register with Service Manager's Data Warehouse** section. Click the **Register with Service manager Data Warehouse** link to enable reporting.

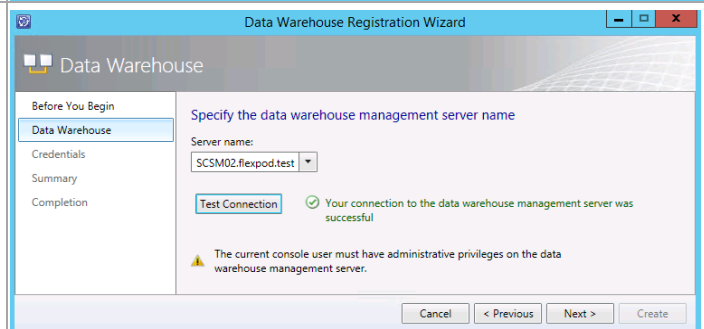
**Note:** If the console was open from the previous installation, close it and re-open the console.

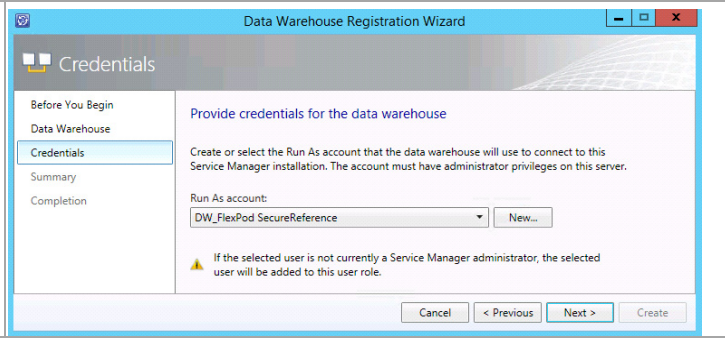
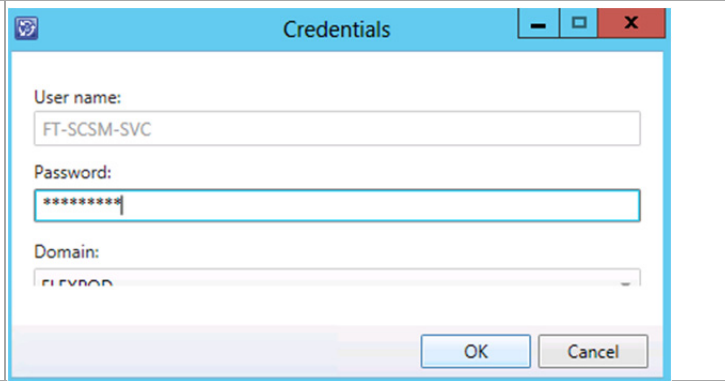
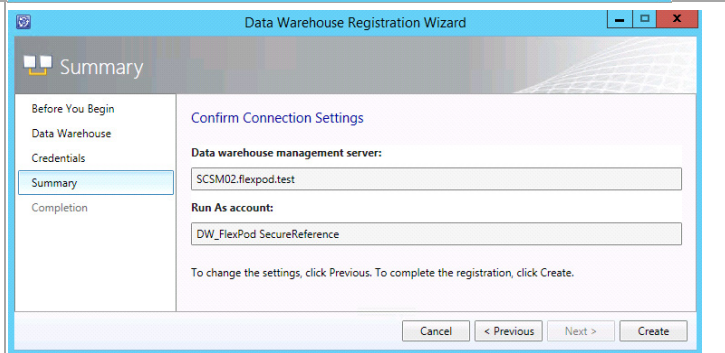
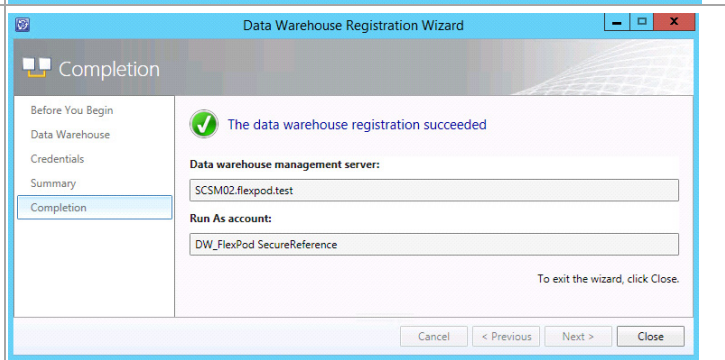
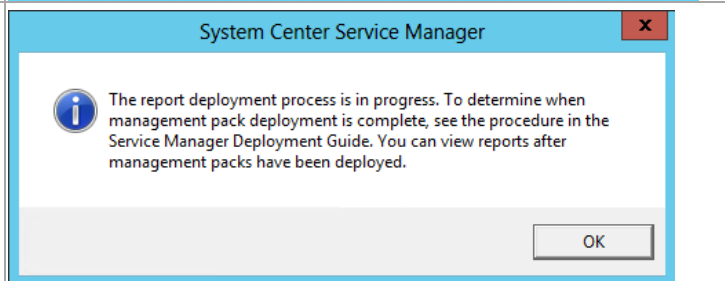


The **Data Warehouse Registration Wizard** will launch. Click **Next** to begin registration.

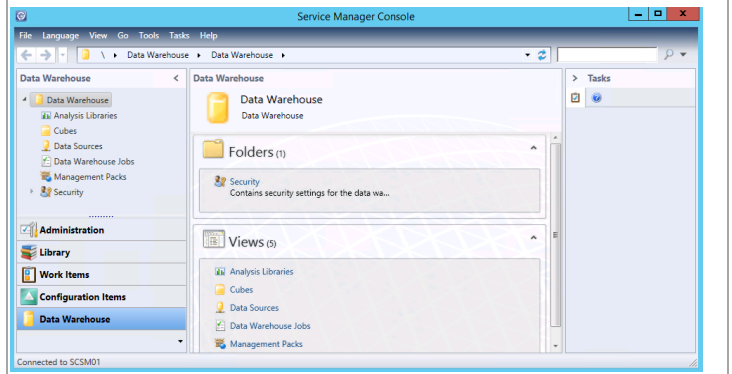


In the **Specify the data warehouse management server name** dialog, specify the Service Manager Data Warehouse server FQDN in the **Server name** drop-down menu. When selected, click the **Test Connection** button to validate connectivity between the Service Manager management and Data Warehouse servers. Click **Next** to continue.



<p>In the <b>Provide credentials for the data warehouse</b> dialog. Click <b>Next</b> to use the current SM and DW service account as the <b>Run As account</b> for the Data Warehouse connection.</p>	
<p>A <b>Credentials</b> dialog will appear and prompt you for the password for the SM service account. When provided, click <b>OK</b> to continue.</p>	
<p>The <b>Summary</b> dialog will appear. Review the information that was provided earlier and click <b>Create</b> to begin the registration process.</p>	
<p>The <b>Completion</b> dialog will show the successful registration of the Data Warehouse. Click <b>Close</b> to exit the wizard.</p>	
<p><i>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.</i></p>	

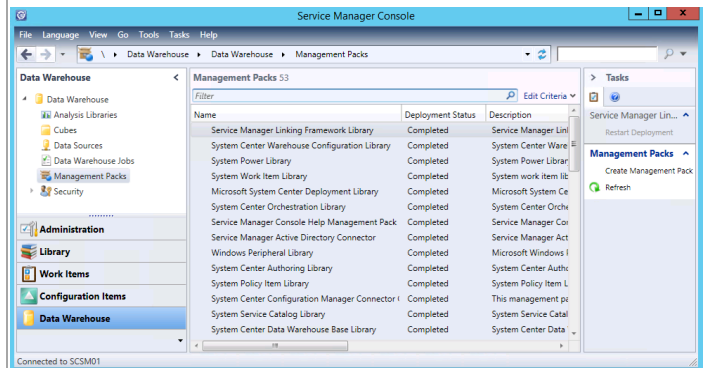
After a few minutes the **Data Warehouse** button will be added to the **Service Manager Console**.



**Note:** this deployment and association process can take up to two hours to complete.

The status of the management pack imports can be checked by selecting **Management Packs** in the **Data Warehouse** pane.

Deployment is complete when all listed management packs show a deployment status of **Completed**.



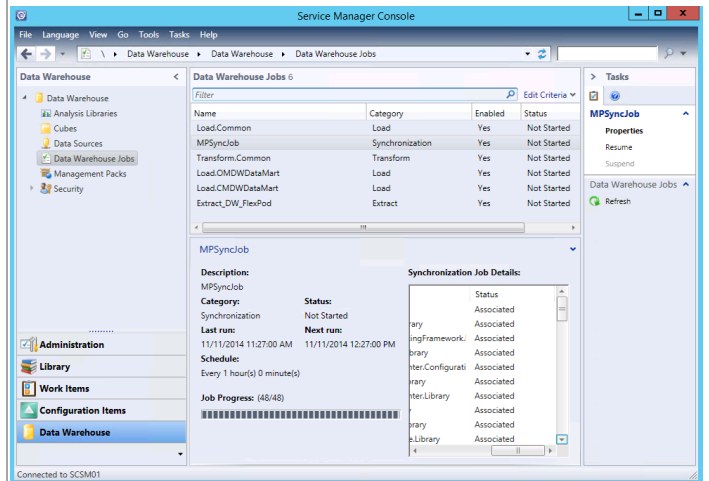
**Note:** this deployment and association process can take up to two hours to complete.

In the **Data Warehouse** pane, select **Data Warehouse Jobs**.

In the **Data Warehouse Jobs** pane, click **MPSyncJob**.

In the **MPSyncJob** details pane, in the **Synchronization Job Details** list, scroll to the right to view the **Status** column, and then click **Status** to alphabetically sort the status column.

Scroll through the **Status** list. The management pack deployment process is complete when the status for all of the management packs is **Associated** or **Imported**. Confirm that there is no status of either **Pending Association** or **Failed** in the status list. In the **Data Warehouse Jobs** pane, the status of the **MPSyncJob** will have changed from **Running** to **Not Started** when the registration process is complete.



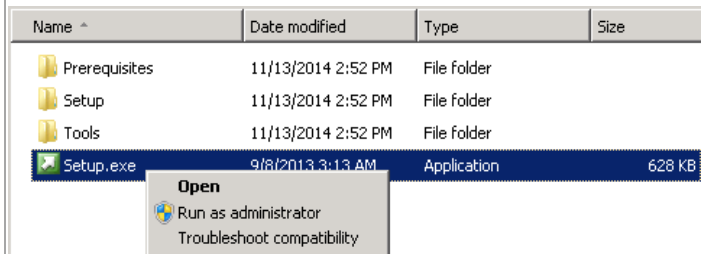
## Install the Service Manager Self-Service Portal Server

The following steps must to be completed in order to install the Service Manager self-service portal server role.

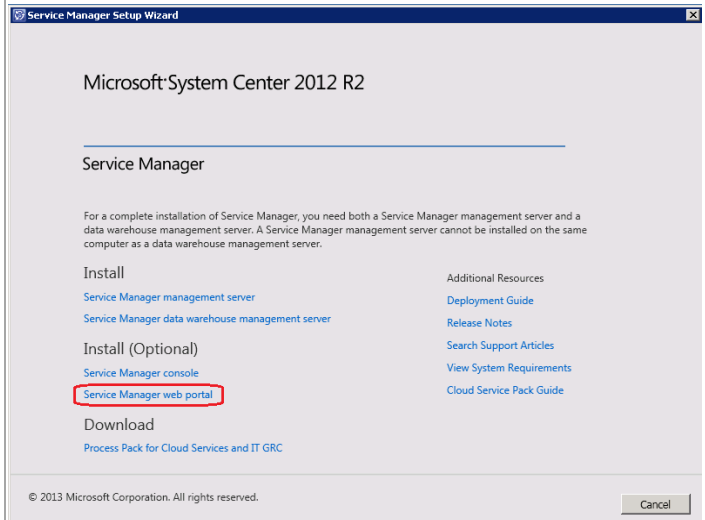
**Perform the following steps on the System Center Service Manager self-service portal (SCSM03) virtual machine.**

Log on to Service Manager self-service portal server (**NOT** the Service Manager management server or the Data Warehouse server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

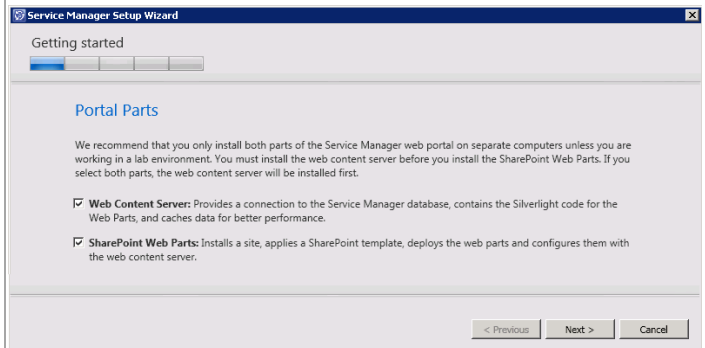


The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager web portal** to begin the Service Manager self-service portal server installation.



The **Service Manager Setup Wizard** will open. In the **Portal Parts** dialog, select the **Web Content Server** and **SharePoint Web Parts** check boxes and click **Next** to continue.

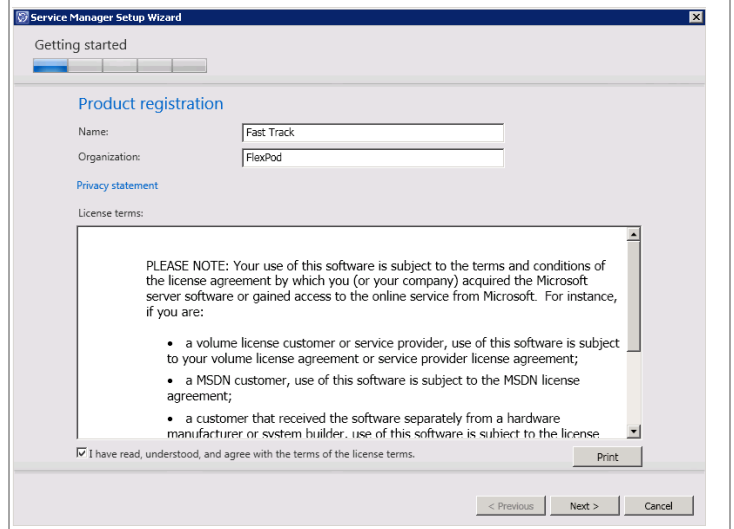
**Note:** The warning about installing both Portal Parts on a single server can be safely ignored. The setup wizard assumes that the SharePoint Farm is using a local SQL Server installation whereas the Fast Track design uses a dedicated SQL Server instance for the SharePoint farm drastically reducing the load on the SharePoint Web Parts installation.



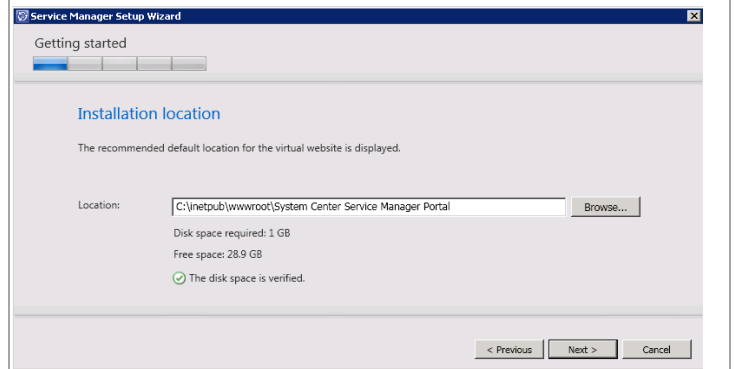
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name** – specify the name of the primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.

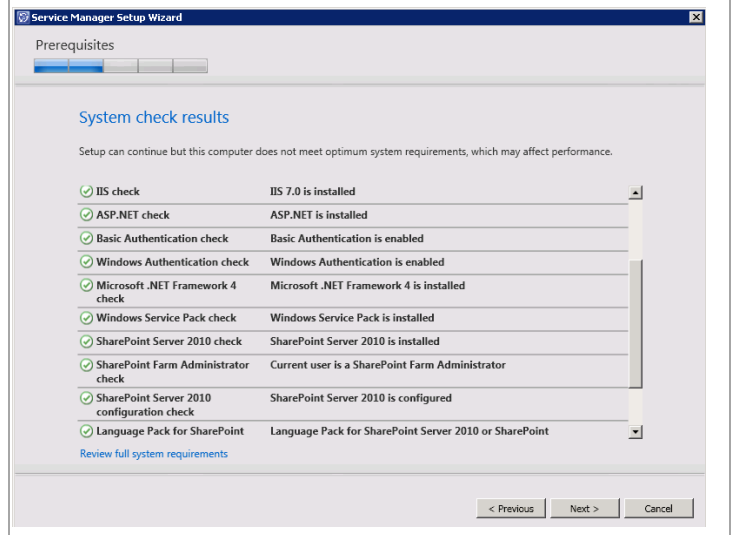
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of `C:\inetpub\wwwroot\System Center Service Manager Portal` for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





In the **Configure the Service Manager Self-Service Portal name and port** dialog, specify the following information in the provided text boxes:

- **Website name** – specify the name of the website used for the self-service portal. In most cases, the default name of *SCSMWebContentServer* should be used.
- **Port** – specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases this value should be changed to **444**.

In addition, select the appropriate Server Authentication certificate from the **SSL certificate** drop-down menu. The certificate CN field must match the name of the server.

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' dialog box, specifically the 'Configure the Service Manager Self-Service Portal name and port' step. The dialog has a title bar with the wizard's name and a close button. Below the title bar is a progress indicator with four steps, the second of which is active. The main content area has a blue header with the step title. Below the header, there is a sub-header 'Configure the Service Manager Self-Service Portal name and port' and a brief instruction: 'Specify a name for your Self-Service Portal and the port that this website will use.' There are three input fields: 'Website name' with the value 'SCSMWebContentServer', 'Port' with the value '444', and 'SSL certificate' with a dropdown menu showing 'SCSM01, OU=Fast Track, O=FlexPod, L=San Jose, S=CA'. A checkbox labeled 'Enable SSL encryption (recommended)' is checked. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

In the **Select the Service Manager database** dialog, specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server cluster CNO created for the Service Manager Management server.
- **SQL Server instance** – specify **Default** as the SQL Server database instance created for the Service Manager Management server.
- **Database** – specify the name of the Service Manager database configured earlier. In most cases the default value of *ServiceManager* should be used.

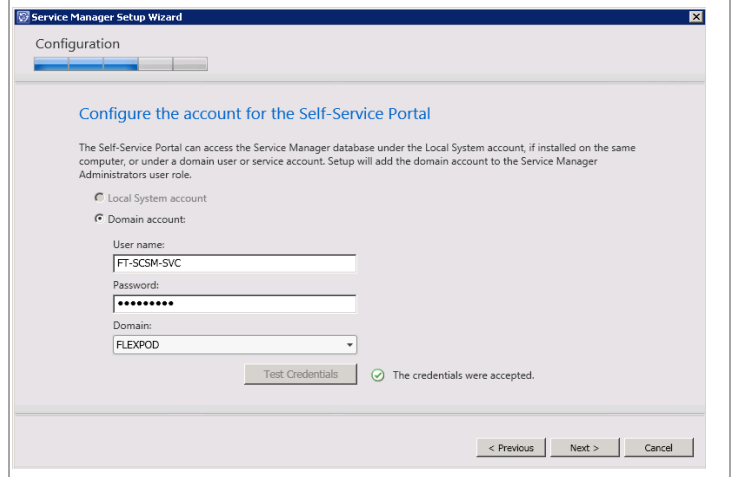
Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' dialog box, specifically the 'Select the Service Manager database' step. The dialog has a title bar with the wizard's name and a close button. Below the title bar is a progress indicator with four steps, the third of which is active. The main content area has a blue header with the step title. Below the header, there is a sub-header 'Select the Service Manager database' and a brief instruction: 'Specify the name of the server that hosts the instance of SQL Server 2008 R2 or SQL Server 2012 that contains the Service Manager database, and then select the Service Manager database.' There is a blue information icon followed by the text: 'Service Manager Self-Service Portal will use the existing 'ServiceManager' database.' There are three input fields: 'Database server' with the value 'SCSMDB', 'SQL Server instance' with a dropdown menu showing 'Default', and 'Database' with a dropdown menu showing 'ServiceManager'. A yellow warning icon is followed by the text: 'To connect to the existing configuration database, you must be logged on as a member of the Administrators user role on Service Manager management server, otherwise setup will fail.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

In the **Configure the account for the Self-Service Portal** dialog, verify that the **Domain account** option is selected and specify the SM Service Account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

When successful, click **Next** to continue.



In the **Configure the Service Manager SharePoint Web site** dialog, provide the following information:

- In the **SharePoint site** section, specify the following information in the provided text boxes:
  - **Website name** – specify the name of the website used for the self-service portal. In most cases, the default name of Service Manager Portal should be used.
  - **Port** – specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases the default value of **443** should be kept.
- Select the appropriate server authentication certificate from the **SSL certificate** drop-down menu. This will be the same certificate used for the content server in the previous step.
- In the SharePoint database section, specify the following information in the provided text boxes:
  - **Database server** – specify **Default** as the name of the SQL Server cluster network name created for the Service Manager installation SharePoint Farm (SCDB).
  - **SQL Server instance** – specify the SQL Server database instance created for the Service Manager installation SharePoint Farm(SCDB).
  - **Database name** – specify the database name for the portal. In most cases, the default value of *SharePoint\_SMPortalContent* will be used.

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step for 'Configure the Service Manager SharePoint Web site'. The dialog contains the following fields and options:

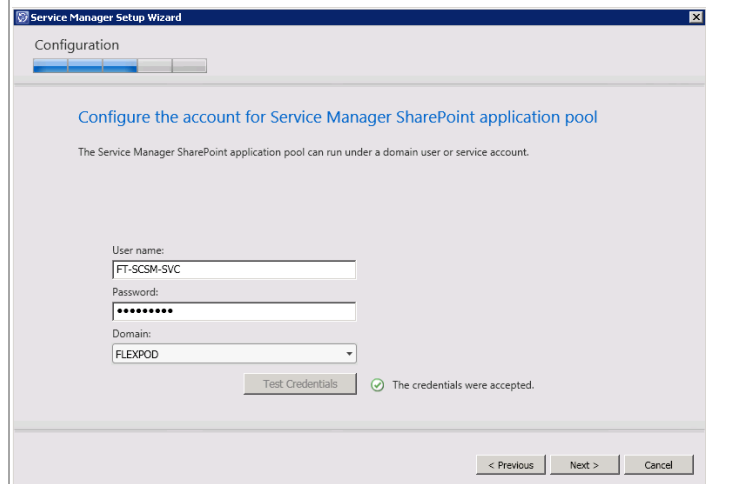
- SharePoint site:**
  - Website name: Service Manager Portal
  - Port: 443
- Enable SSL encryption (recommended)
- SSL certificate: SCISM01, OU=Fast Track, O=FlexPod, L=San Jose, S=CA (highlighted with a red box)
- SharePoint database:**
  - Database server: SCDB (highlighted with a red box)
  - SQL Server instance: Default (highlighted with a red box)
  - Database name: SharePoint\_SMPortalContent
- Web content server:**
  - URL: https://SCISM03:444

Navigation buttons at the bottom: < Previous, Next >, Cancel.

In the **Configure the account for Service Manager SharePoint application pool** dialog, specify the SM service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

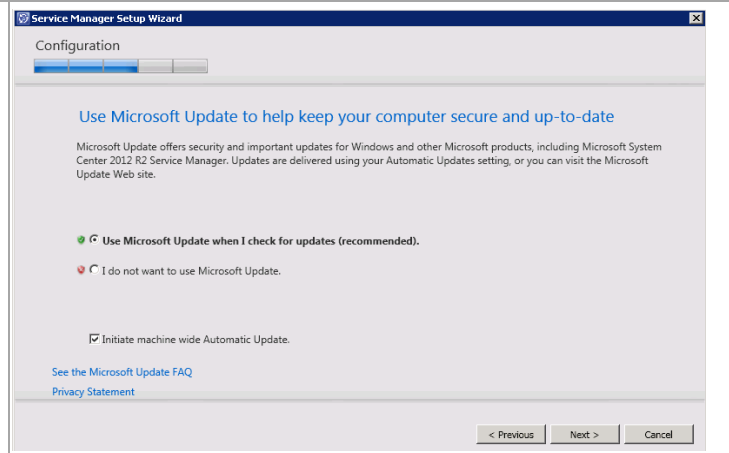
When successful, click **Next** to continue.



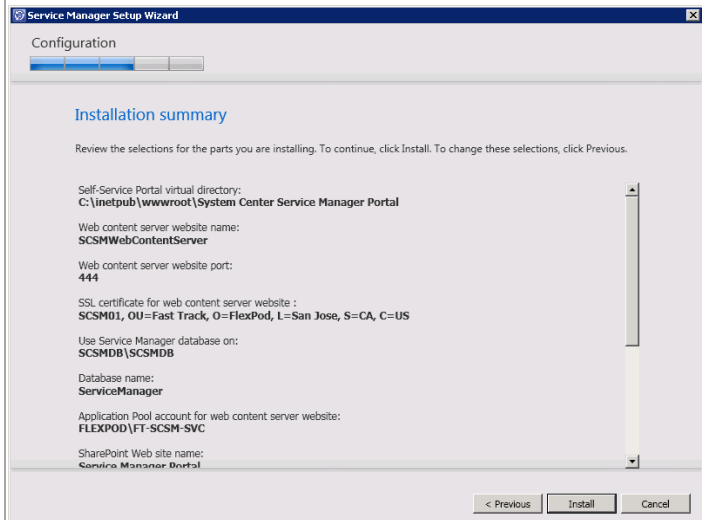
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.



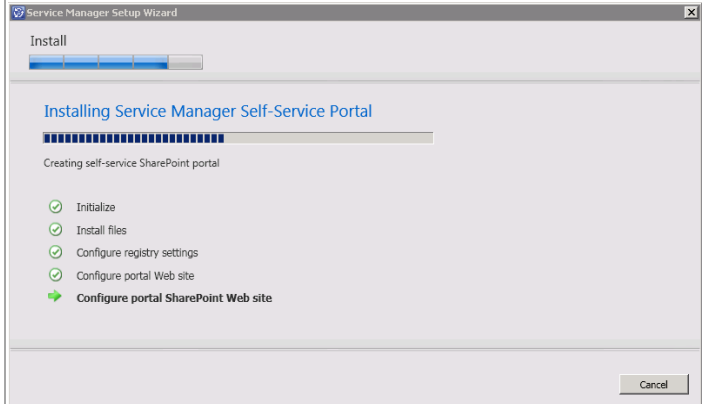
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

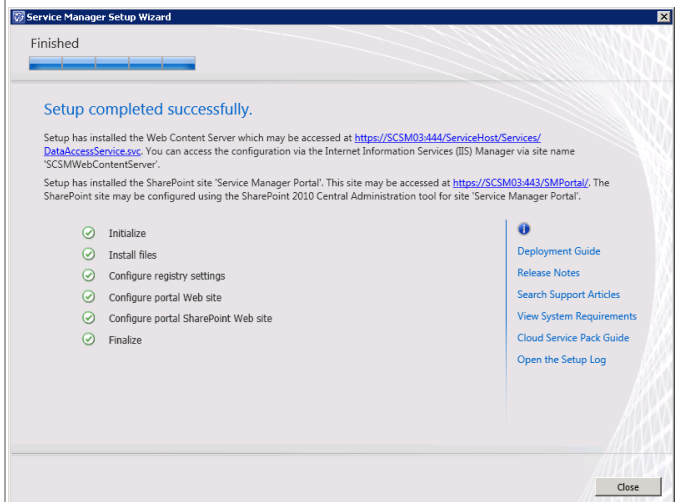


The wizard will display the progress while installing features.

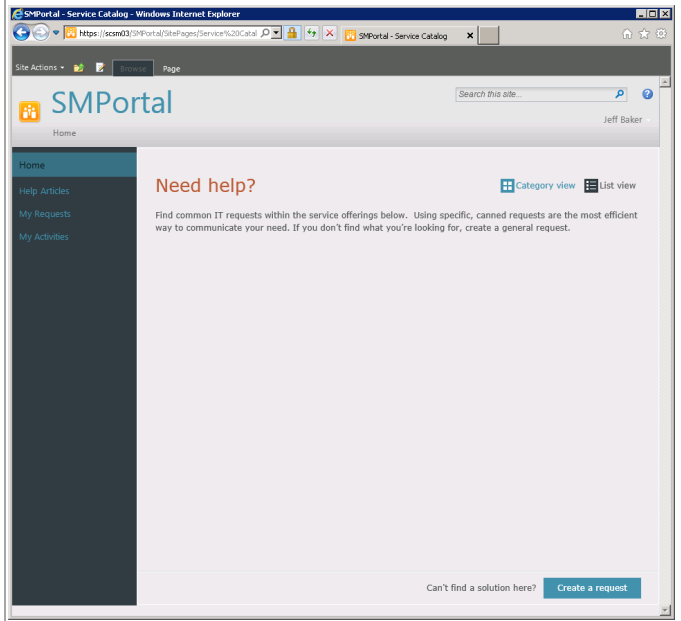


When completed, the **Service Manager Setup Wizard** will display the **Setup completed successfully** dialog. Click **Close** to finish the installation.

Note the SMPortal link provided in the dialog.

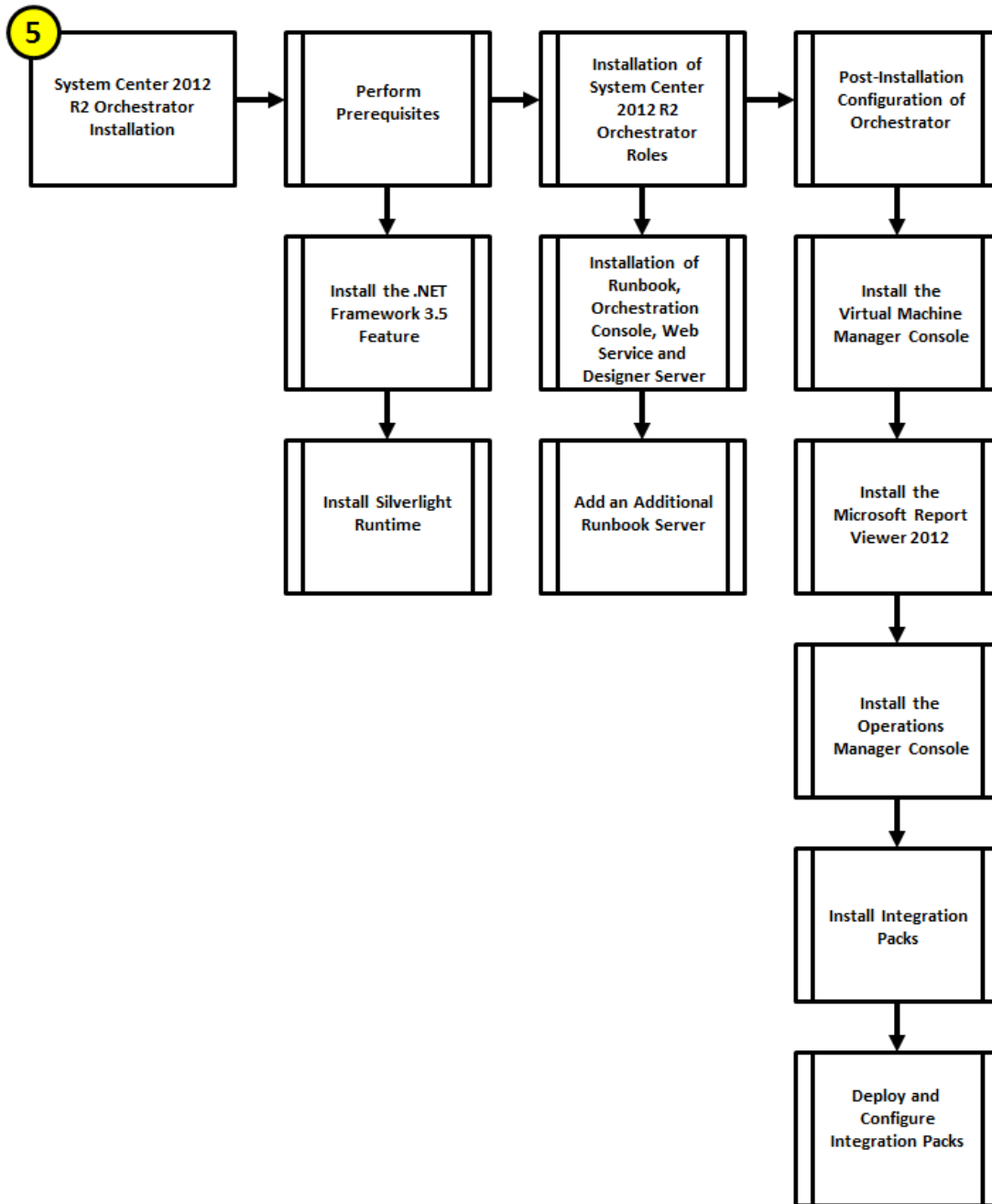


From Microsoft Internet Explorer®, open the Service Manager self-service portal at <https://<servername>/SMPortal>. Verify that the page loads completely and that all sections display as expected.



## 22 Orchestrator

The Orchestrator installation process includes the following high-level steps:



### 22.1 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 R2 have been provisioned.
- A multi-node, SQL Server 2012 SP2 cluster with dedicated instance has been established in previous steps for Orchestrator.

- The .NET Framework 3.5 Feature is installed.

## 22.2 Prerequisites

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	<p>This account will need:</p> <ul style="list-style-type: none"> <li>• Full admin permissions on all target systems to be managed</li> <li>• Log on As a Service rights (User Rights)</li> <li>• <i>Sysadmin</i> on the SQL Server, or dba rights to the Orchestrator database after its created</li> </ul> <p>This account will need to be a member in the following groups:</p> <ul style="list-style-type: none"> <li>• FT-VMM-Admins</li> </ul>

### 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

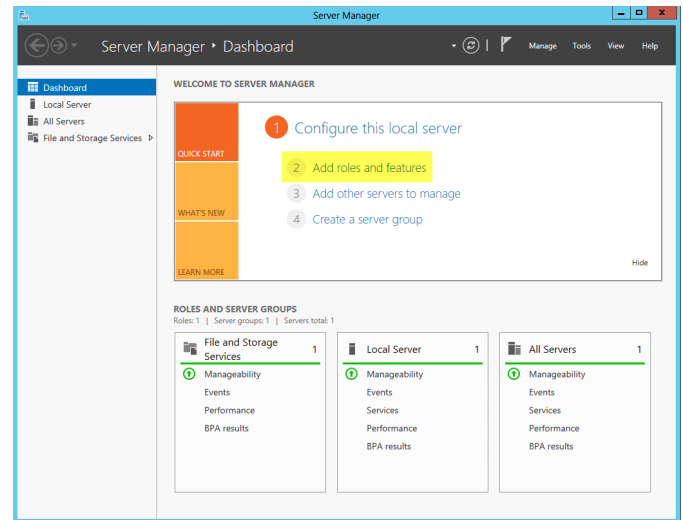
### Add the .NET Framework 3.5 Feature

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.

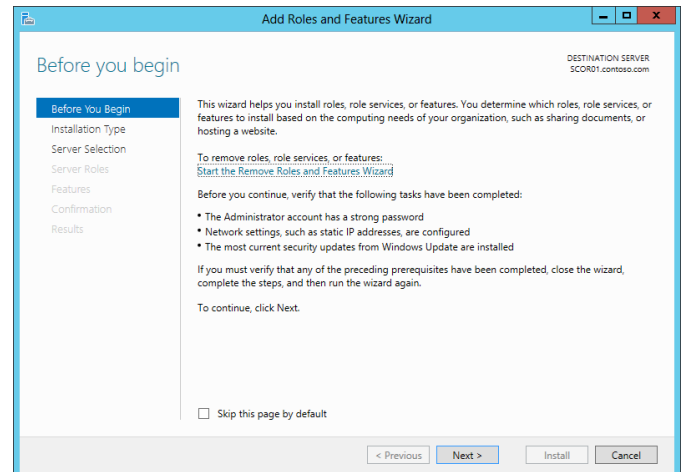


Perform the following steps on all **Orchestrator** virtual machines.

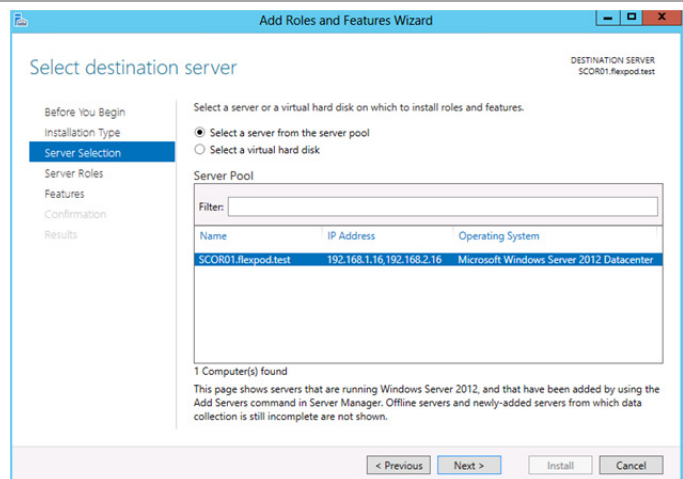
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



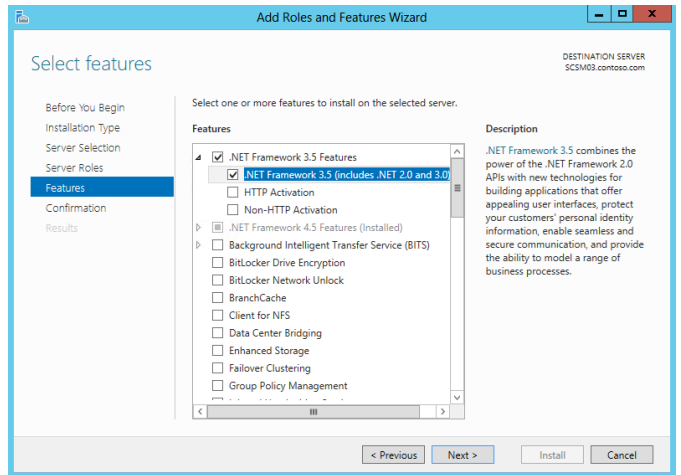
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next** - for this installation, click the **Features** menu option to continue.



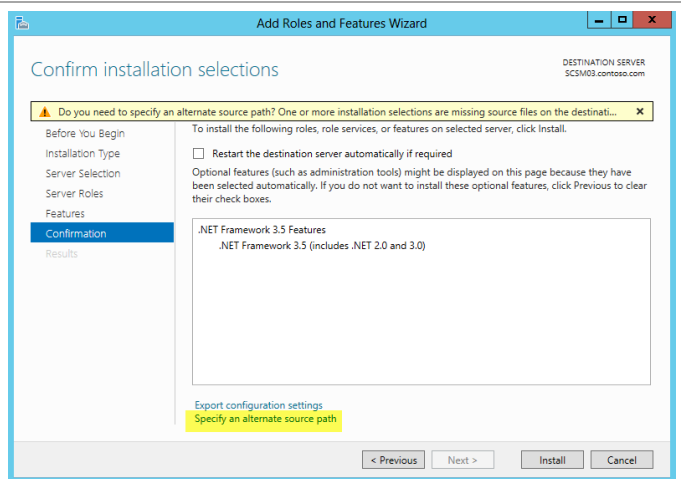
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



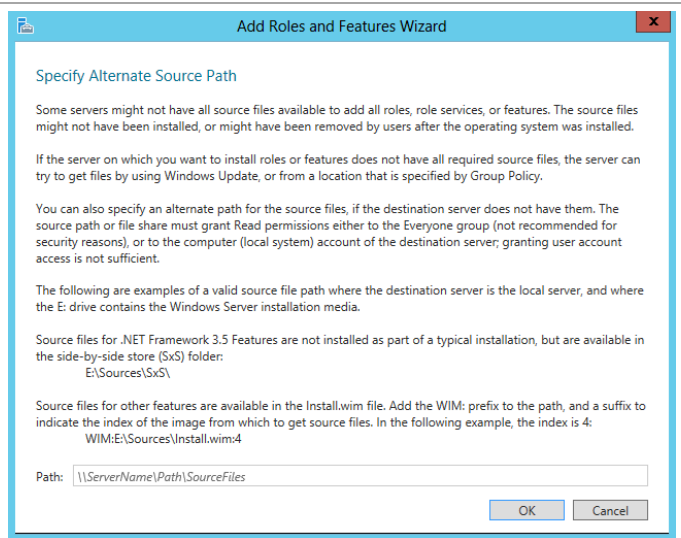
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

*Note that 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.*

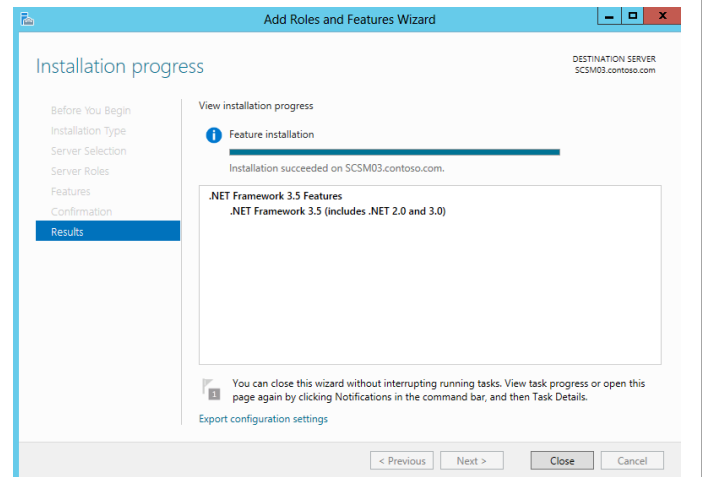
*Also, If the server does not have internet access an alternate source path can be specified by clicking the **Specify and alternate source patch link**.*



*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.*



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

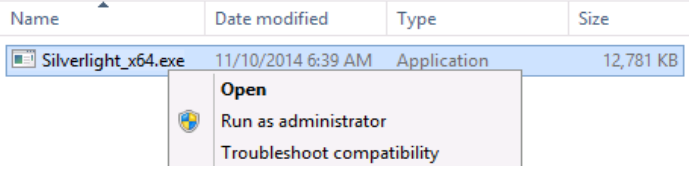
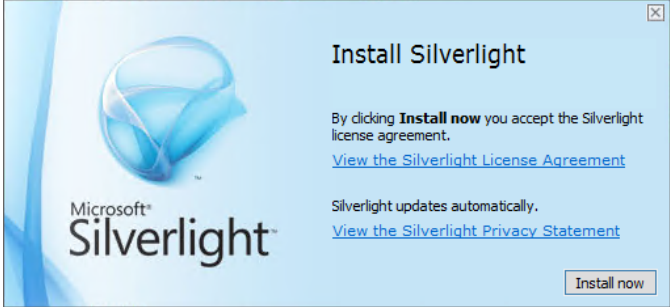

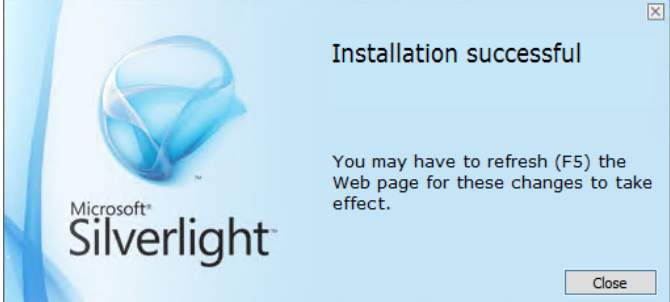


Note that while the previous installation was performed interactively, the installation of roles and features can be automated using the shown PowerShell cmdlet.

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

## Install the Silverlight Runtime

Perform the following steps on both **Orchestrator** virtual machines.

<p>From the installation media source, right-click <b>Silverlight.exe</b> and select <b>Run as administrator</b> from the context menu to begin setup.</p>	
<p>In the <b>Install Silverlight</b> dialog, click <b>Install now</b>.</p>	
<p>In the <b>Enable Microsoft Update</b> dialog, select or clear the <b>Enable Microsoft Update</b> check box based on organizational preferences and click <b>Next</b> to continue.</p>	
<p>In the <b>Installation Successful</b> dialog, click <b>Close</b> to exit the installation.</p>	

## 22.3 Installation

### Install the Orchestrator Runbook, Web Service, and Designer Server

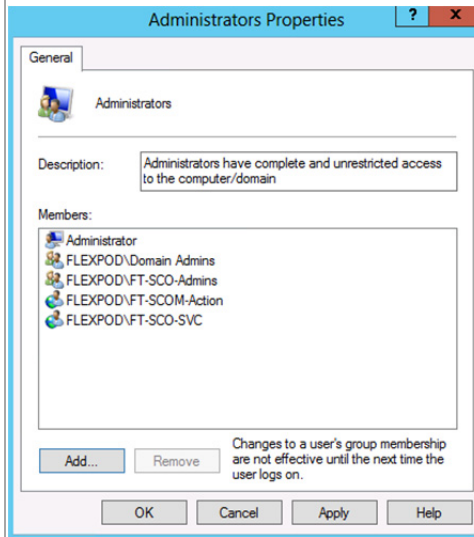
The following steps need to be completed in order to install the Orchestrator Runbook Server component.

Perform the following steps on the first **Orchestrator** virtual machine.

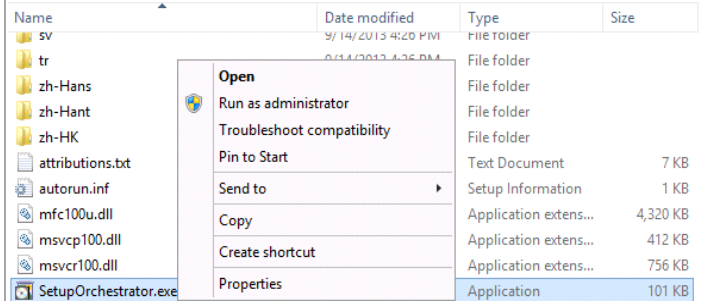
Log in to the Orchestrator virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:

- Orchestrator service account.
- Orchestrator Admins group.
- Operations Manager Action account.



From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



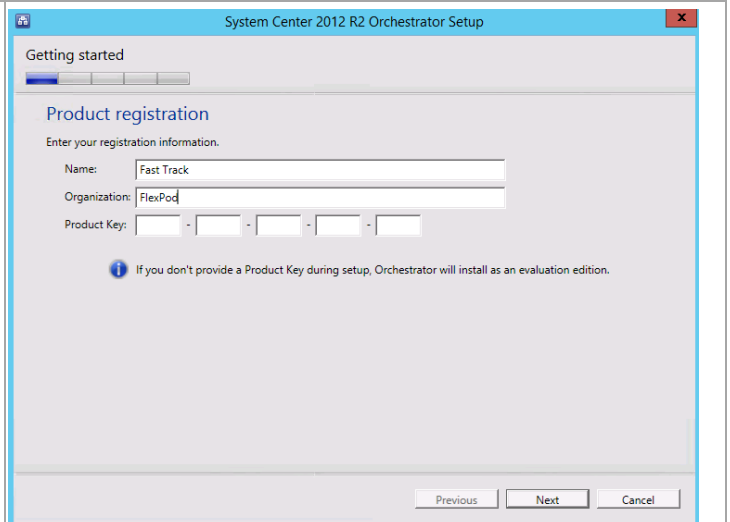
The Orchestrator installation wizard will begin. At the splash page, click **Install** to begin the Orchestrator server installation.



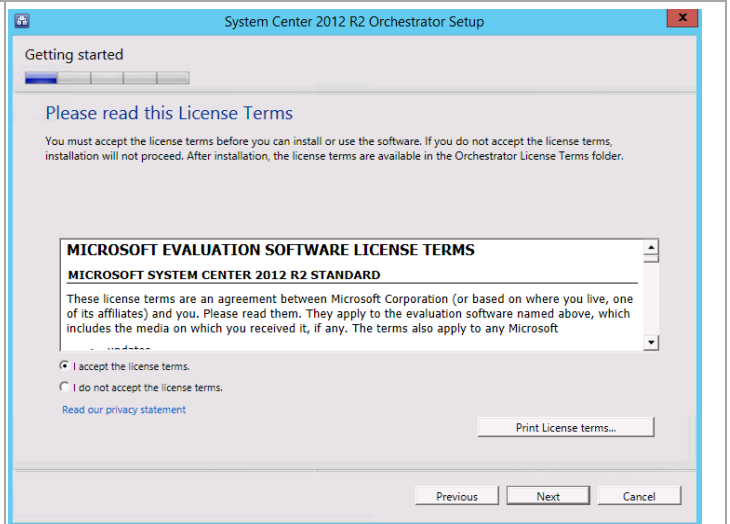
In the **Product registration information** dialog, provide the following information in the provided text boxes:

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

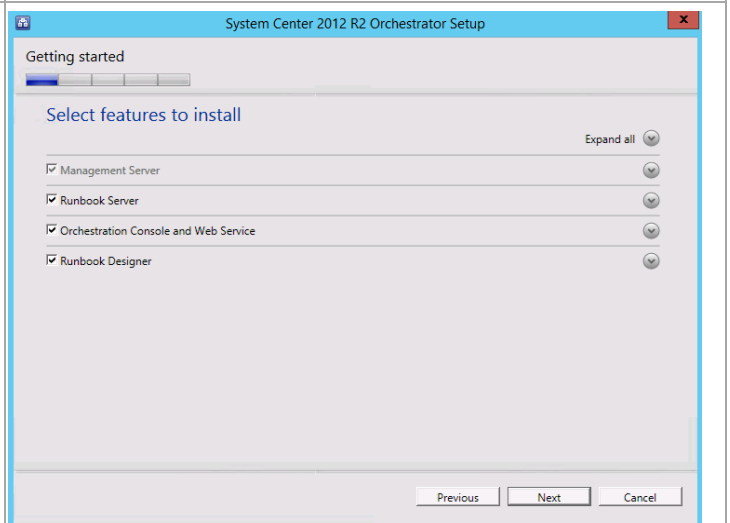
Click **Next** to continue.



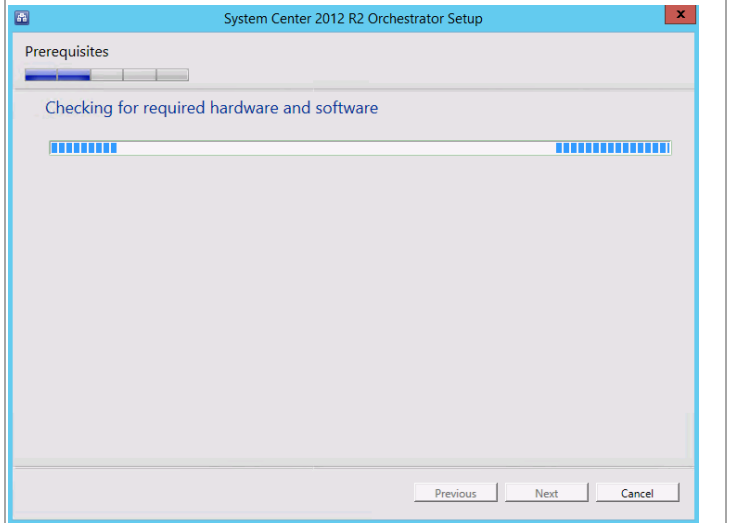
In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option check box is selected and click **Next** to continue.



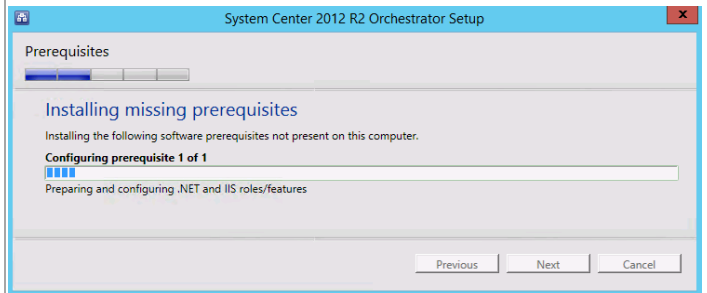
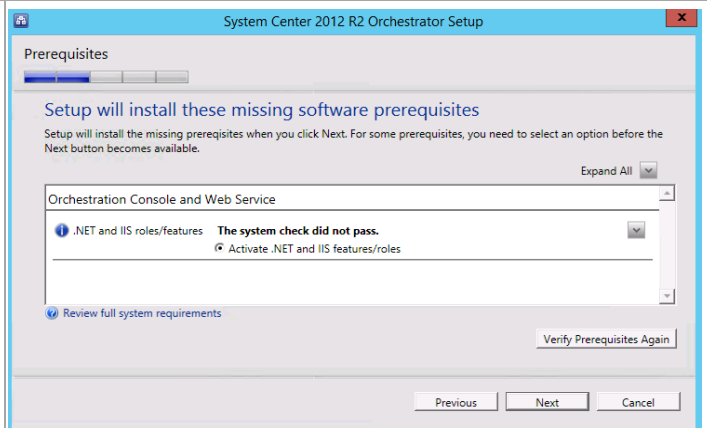
In the **Select Features to install** dialog, select the **Management Server** (default selected), **Runbook server**, **Orchestration console and web service**, **Runbook Designer** check boxes and click **Next** to continue.



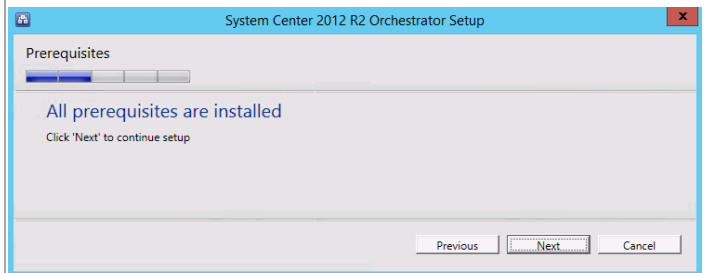
The **Checking for required hardware and software** dialog will appear to verify the installation prerequisites. When validation completes, click **Next** to continue.



The Orchestrator setup will identify any prerequisite software required for the installation to complete. The **Setup will install these missing software prerequisites** dialog will attempt to perform the installation of missing prerequisites. When completed, click **Next** to continue.



When the installation of the missing prerequisites is completed, click **Next** to continue.



In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test** button to verify the credentials provided.

When successful, click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the service account

Enter the user account to use to run runbooks and access remote system resources. This account must have "Log on as a service" rights enabled. Orchestrator will enable this right if it is not already enabled.

As a security best practice, do not use a domain administrator account. To learn more about security best practices and how this account is configured to access Orchestrator database, see the [Orchestrator deployment guide](#).

Username (you may enter domain\username):  
FT-SCO-SVC

Password:  
\*\*\*\*\*

Domain:  
FLEXPOD Test

Credentials accepted

Previous Next Cancel

In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – specify the SQL Server cluster name and instance name created in the steps above.
- **Port** – specify the TCP port used for the SQL Server if not the default.

In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.

When successful, click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the database server

Specify the database server, instance name, and port number for the Orchestrator database. You must have sufficient permissions on the database instance. To learn more about the database permissions, see the [Orchestrator deployment guide](#).

Server (you may enter server\instance): SCDB\SCDB Browse... Port: 10474

**Authentication Credentials**

Windows Authentication  
 SQL Authentication

Username: \_\_\_\_\_  
Password: \_\_\_\_\_

Test Database Connection

Database connection succeeded.

Previous Next Cancel

In the **Configure the database** dialog in the **Database** section, select the **New Database** option. Specify the default database name of *Orchestrator*.

Click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the database

Specify a new or existing database. You must have sufficient permissions on the database instance.

If you select Existing Database option, only the SQL server databases compatible with Orchestrator are available for selection. To learn more about Orchestrator compatible databases, see the [Orchestrator deployment guide](#).

**Database**

Specify a database.

New database: Orchestrator  
 Existing database: \_\_\_\_\_

Previous Next Cancel



In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse...** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.

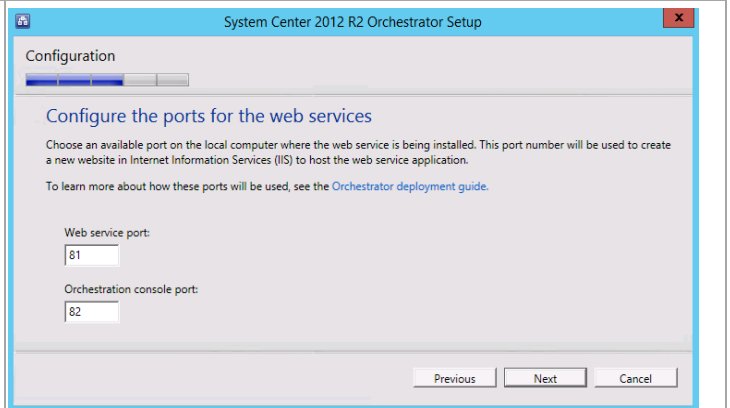
Verify that that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



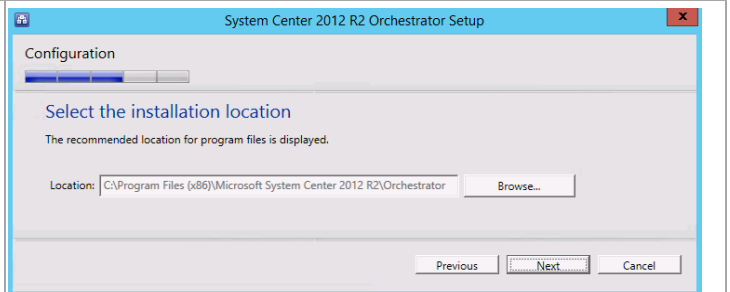
In the **Configure the ports for the web services** dialog, provide the following information in the provided text boxes:

- **Web service port** – specify the TCP port used for the Orchestrator Web Service. The default value of 81 is recommended.
- **Orchestration console port** – specify the TCP port used for the Orchestrator console port. The default value of 82 is recommended.

When successful, click **Next** to continue.



In the **Select the installation location** dialog, specify a location or accept the default location of `%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator` for the installation. Click **Next** to continue.



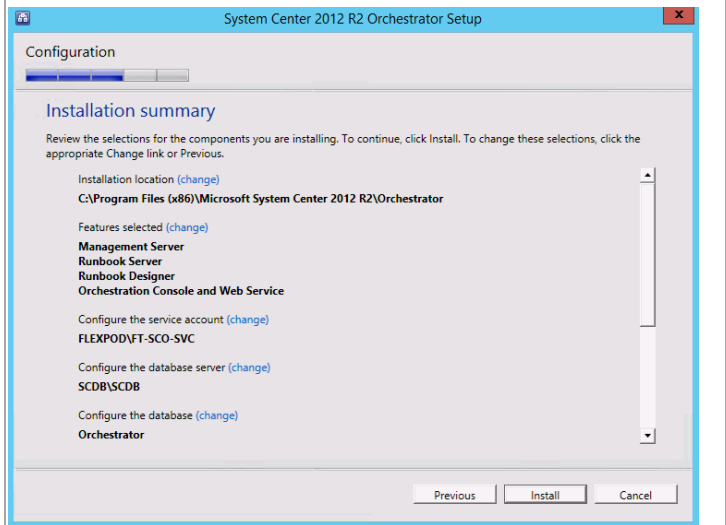
The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

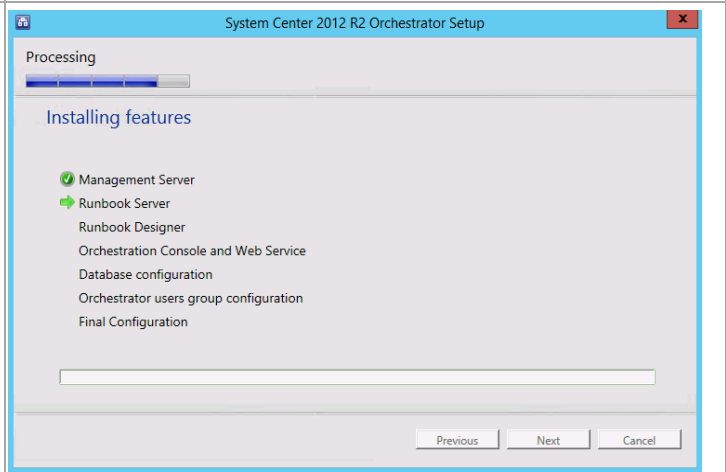
Select the appropriate option based on your organization's policies and click **Next** to continue.



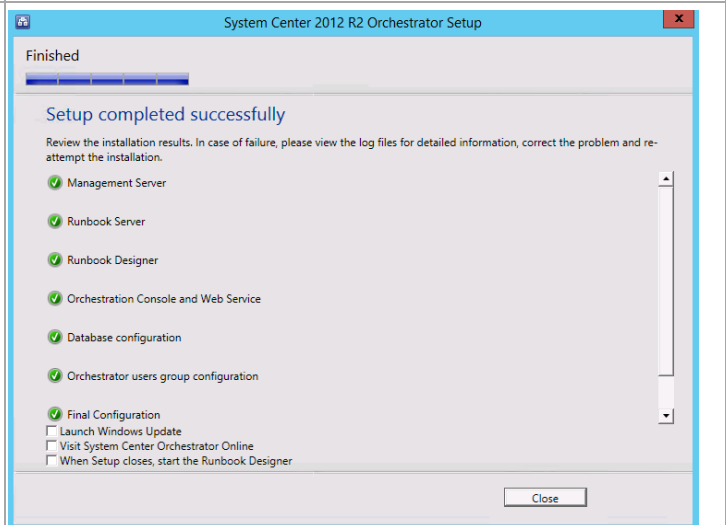
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



In the **Installing features** dialog, the installation will proceed and show progress.



The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.

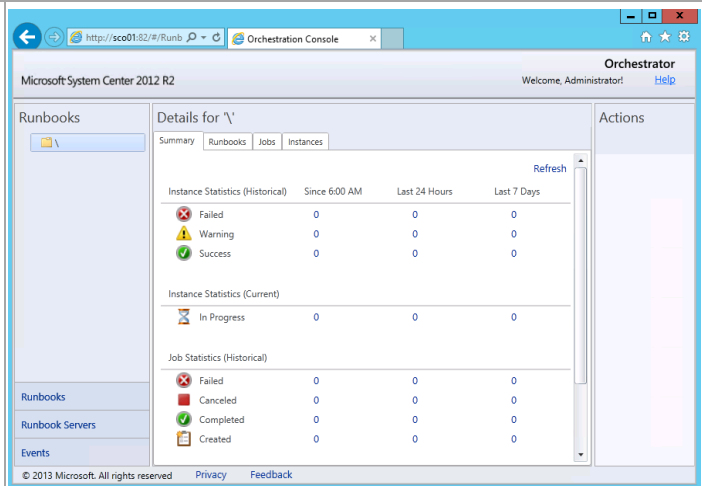


When installed, verify that the Orchestrator roles installed properly by opening the consoles. From the **Start** screen, then select the **Orchestration Console** tile.

**Note:** In order to run the Orchestration Console on the Orchestrator server, Internet Explorer Enhanced Security must be disabled or configured to function with the console.



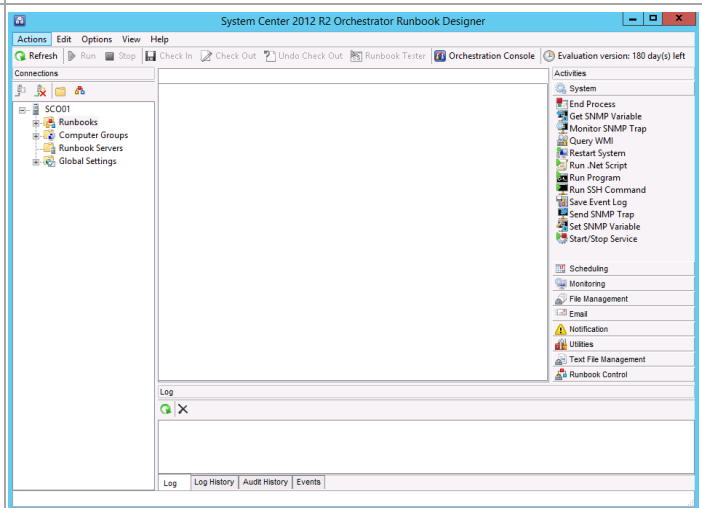
Validate that the **Orchestration console** performs properly in Internet Explorer.



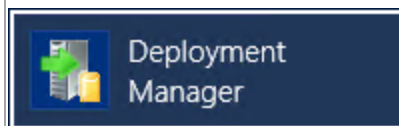
From the **Start Menu**, then select the **Runbook Designer** tile.



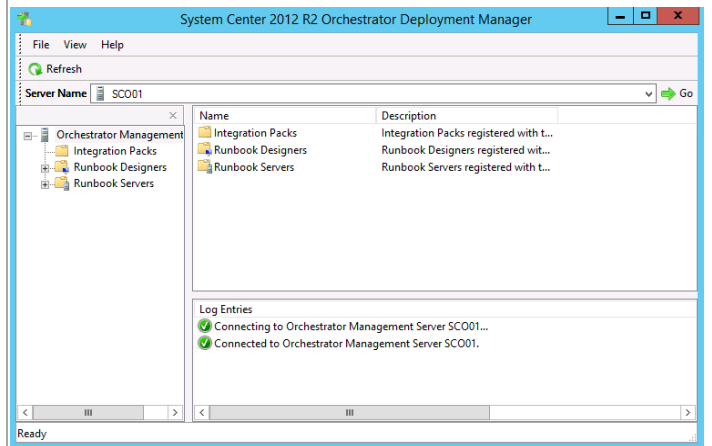
Launch the **Runbook Designer** console and verify that it performs properly.



From the **Start Menu**, then select the **Deployment Manager** tile.



Launch the **Deployment Manager** console and verify that it performs properly.

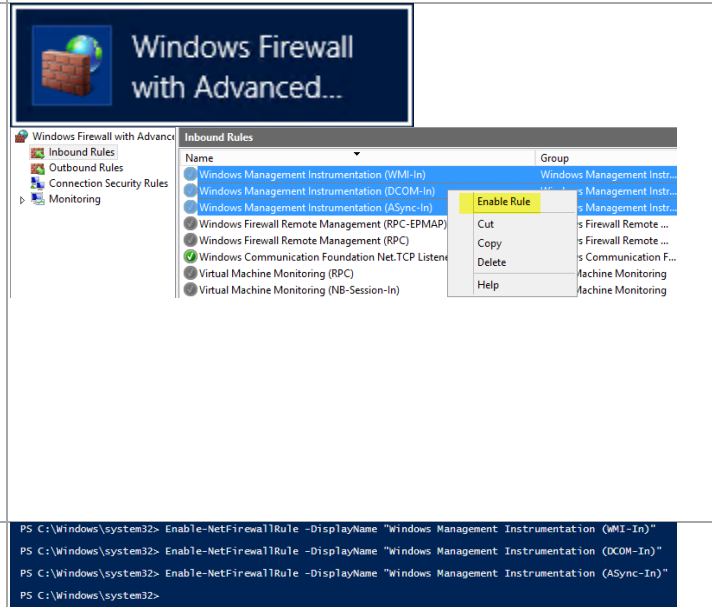


From the Start Screen, click on the Windows Firewall tile. Configure Windows Firewall for the first Orchestrator Runbook Server.<sup>15</sup>

If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:

- Windows Management Instrumentation (WMI-In).
- Windows Management Instrumentation (DCOM-In).
- Windows Management Instrumentation (ASync-In).

Right-click each rule and select **Enable Rule** from the context menu.



Alternatively, the following PowerShell commands can be executed 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)"
```

<sup>15</sup> 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>.

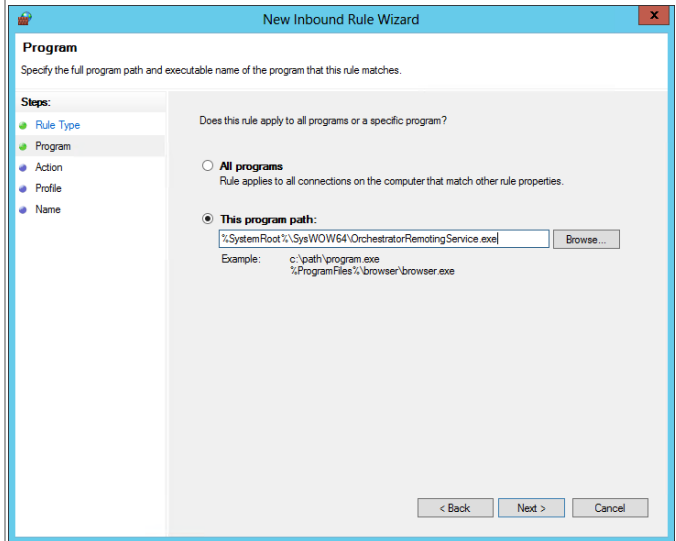
In Windows Firewall create a new Program rule using the following program path:

- %SystemRoot%\SysWOW64\orchestratorRemotingService.exe

Name the rule **SCO - Orchestrator Remoting Service (x64)**.

Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO - Orchestrator Remoting Service (x64)" -Program C:\Windows\syswow64\orchestratorRemotingService.exe
```



```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "SCO - Orchestrator Remoting Service (x64)" -Program %SystemRoot%\SysWOW64\orchestratorRemotingService.exe
Name                : {abd2120c-7c27-4e12-be18-d30ec87fb805}
DisplayName         : SCO - Orchestrator Remoting Service (x64)
Description        :
DisplayGroup       :
Group              :
Enabled            : True
Profile            : Any
Platform          : {}
Direction         : Inbound
Action            : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping  : False
Owner             :
PrimaryStatus     : OK
Status            : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
PS C:\Windows\system32>
```

Since the first server runs the Orchestration console and web service, two additional ports (TCP 81 and 82) must be opened on the Windows Firewall as well. Create two additional firewall port rules named **SCO - Orchestration Console (TCP 81)** and **SCO - Web Service (TCP 82)** for each port and enable them.

Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO - Orchestration Console (TCP-In 81)"
```

```
New-NetFirewallRule -DisplayName "SCO - Web Service (TCP-In 82)"
```

Inbound Rules				
Name	Group	Profile	Enabled	Action
SCO - Orchestration Console (TCP-In 81)		All	Yes	Allow
SCO - Orchestrator Remoting Service (x64)		All	Yes	Allow
SCO - Web Service (TCP-In 82)		All	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discov...	All	No	Allow

```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "SCO - Web Service (TCP-In 82)"
Name                : {b71b0a5b-d013-4372-8519-beafe3afb6a8}
DisplayName         : SCO - Web Service (TCP-In 82)
Description        :
DisplayGroup       :
Group              :
Enabled            : True
Profile            : Any
Platform          : {}
Direction         : Inbound
Action            : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping  : False
Owner             :
PrimaryStatus     : OK
Status            : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
PS C:\Windows\system32>
```

Restart the Orchestrator server.

## Install an Additional Orchestrator Runbook Server

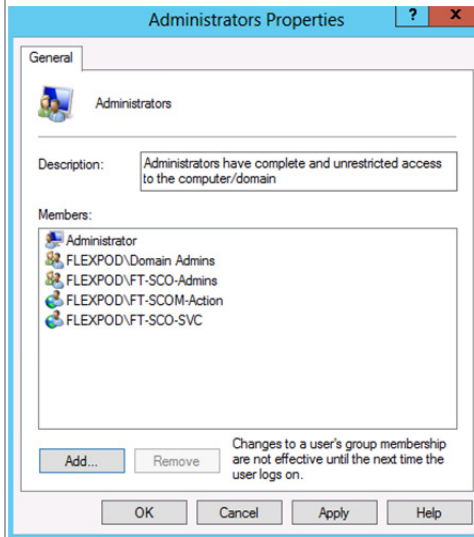
The following steps need to be completed in order to install an additional Orchestrator Runbook Server.

Perform the following steps on the **second Orchestrator Runbook Server** virtual machine.

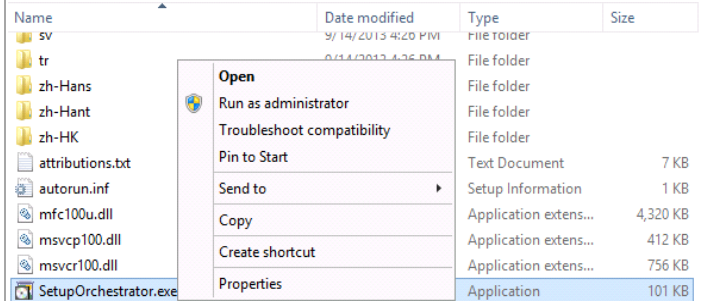
Log on to the Orchestrator virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:

- Orchestrator service account.
- Orchestrator Admins group.
- Operations Manager Action account.



Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



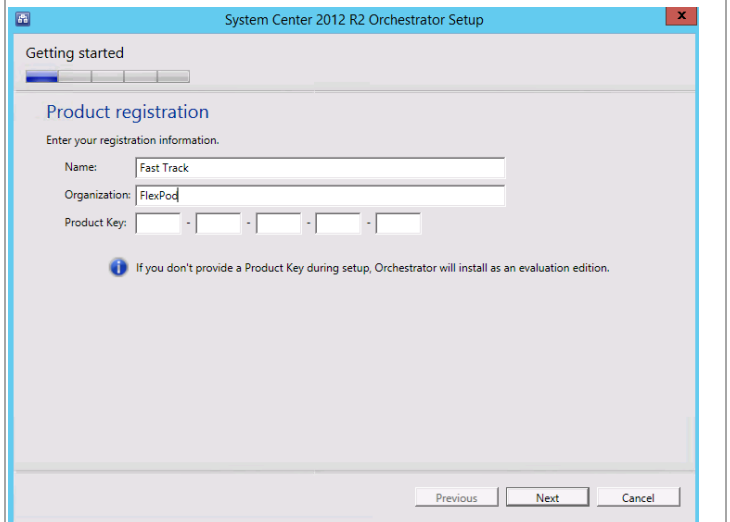
The Orchestrator installation wizard will begin. At the splash page, click **Install** begin the Orchestrator server installation.



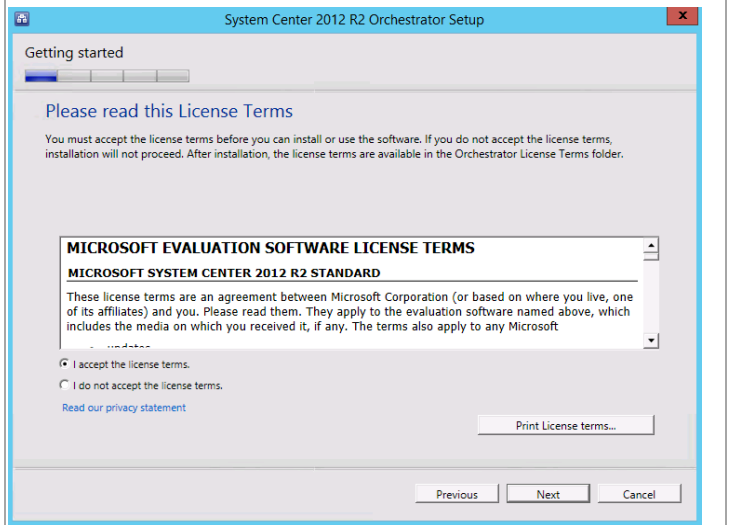
In the **Product registration information** dialog, enter the following information in the provided text boxes:

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

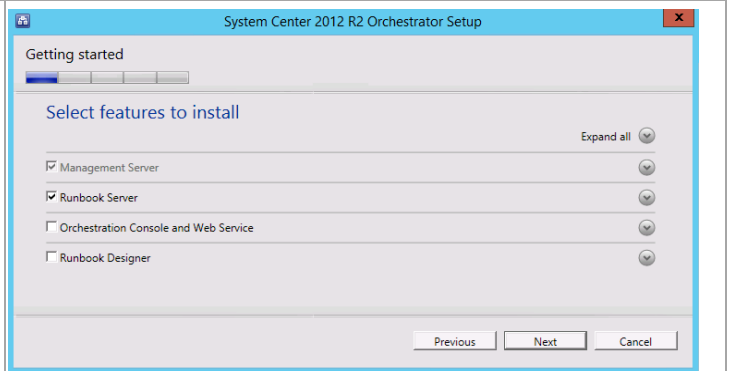
Click **Next** to continue.



In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option check box is selected and click **Next** to continue.



In the **Select Features to install** dialog, select the **Management Server** (default selected) and **Runbook server** check boxes and click **Next** to continue.



In the **Configure the service account** dialog, specify the Orchestrator service account in the **Username** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test** button to verify the credentials provided.

When successful, click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the service account

Enter the user account to use to run runbooks and access remote system resources. This account must have "Log on as a service" rights enabled. Orchestrator will enable this right if it is not already enabled.

As a security best practice, do not use a domain administrator account. To learn more about security best practices and how this account is configured to access Orchestrator database, see the [Orchestrator deployment guide](#).

Username (you may enter domain\username):  
FT-SCO-SVC

Password:  
\*\*\*\*\*

Domain:  
FLEXPOD [Test]

Credentials accepted

Previous Next Cancel

In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – specify the SQL Server cluster name and instance name created in the steps above.
- **Port** – specify the TCP port used for the SQL Server if not the default.

In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.

When successful, click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the database server

Specify the database server, instance name, and port number for the Orchestrator database. You must have sufficient permissions on the database instance. To learn more about the database permissions, see the [Orchestrator deployment guide](#).

Server (you may enter server\instance): SCDB\SCDB [Browse...]

Port: 10474

**Authentication Credentials**

Windows Authentication  
 SQL Authentication

Username: [ ]  
Password: [ ]

[Test Database Connection]

Database connection succeeded.

Previous Next Cancel

In the **Configure the database** dialog in the **Database** section, select the **Existing Database** option. Select the default database name of *Orchestrator* from the drop-down menu.

Click **Next** to continue.

System Center 2012 R2 Orchestrator Setup

Configuration

### Configure the database

Specify a new or existing database. You must have sufficient permissions on the database instance.

If you select Existing Database option, only the SQL server databases compatible with Orchestrator are available for selection. To learn more about Orchestrator compatible databases, see the [Orchestrator deployment guide](#).

**Database**

Specify a database.

New database: Orchestrator

Existing database: Orchestrator

Previous Next Cancel

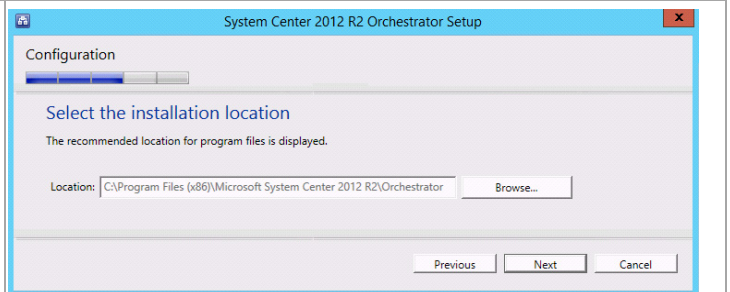


In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse...** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.

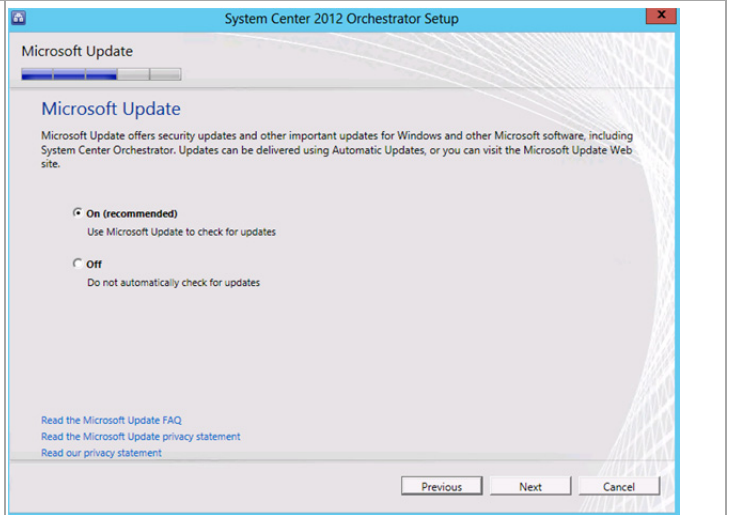
Verify that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



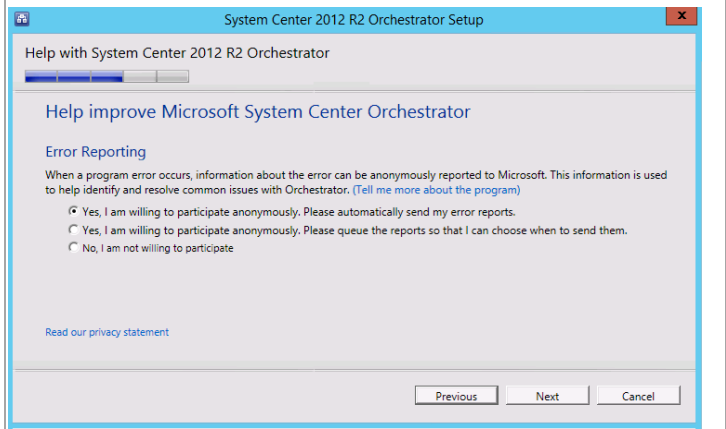
In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.



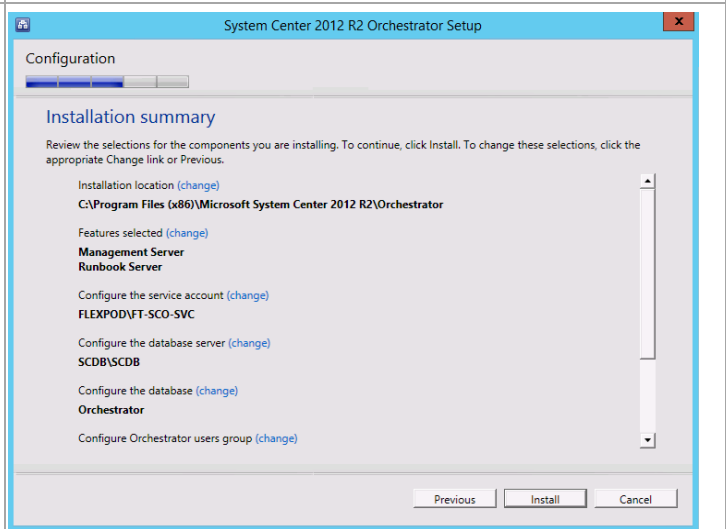
Depending on the current configuration of the server the Microsoft Updates Dialog may appear. The **Microsoft Update** dialog provides options for participating in automatic updates for Orchestrator. Select the appropriate option based on your organization's policies and click **Next** to continue.



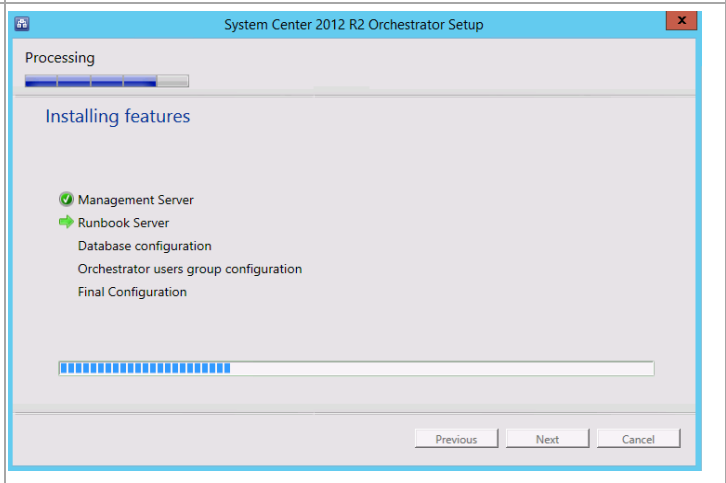
The **Help Improve Microsoft System Center Orchestrator** dialog provides the option for participating in the Error Reporting program. Select the appropriate option based on your organization's policies and click **Next** to continue.



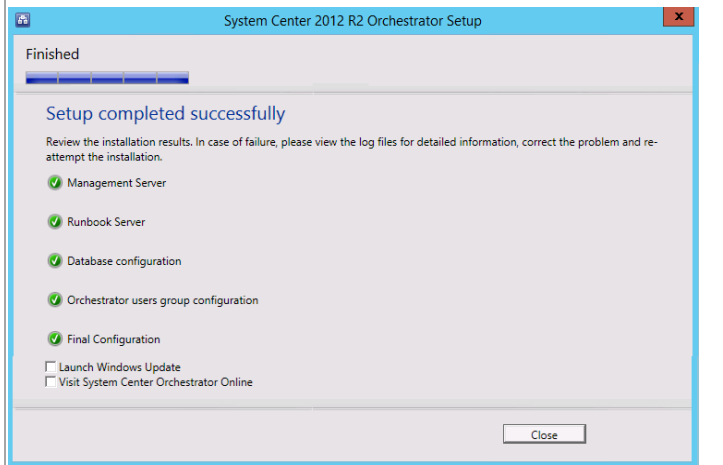
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



In the **Installing features** dialog, the installation will proceed and show progress.



The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.



Configure Windows Firewall for the second Orchestrator Runbook Server.<sup>16</sup>

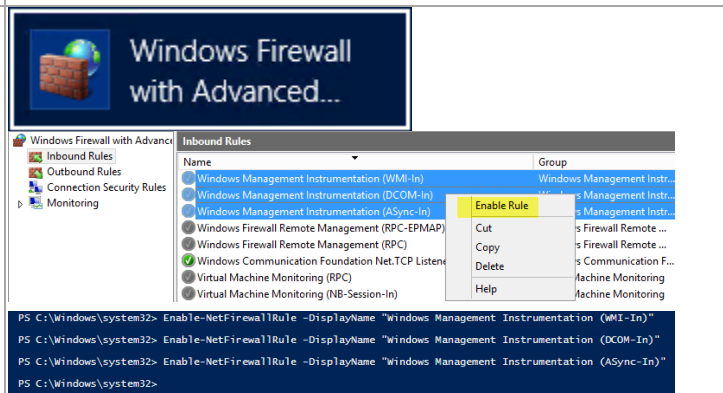
If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:

- Windows Management Instrumentation (WMI-In).
- Windows Management Instrumentation (DCOM-In).
- Windows Management Instrumentation (ASync-In).

Right-click each rule and select **Enable Rule** from the context menu.

Alternatively, the following PowerShell commands can be executed:

```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
```



<sup>16</sup> Orchestrator guidance is provided from the following TechNet resources: Using Windows Firewall with Orchestrator - <http://technet.microsoft.com/en-us/library/hh912321.aspx> and TCP Port Requirements <http://technet.microsoft.com/en-us/library/hh420382.aspx>.

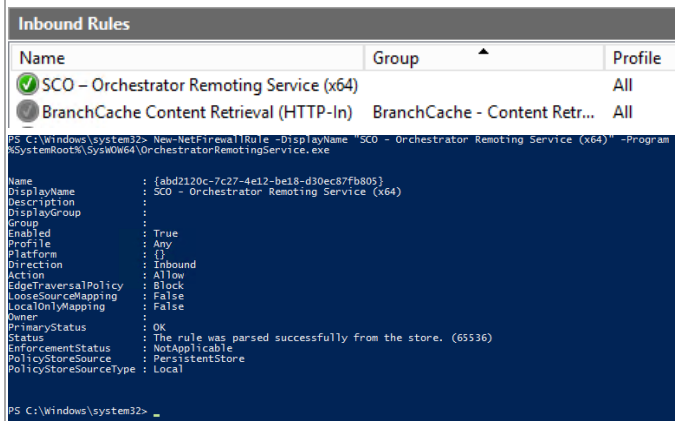
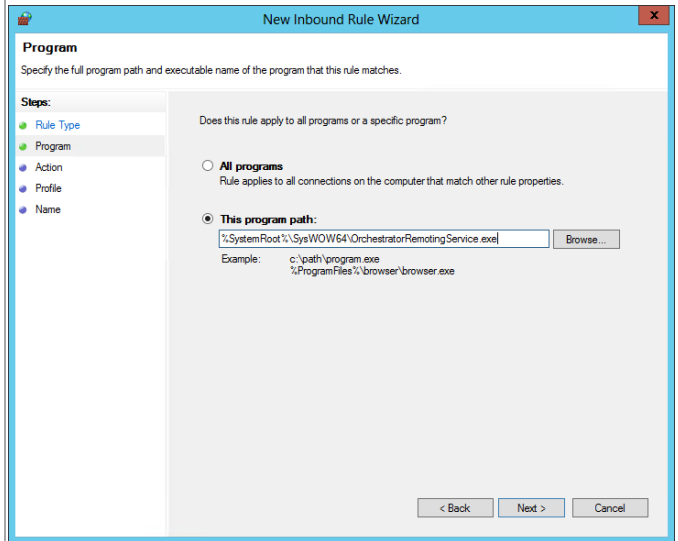
In Windows Firewall create a new Program rule using the following program path:

- %SystemRoot%\SysWOW64\orchestratorRemotingService.exe

Name the rule **SCO - Orchestrator Remoting Service (x64)**.

Alternatively, the following PowerShell commands can be executed:

```
New-NetFirewallRule -DisplayName "SCO - Orchestrator Remoting Service (x64)" -Program C:\Windows\SysWOW64\OrchestratorRemotingService.exe
```



Restart the Orchestrator server.

## 22.4 Install Cisco UCS Integration Pack

The following steps need to be completed in order to install the Cisco UCS Integration Pack.

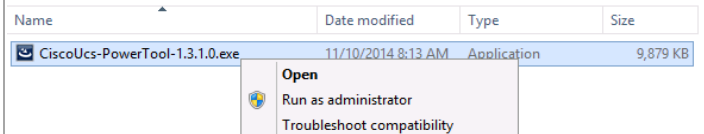
The Cisco UCS Integration Pack uses Cisco UCS PowerTool. Download the latest PowerTool from:

[http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.3\(1\)&relind=AVAILABLE&rellifecycle=&reltype=latest](http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.3(1)&relind=AVAILABLE&rellifecycle=&reltype=latest).

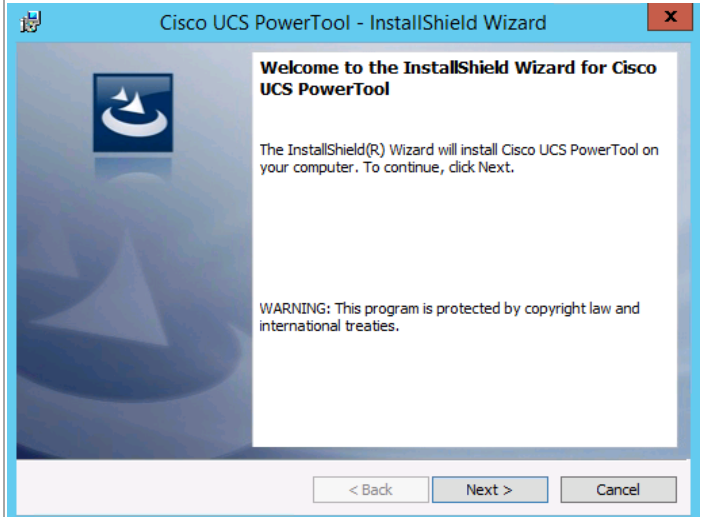
Download the integration pack from <https://communities.cisco.com/docs/DOC-37155>.

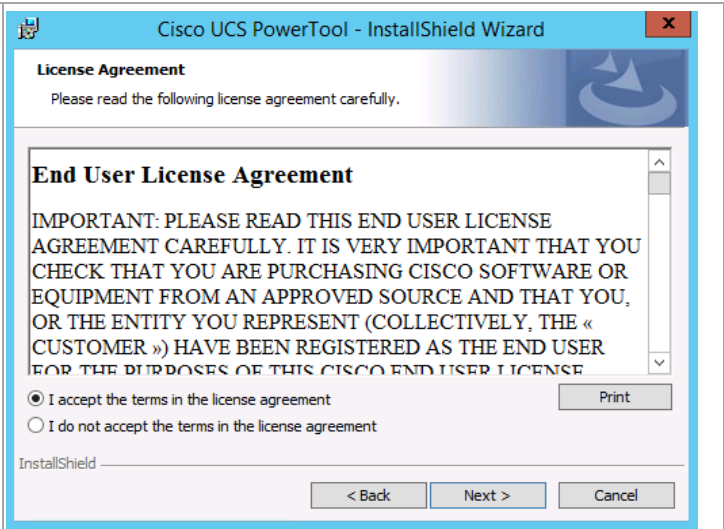
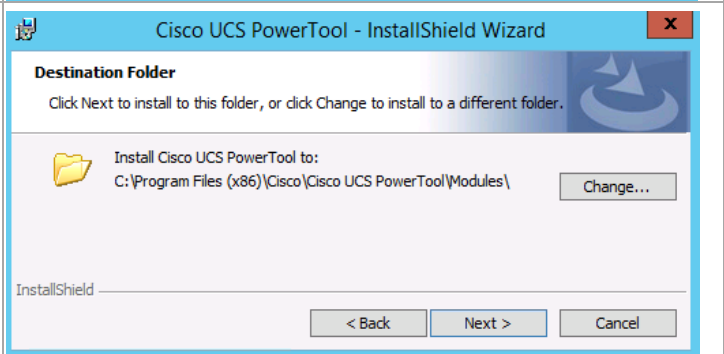
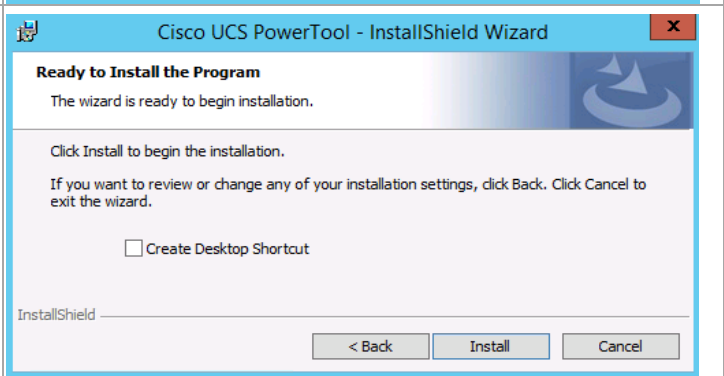
Perform the following steps on both **Orchestrator** virtual machines.

Log on to the Orchestrator server with a privileged user account that has Administrator privileges. From the Cisco UCS PowerTool installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

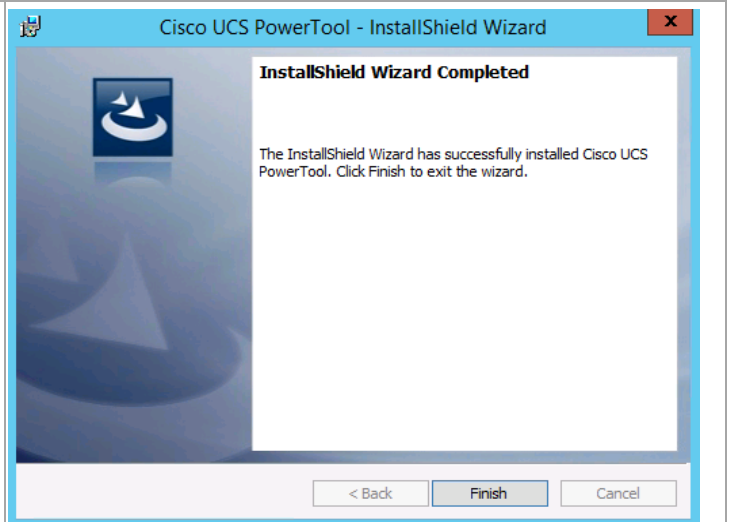


On the Welcome window, click **Next** to continue.

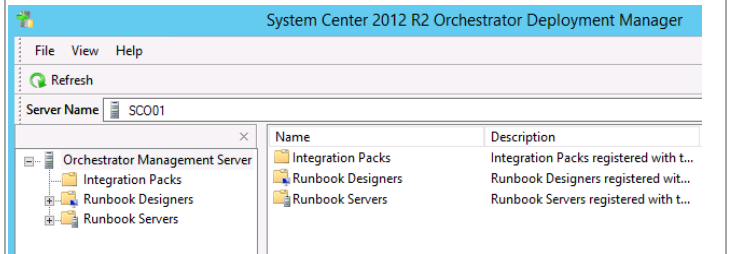


<p>On the License Agreement window, select the radio button by <b>I accept the terms in the license agreement</b> and click <b>Next</b> to continue.</p>	
<p>On the Destination Folder window accept the default location and click <b>Next</b> to continue.</p>	
<p>On the Ready to Install the Program window, you may select the option to Create Desktop Shortcut. Click <b>Install</b> to start the installation.</p>	

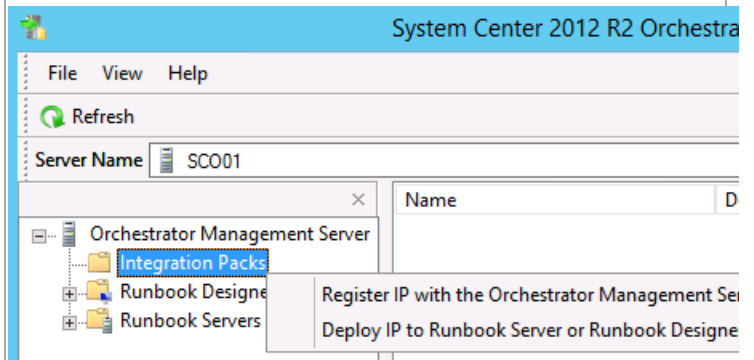
When the installation completes, click **Finish**.



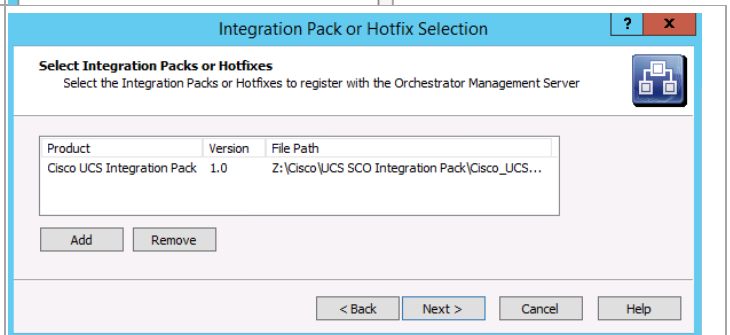
Launch the System Center 2012 R2 Orchestrator Deployment Manager.



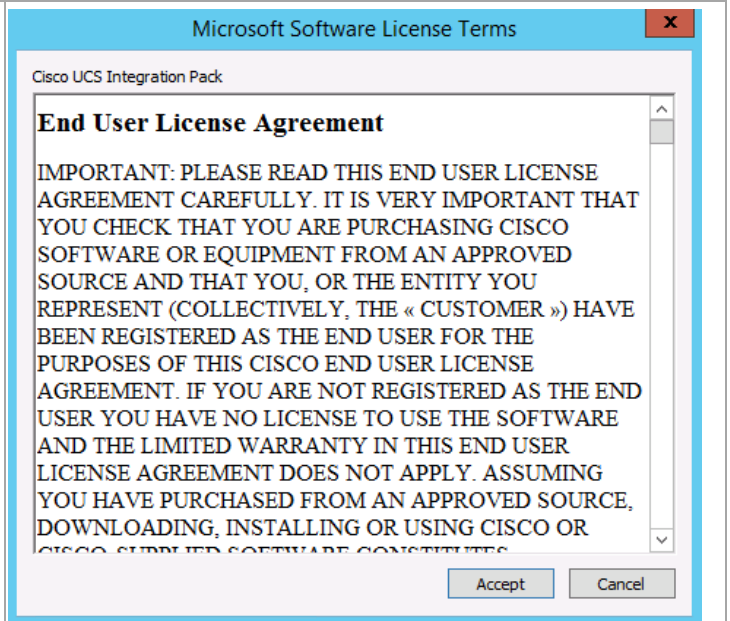
Right-click **Integration Packs** and select **Register IP with the Orchestrator Management Server**. Click **Next** on the Welcome window.



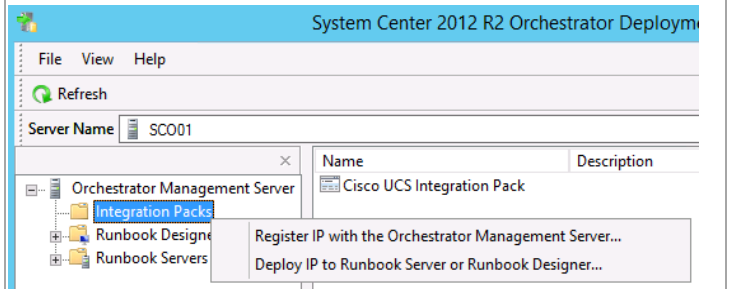
On the **Select Integration Packs or Hotfixes** window, click **Add**. Browse to the location you extracted the OIP file and select the file. Click **Next** to continue. Click **Finish** on the **Completing the Integration Pack Wizard** window.



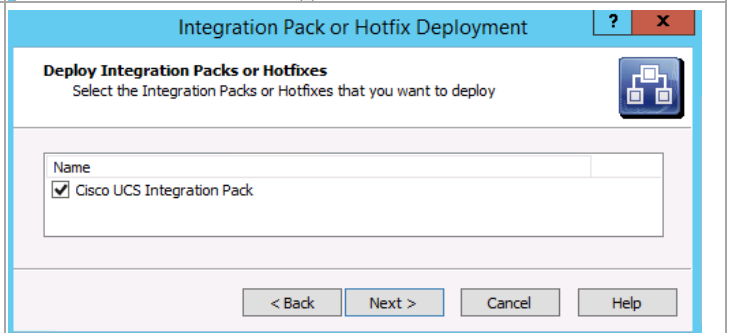
Click **Accept** on the **End User License Agreement** window to complete the installation.



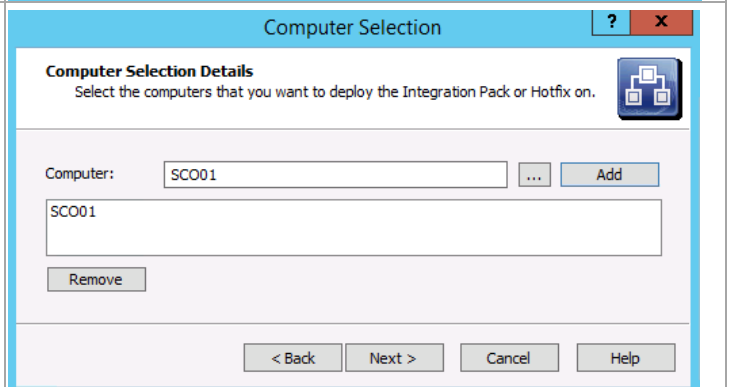
From the Deployment Manager, right-click **Integration Packs** and select **Deploy IP to Runbook Server or Runbook Designer...** Click **Next** on the Welcome screen.



On the **Deploy Integration Packs or Hotfixes** window, select the **Cisco UCS Integration Pack**. Click **Next** to continue.

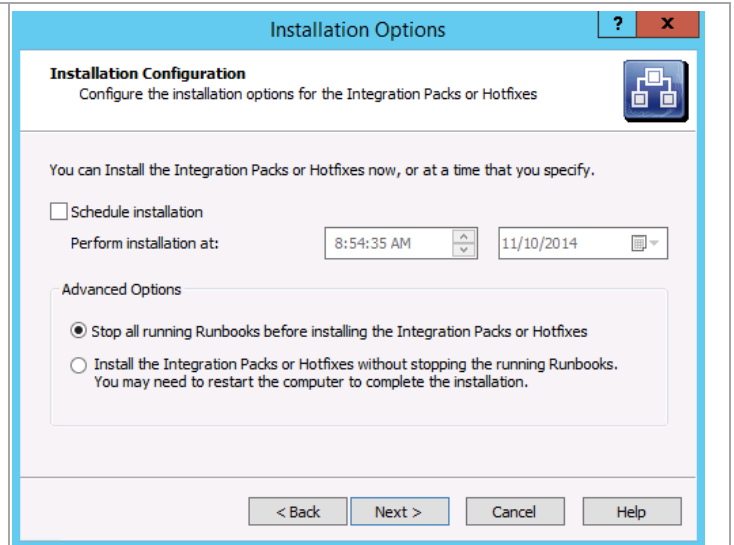


On the **Computer Selection Details** window, enter the name of the Runbook Server. Click **Next** to continue.

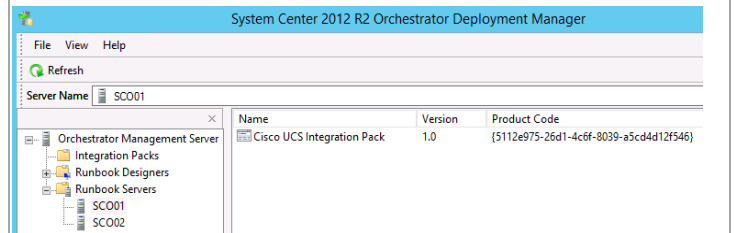




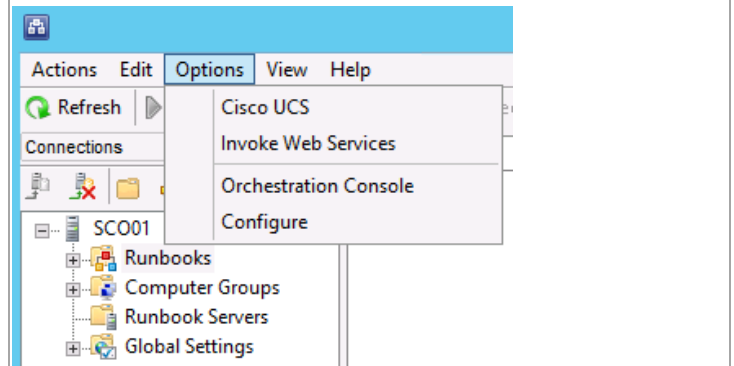
On the **Installation Configuration** window, ensure the radio button by **Stop all running Runbooks before installing the Integration Packs or Hotfixes** is selected. Click **Next** to continue. Click **Finish** on the Summary page that comes up. Status windows will display for each server previously entered.



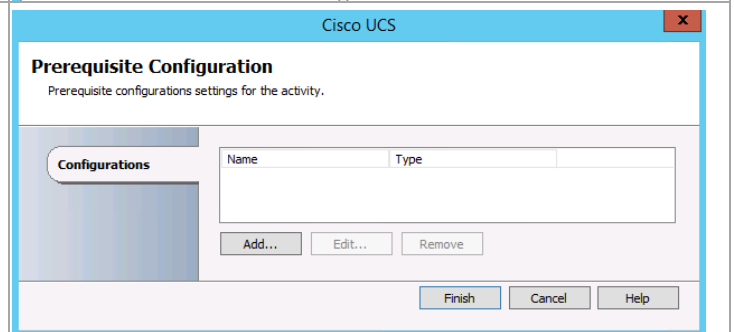
In the Deployment Manager console, expand Runbook Servers. Ensure the server is listed. Select the server to validate the integration pack is deployed. Repeat for each Runbook Server.



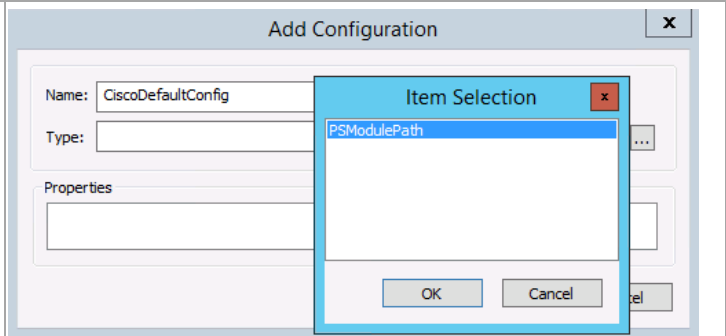
On any system on which the RunBook Designer was installed, launch the Runbook Designer and select **Options > Cisco UCS**. If PowerTool was not installed, you will not see the Cisco UCS menu option.



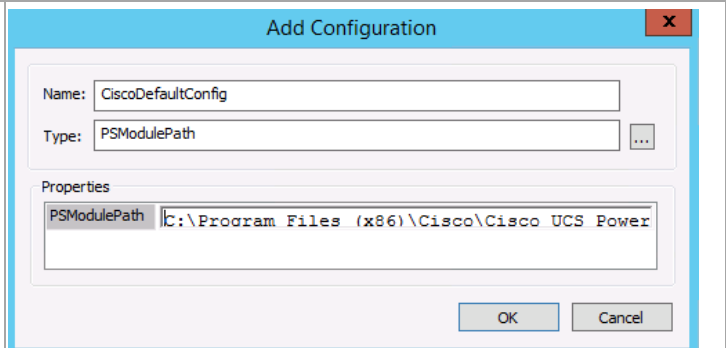
On the **Prerequisite Configuration** page, click **Add...**



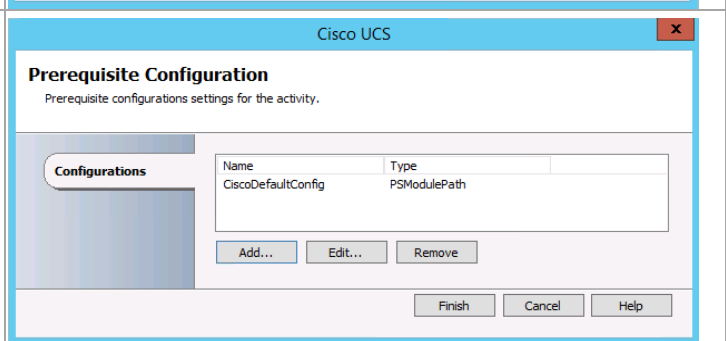
On the **Add Configuration** page, enter a **Name** for this configuration. Click the ... at the end of the **Type** field and select **PsModulePath**. Click **OK** on the **Item Selection** window.



In the **Properties** field of **PsModulePath** field, enter the location where the Cisco UCS PowerTool PowerShell module is installed. By default, this is located at C:\Program Files (x86)\Cisco\Cisco UCS PowerTool\Modules\CiscoUcsPS\CiscoUcsPS.psd1. Click **OK** to continue.



On the **Prerequisite Configuration** page, click **Finish** to complete the configuration.

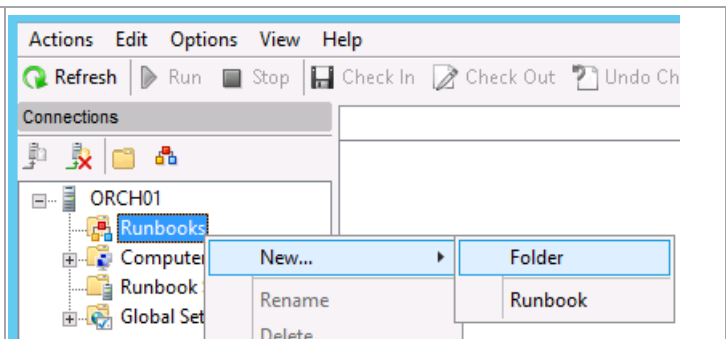


## Install Sample Cisco Runbooks (Optional)

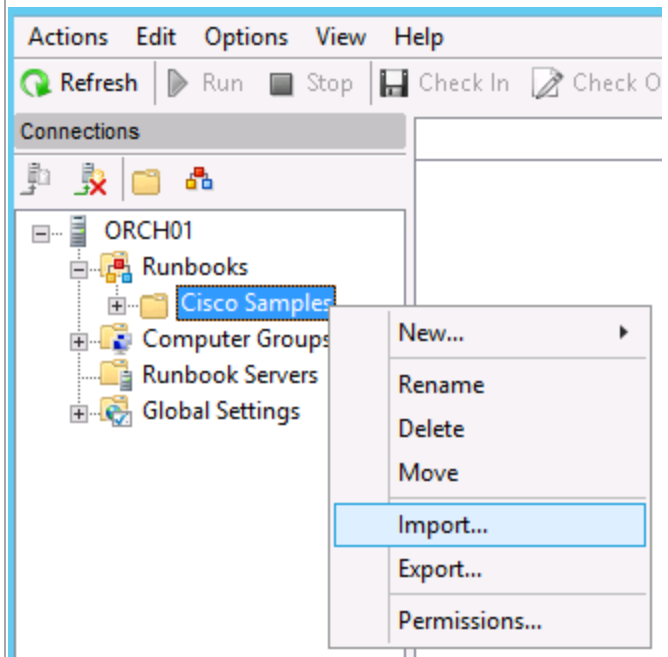
Cisco provides a small set of sample runbooks that assist in learning how to use the various activities available in their Integration Pack. Download the zip file and extract its contents. Perform the import of the sample runbooks on any Runbook Designer system.

In the Runbook Designer, right-click **Runbooks**, then click **New...** and select **Folder** to create a new folder in which to store the sample runbooks. Provide a name for the new folder.

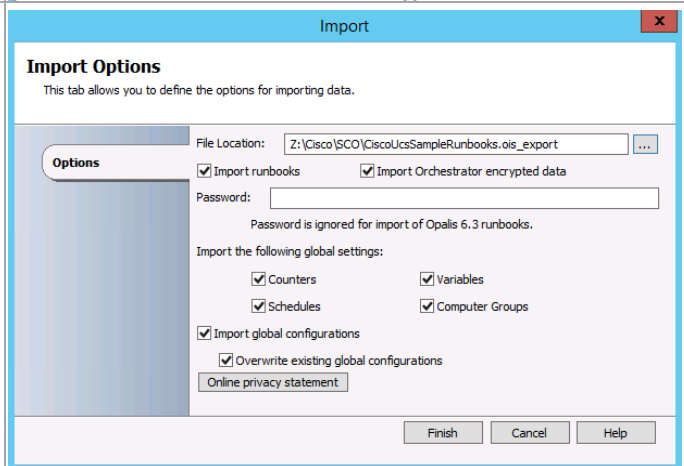
**Note:** Creating a new folder is optional. By default, the sample runbooks will import into a folder named Sample Runbooks under whatever level you import to.



Right-click the newly created folder and select **Import...**

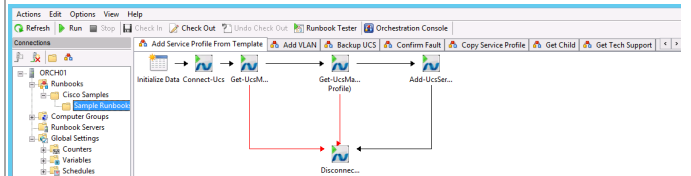


On the **Import Options** page, browse to the **File Location** where you extracted the contents of the sample runbooks zip file. Click **Finish** to complete the import. When the process is complete, click **OK** on the successful completion window.



Open the newly create folder to view the sample runbooks.

**Note:** There are variables added to Global Settings > Variables that must be set to the values for your environment for these sample runbooks to execute.



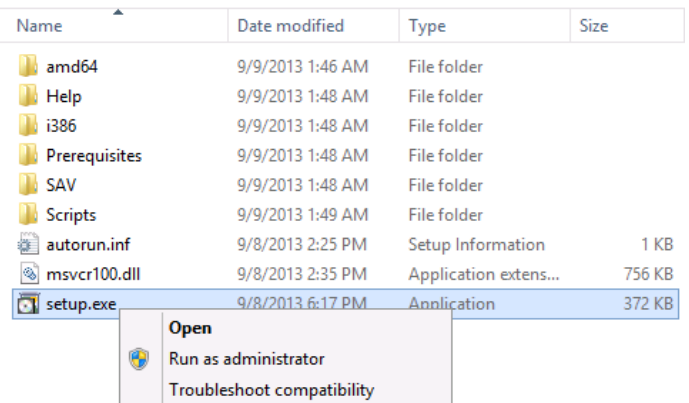
## 22.5 Post-Installation Tasks

When the installation is complete, connect Orchestrator to other System Center components and install and configure Orchestrator Integration Packs on the target Runbook Servers.

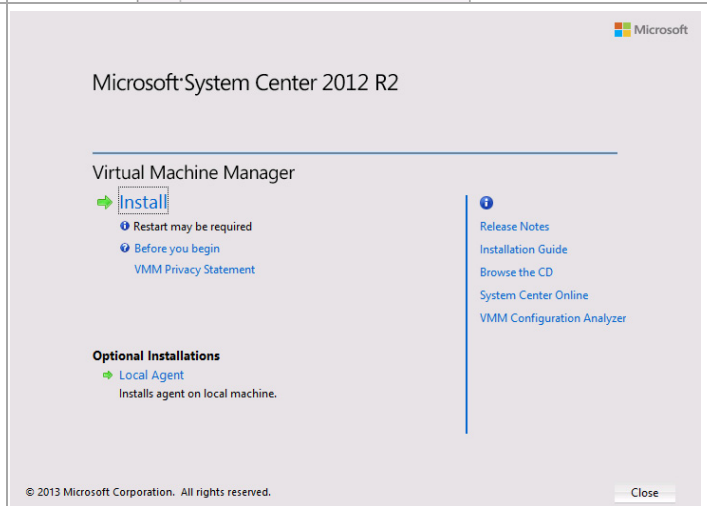
## Install the Virtual Machine Manager Console

Perform the following steps on each **Orchestrator** virtual machine with the Runbook role.

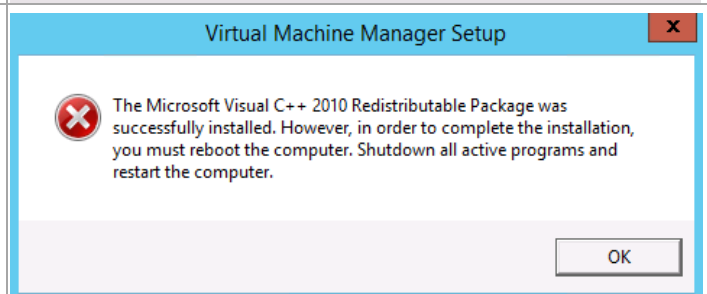
Log on to the Orchestrator server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



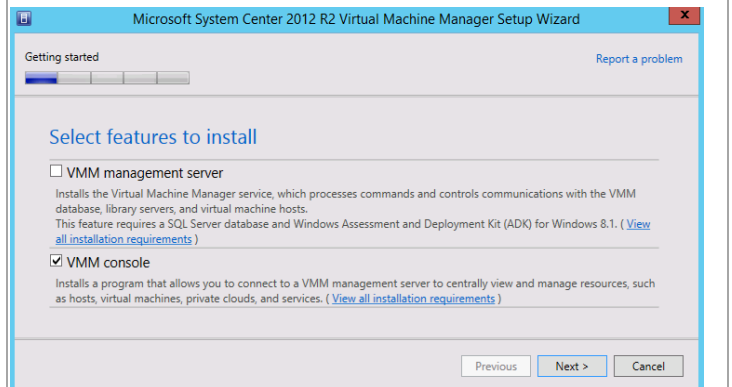
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



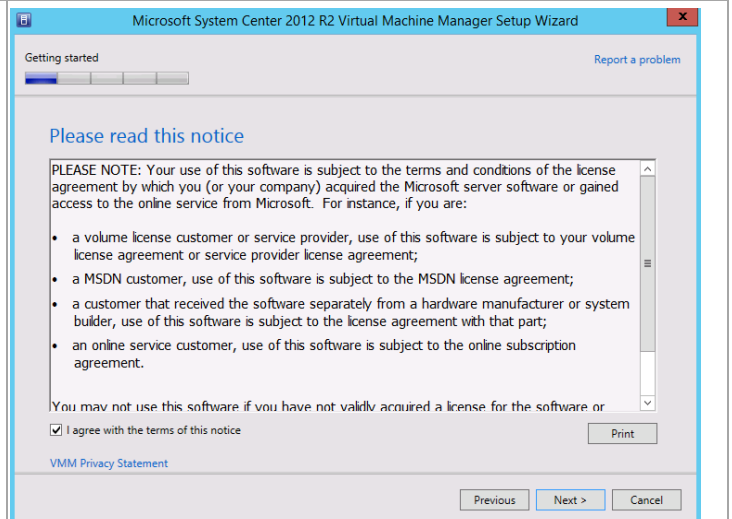
Depending upon the configuration, the installation may automatically install some prerequisite software that requires a reboot of the server. If instructed, reboot the server.



In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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

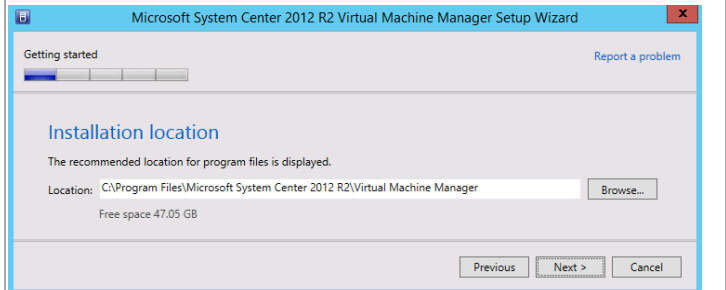


In the **Customer Experience Improvement Program** dialog, click **Next** to continue.

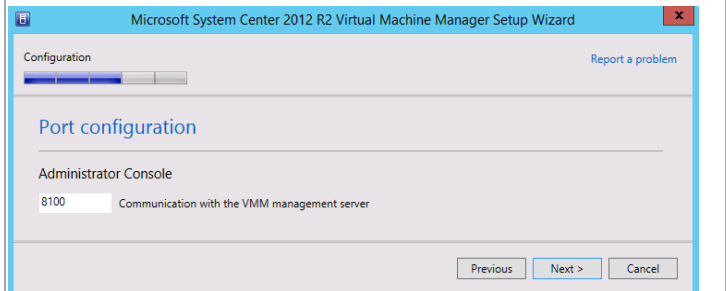


Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.

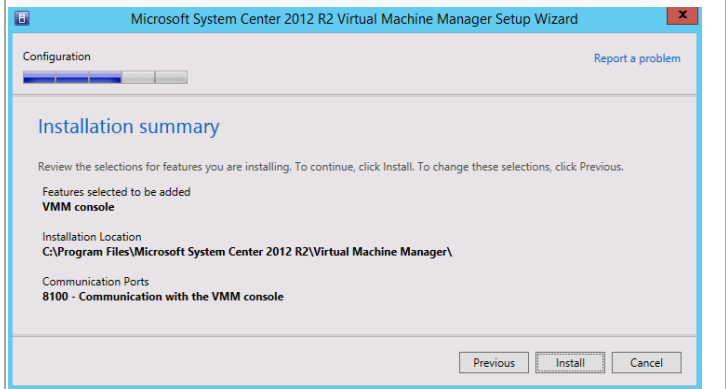
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.



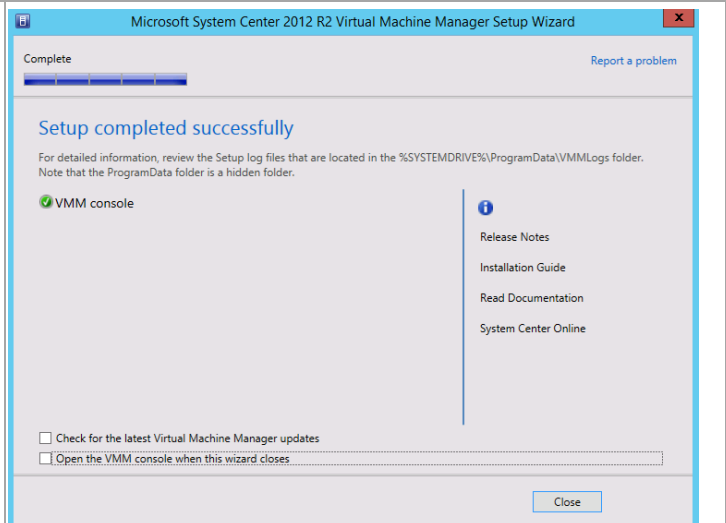
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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

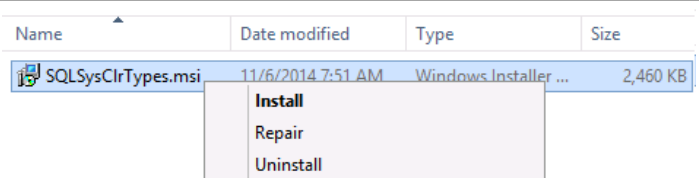


## Install the Microsoft Report Viewer 2012

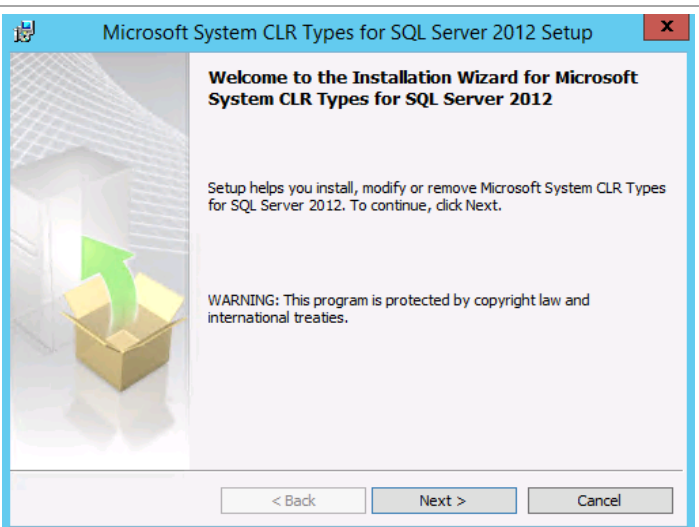
Additionally, inside Orchestrator the Operations Manager console is required, but this also requires the System CLR Types for SQL and Microsoft Report Viewer 2012 package be installed prior to installation.<sup>17</sup> Follow the provided steps to install these packages.

Perform the following steps on both **Orchestrator** virtual machines.

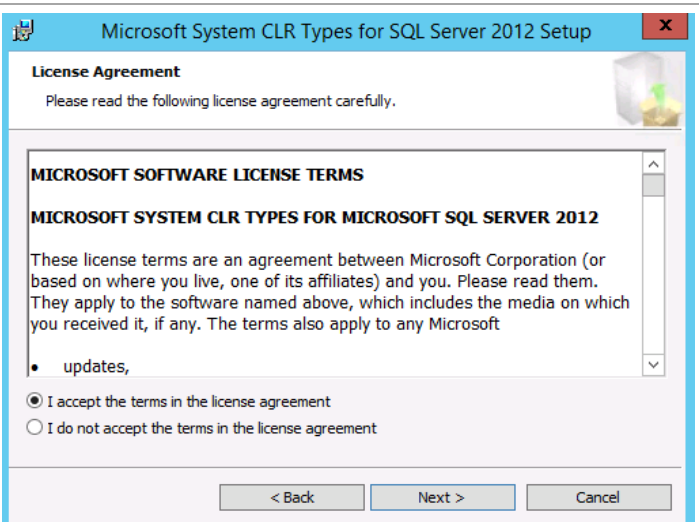
From the SQLSysClrTypes installation media, right-click **SQLSysClrTypes.msi** and select **Install** from the context menu to begin setup.



On the Welcome window click **Next** to continue.

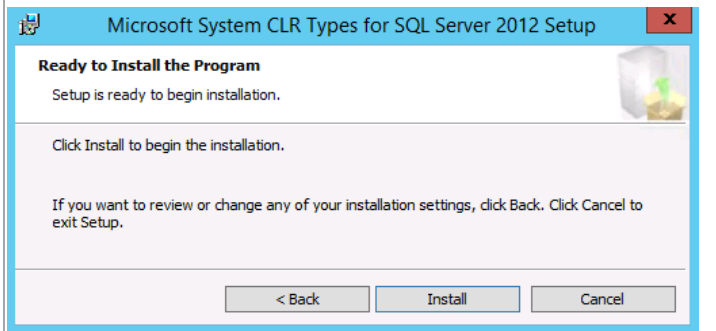


Select the radio button to accept the terms of the license and click **Next** to continue.

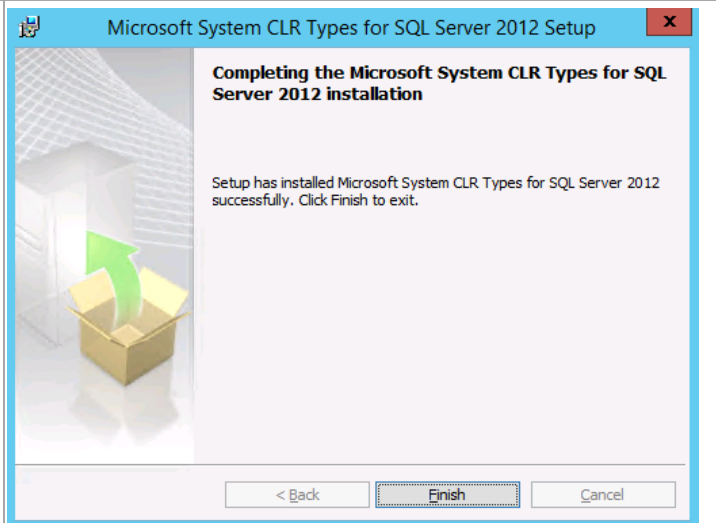


<sup>17</sup> Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&amp;amp;displaylang=r&displaylang=en>.

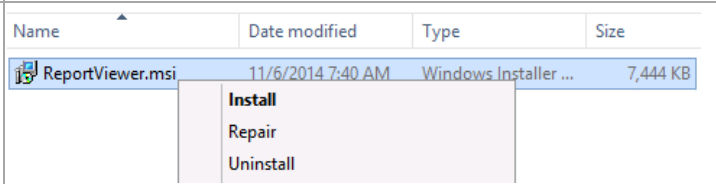
Accept the default installation directory and click **Install** to start the installation.



On the completion window click **Finish** to complete the installation.



From the Report Viewer installation media source, right-click **ReportViewer.exe** and select **Install** from the context menu to begin setup.

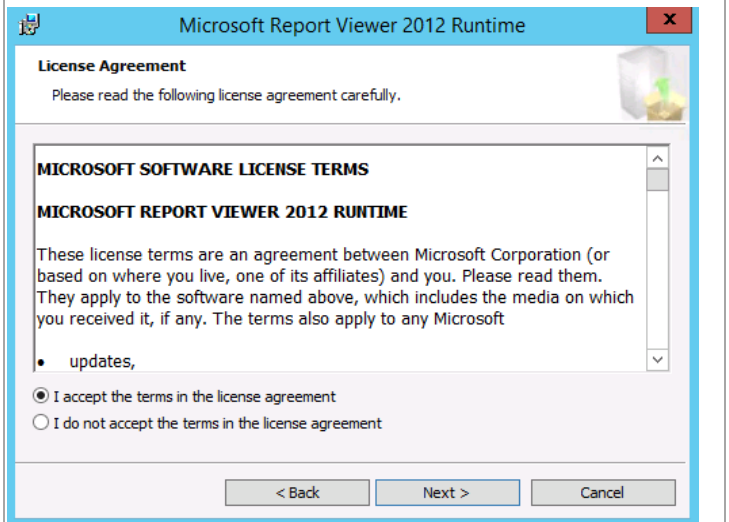


Within the **Microsoft ReportViewer 2012 Redistributable Setup** dialog, select **Next** to begin the installation.

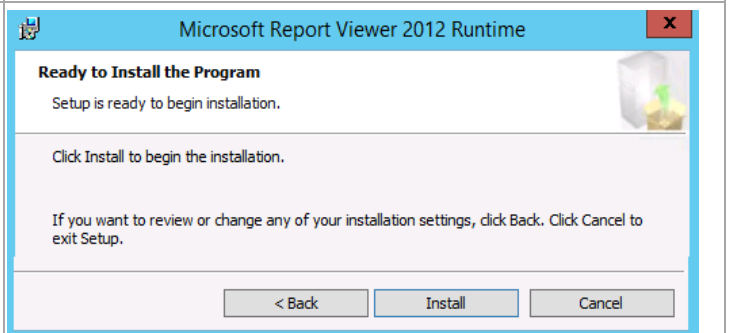




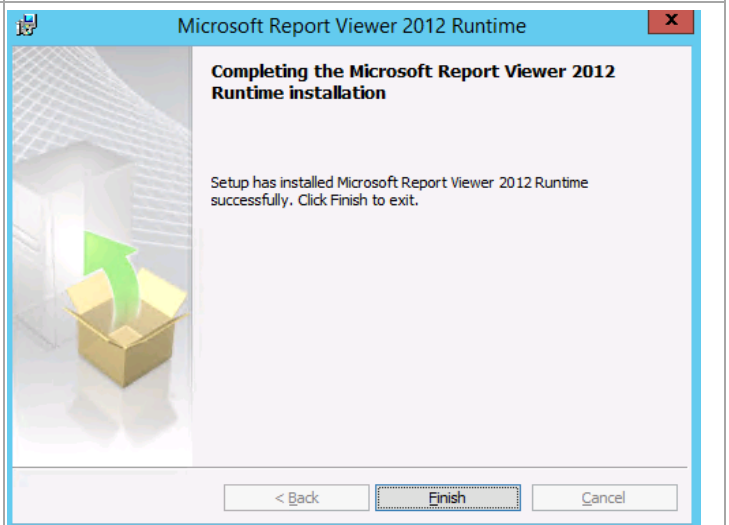
Select the **I accept the terms in the license agreement** radio button and click **Next**.



Accept the default installation directory and click **Install** to start the installation process.



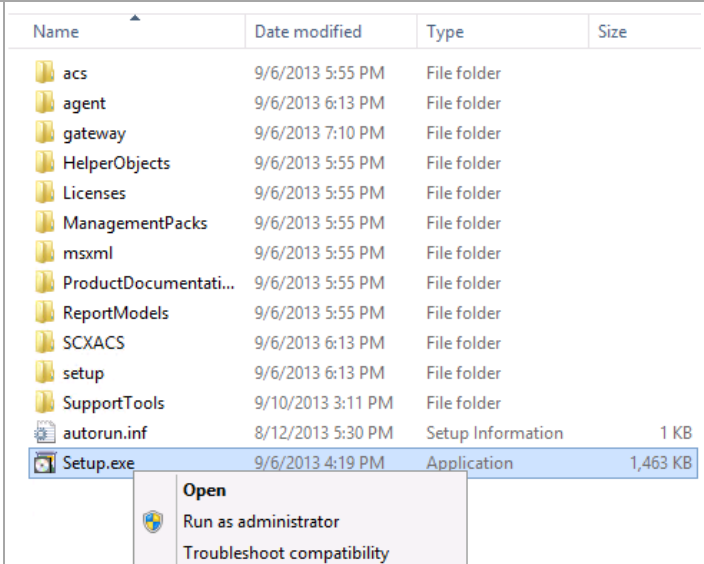
The installation progress will be displayed in the setup wizard. When completed, click **Finish** to exit the installation.



## Install the Operations Manager Console

Perform the following steps on both **Orchestrator** virtual machines.

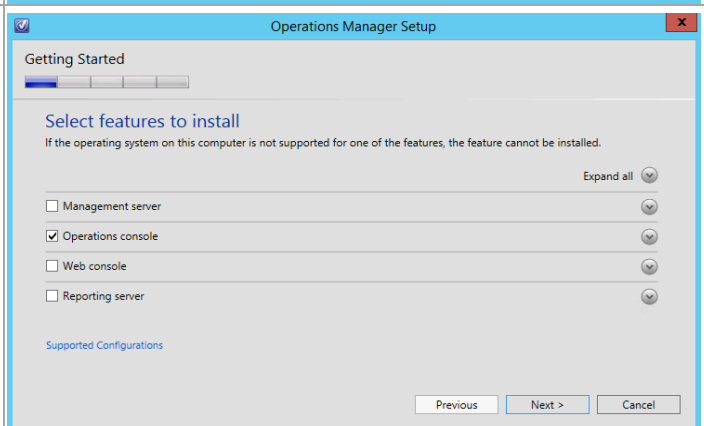
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



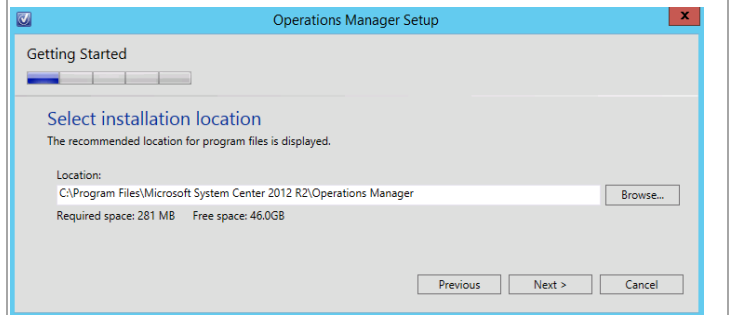
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



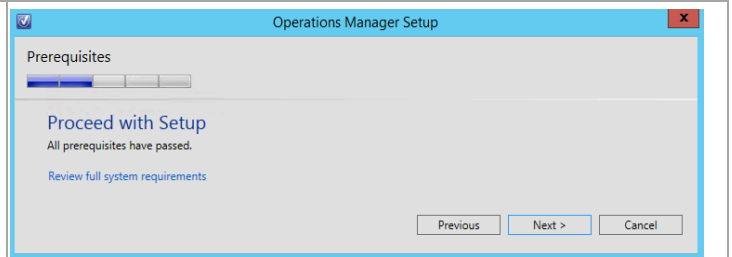
In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.



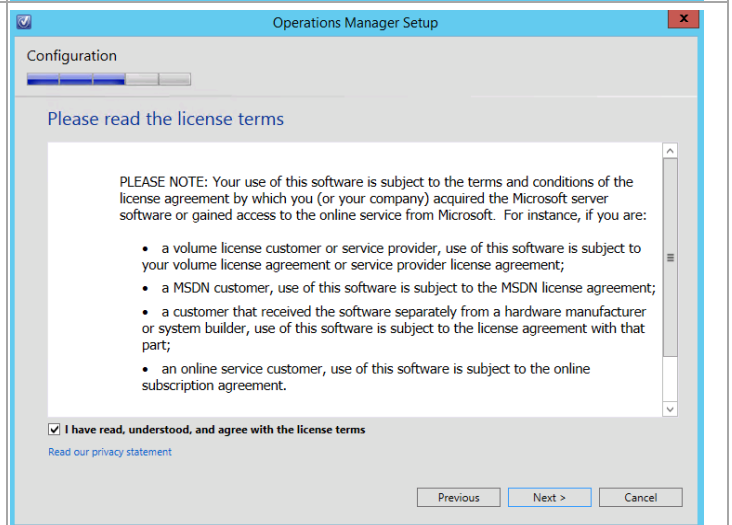
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012 R2\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



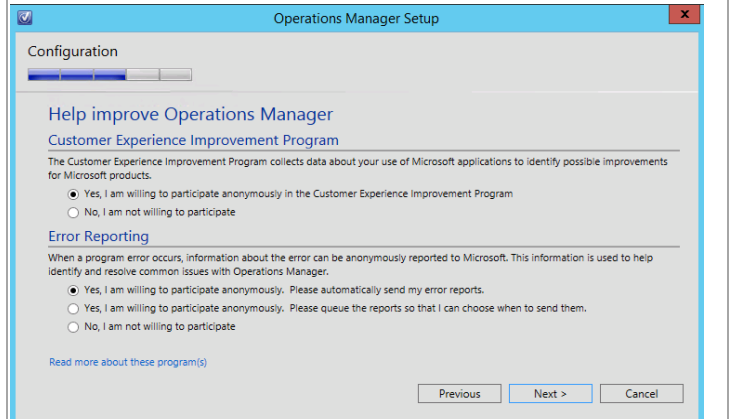
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

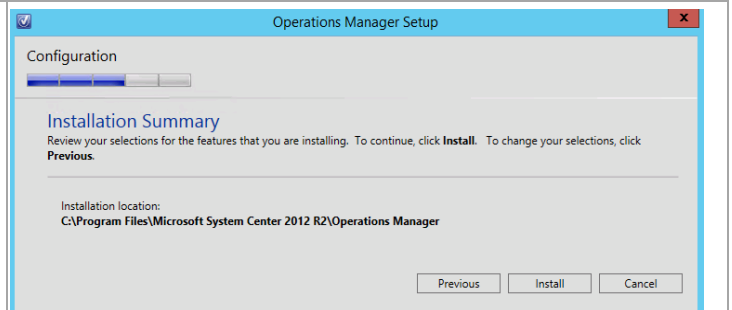
Select the appropriate option based on your organization's policies and click **Next** to continue.



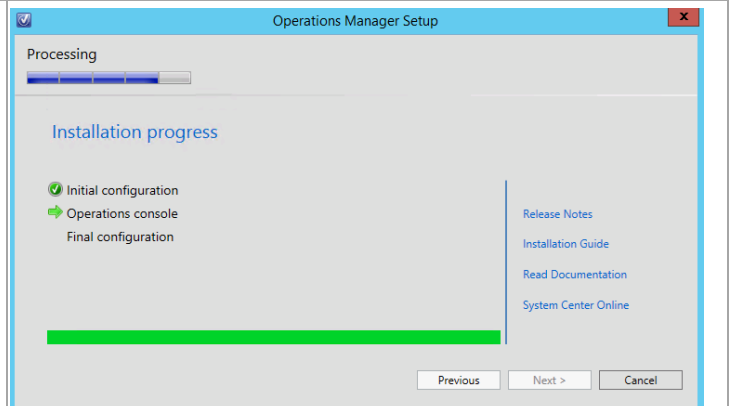
Unless a different method of applying patches is deployed, it is recommended to use Microsoft Update to check for updates. Click **Next** to continue.



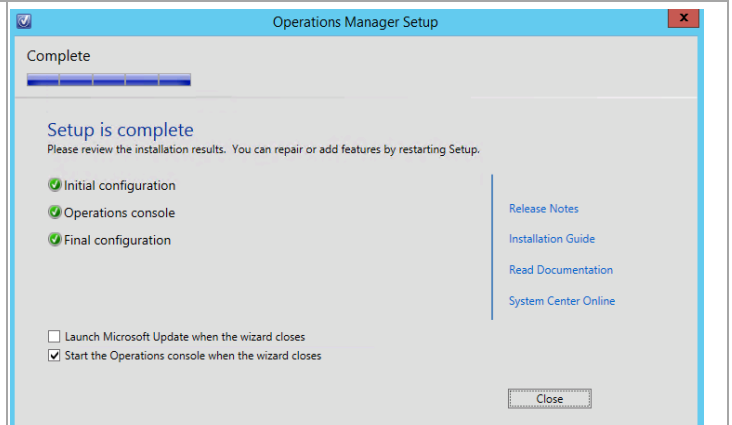
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



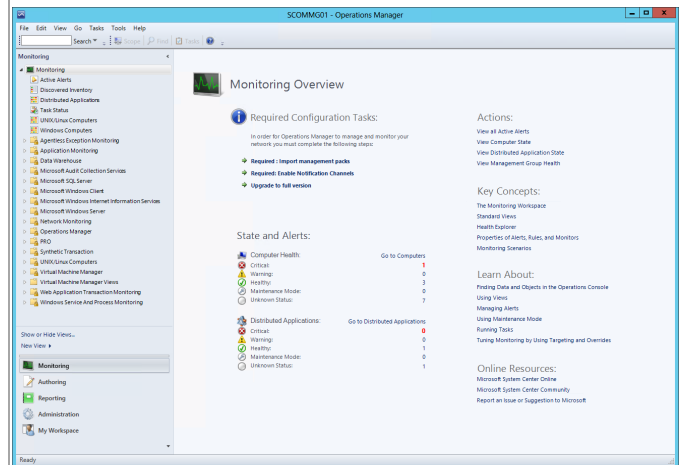
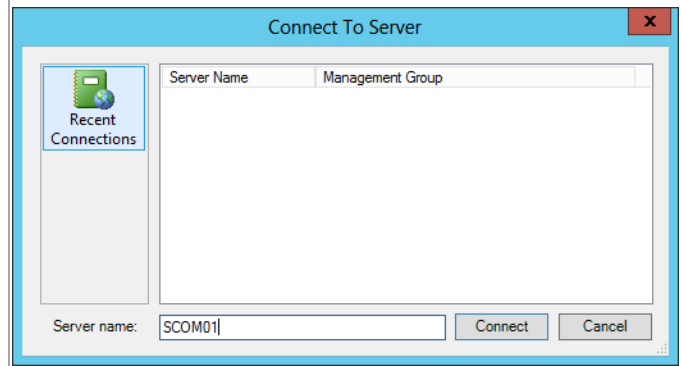
The installation progress will be displayed during the installation.



When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.



When completed, the Operations Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



## Install System Center 2012 R2 Integration Packs

The following steps needs to be completed in order to install the Orchestrator Integration Packs.

**Perform the following steps on the Orchestrator Runbook Server virtual machine.**

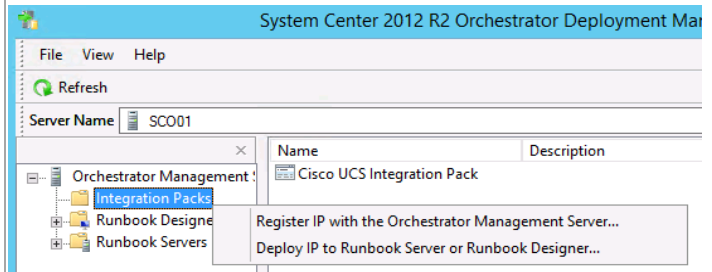
Download the System Center 2012 R2 Integration Packs from <http://www.microsoft.com/en-us/download/confirmation.aspx?id=39622&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1> and expand them to a single location so the Orchestrator Integration Pack files are expanded.

Name	Date modified	Type	Size
attributions	9/17/2013 5:13 PM	Text Document	2 KB
SC2012R2_Integration_Pack_for_Azure.oip	9/17/2013 5:52 PM	OIP File	880 KB
SC2012R2_Integration_Pack_for_Configur...	3/14/2014 7:13 PM	OIP File	858 KB
SC2012R2_Integration_Pack_for_Data_Prot...	9/17/2013 5:52 PM	OIP File	707 KB
SC2012R2_Integration_Pack_for_Operation...	3/14/2014 7:13 PM	OIP File	447 KB
SC2012R2_Integration_Pack_for_REST.oip	3/14/2014 7:13 PM	OIP File	623 KB
SC2012R2_Integration_Pack_for_Service_M...	9/17/2013 5:52 PM	OIP File	1,523 KB
SC2012R2_Integration_Pack_for_Virtual_Ma...	9/17/2013 5:52 PM	OIP File	988 KB
System_Center_2012_R2_Integration_Pack...	9/17/2013 5:23 PM	OIP File	874 KB
System_Center_2012_R2_Integration_Pack...	3/14/2014 3:42 PM	OIP File	703 KB
System_Center_2012_R2_Integration_Pack...	9/17/2013 5:26 PM	OIP File	937 KB
System_Center_2012_R2_Integration_Pack...	9/17/2013 5:29 PM	OIP File	1,047 KB
System_Center_2012_R2_Integration_Pack...	3/15/2014 12:38 PM	OIP File	1,500 KB

From the **Start** screen, click the **Deployment Manager** tile.



In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Register IP with the Orchestrator Management Server...** option from the context menu.

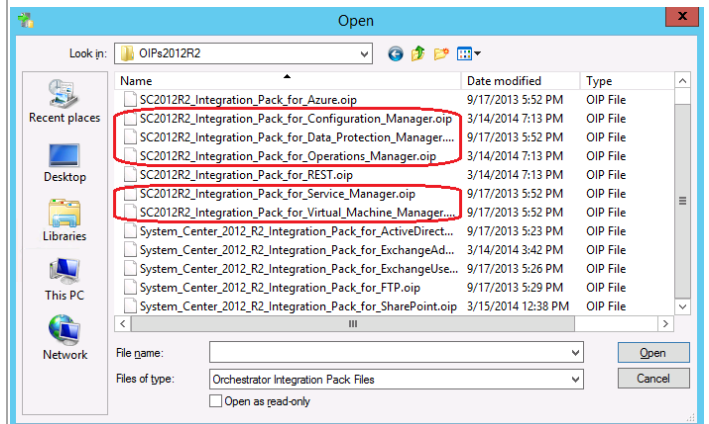
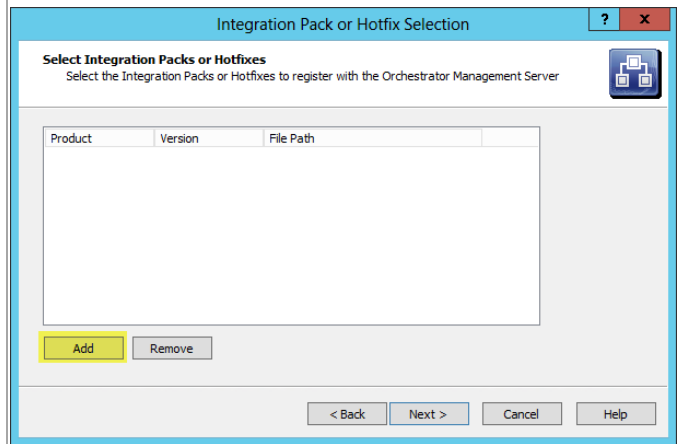


The **Integration Pack Registration Wizard** will appear. Click **Next** to continue.

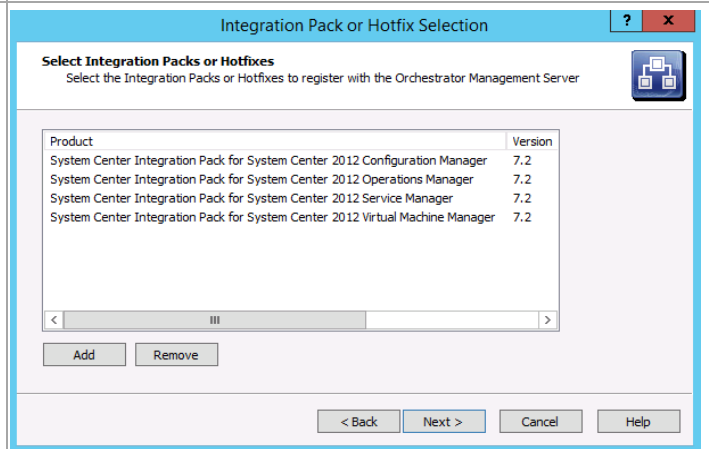


In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the expanded integration packs folder created earlier and select, at a minimum, the following integration packs and click **Open**:

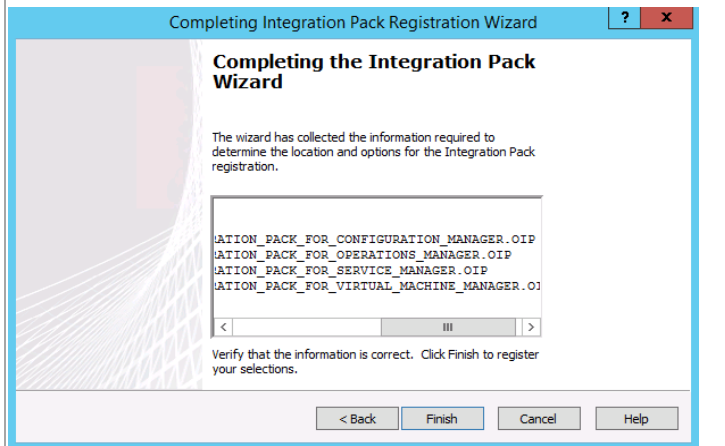
- System Center 2012 R2 Configuration Manager.
- System Center 2012 R2 Operations Manager.
- System Center 2012 R2 Service Manager.
- System Center 2012 R2 Virtual Machine Manager.



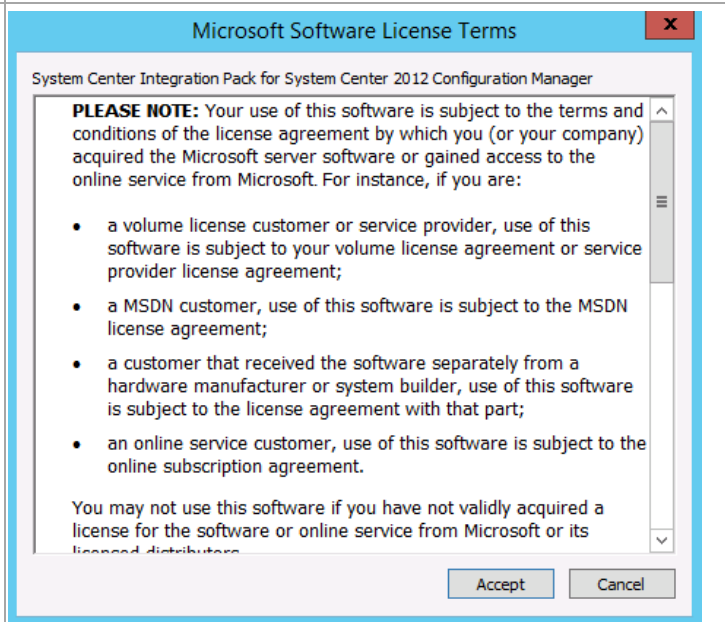
When all integration packs are selected, click **Next** to continue.



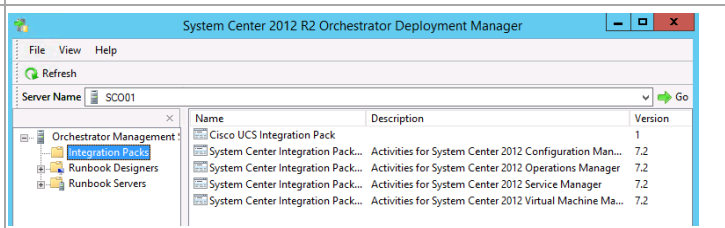
The **Completing the Integration Pack Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.



When complete, each integration pack will be displayed in the Deployment Manager interface.



## Deploy Integration Packs

The following steps need to be completed in order to install the Orchestrator Integration Packs.<sup>18</sup>

<sup>18</sup> System Center 2012 SP1 – Orchestrator Component Add-ons and Extensions - <http://www.microsoft.com/en-us/download/details.aspx?id=34606>

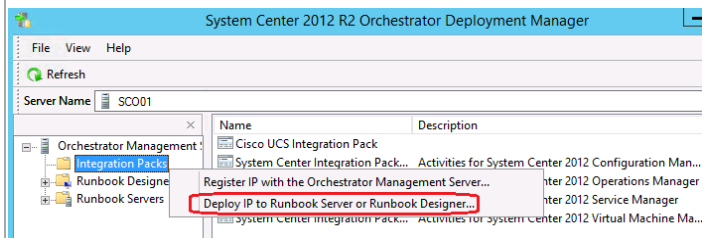


Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

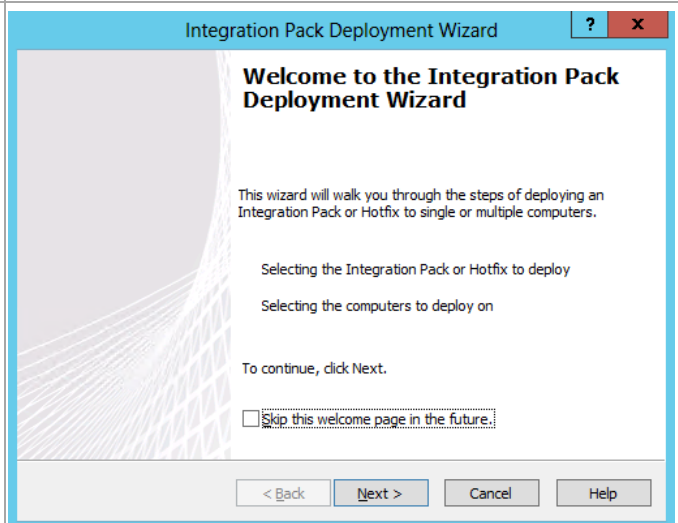
From the **Start** screen, click the **Deployment Manager** tile.



In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer...** option from the context menu.



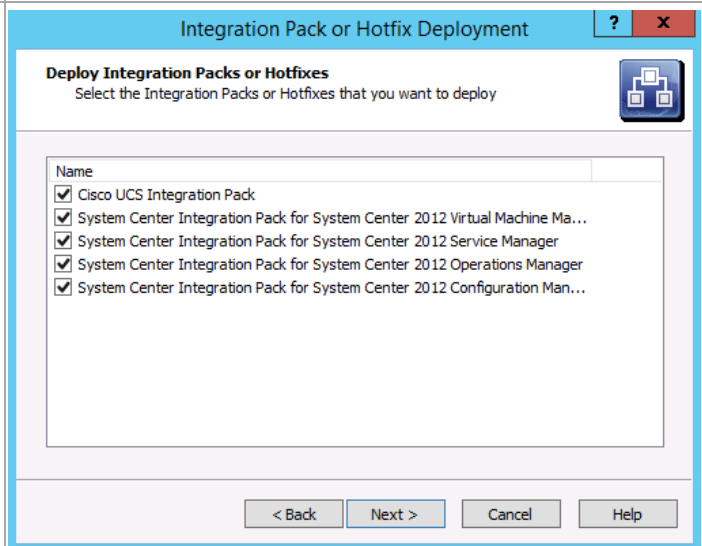
The **Integration Pack Deployment Wizard** will appear. Click **Next** to continue.



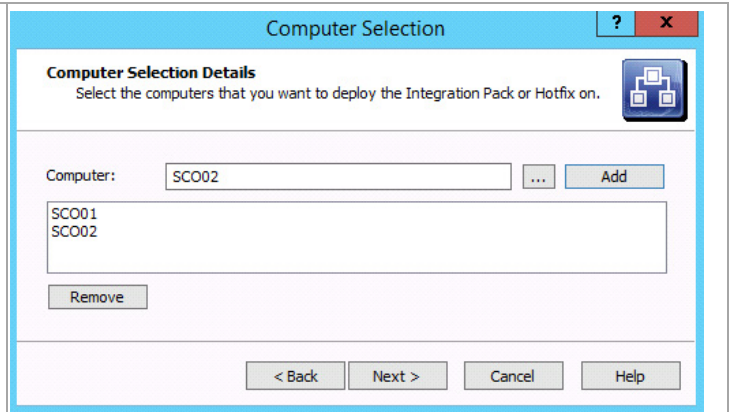
In the **Deploy Integration Packs or Hotfixes** dialog, select the check boxes integration packs folder created earlier and select the following integration packs:

- System Center 2012 R2 Configuration Manager.
- System Center 2012 R2 Operations Manager.
- System Center 2012 R2 Service Manager.
- System Center 2012 R2 Virtual Machine Manager.
- Cisco UCS Integration Pack

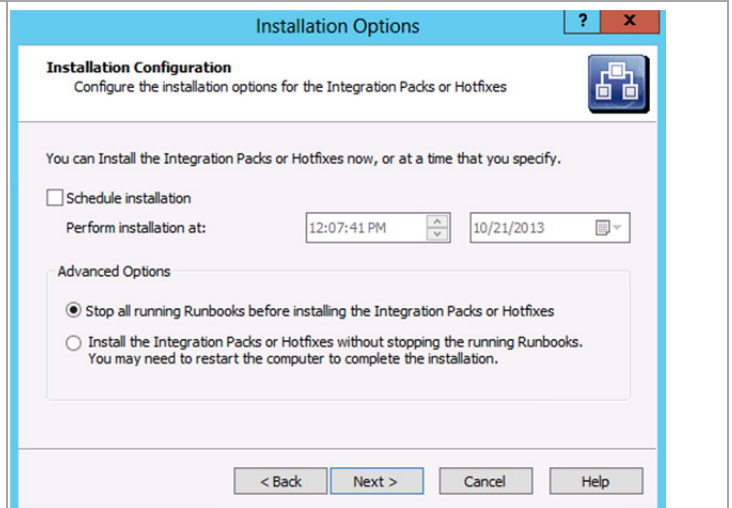
When complete, click **Next** to continue.



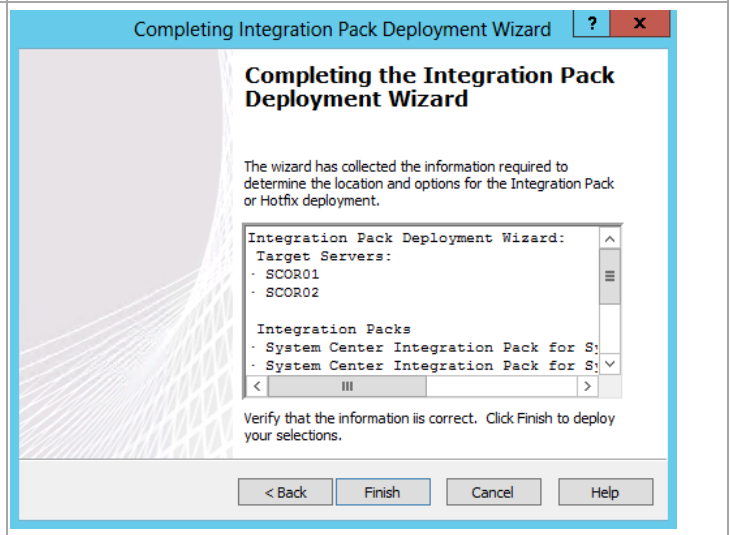
In the **Computer Selection Details**, type the name of each Orchestrator runbook server and click **Add**. When added, click **Next** to continue.



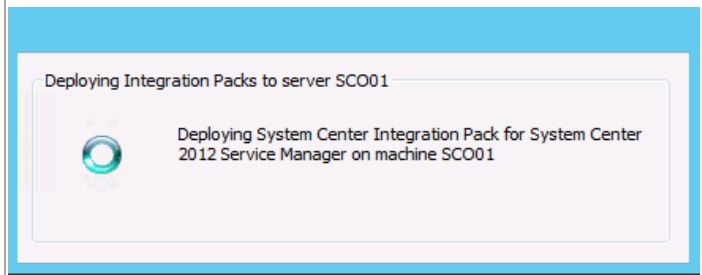
In the **Installation Configuration** dialog, in the **Advanced Options** pane select **Stop all running Runbooks before installing the Integration Packs or Hotfixes** option. Click **Next** to continue.



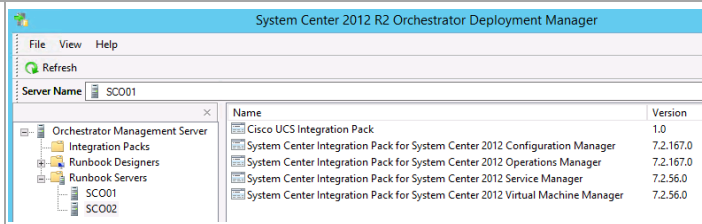
The **Completing the Integration Pack Deployment Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



During the installation each integration pack will display a status window.



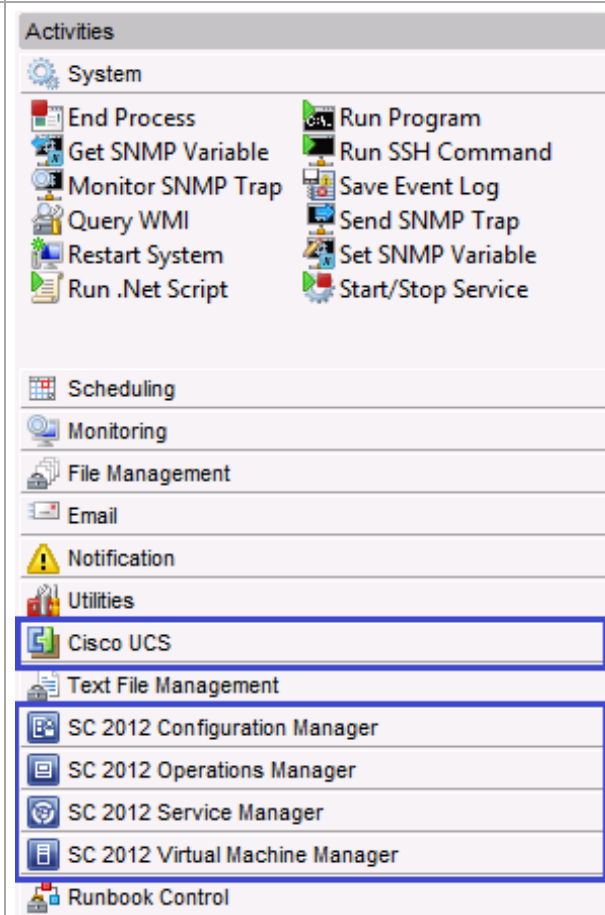
When completed, you can validate the deployment to each runbook server by expanding **Runbook Servers** in the deployment console and selecting the runbook server names.



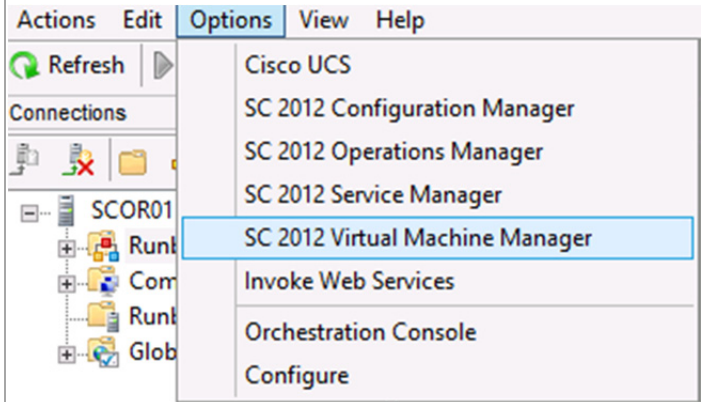
From the **Start** screen, click the **Runbook Designer** tile.



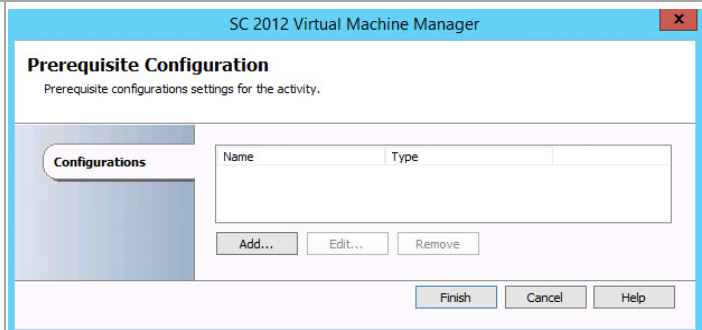
When complete, each integration pack will be displayed in the Runbook Designer interface.



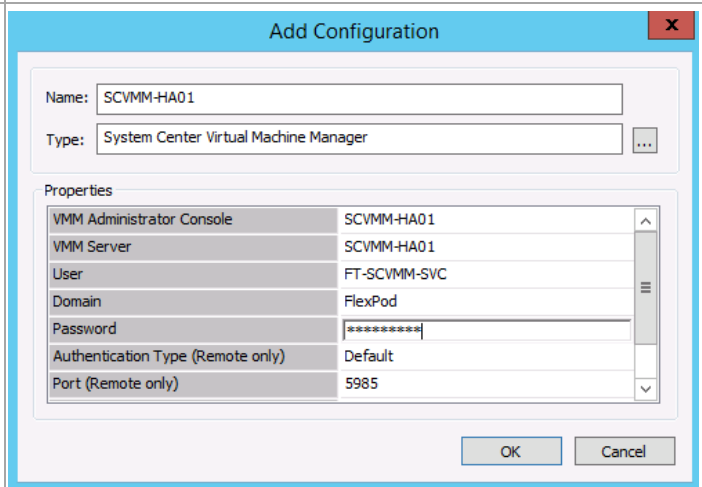
To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Virtual Machine Manager** option.



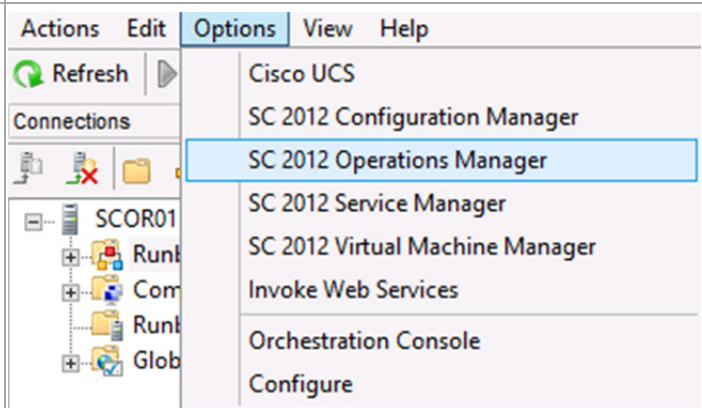
In the Prerequisite Configuration dialog, click **Add**.



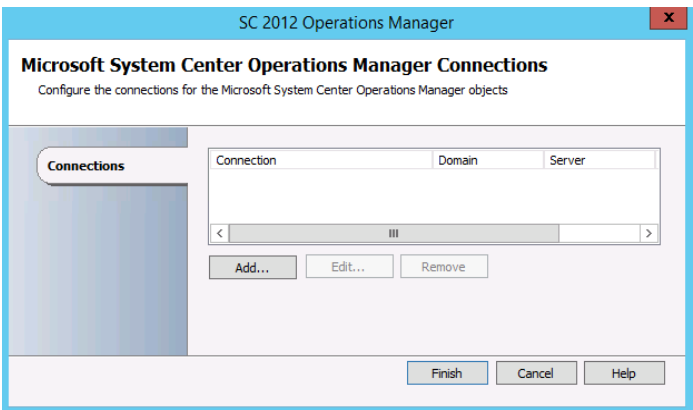
In the **Add Configuration** dialog, provide a descriptive name for this configuration and click the .... Select System Center Virtual Machine Manager from the pop-up window. Complete the required information for the highly available Virtual Machine Manager server as shown and click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.



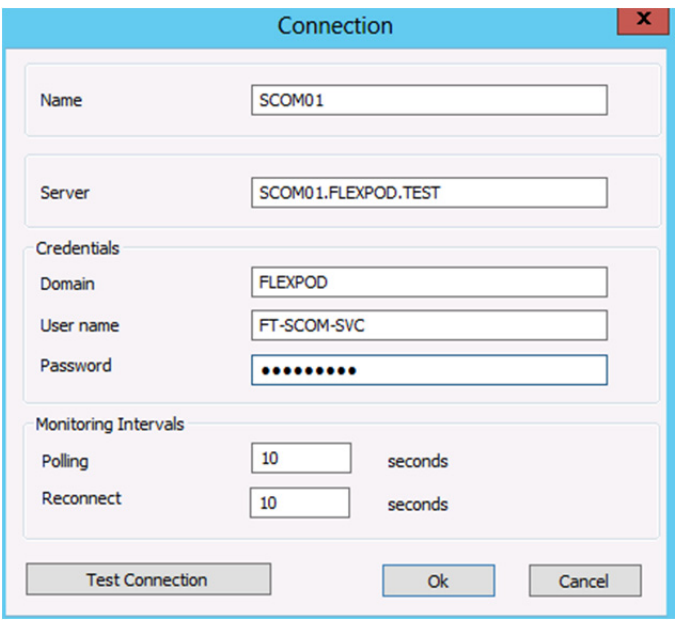
While still in the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Operations Manager** option.



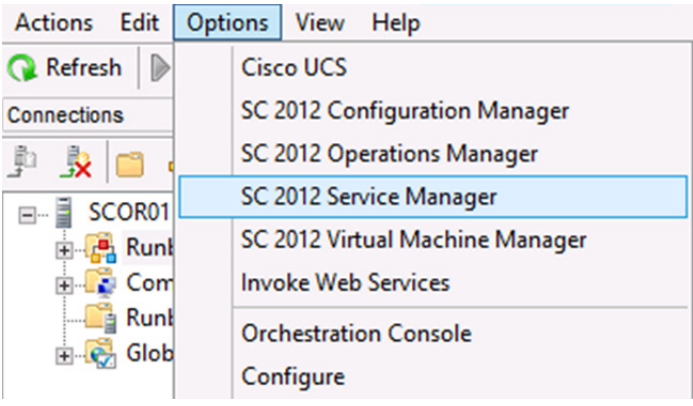
In the **Microsoft System Center Operations Manager Connections** dialog, click **Add**.



In the **MS System Center Operations Manager Connection Settings** dialog, fill in the required information for the Operations Manager management server and click **Test Connection**<sup>19</sup>. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

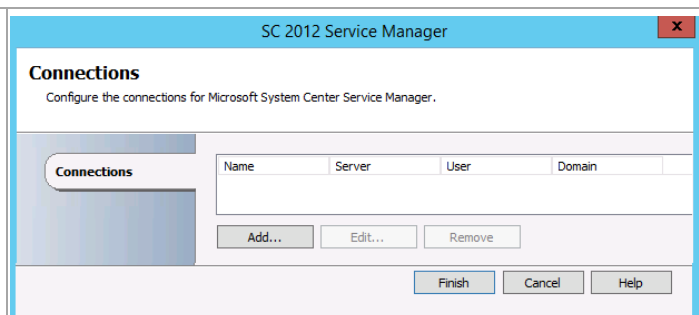


In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **SC 2012 Service Manager** option.

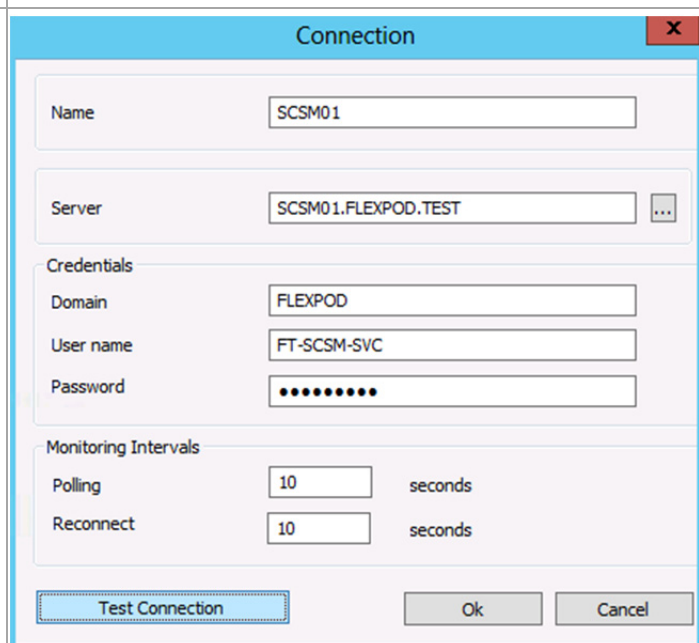


<sup>19</sup> The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

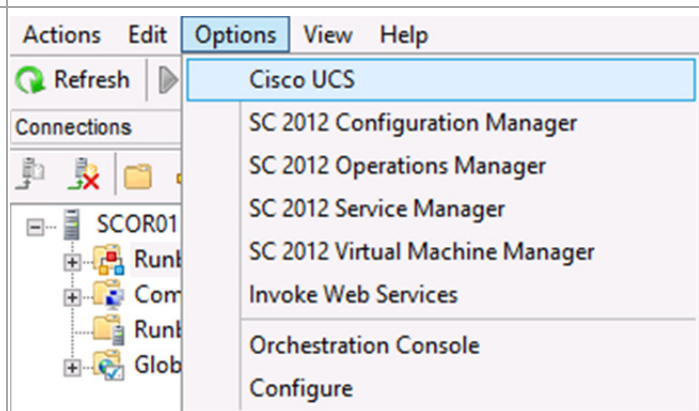
In the **Connections** dialog, click **Add**.



In the **Connection** dialog, fill in the required information for the Operations Manager management server<sup>20</sup> and click **Test Connection**. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

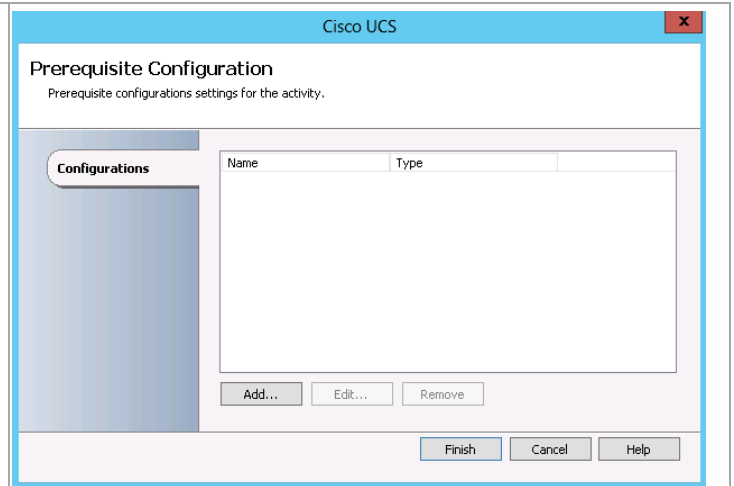


In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **Cisco UCS** option.

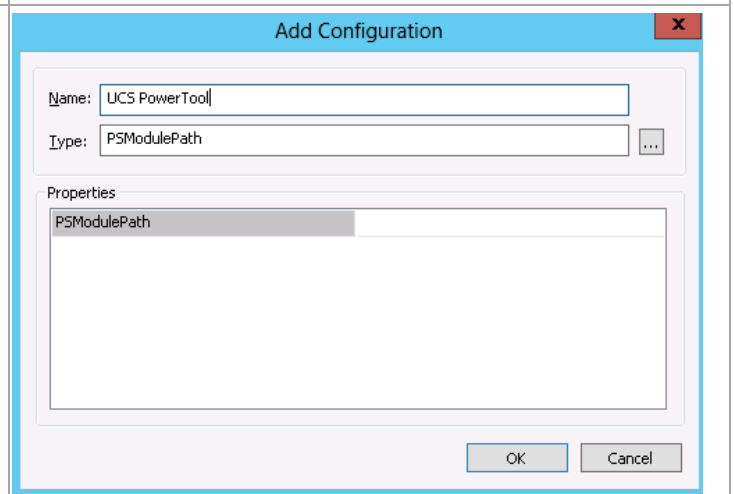


<sup>20</sup> The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

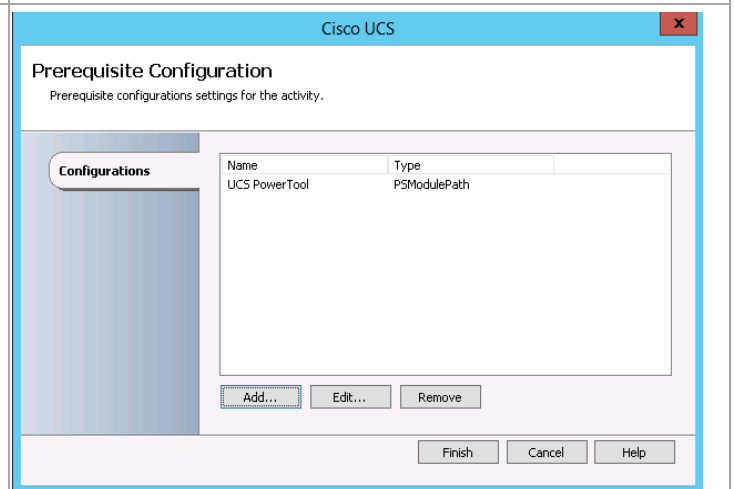
The Cisco UCS **Prerequisite Configuration** window opens. Click the **Add** button.



Type the configuration **name**. Click the “...” button and select **PSModulePath**. Click **OK** to accept the settings and close the windows. Leave **PSModulePath** property blank to use default PowerTool installation or provide custom path of **CiscoUcsPS.psd1** file. Click OK to close the window.

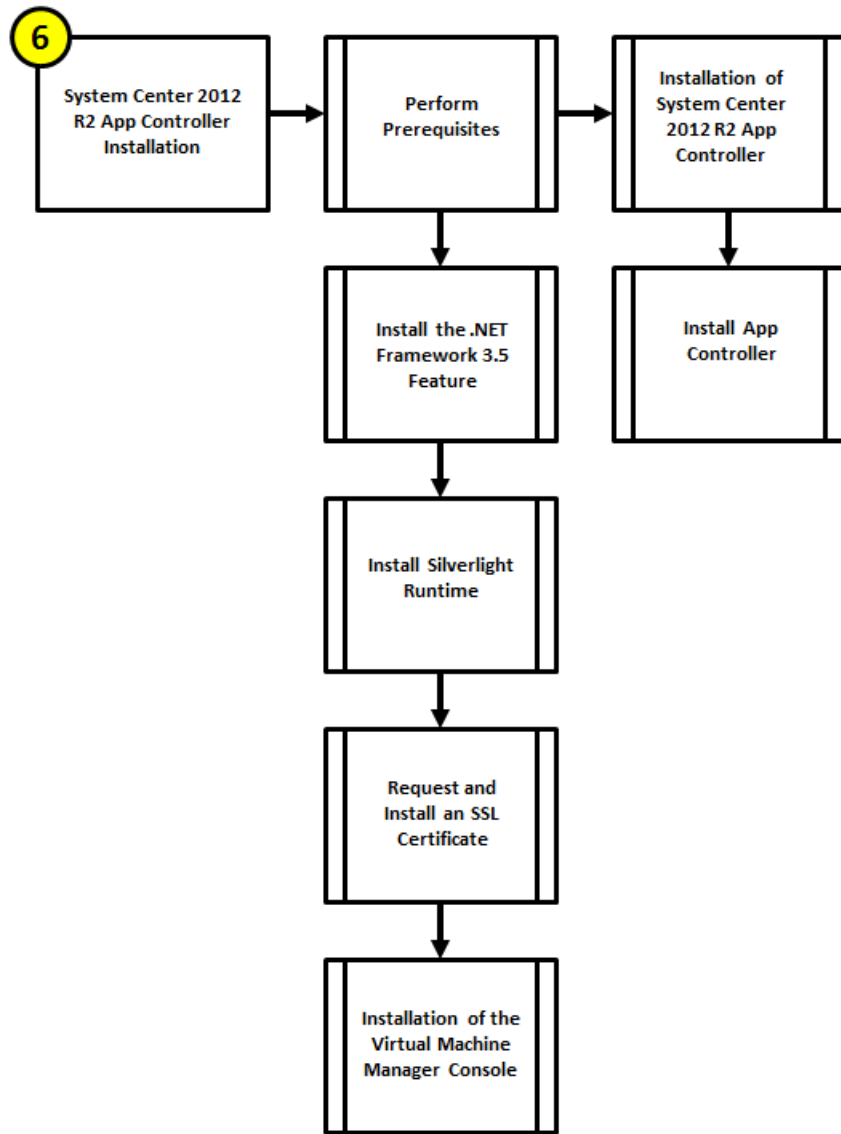


Click **Finish** to save the setting and close the window.



## 23 App Controller

The App Controller installation process includes the following high-level steps:





## 23.1 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 R2 has been provisioned for App Controller.
- A SQL Server 2012 SP2 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.

## 23.2 Prerequisites

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: <ul style="list-style-type: none"><li>• FT-SCAC-Admins</li><li>• FT-VMM-Admins</li></ul>

### Groups

Verify that the following security groups have been created:

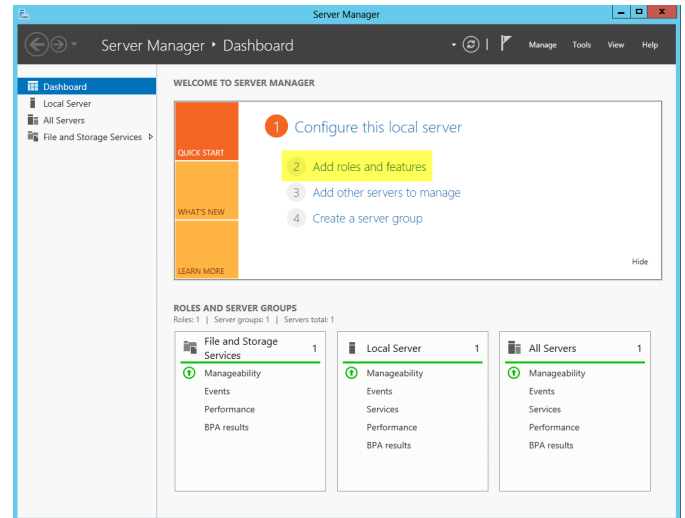
Group name	Purpose	Members
<DOMAIN>\ FT-SCAC-Admins	App Controller Admin group	<DOMAIN>\ FT-SCAC-SVC <DOMAIN>\ FT-VMM-Admins

## Install the .NET Framework 3.5 Feature

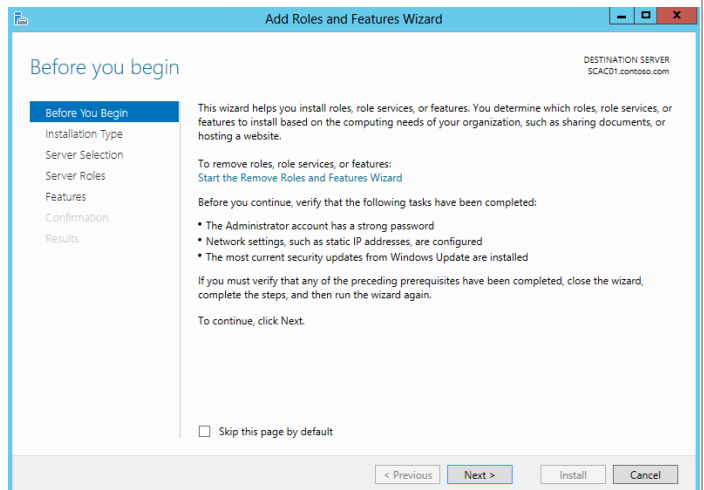
The App Controller installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

Perform the following steps on the **App Controller** virtual machine.

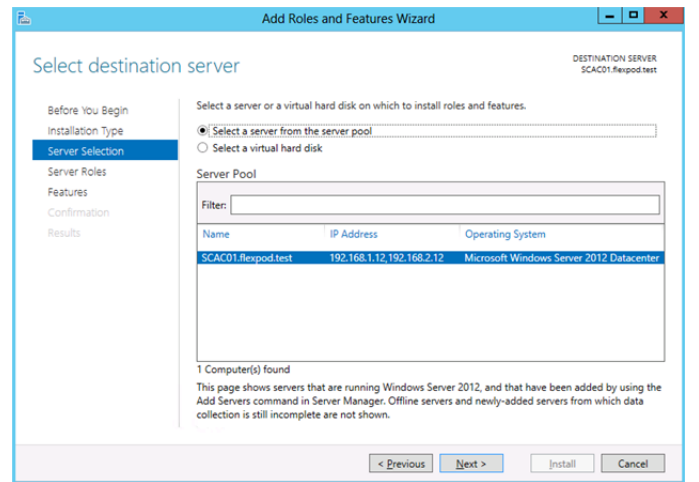
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



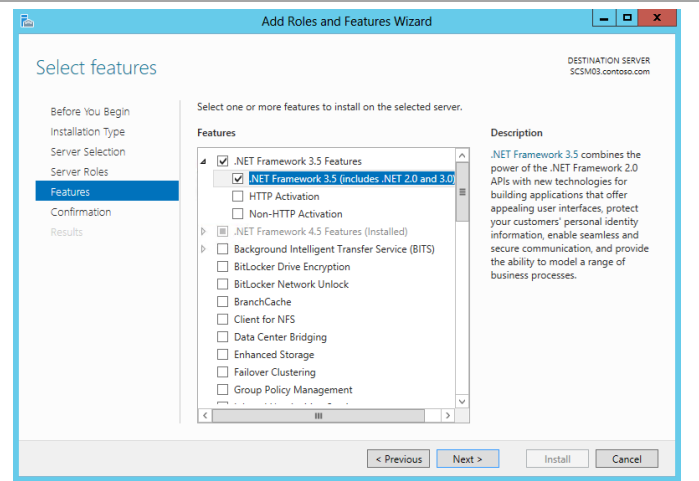
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



In the **Select destination server** dialog, select the **Select a server from the server pool** radio button, select the local server and do not click **Next** - for this installation, click the **Features** menu option to continue.



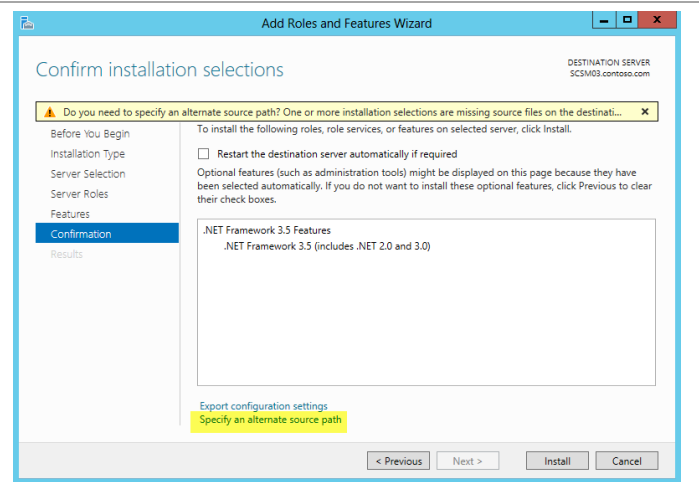
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



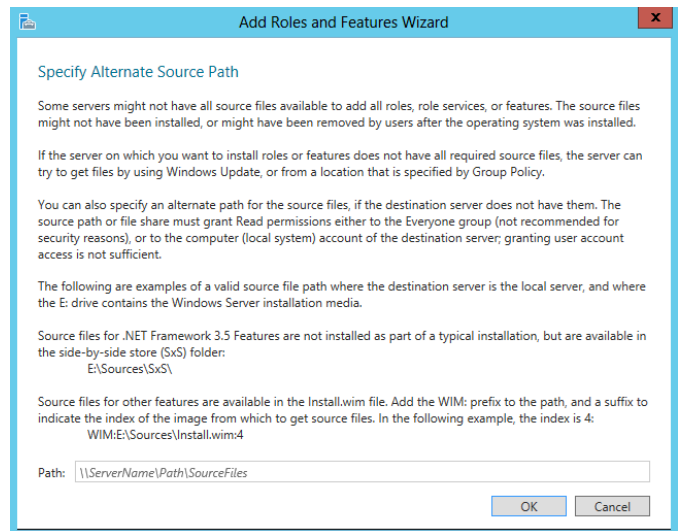
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

*Note that 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.*

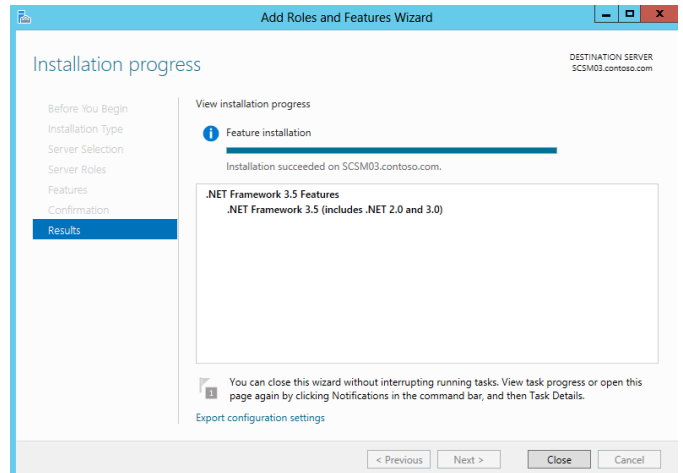
*Also, If the server does not have internet access an alternate source path can be specified by clicking the **Specify an alternate source path** link.*



*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.*



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



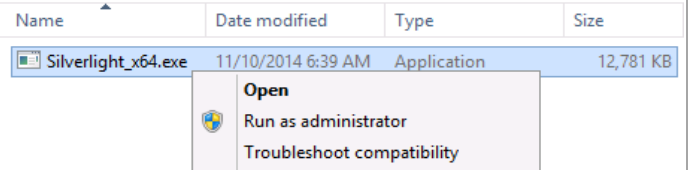
Note that while the previous installation was performed interactively, the installation of roles and features can be automated using the shown PowerShell cmdlet.

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

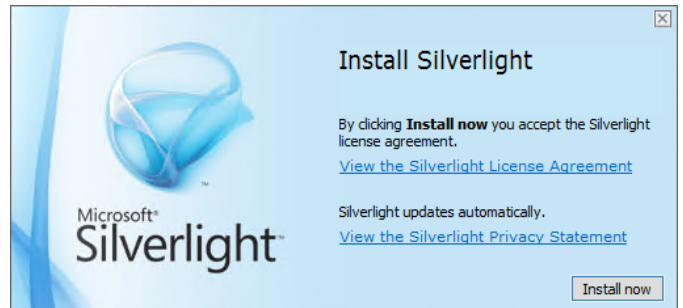
## Install Silverlight Runtime

Perform the following steps on the **App Controller** virtual machine.

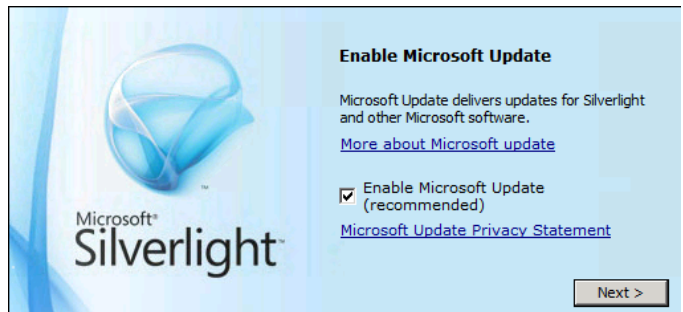
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.



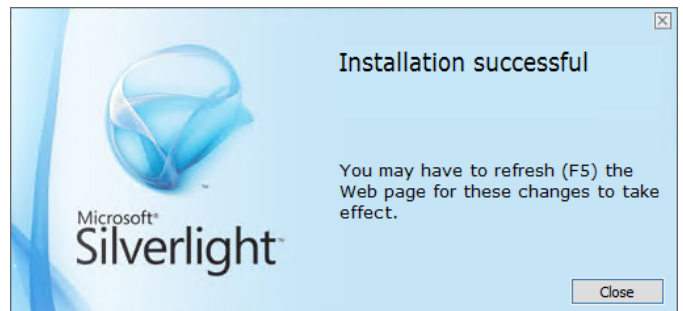
In the **Install Silverlight** dialog, click **Install now**.



In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.



In the **Installation Successful** dialog, click **Close** to exit the installation.



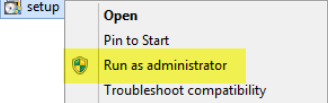
## Install the Virtual Machine Manager Console

The following steps need to be completed in order to install the Virtual Machine Manager console on the target App Controller virtual machine.

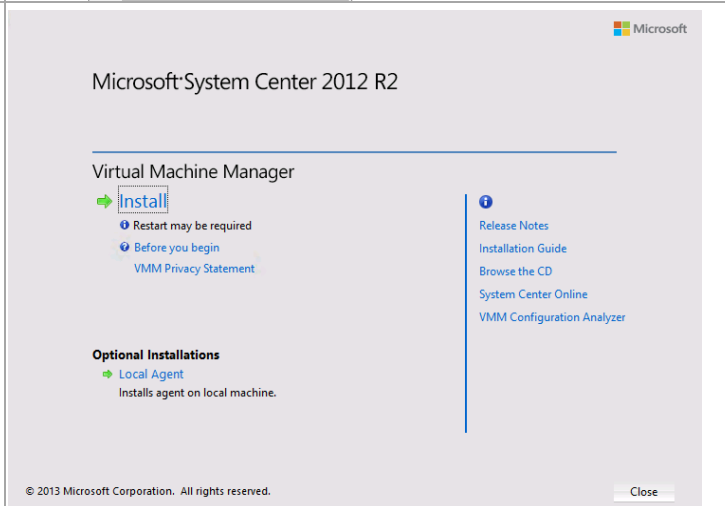
Perform the following steps on the **App Controller** virtual machines.

Log on to the App Controller server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

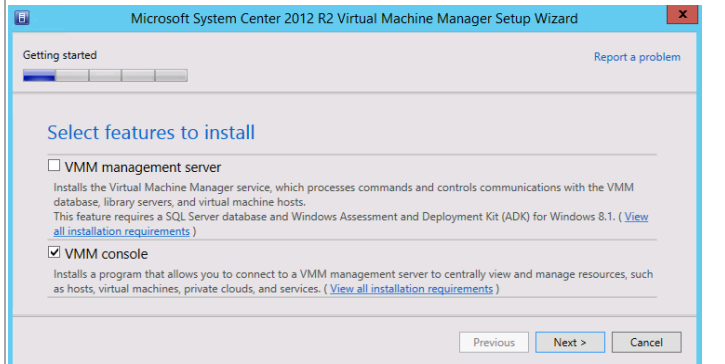
Name	Date modified	Type	Size
amd64	11/26/2012 3:32 PM	File folder	
Help	11/26/2012 3:32 PM	File folder	
i386	11/26/2012 3:33 PM	File folder	
Prerequisites	11/26/2012 3:33 PM	File folder	
SAV	11/26/2012 3:33 PM	File folder	
Scripts	11/26/2012 3:33 PM	File folder	
autorun	10/17/2012 12:16 ...	Setup Information	1 KB
msvcr100.dll	10/31/2012 6:47 PM	Application extens...	756 KB
setup	11/26/2012 6:58 PM	Application	372 KB



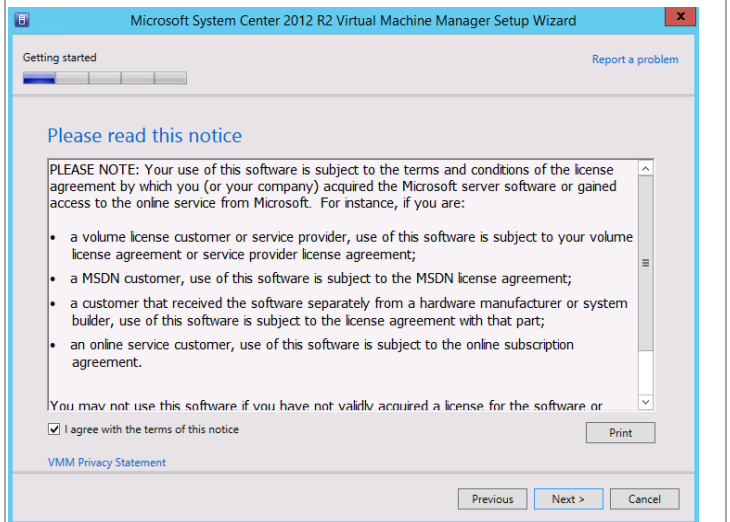
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



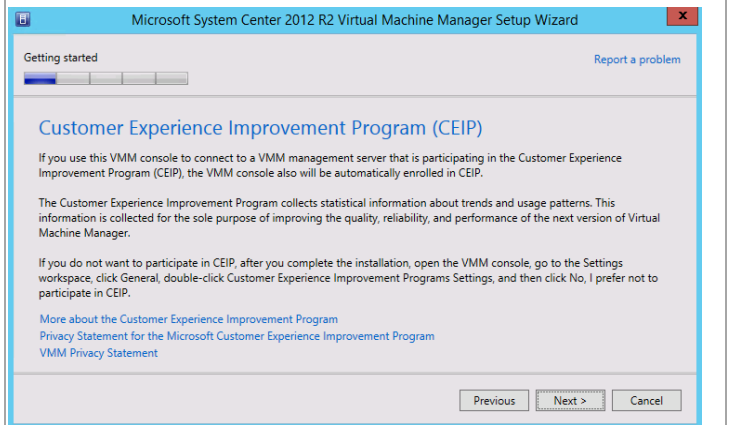
In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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

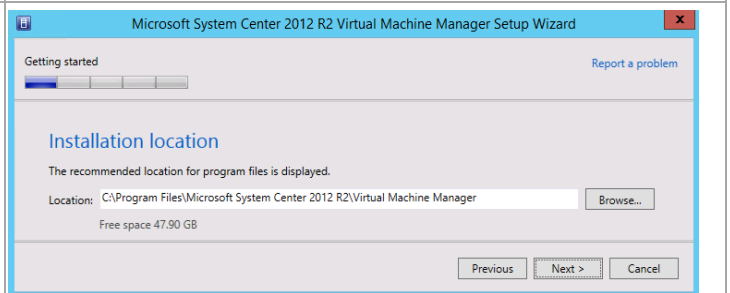


In the **Customer Experience Improvement Program** dialog, click **Next** to continue.

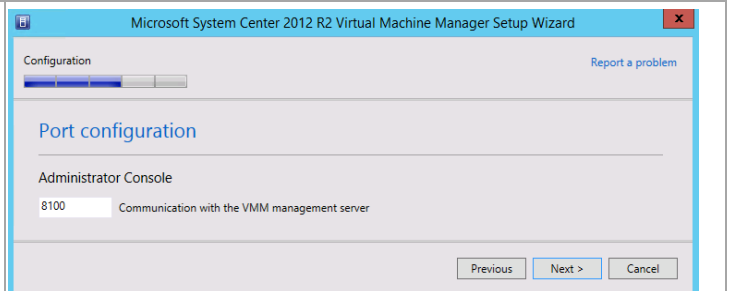


Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.

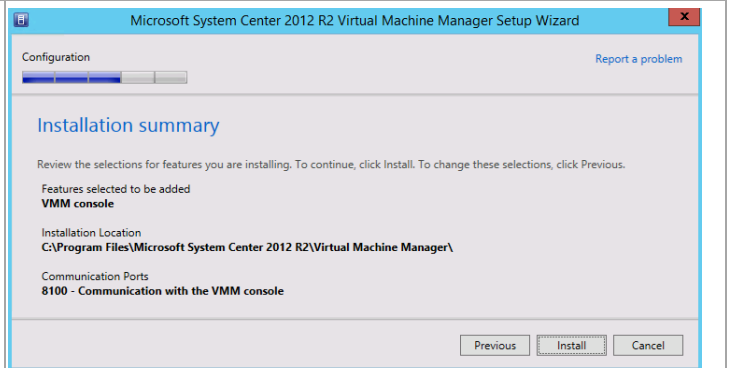
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.



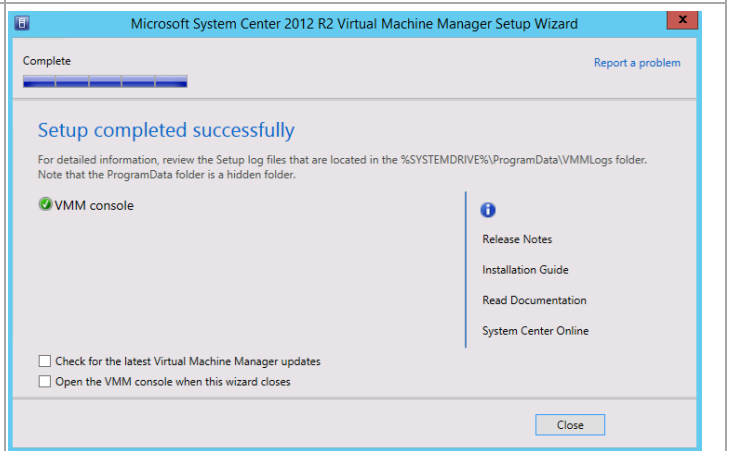
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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



## 23.3 Installation

### Install the App Controller Portal Server

The following steps need to be completed in order to install App Controller.

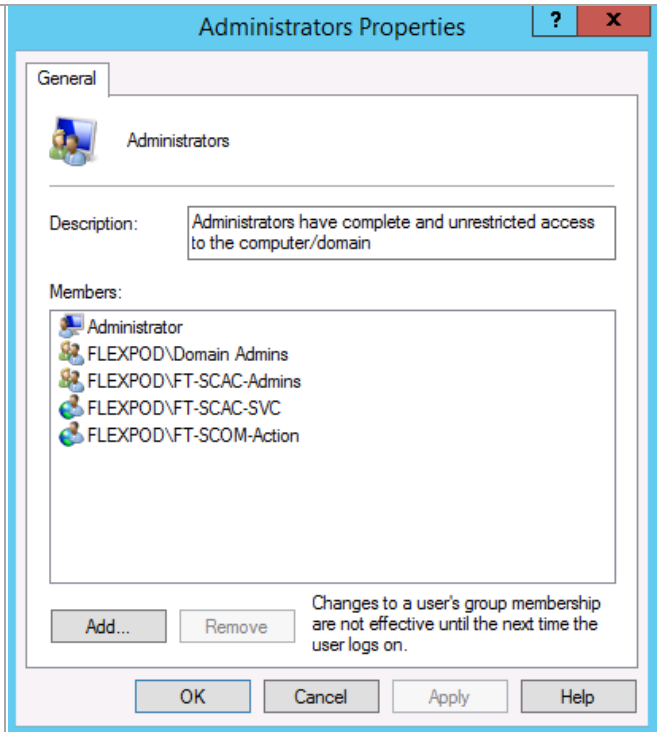


Perform the following steps on the **App Controller** virtual machine.

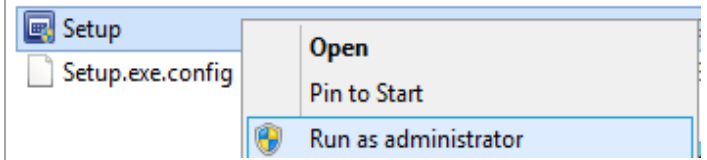
Log on to the App Controller virtual machine with a user with local admin rights.

Verify the following accounts and/or groups are members of the Local Administrators group on the App Controller portal virtual machine:

- Fast Track Operations Manager action account.
- Fast Track App Controller service account.
- Fast Track App Controller Admins group.



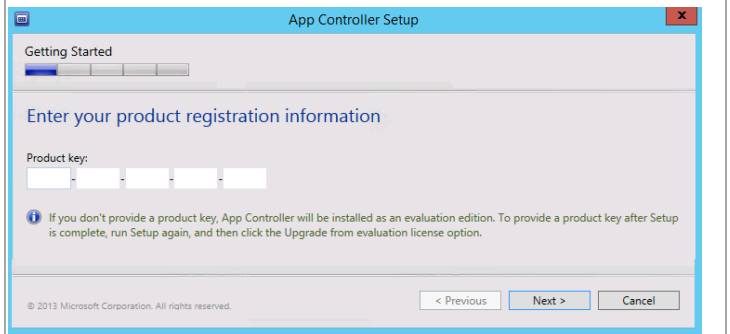
Log on to System Center App controller server. From the **System Center App Controller** installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



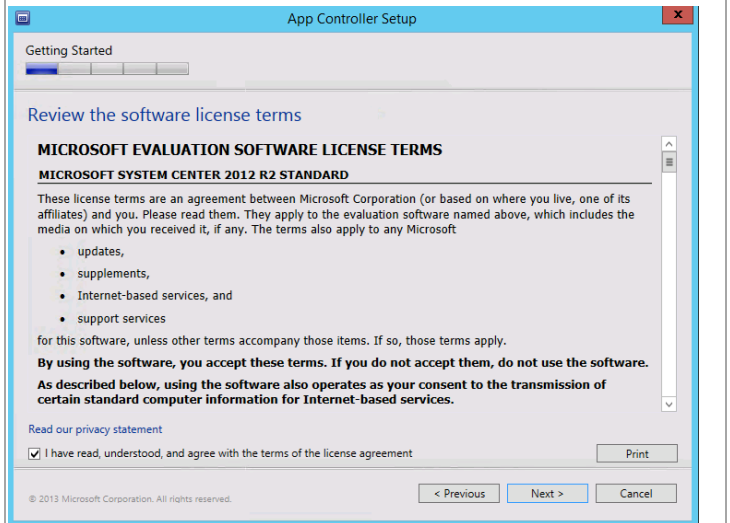
The **App Controller Setup** wizard will begin. At the splash page, click **Install** begin the App Controller server installation.



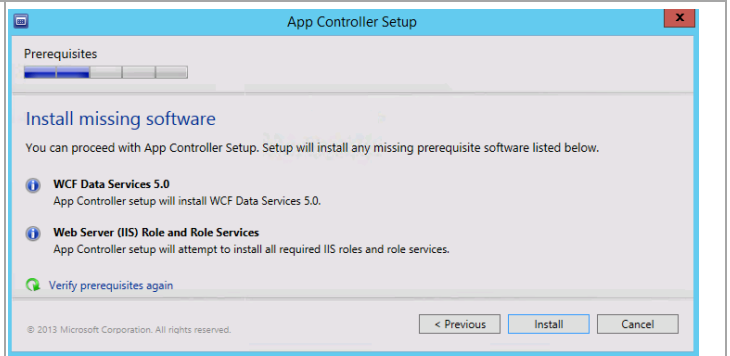
In the **Enter your product registration information** dialog, provide a valid product key for installation of Orchestrator. If no key is provided, App Controller will be installed in evaluation mode. Click **Next** to continue.



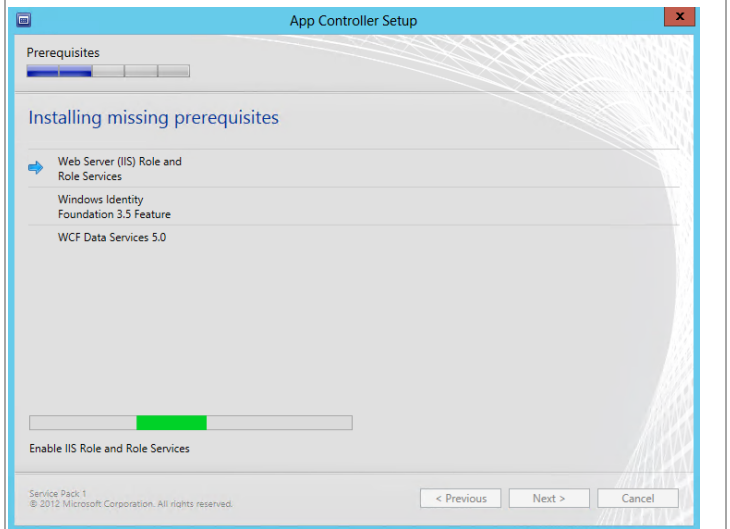
In the **Review the software license terms** dialog, verify that the **I have read, understood and agree with the terms of this license agreement** installation option check box is selected and click **Next** to continue.



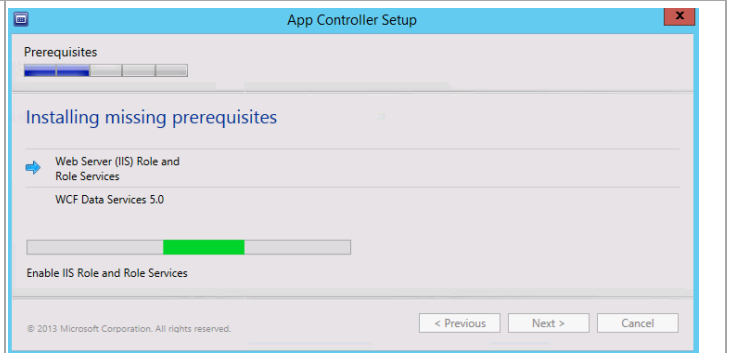
In the **Install missing software** dialog, the wizard will detect missing roles and software and attempt installation of missing prerequisites. Click **Install** to enable missing roles and features.



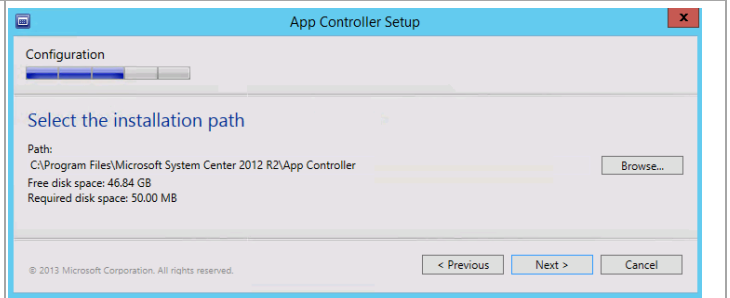
The wizard will detect missing roles and software and attempt installation of missing prerequisites. Please be patient during this process.



Any detected missing prerequisite software will be installed.



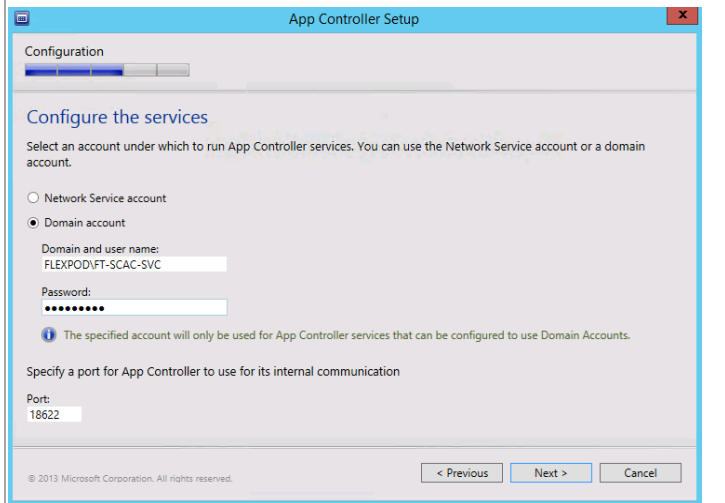
In the **Select the installation path** dialog, accept the default installation location of *%ProgramFiles%\Microsoft System Center 2012 R2\App Controller* or specify a different location by hitting the **Browse** button. After making a selection hit **Next** to continue.



In the **Configure the services** dialog, verify that the **Domain account** option is selected and specify the App Controller service account in the **Domain and user name** text box. Provide the associated **Password** in the supplied text box.

In the **Port** text box, accept the default TCP port of 18622 or change the port to meet your organization's requirements. In most cases the default port selection should be kept.

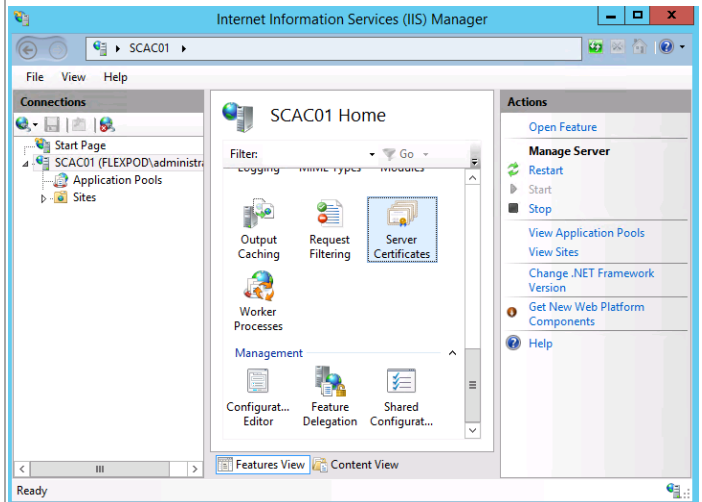
When complete, click **Next** to continue.



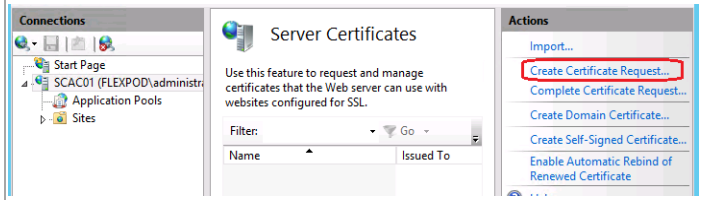
Before proceeding with the App Controller installation, install a certificate on this system. Launch the Internet Information Services (IIS) Manager.



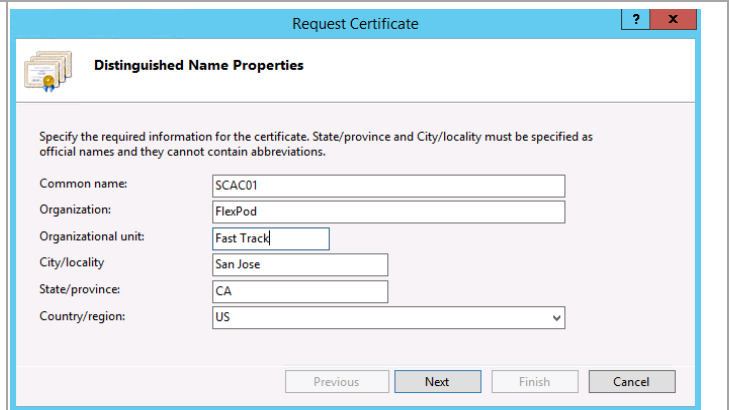
Click the Application Controller home page in the Connections pane. From the IIS section in the middle, double-click **Server Certificates**.



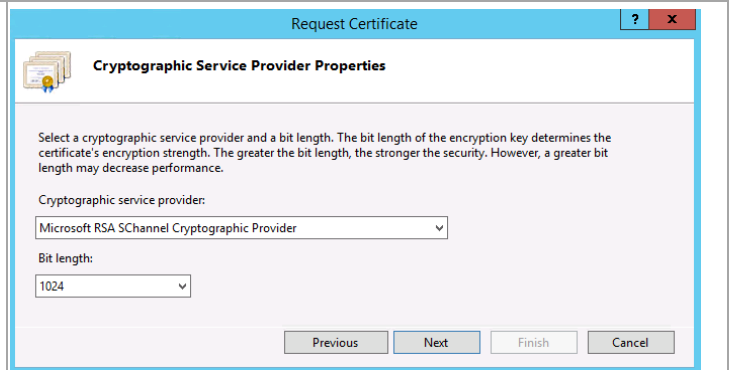
From the **Actions** pane click on **Create Certificate Request...**



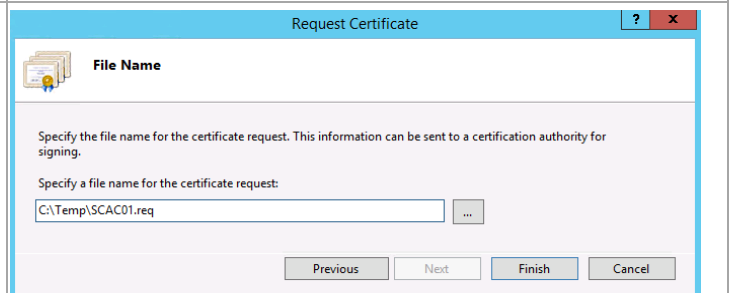
The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name of the server will be accessed in the web browser. Click **Next** to continue.



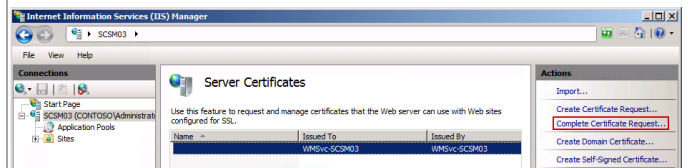
Accept the default properties unless you have implemented different certificate requirements in your environment. Click **Next** to continue.



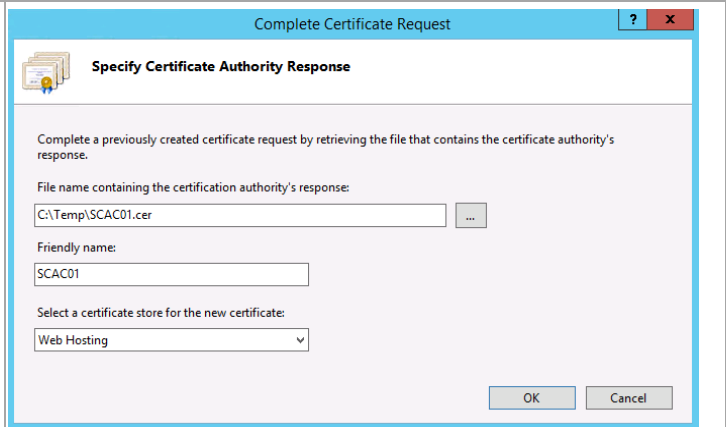
Provide a location to store the certificate request. Click **Finish** to create the request.



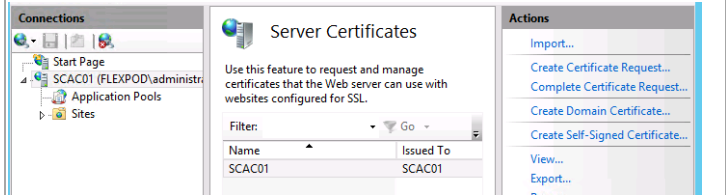
After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** once again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. From the certificate store dropdown select the **Personal**. Click **OK** to complete the operation.



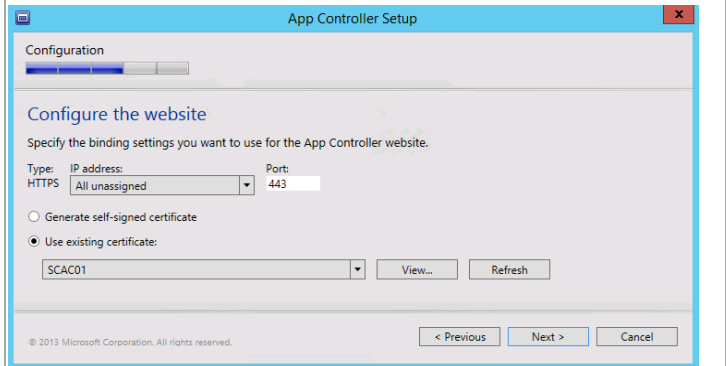
In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.



Return to the App Controller installation.

In the **Configure the website** dialog, provide the following information:

- Click the **Refresh** button to read the updated certificate store
- Under Website, in **Type: HTTPS**, set the **IP address** drop-down menu to **All unassigned**. Set the **Port** value to **443**
- Verify that the **Use existing certificate** option is selected and select the proper Server Authentication certificate that installed within the virtual machine from the drop-down menu



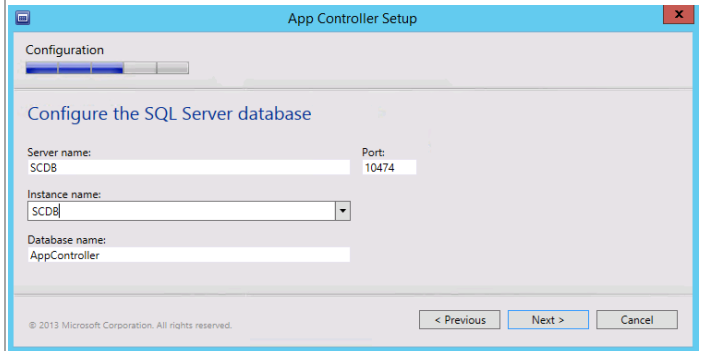
When complete, click **Next** to continue.

**Note:** While not recommended, if a Server Authentication certificate cannot be obtained and installed on the App Controller server, you may choose the **Generate self-signed certificate** option to satisfy installation requirements.

In the **Configure the SQL Server database** dialog, make the following selections install the App Controller database in the SCO instance (refer to the worksheet created earlier):

- **Server Name** – specify the cluster network name of the SQL Server failover cluster hosting the instance.
- **Port** – specify the TCP port used for SQL Server connectivity.
- **Instance name** - specify the instance name where the AppController database will be installed to (the SCDB instance).
- **Database name** – specify the name of the App Controller database. In most cases the default value of AppController should be used.

Click **Next** to continue.



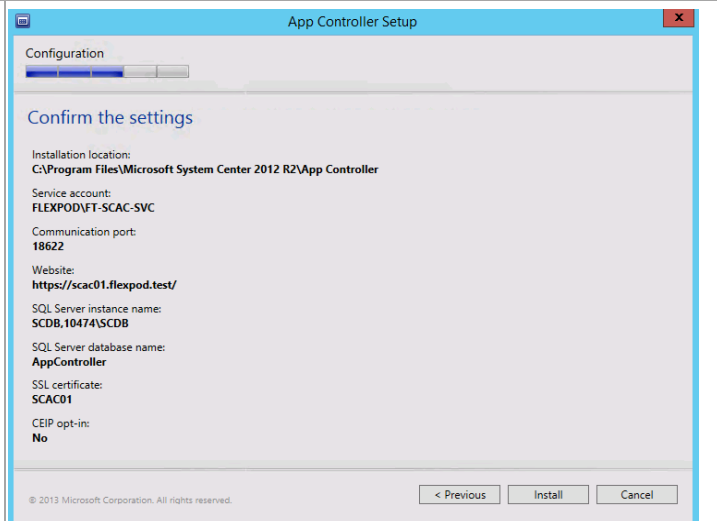
The **Help Improve App Controller for System Center 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Microsoft Update**

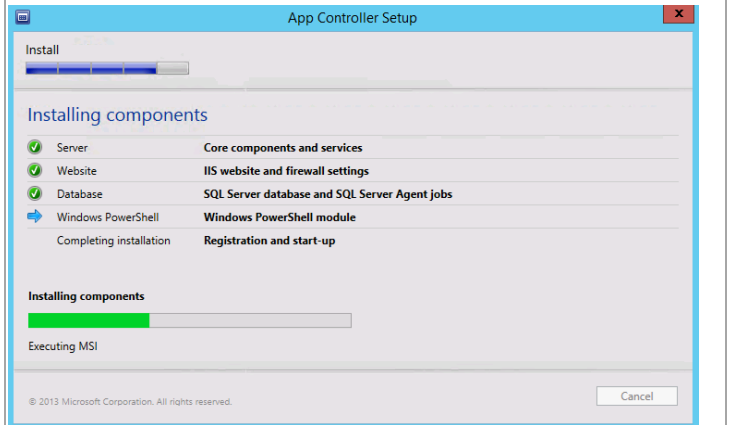
Select the appropriate option based on your organization's policies and click **Install** to continue.



In the **Confirm the settings** dialog, verify the settings provided during the installation wizard and click **Install** to begin the installation.

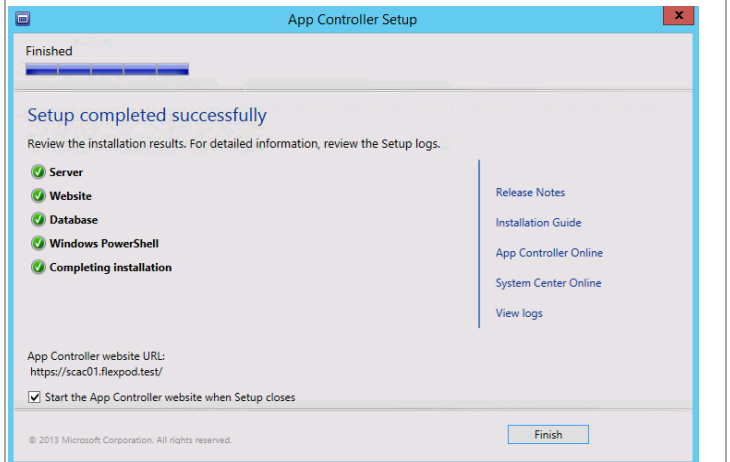


The required components will install and progress of the installation will be provided in the wizard.

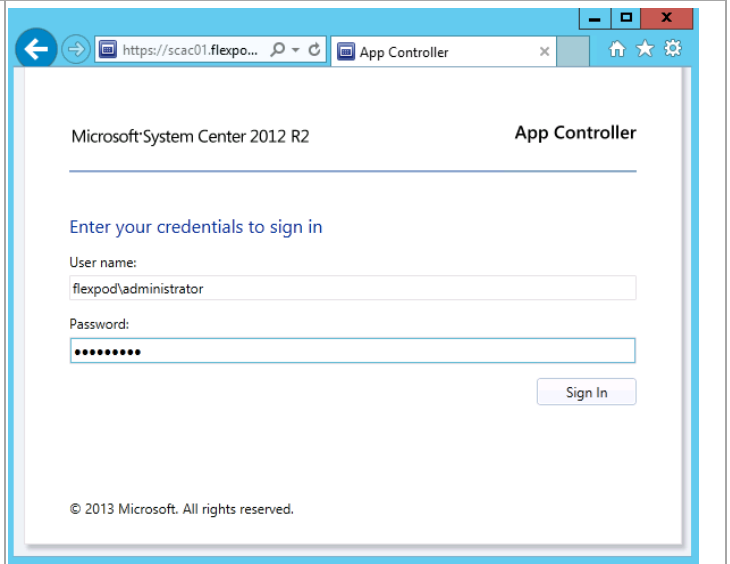


When complete, the **Setup completed successfully** dialog will appear with progress of each component. Verify that each component successfully. Note the App Controller website in the provided text box.

Verify that the **Start the App Controller website when Setup closes** check box is selected and click **Finish**.

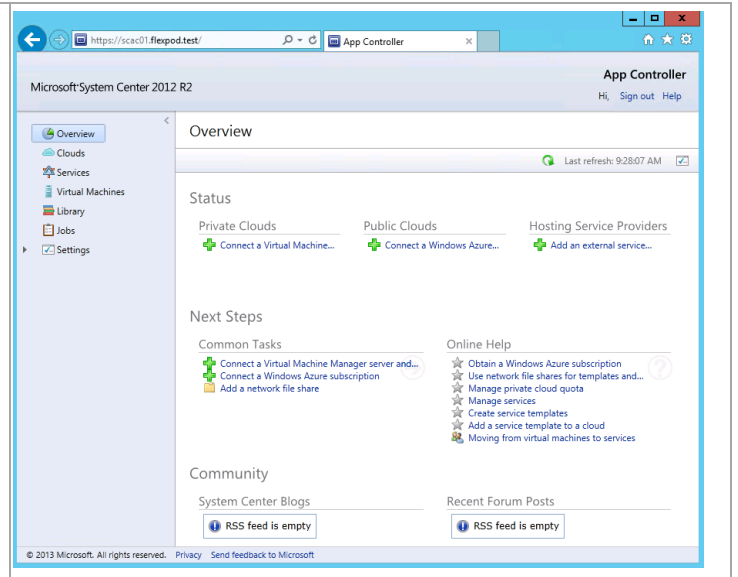


The **System Center 2012 App Controller website** will launch. Because no users have been created in SCVMM, enter in the administrative account used to install Virtual Machine Manager (which has been assigned an admin role in SCVMM). When complete, click **Sign in**.





The App Controller portal will appear. After validating functionality, the App Controller installation is considered complete.



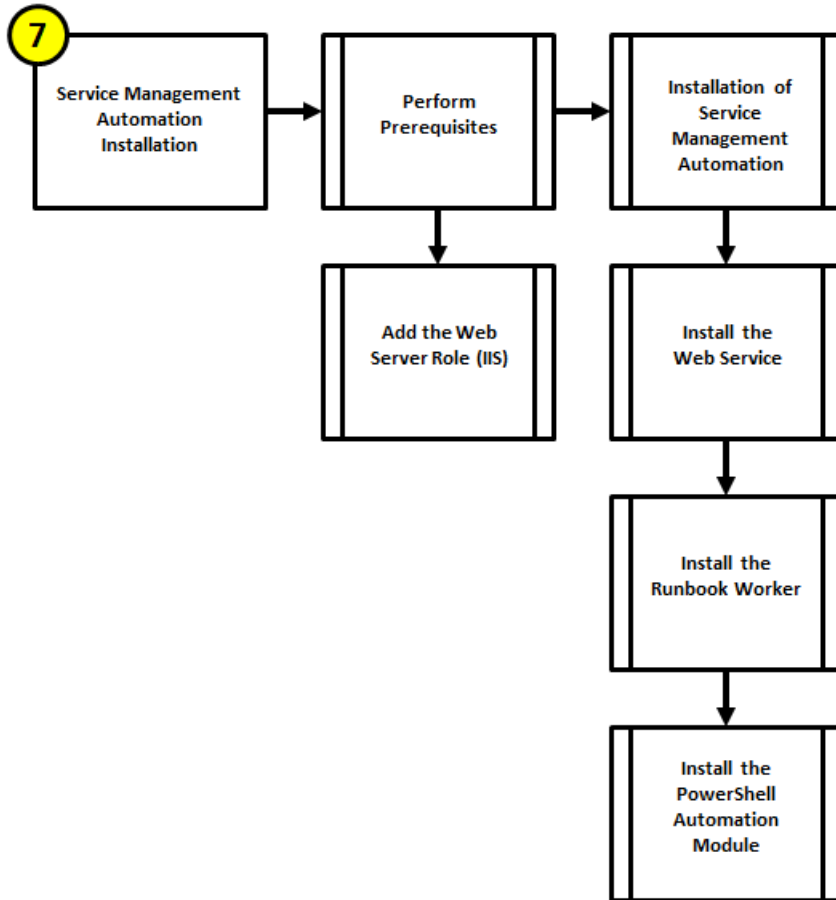
## 24 Service Management Automation

Service Management Automation is included in the System Center 2012 R2 release as an add-on component of Windows Azure Pack allowing for the automation of various tasks, similar to those performed using Orchestrator runbooks.

Service Management Automation also incorporates the concept of a runbook for developing automated management sequences, but rather than use activities to piece together the tasks, Service Management Automation relies on PowerShell workflows. PowerShell workflows are based on Windows Workflow Foundation and allow for asynchronous task management of multiple devices in IT environments.

Service Management Automation is made up of three roles: the runbook worker(s), web service(s), and the Service Management Automation PowerShell module. The Web Service provides an endpoint to which Windows Azure Pack connects. It is also responsible for assigning runbook jobs to runbook workers and delegating access user rights to Service Management Automation. Runbook workers actually initiate runbook jobs and can be deployed in a distributed fashion for redundancy purposes. A Service Management Automation PowerShell module is also included which provides a set of additional cmdlets.

The Service Management Automation installation process includes the high-level steps shown in the following figure:



## 24.1 Overview

Service Management Automation is a set of tools that is integrated as the Automation extension in Windows Azure Pack for Windows Server. IT pros and IT developers can use Automation to construct, run, and manage runbooks to integrate, orchestrate, and automate IT business processes. Automation runbooks run on the Windows PowerShell workflow engine.

## 24.2 Prerequisites

The following environment prerequisites must be met before proceeding.

### Accounts

Verify the following service accounts have been created:

**Table 18 Service Management Automation Accounts**

User name	Purpose	Permissions
<DOMAIN>\ FT-SCSMA-SVC	Service Manager Automation service account	

## Groups

Verify the following security groups have been created:

**Table 19 Service Manager Automation Security Groups**

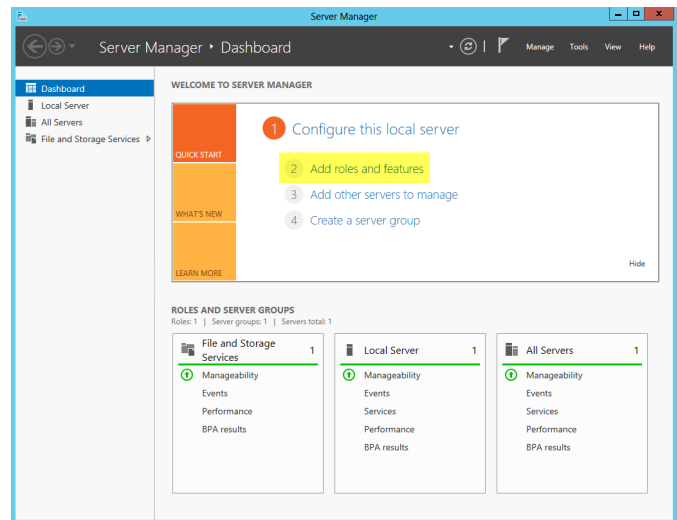
Group name	Purpose	Members
<DOMAIN>\ FT-SCSMA-Admins	Service Manager Automation Admin group	

## Add Web Server Role (IIS)

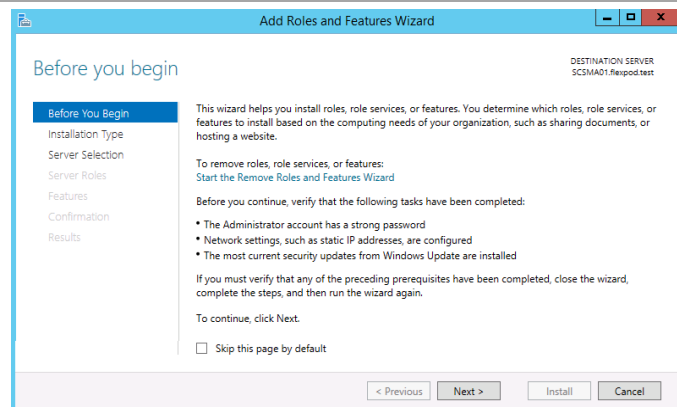
The Service Management Automation installation requires the Web Server Role and several additional role features. Use the following procedure to add this role and features to the server.

**Perform the following steps on each Service Management Automation server virtual machine.**

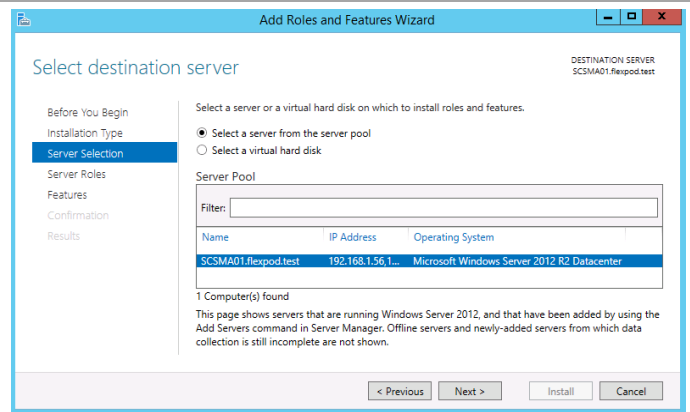
Open **Server Manager** and navigate to the Dashboard node. In the main pane, under **Configure this local server**, select **Add roles and features**.



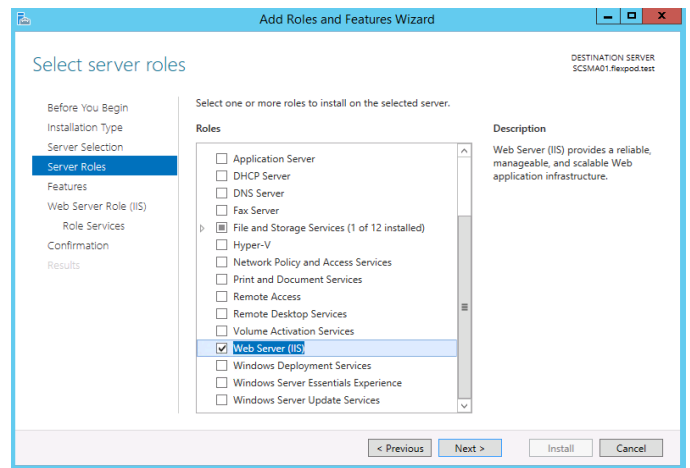
The **Add Roles and Features Wizard** appears. On the **Before You Begin** page, click **Server Selection** in the left pane. (Do not click **Next**.)



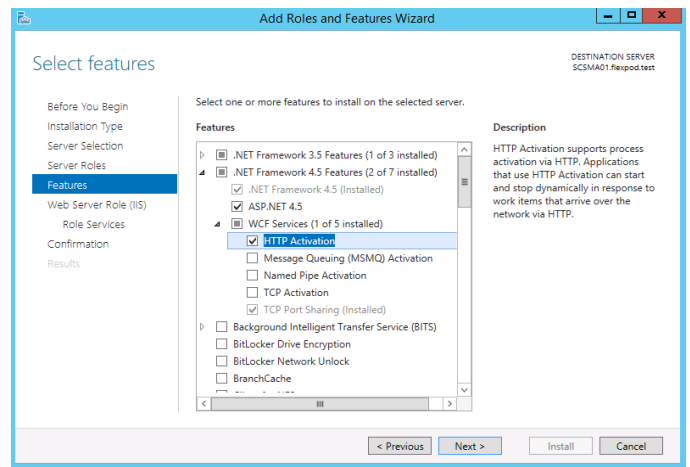
On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server and then click **Features** in the left pane. (Do not click **Next**.)



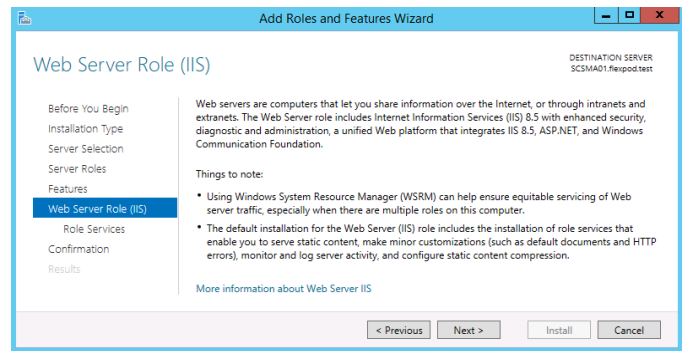
On the **Select Server roles** page, select the **Web Server (IIS)** role. A window will display asking to add features that are required for this role. Click **Add Features**. Click **Next** to continue.



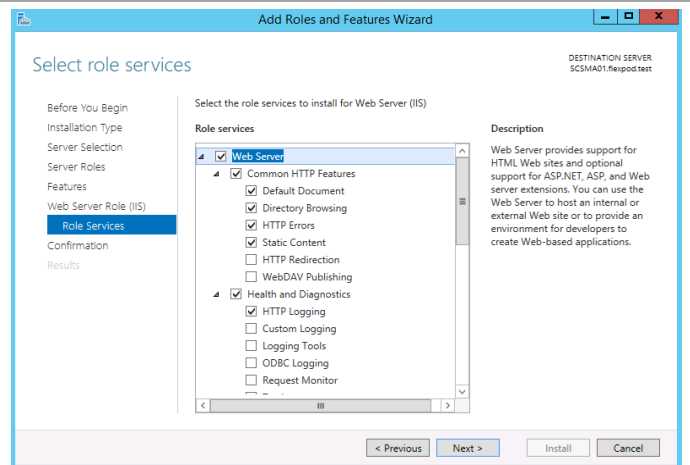
In the **Select features** section, expand **.NET Framework 4.5 Features** item and then expand the **WCF Services** item. Select **HTTP Activation**. A window will display asking to add features that are required for this feature. Click **Add Features**. Click **Next** to continue.



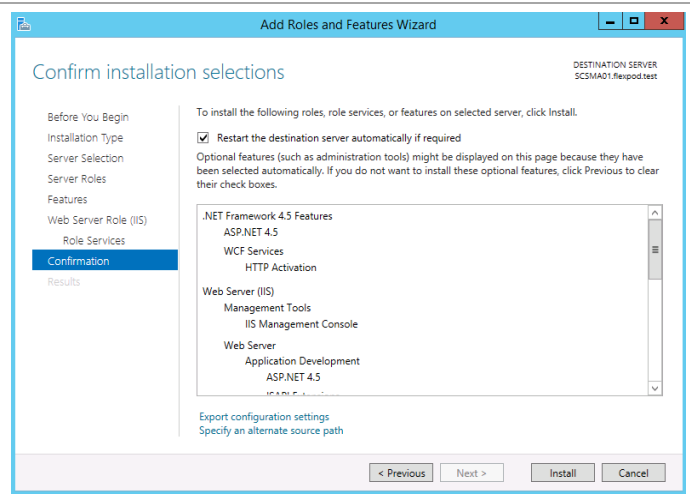
On the **Web Server Role (IIS)** page click **Next** to continue.



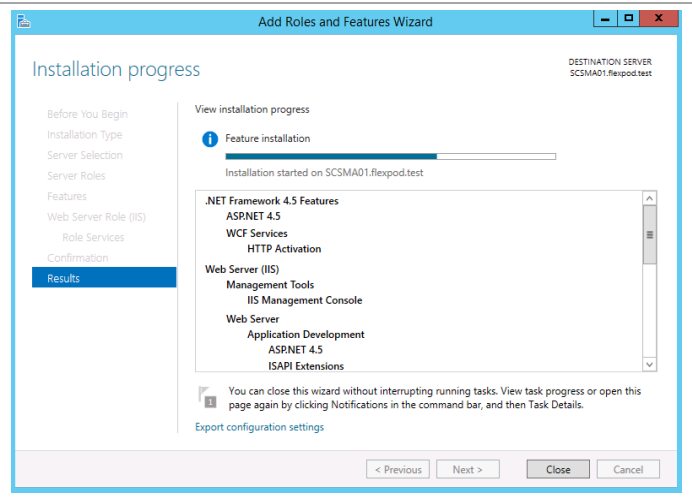
On the **Select role services** page, expand **Security** and select the **Request Filtering**, **Basic Authentication**, **URL Authorization**, and **Windows Authentication** checkboxes and then click **Next**.



On the **Confirm installation selections** page, verify that the previously selected roles and features are listed. Ensure that the **Restart each destination server automatically if required** is selected. A window will display asking if you want the automatic restart. Click **Yes**. Click **Install** to begin installation.



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



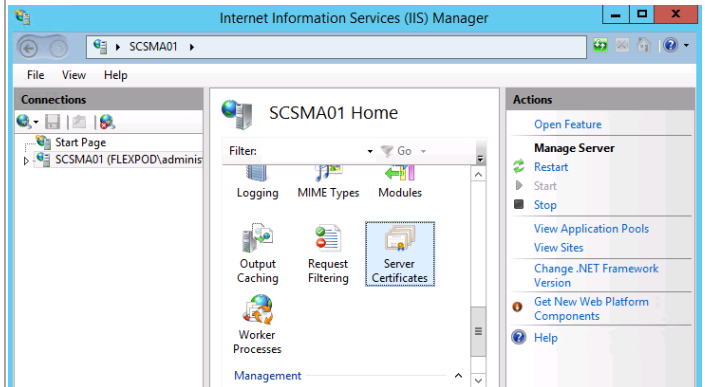
## Request and Install SSL Certificate

Perform the following steps on each Service Management Automation server virtual machine.

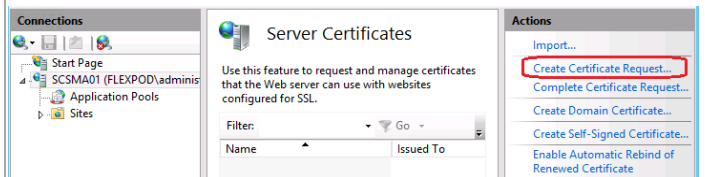
Launch the Internet Information Services (IIS) Manager.



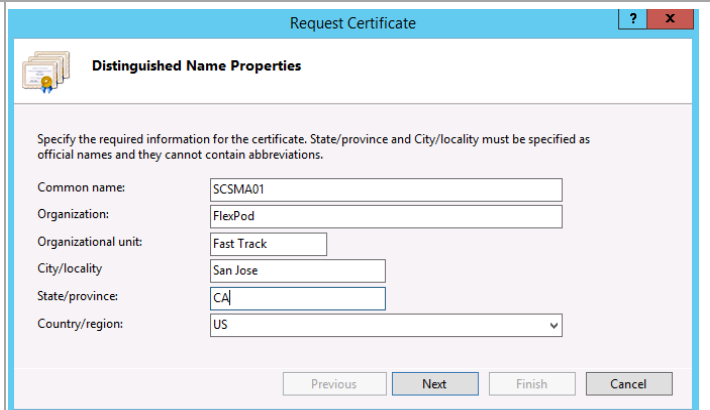
Click the Application Controller home page in the Connections pane. From the IIS section in the middle, double-click **Server Certificates**.



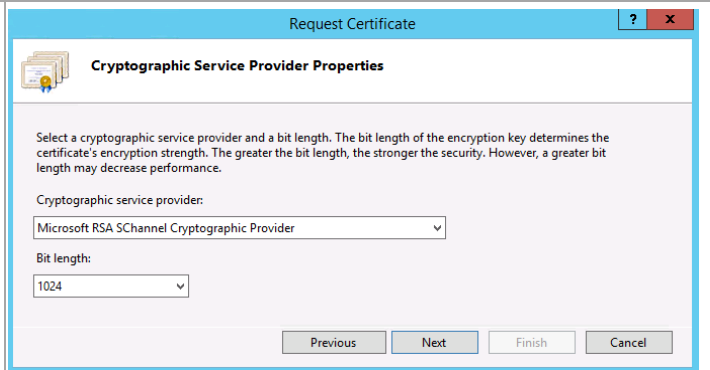
From the **Actions** pane click on **Create Certificate Request...**



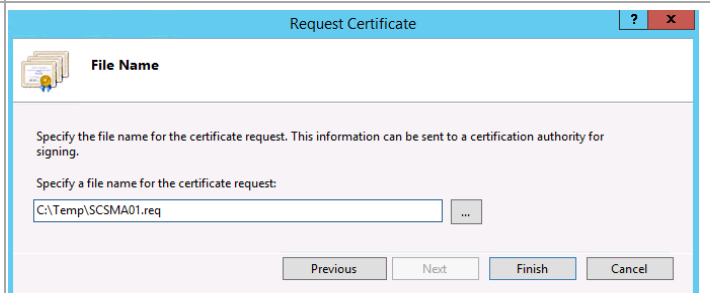
The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name of the server will be accessed in the web browser. Click **Next** to continue.



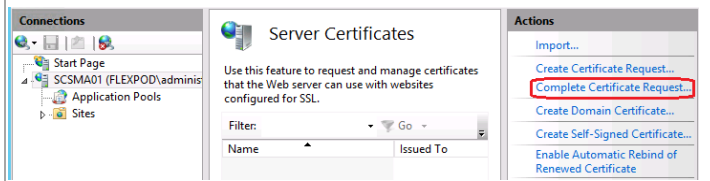
Accept the default properties unless you have implemented different certificate requirements in your environment. Click **Next** to continue.



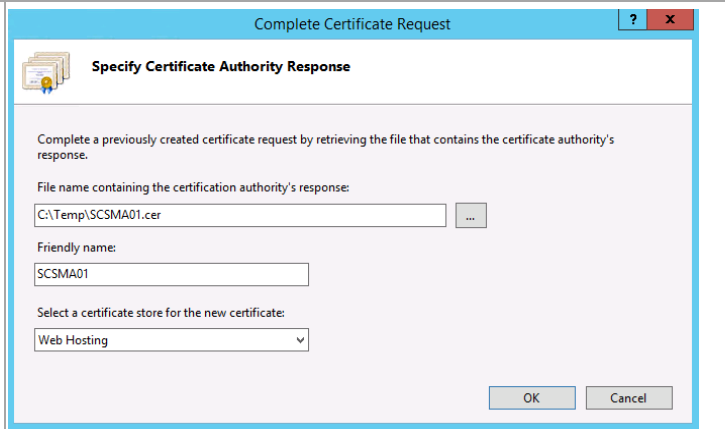
Provide a location to store the certificate request. Click **Finish** to create the request.



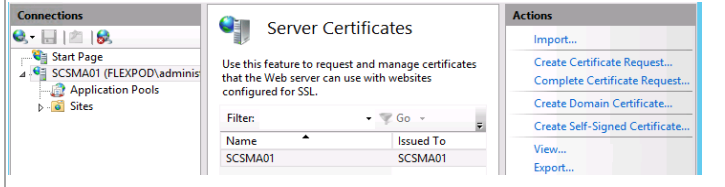
After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** once again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. From the certificate store dropdown select the **Personal**. Click **OK** to complete the operation.



In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.



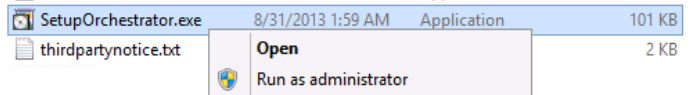
## 24.3 Installation

### Install the Web Service

Complete the following steps to install the Web Service.

**Perform the following steps on each Service Management Automation server virtual machine.**

From the **System Center Orchestrator** installation media source, right-click **setupOrchestrator.exe** and select **Run as administrator** to begin setup.

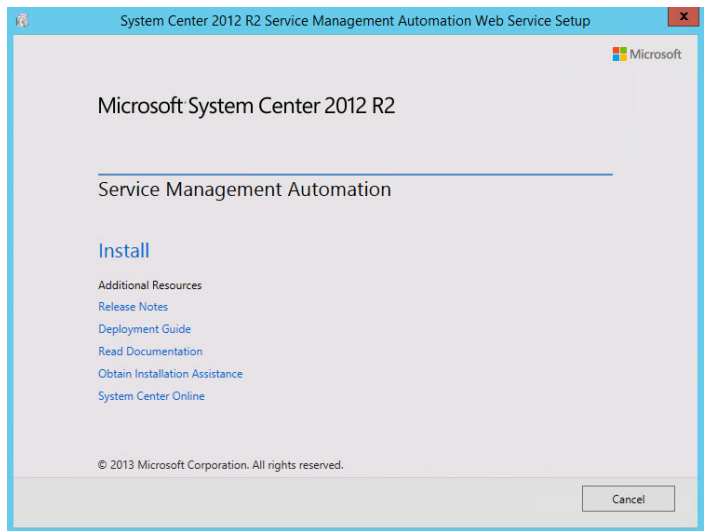


The Orchestrator Setup Wizard will appear. Under Automation click **Web Service** to begin the SMA Web Service installation Wizard.





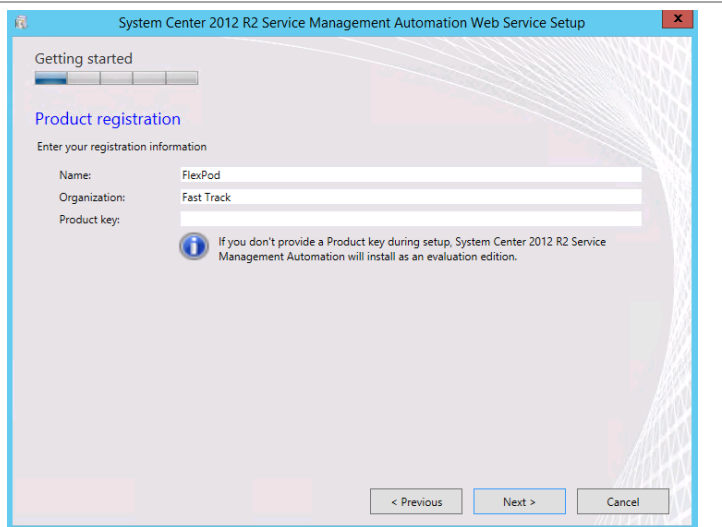
The Service Management Automation Wizard will appear. Click **Install** to begin the SMA Web Service installation.



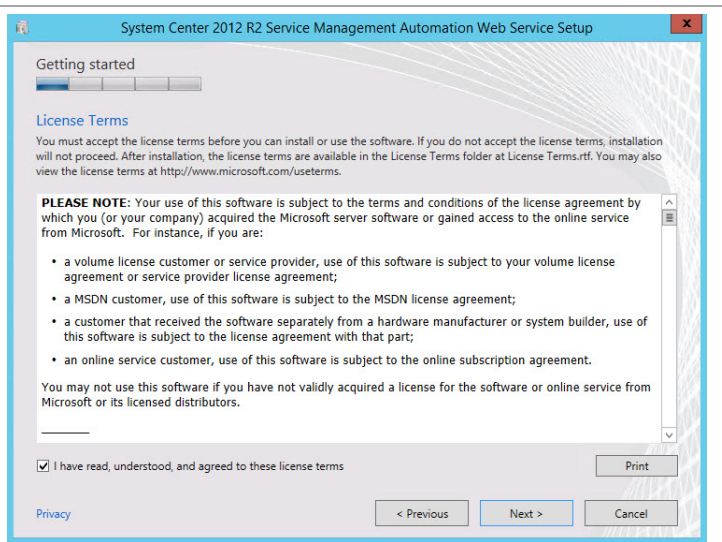
On the **Product registration information** page, type the following information in the provided text boxes:

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

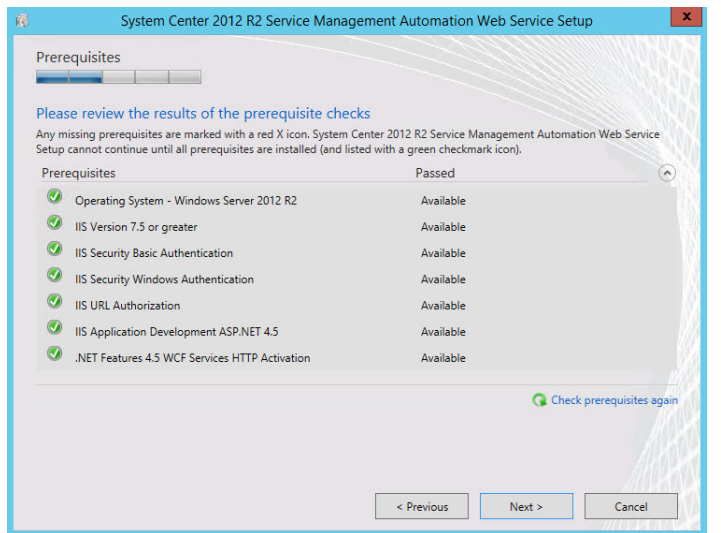
Click **Next** to continue.



On the **License Terms** page, 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.



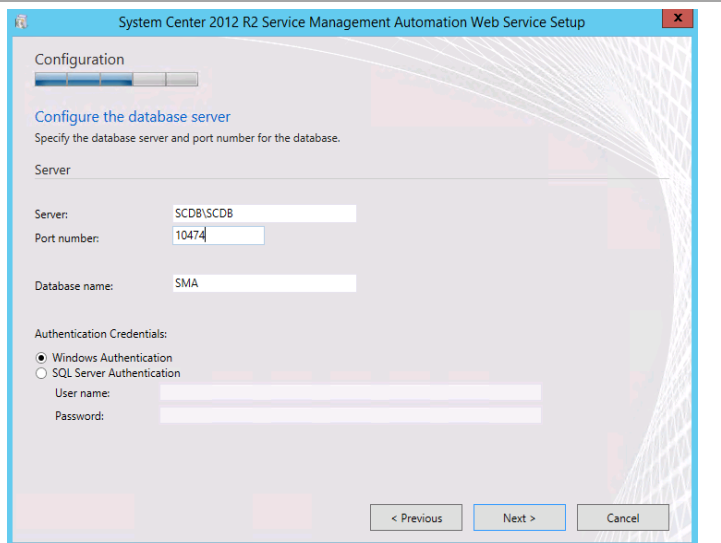
On the **Prerequisites** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Configure the database server** page, specify the following information in the provided text boxes:

- **Server** – Specify the name of the database instance created for the shared System Center SQL instance.
- **Port Number** – Specify number of the SCDB port recorded earlier in the installation (found in the section on building the SQL Server cluster in the previous CVD)
- **Database name** – Specify the name of the database. In most cases, use the default value.

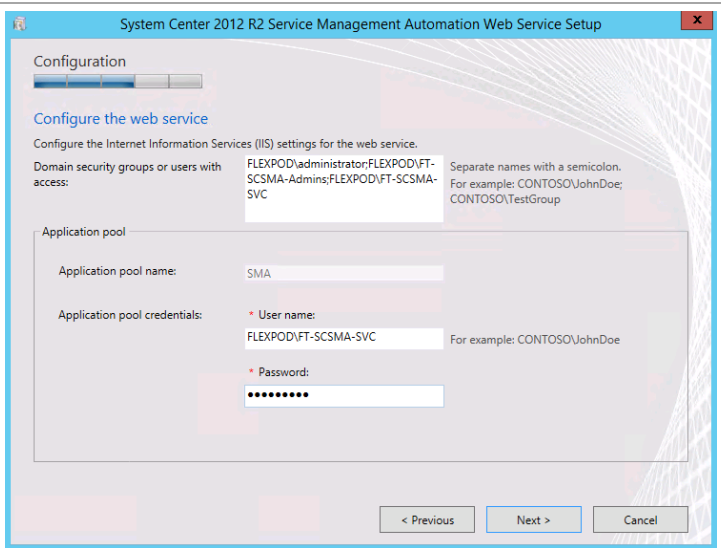
Under Authentication Credentials select **Windows Authentication**. Click **Next** to continue.



On the **Configure the web service** page, specify the following accounts in the Domain Security groups or users with access box:

- SMA Admins Group
- SMA Service Account

In the **Application pool credentials** section, specify the SMA Service Account and password. Click **Next** to continue.

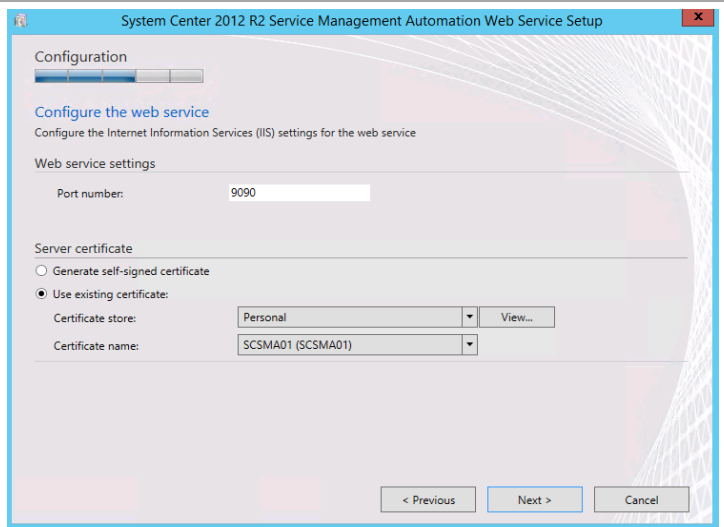


On the **Configure the web service** page, specify the following information in the provided text boxes:

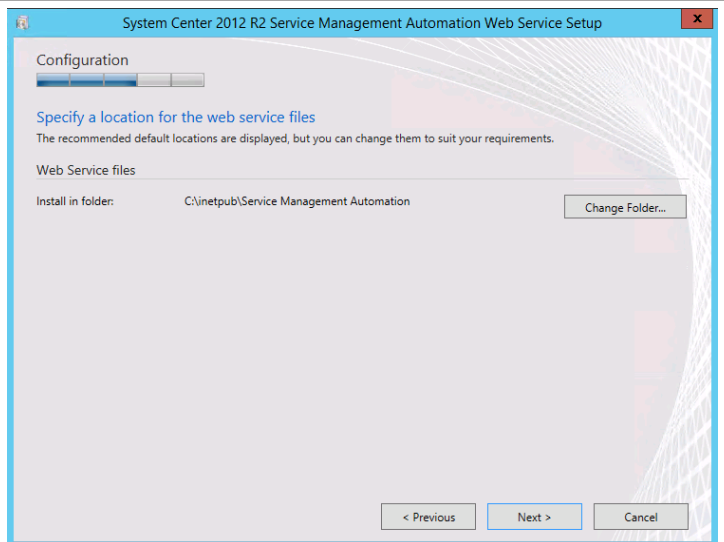
- **Port Number** – Accept the default of 9090.

Under Server Certificate select **Use existing certificate** and select the previously installed certificate. Click **Next** to continue.

**Note:** While a self-signed certificate can be used, it is recommended in production scenarios to use a valid certificate issued from a trusted certification authority.



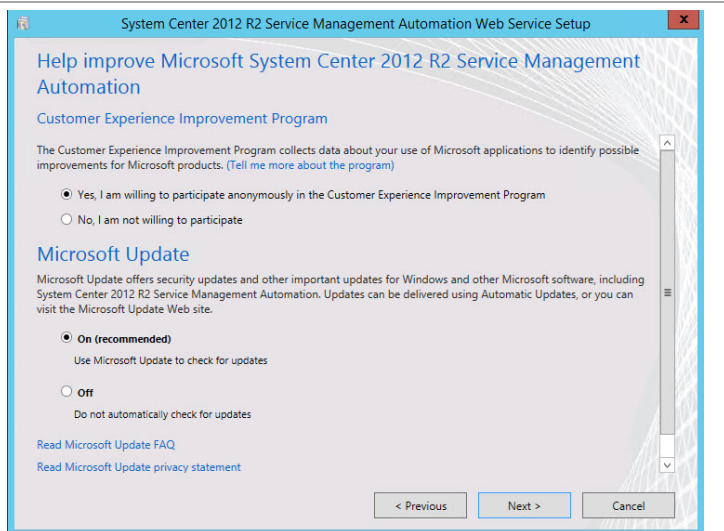
On the **Specify a location for the web service files** page, accept the default path, click **Next** to continue.



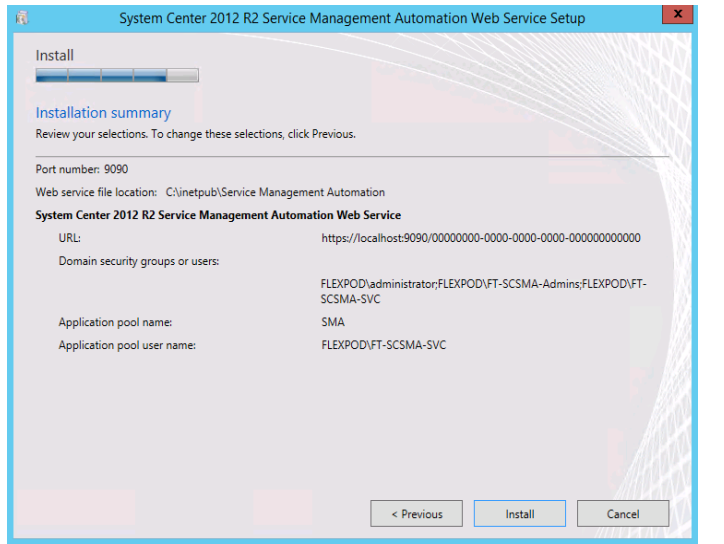
On the **Help improve Microsoft System Center 2012 R2 Service Management Automation** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft.

Under the **Microsoft Update** portion of the page. Select the appropriate option to participate or not participate in automatic updating.

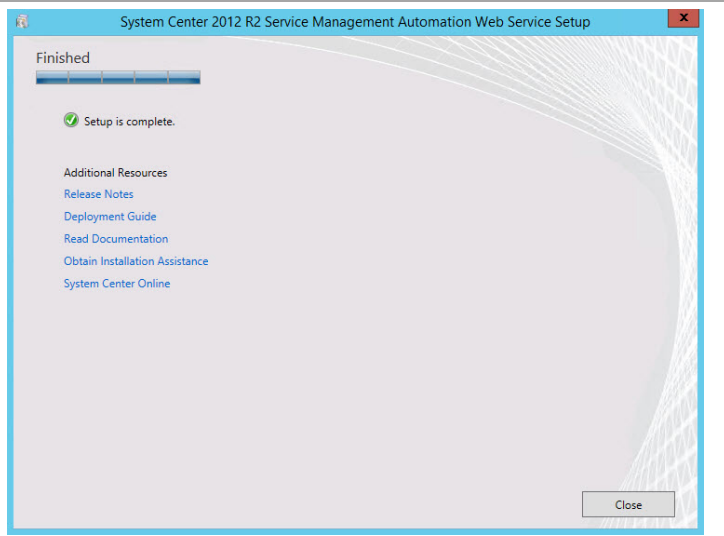
Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.



When the installation completes, the wizard will display the **Finished** page. Click **Close** to complete the installation.

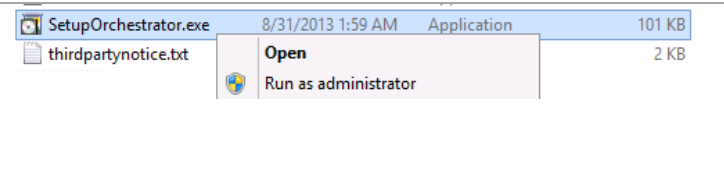


## Install the Runbook Worker

Complete the following steps to install the Runbook Worker.

**Perform the following steps on each Service Management Automation server virtual machine.**

From the **System Center Orchestrator** installation media source, right-click **setupOrchestrator.exe** and select **Run as administrator** to begin setup.



The Orchestrator Setup Wizard will appear. Under Automation click **Runbook Worker** to begin the SMA Runbook Worker installation Wizard.



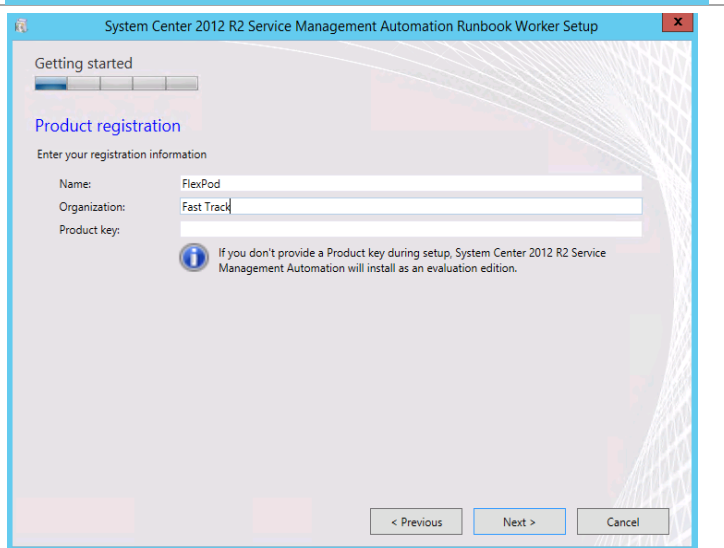
The Service Management Automation Wizard will appear. Click **Install** to begin the SMA Runbook Worker installation.



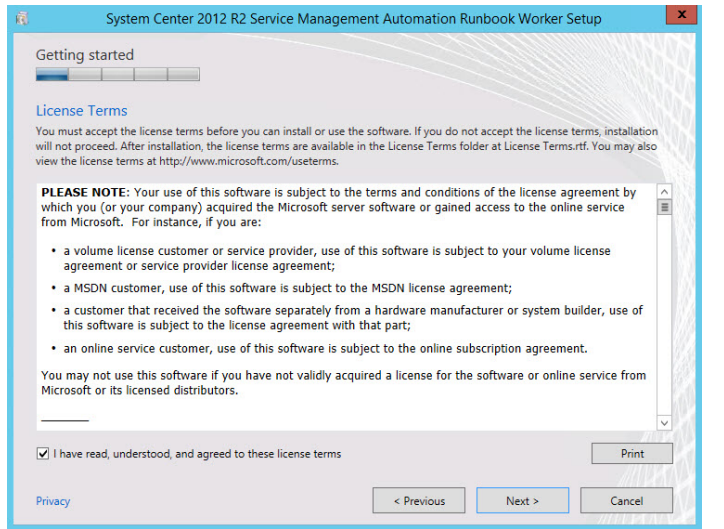
The On the **Product registration information** page, type the following information in the provided text boxes:

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

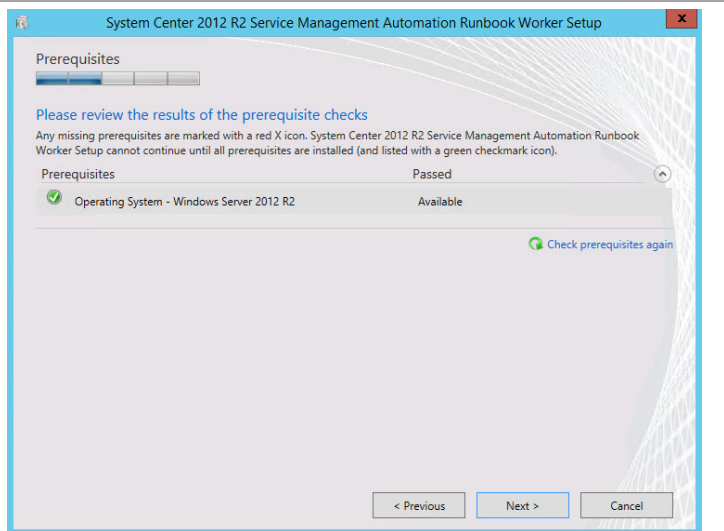
Click **Next** to continue.



On the **License Terms** page, 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.



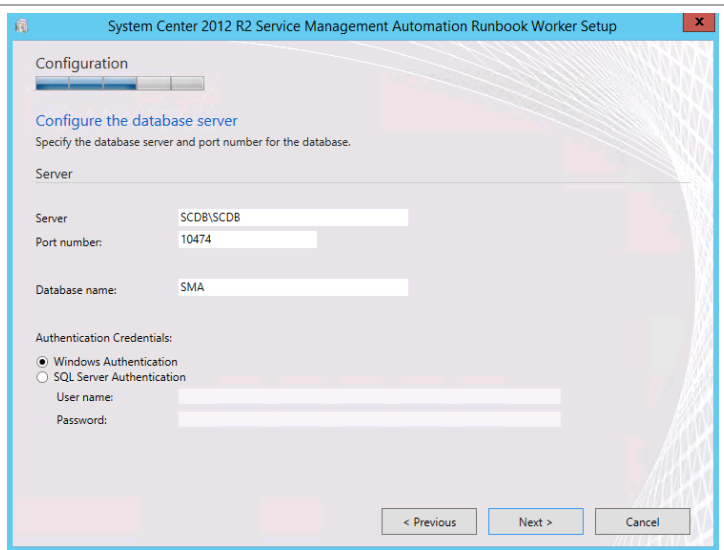
On the **Prerequisites** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Configure the database server** page, specify the following information in the provided text boxes:

- **Server** – Specify the name of the Service Reporting Server.
- **Port Number** – Specify number of the SCDB port recorded earlier in the installation
- **Database name** – Specify the name of the database. In most cases, use the default value.
- Under Authentication Credentials select **Windows Authentication**.

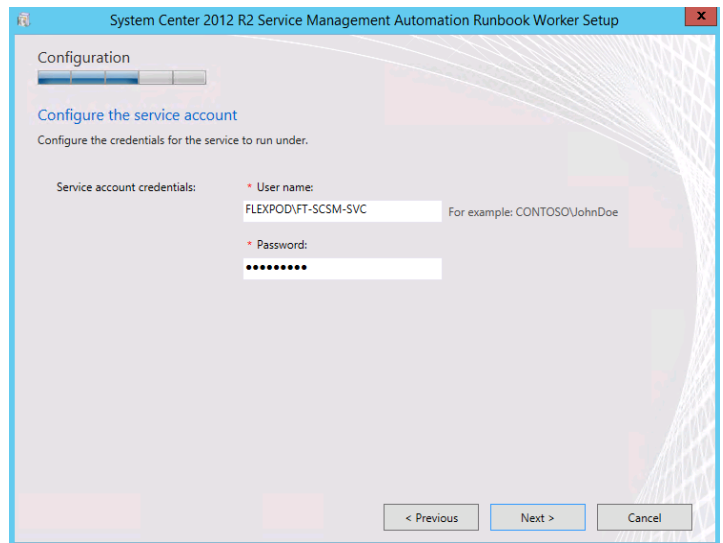
Click **Next** to continue.



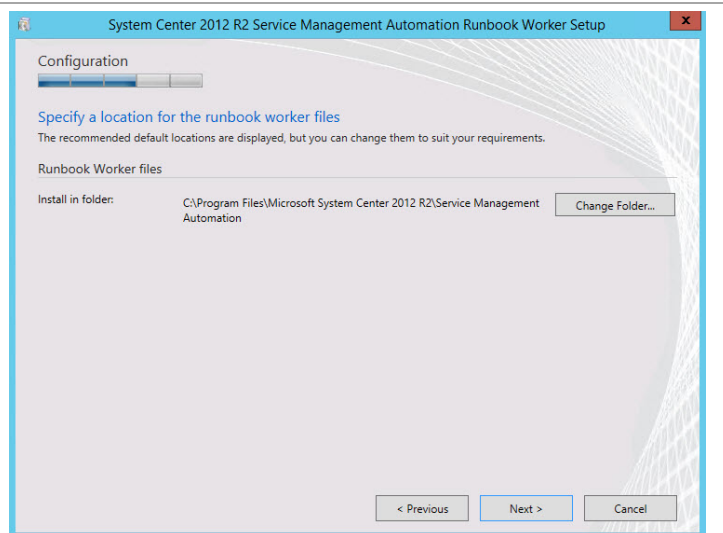
On the **Configure the service account** page, specify the following information in the provided text boxes:

- **Service account credentials** – Specify the SMA Service account.

Click **Next** to continue.



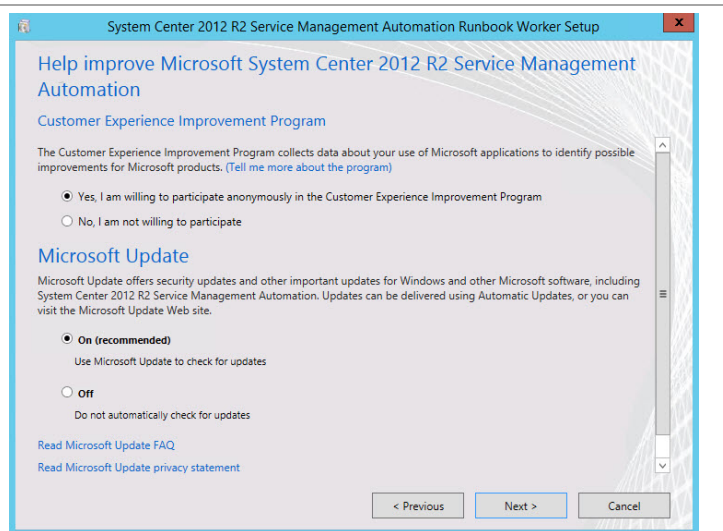
On the **Specify a location for the runbook worker files** page, accept the default path, click **Next** to continue.



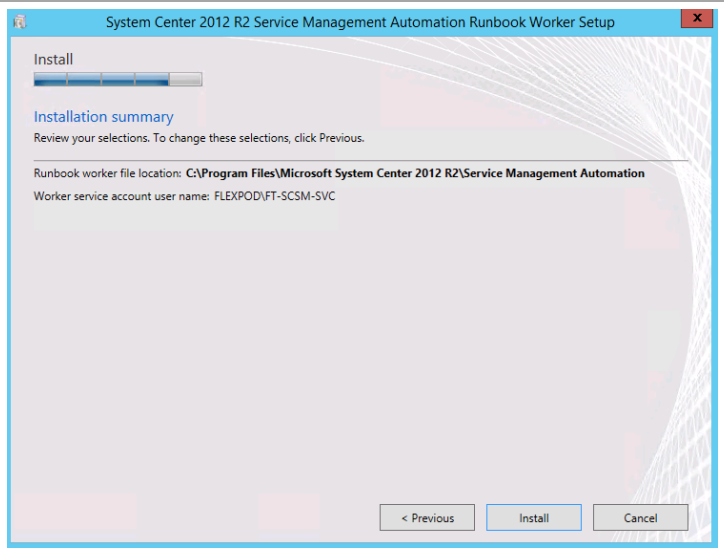
On the **Help improve Microsoft System Center 2012 R2 Service Management Automation** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft.

Under the **Microsoft Update** portion of the page. Select the appropriate option to participate or not participate in automatic updating.

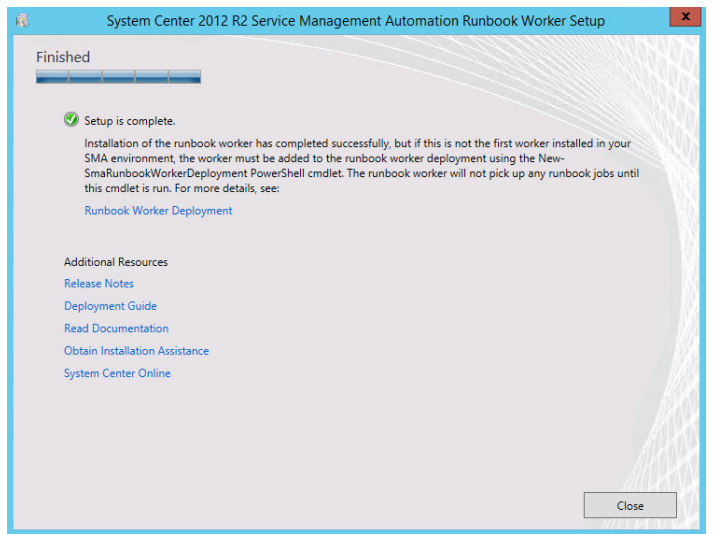
Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.



When the installation completes, the wizard will display the **Finished** page. Click **Close** to complete the installation.

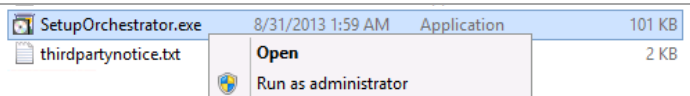


## Install the PowerShell Automation Module

Complete the following steps to install the PowerShell Automation Service.

**Perform the following steps on each Service Management Automation server virtual machine.**

From the **System Center Orchestrator** installation media source, right-click **setupOrchestrator.exe** and select **Run as administrator** to begin setup.

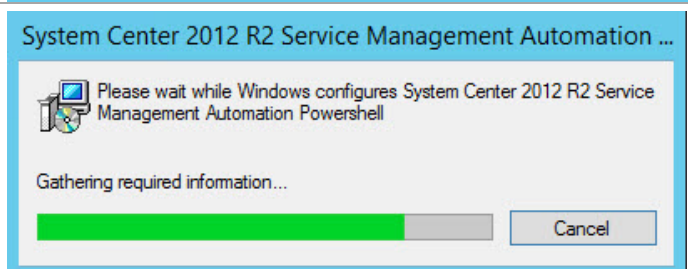




The Orchestrator Setup Wizard will appear. Under Automation click **PowerShell Module** to begin the SMA PowerShell Module installation.



The Install will run silently to install the PowerShell Module. This takes only a few moments to run.



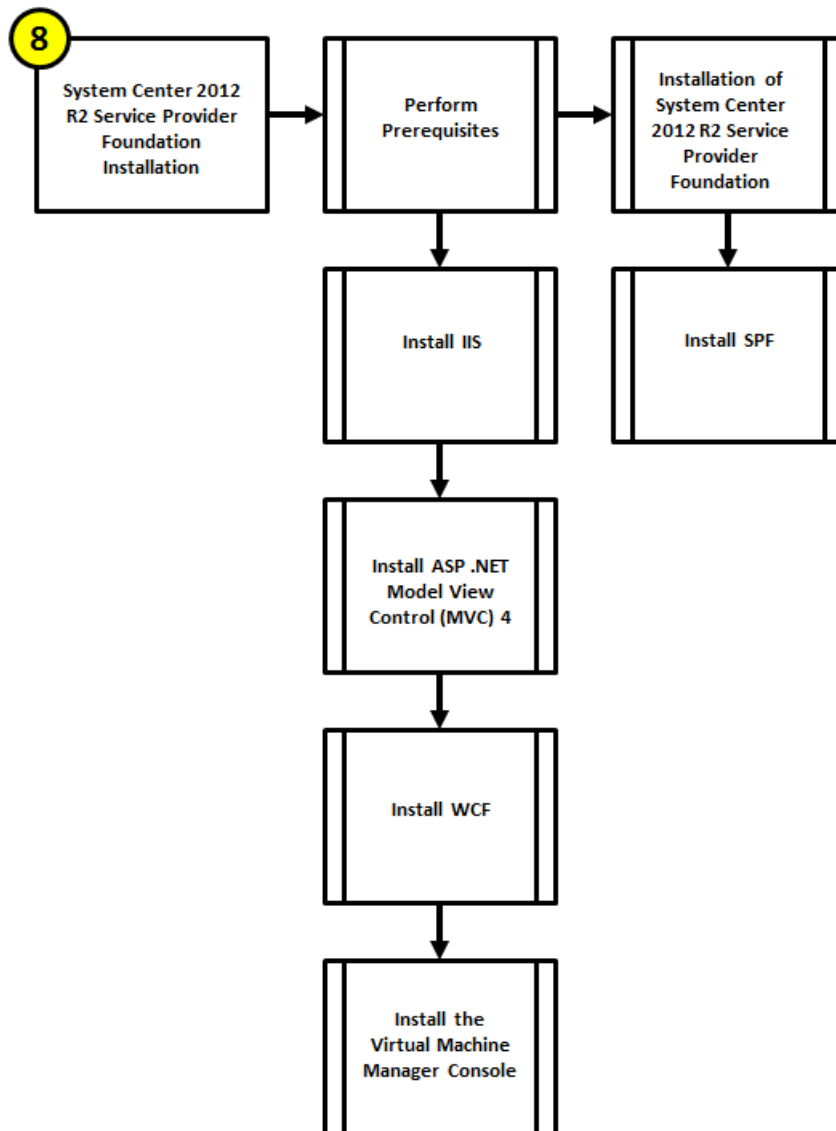
## 25 Service Provider Foundation

In System Center 2012 R2, Service Provider Foundation (SPF) provides web service API that integrates with Virtual Machine Manager. Its primary purpose is to provide service providers and 3rd party vendors with the ability to develop portals that seamlessly front end the infrastructure components of System Center.

The SPF architecture allows for compute resource management via a REST API that facilitates communication with a web service via the OData protocol. Claims-based authentication can be used to verify authorized tenant resources assigned by the service provider. These resources are housed in a database.

The System Center Service Provider Foundation (SPF) 2012 R2 installation process includes the high-level steps shown in the following figure:

Figure 3 Service Provider Foundation Installation Process



## 25.1 Overview

Service providers can use Service Provider Foundation technology to offer infrastructure as a service (IaaS) to their clients. If a service provider has a front-end portal for clients to interact with, Service Provider Foundation makes it possible for the clients to access the resources on their hosting provider's system without making changes to the portal.

This section provides a high-level walkthrough for how to set up Service Provider Foundation. The following requirements are necessary for the setup:

- A base virtual machine running Windows Server 2012 R2 has been provisioned for Service Provider Foundation.
- A SQL Server 2012 SP1 cluster has been established in previous steps with a dedicated instance for Service Provider Foundation.

- The System Center Virtual Machine Manager console is installed.
- A Trusted Server Authentication (SSL) Certificate (the CN field of the certificate must match the server name) is installed.

## 25.2 Prerequisites

The following environment prerequisites must be met before proceeding.

### Accounts

Verify the following service accounts have been created:

**Table 20 Service Provider Foundation Accounts**

User name	Purpose	Permissions
<DOMAIN>\ FT-SCSPF-SVC	Service Provider Foundation service account. Account used to run the SPF service, the identity for the four SPF IIS application pools and the account used for VMM access and integration.	This domain account needs to be a member in the following groups: FT-SCVMM-Admins FT-SCSPF-Admins FT-SCSPF-Provider FT-SCSPF-VMM FT-SCSPF-Usage <SPF Server>\Administrators <SPF Server>\SPF_Admin <SPF Server>\SPF_Provider <SPF Server>\SPF_Usage <SPF Server>\SPF_VMM
<SPF Server>\Local-SCSPF-SVC	Service Provider Foundation local account used as the integration account for Windows Azure Pack.	This local account needs to be a member in the following groups: <SPF Server>\Administrators <SPF Server>\SPF_Admin <SPF Server>\SPF_Provider <SPF Server>\SPF_Usage <SPF Server>\SPF_VMM

### Groups

Verify the following security groups have been created:

Group name	Purpose	Members
<DOMAIN>\ FT-SCSPF-Admins	Service Provider Admin domain group used to provide domain accounts admin rights to	<DOMAIN>\ FT-SCSPF-SVC

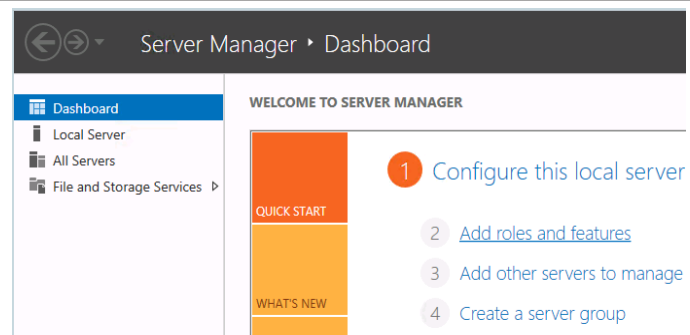
Group name	Purpose	Members
	all SPF components and web services.	
<DOMAIN>\ FT-SCSPF-Provider	Service Provider domain group used to provide domain accounts access to the SPF Provider web service.	Appropriate domain accounts to be delegated permissions to services.
<DOMAIN>\ FT-SCSPF-VMM	Service Provider domain group used to provide domain accounts access to the SPF VMM web service.	Appropriate domain accounts to be delegated permissions to services.
<DOMAIN>\ FT-SCSPF-Usage	Service Provider domain group used to provide domain accounts access to the SPF Usage web service.	Appropriate domain accounts to be delegated permissions to services.
<SPF Server>\SPF_Admin	Local group created by SPF setup process to provide access to the Admin web service. Domain groups and accounts must be added after setup completes.	This local group should contain the following members: <SPF Server>\Local-SPF-SVC <DOMAIN>\FT-SCSPF-Admins
<SPF Server>\SPF_Provider	Local group created by SPF setup process to provide access to the Admin web service. Domain groups and accounts must be added after setup completes.	<SPF Server>\Local-SPF-SVC <DOMAIN>\FT-SCSPF-Admins <DOMAIN>\ FT-SCSPF-Provider
<SPF Server>\SPF_VMM	Local group created by SPF setup process to provide access to the Admin web service. Domain groups and accounts must be added after setup completes.	<SPF Server>\Local-SPF-SVC <DOMAIN>\FT-SCSPF-Admins <DOMAIN>\ FT-SPF-VMM
<SPF Server>\SPF_Usage	Local group created by SPF setup process to provide access to the Admin web service. Domain groups and accounts must be added after setup completes.	<SPF Server>\Local-SPF-SVC <DOMAIN>\FT-SCSPF-Admins <DOMAIN>\ FT-SCSPF-Usage

## Add Web Server Role (IIS)

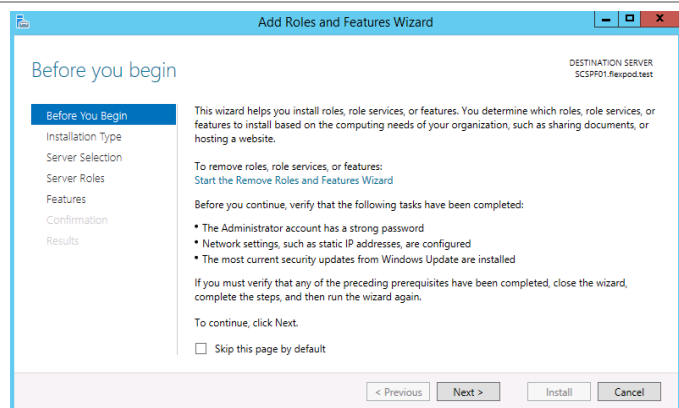
The Service Provider Foundation installation requires the Web Server Role and several additional role features. Use the following procedure to add this role and features to the server.

**Perform the following steps on each Service Provider Foundation server virtual machine.**

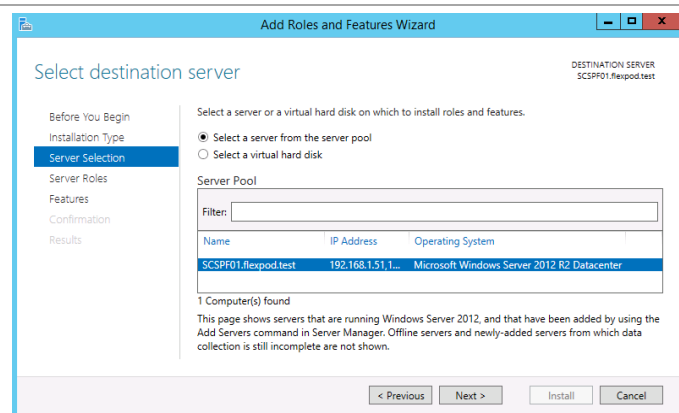
Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add** roles and features.



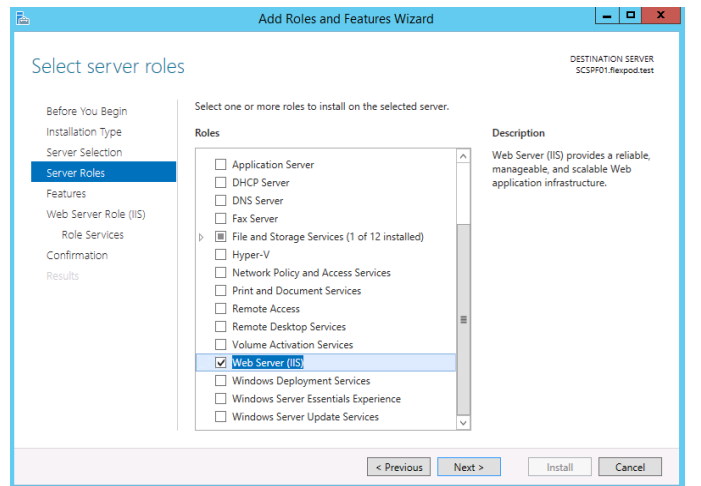
The **Add Roles and Features Wizard** appears. On the **Before You Begin** page, click **Server Selection** in the left pane. (Do not click Next.)



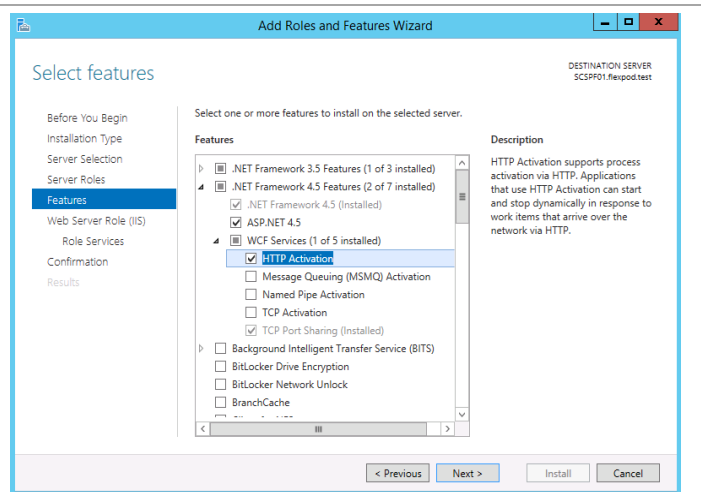
On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server and then click **Next**.



On the **Select Server Roles** page, in the **Roles** pane, scroll down and select the **Web Server (IIS)** check box. A window will display asking to Add features that are required for Web Server (IIS). Click **Add Features**. Click **Next** to continue.



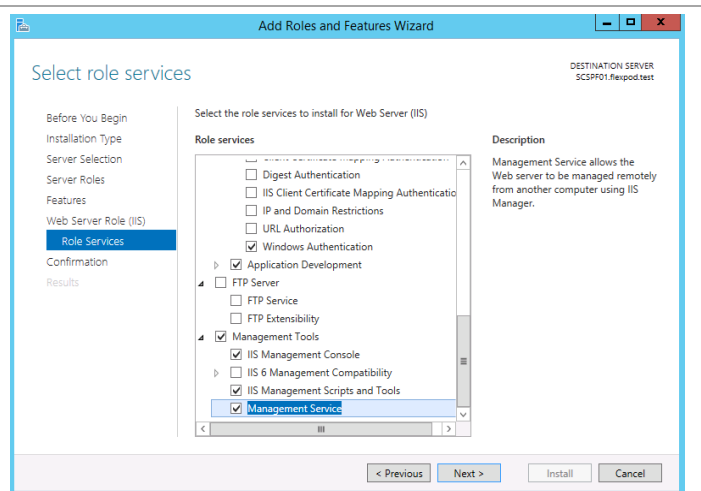
On the **Select features** page, expand **.NET Framework 4.5 Features > WCF Services**. Select **HTTP Activation**. A window will display asking to Add features that are required for HTTP Activation. Click **Add Features**. Also select **Management OData IIS Extension** and accept its required features. Click **Role Services** (not Next) to continue.



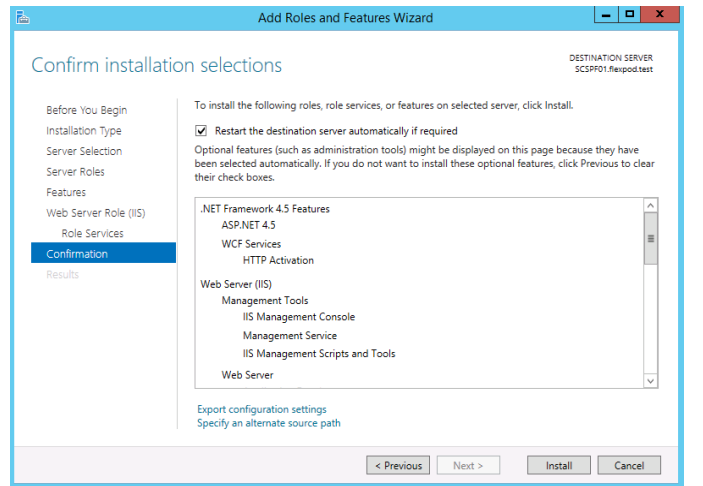
After clicking **Role Services** page, select the following services. Click **Next**.

- Web Server

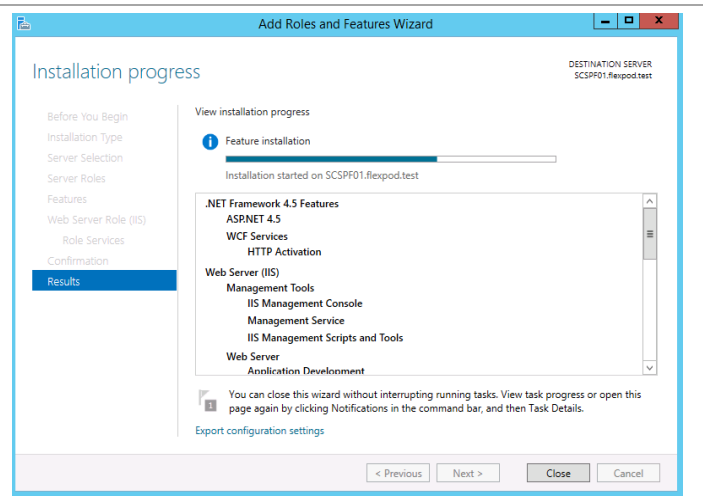
- Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
- Health and Diagnostics
  - HTTP Logging
- Performance
  - Static Content Compression
- Security
  - Request Filtering
  - Basic Authentication
  - Windows Authentication
- Application Development
- Management Tools
  - IIS Management Console
  - IIS Management Scripts and Tools
  - Management Service



On the **Confirm installation selections** page, verify that the previously selected roles and features are listed. Ensure that the **Restart each destination server automatically if required** is selected. Clicking the restart option displays a verification window; click **Yes** on this window. Click **Install** to begin installation.



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

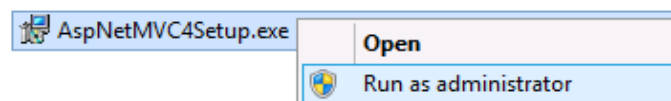


## Install Microsoft ASP .NET Model View Control (MVC) 4

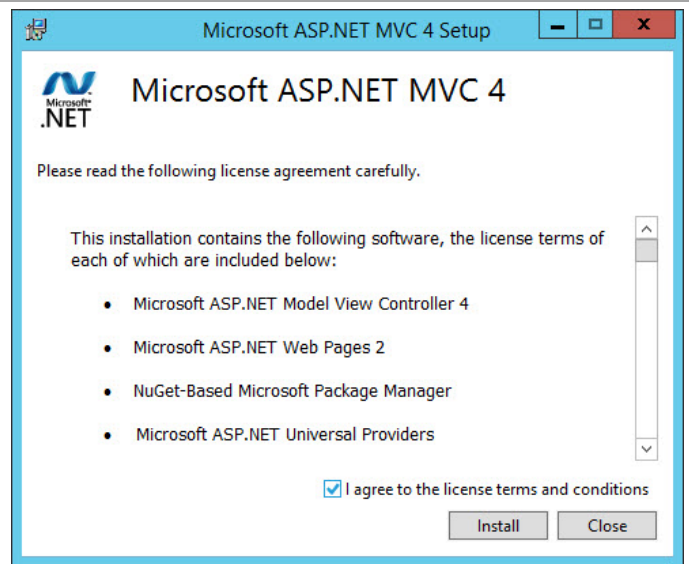
Perform the following steps on each Service Provider Foundation server virtual machine.

Right-click the **AspNetMVC4Setup.exe** file and **Run as administrator**.

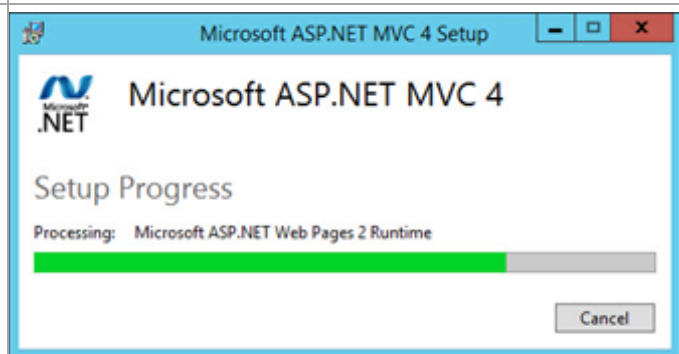
<http://download.microsoft.com/download/2/F/6/2F63CCD8-9288-4CC8-B58C-81D109F8F5A3/AspNetMVC4Setup.exe>



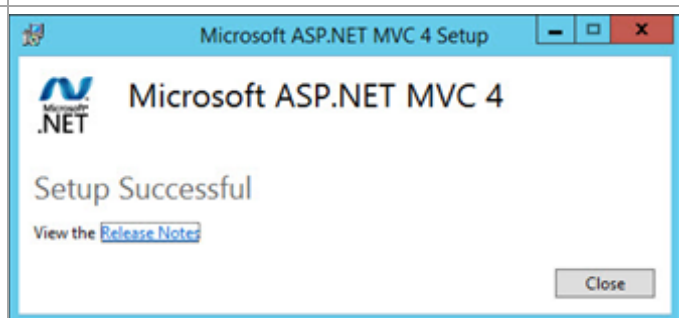
In the **Setup** Window, select **Install**.



The **Setup Progress** page will launch and show the progress of the installation.



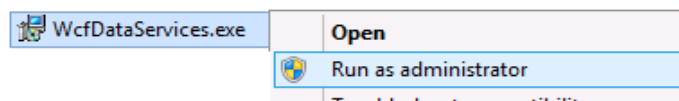
On the **Setup Successful** page, select **Close**.



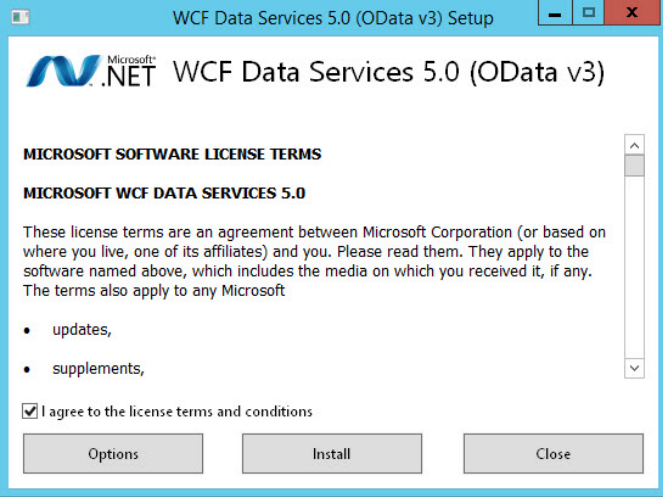
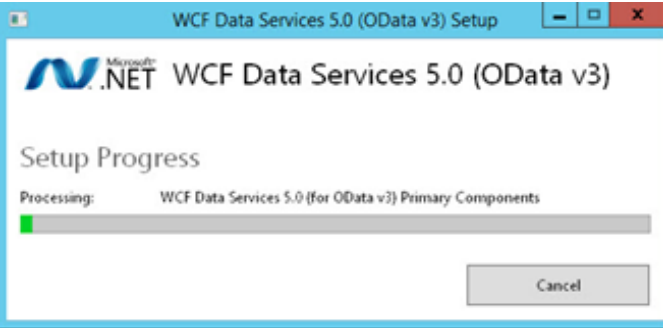
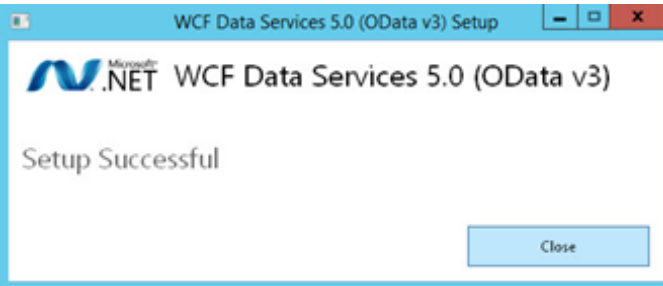
## Install WCF

Perform the following steps on each Service Provider Foundation server virtual machine.

Right-click the **WcfDataServices.exe** file and **Run as administrator**.  
<http://www.microsoft.com/en-ie/download/details.aspx?id=29306>



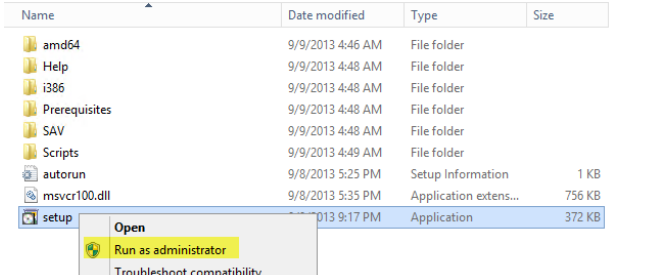


<p>In the <b>Setup</b> Window, select <b>Install</b>.</p>	
<p>The <b>Setup Progress</b> page will launch and show the progress of the installation.</p>	
<p>On the <b>Setup Successful</b> page, select <b>Close</b>.</p>	

## Install the Virtual Machine Manager Console

Complete the following steps to install the Virtual Machine Manager console on the target Service Provider Foundation virtual machine.

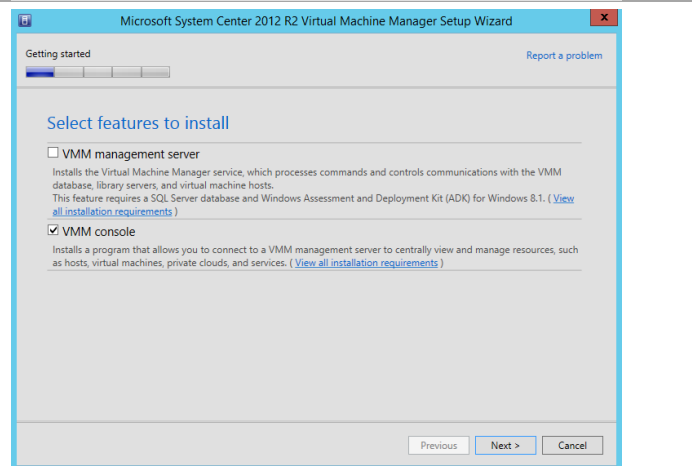
**Perform the following steps on each Service Provider Foundation server virtual machine.**

<p>Log on to the Service Provider Foundation server as a user with Administrator privileges. From the Virtual Machine Manager installation media source, right-click <b>setup.exe</b> and select <b>Run as administrator</b> to begin setup.</p>	
--	--

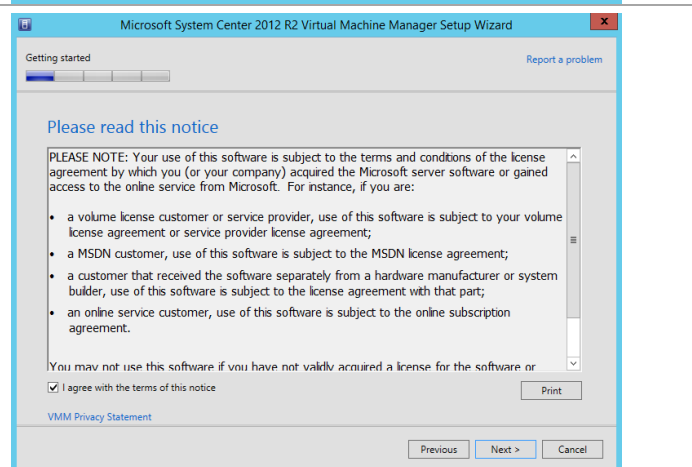
The Virtual Machine Manager Setup Wizard will appear. Click **Install** to begin the Virtual Machine Manager server installation.



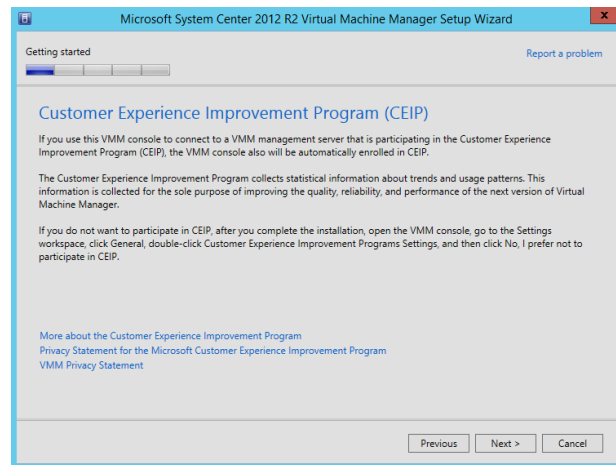
On the **Select features to install** page, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



On the **Please read this license agreement** page, 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.

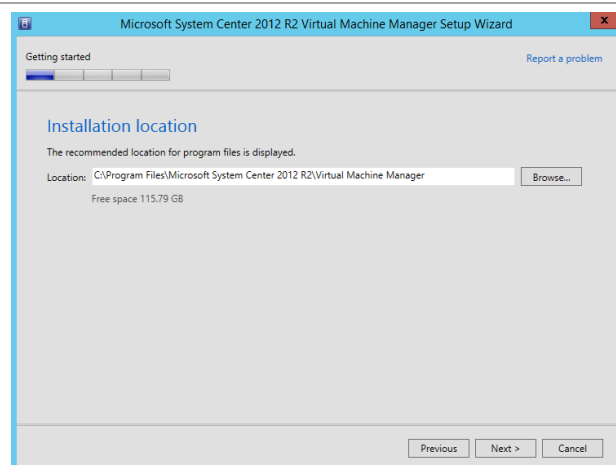


On the **Customer Experience Improvement Program** page, click **Next** to continue.

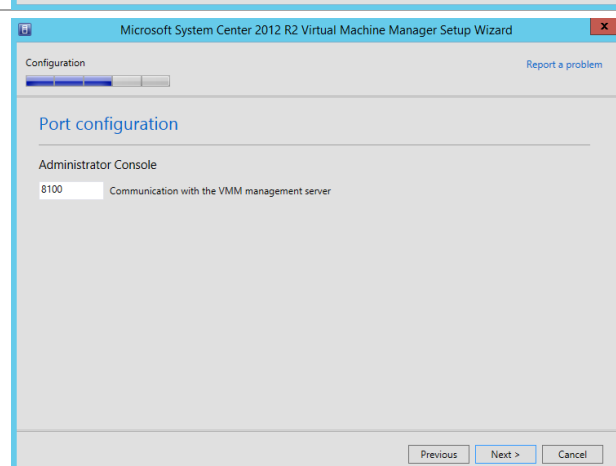


Depending on the current configuration of the server, the Microsoft Update page may appear. Select the option to allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates, based on your organization's policies. Click **Next** to continue.

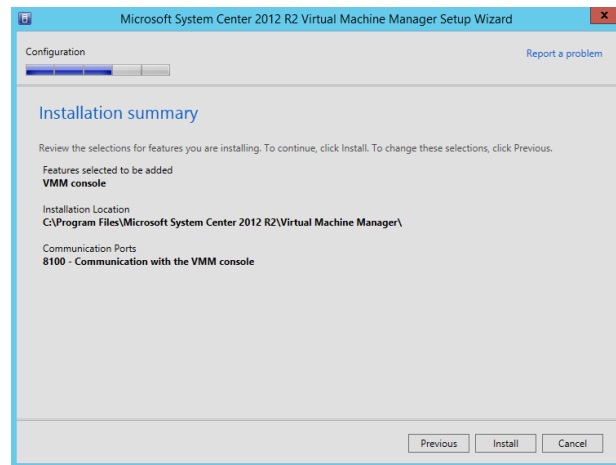
On the **Select installation location** page, specify a location or accept the default location of **C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager** for the installation. Click **Next** to continue.



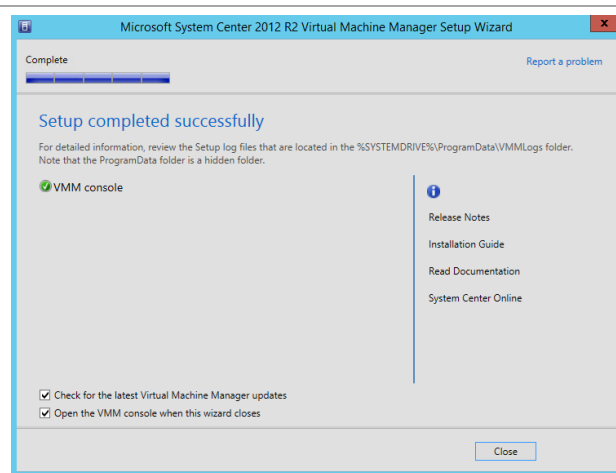
On the **Port Configuration** page, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.



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



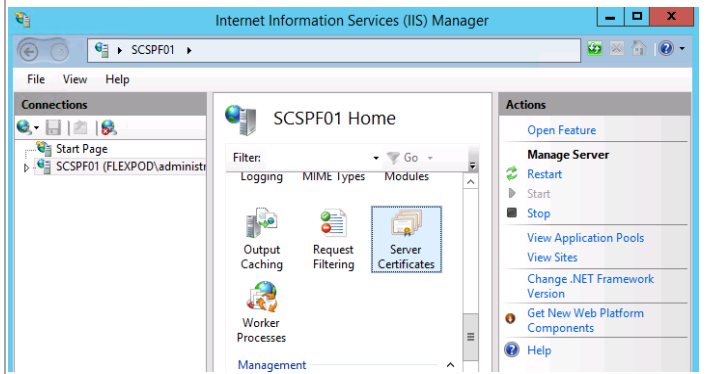
## Request and Install the SSL Certificate

Perform the following steps on each Service Provider Foundation server virtual machine.

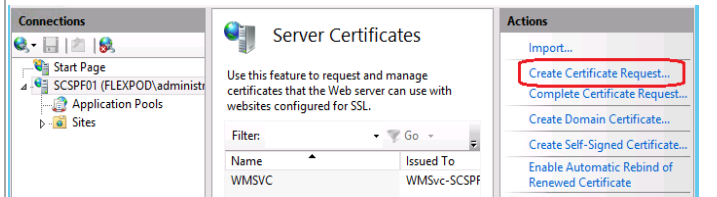
Launch the Internet Information Services (IIS) Manager.



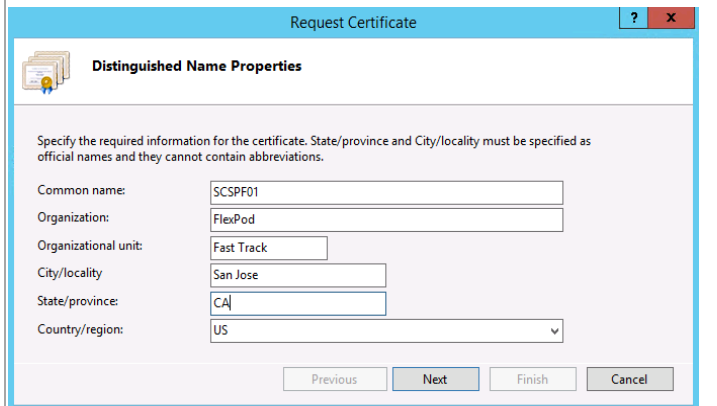
Click the Application Controller home page in the Connections pane. From the IIS section in the middle, double-click **Server Certificates**.



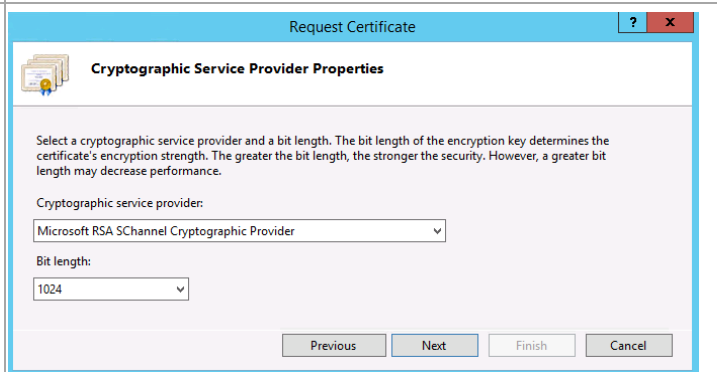
From the **Actions** pane click on **Create Certificate Request...**



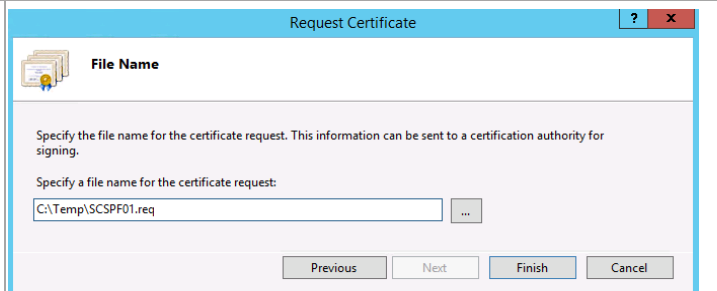
The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name of the server will be accessed in the web browser. Click **Next** to continue.

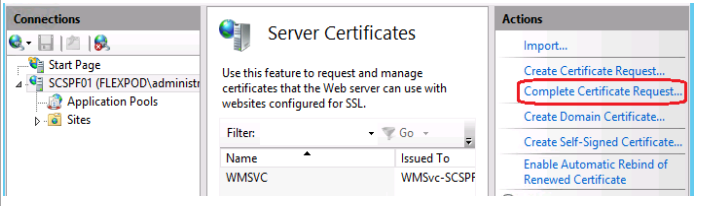
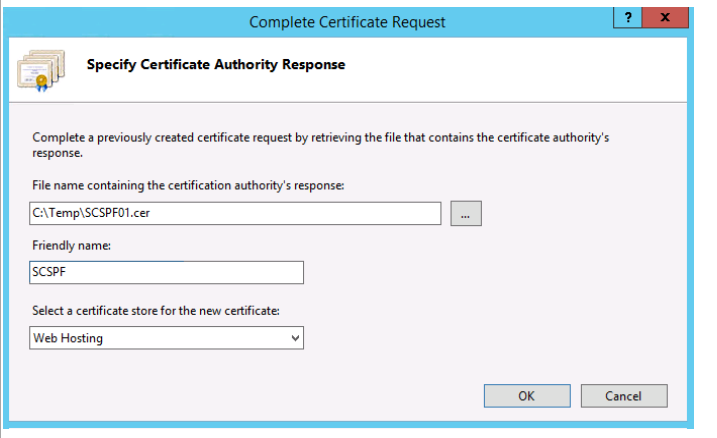
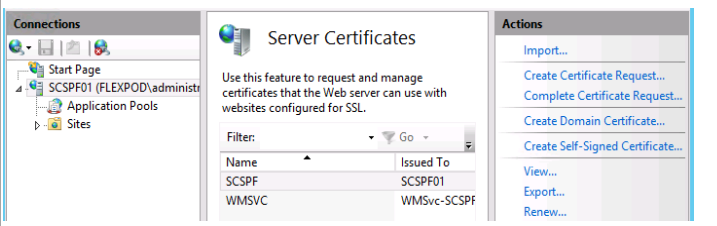


Accept the default properties unless you have implemented different certificate requirements in your environment. Click **Next** to continue.



Provide a location to store the certificate request. Click **Finish** to create the request.



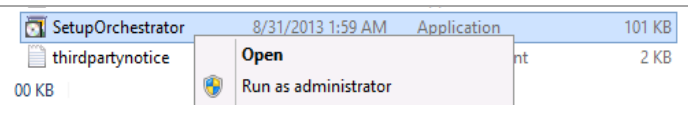
<p>After receiving the issued certificate, open the <b>Internet Information Services (IIS) Manager</b> console and select <b>Server Certificates</b> once again. From the <b>Actions</b> pane, select <b>Complete Certificate Request...</b></p>	
<p>The <b>Complete Certificate Request</b> wizard will appear. In the <b>Specify Certificate Authority Response</b> dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. From the certificate store dropdown select the <b>Personal</b>. Click <b>OK</b> to complete the operation.</p>	
<p>In the <b>Server Certificates</b> section of the IIS Manager, you will now see the newly created and installed certificate.</p>	

## 25.3 Installation

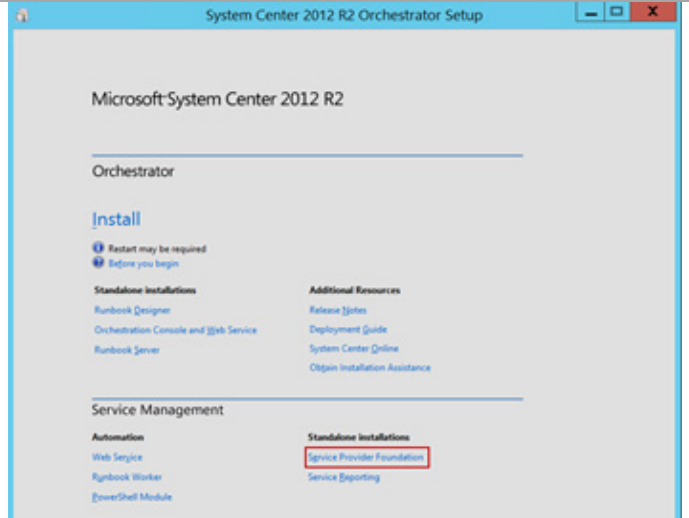
### Install System Center Service Provider Framework

Complete the following steps to install Service Provider Foundation 2012 R2.

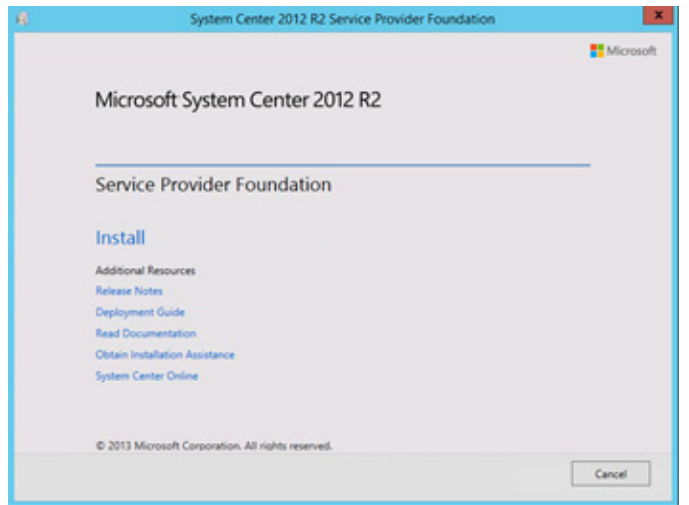
**Perform the following steps on each Service Provider Foundation server virtual machine.**

<p>From the <b>System Center Orchestrator</b> installation media source, right-click <b>setupOrchestrator.exe</b> and select <b>Run as administrator</b> to begin setup.</p>	
--	--

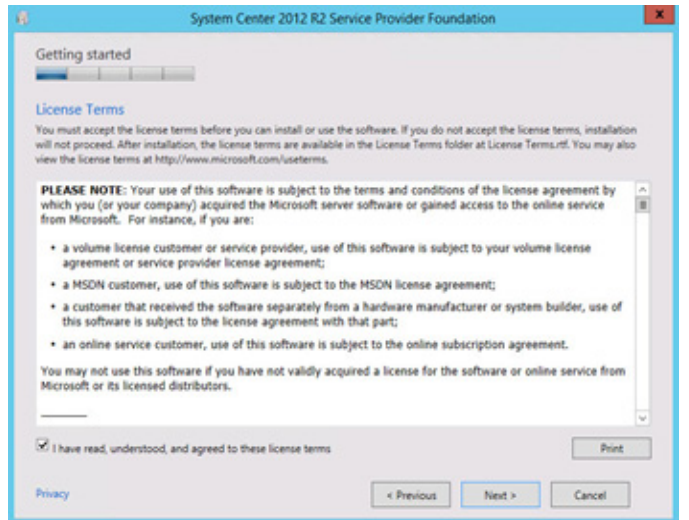
The Orchestrator Setup Wizard will appear. Under Standalone Installations click **Service Provider Foundation** to begin the SPF installation Wizard.



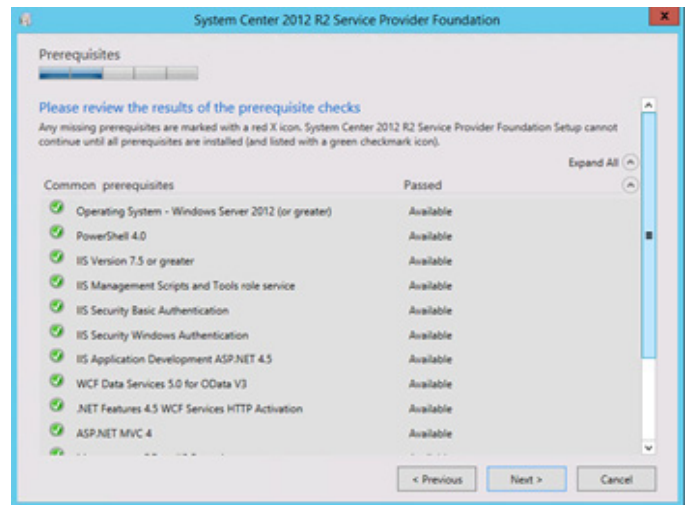
The Service Provider Foundation Wizard will appear. Click **Install** to begin the Service Provider Foundation installation.



On the **License Terms** page, 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.



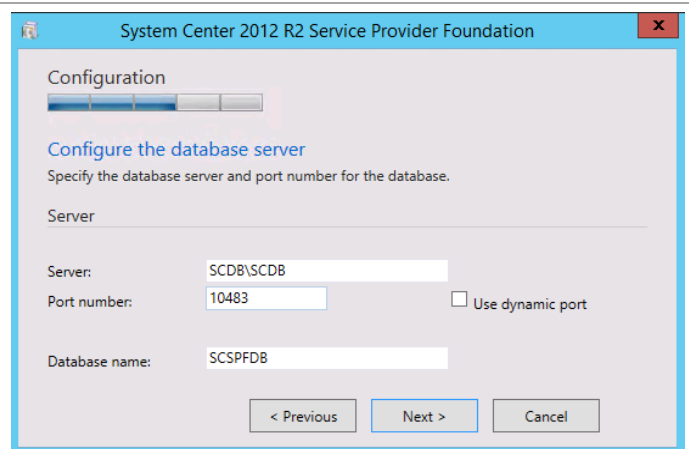
On the **Prerequisites** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Configure the database server** page, specify the following information in the provided text boxes:

- **Server** – Specify the name of the database instance created for the shared System Center SQL instance.
- **Port Number** – Specify number of the SCDB port recorded earlier in the installation
- **Database name** – Specify the name of the database. In most cases, use the default value.

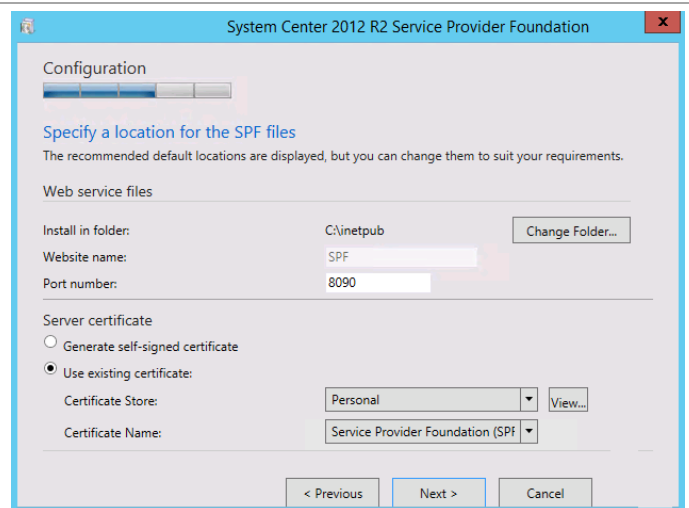
Under Authentication Credentials select **Windows Authentication**. Click **Next** to continue.



On the **Specify a location for the SPF files** page, specify the following information in the provided text boxes:

- **Install in folder** – Accept the default of C:\inetpub.
- **Website name** – Accept the default name of SPF
- **Port Number** – Accept the default of 8090.

Under Server Certificate select Use existing certificate and select the installed certificate. Note: While a self-signed certificate can be used, it is recommended in production scenarios to use a valid certificate issued from a trusted certification authority. Click **Next** to continue.





On the **Configure the Admin web service** page, specify the following accounts in the **Domain Security groups or users** with access box:

- Administrator
- SPF Admins group

In the **Application pool credentials** section, specify the SPF Service Account and password. Click **Next** to continue.

On the **Configure the Provider web service** page, specify the following accounts in the **Domain Security groups or users** with access box:

- Administrator
- SPF Provider group

In the **Application pool credentials** section, specify the SPF Service Account and password. Click **Next** to continue.

On the **Configure the VMM web service** page, specify the following accounts in the **Domain Security groups or users** with access box:

- Administrator
- SPF VMM group

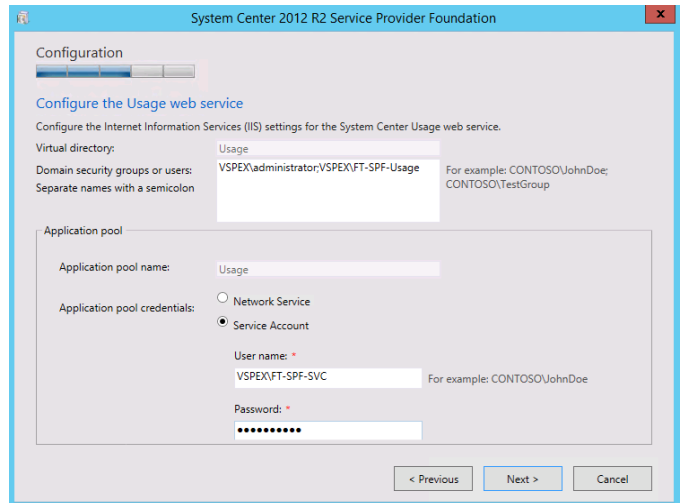
In the **Application pool credentials** section, specify the SPF Service Account and password.

Click **Next** to continue.

On the **Configure the Usage web service** page, specify the following accounts in the **Domain Security groups or users** with access box:

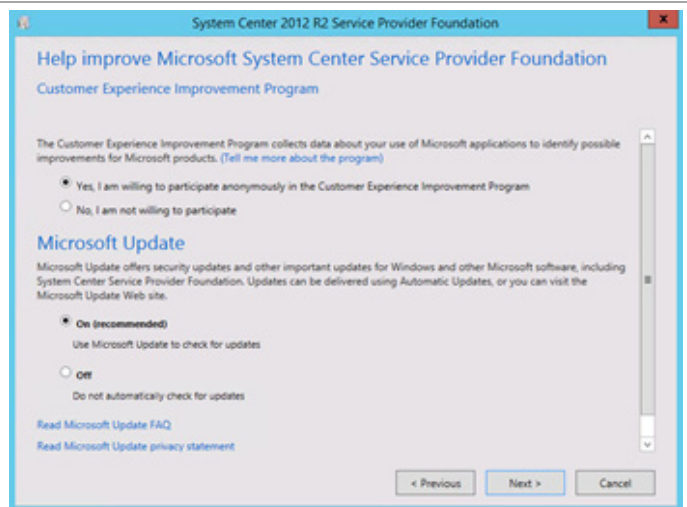
- Administrator
- SPF Usage group

In the **Application pool credentials** section, specify the SPF Service Account and password. Click **Next** to continue.

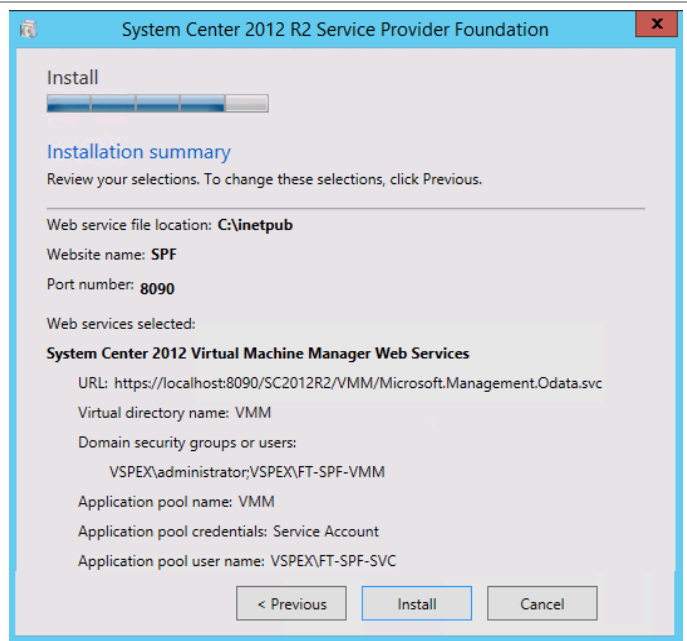


On the **Help improve Microsoft System Center 2012 R2 Service Provider Foundation** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft.

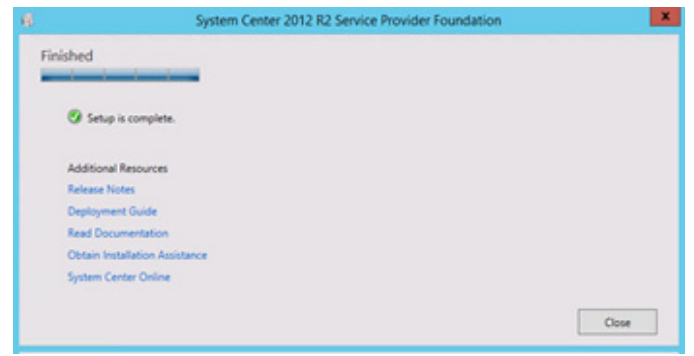
Under the **Microsoft Update** portion of the page, select the appropriate option to participate or not participate in automatic updating. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.



When the installation completes, the wizard will display the **Finished** page. Click **Close** to complete the installation.



## 26 Service Reporting

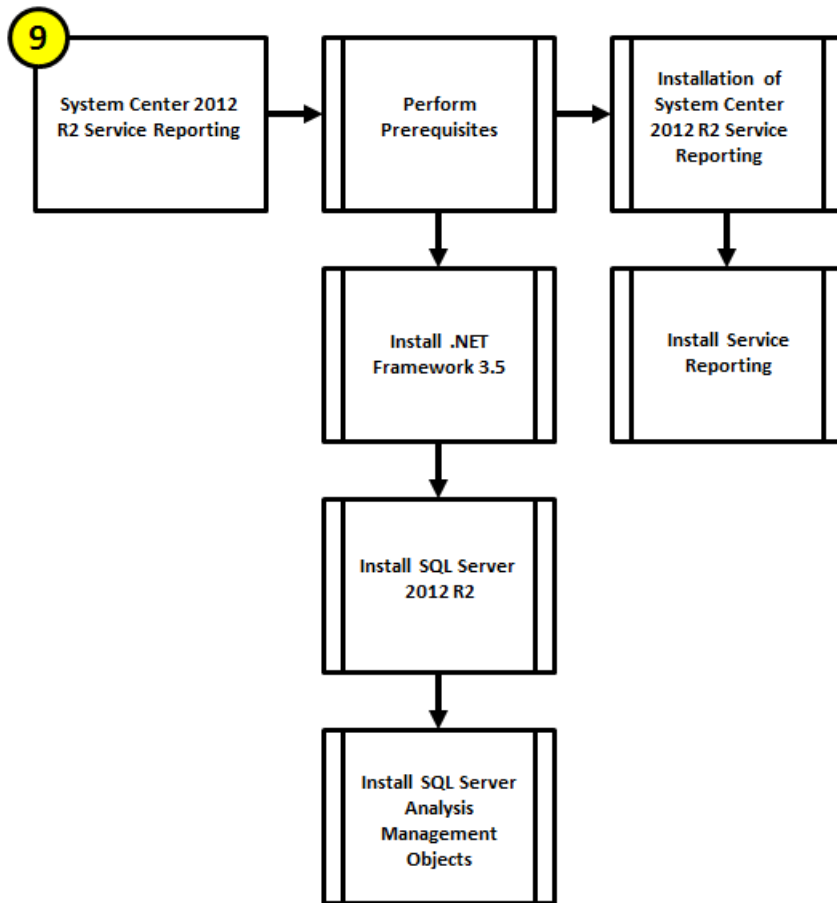
Introduced in System Center 2012 R2, Service Reporting offers cloud administrators the ability to view resource consumption and operating system inventory amongst tenants. It also provides a chargeback model to report on usage expenses.

Data for Service Reporting is collected from both Operations Manager and Windows Azure Pack, and the Service Reporting component itself is configured using PowerShell. In order for Service Reporting to obtain information from Virtual Machine Manager, Operations Manager agents must be installed on all VMM management servers, and the VMM Operations Manager Connector must be configured. Service Provider Foundation (SPF) is required to pass data from Operations Manager to Windows Azure Pack. Windows Azure Pack is then used to collect data from service providers and VMM Clouds.

MS Excel can be used to connect to SQL Server Analysis Services to analyze the collected data. Reports are generated to show usage and capacity data from virtual machines, along with an inventory of used tenant operating systems.

The Service Reporting installation process includes the high-level steps shown in the following figure:

Figure 4 Service Reporting Installation Process



## 26.1 Overview

Service Reporting in System Center 2012 R2 enables administrators at IT hosting providers to view tenant consumption of virtual machines, resources (computation, network, and storage), and operating system inventory in their infrastructure. This section provides a high-level walkthrough for how to set up Service Reporting.

The following requirements are necessary for the setup:

- A base virtual machine running Windows Server 2012 R2 has been provisioned for Service Reporting.
- .NET Framework 3.5 is installed.

## 26.2 Prerequisites

The following environment prerequisites must be met before proceeding.

### Accounts

No specific service accounts are required for this component.

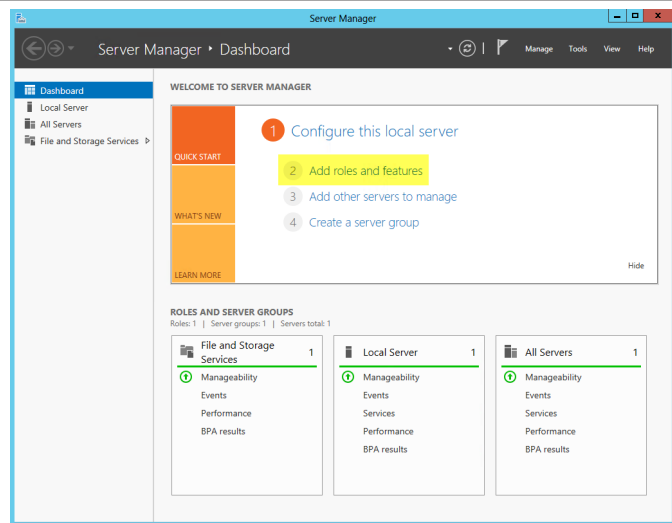
## Groups

No specific groups are required for this component.

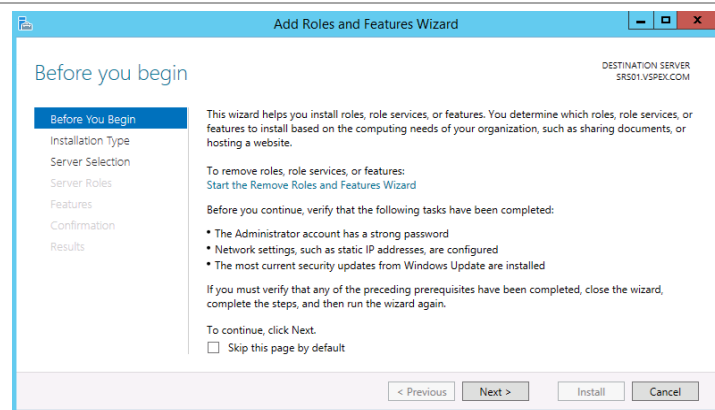
## Add .NET Framework 3.5

The Reporting Services installation requires that .NET Framework 3.5 is enabled to support installation. Use the following procedure to enable .NET Framework 3.5.

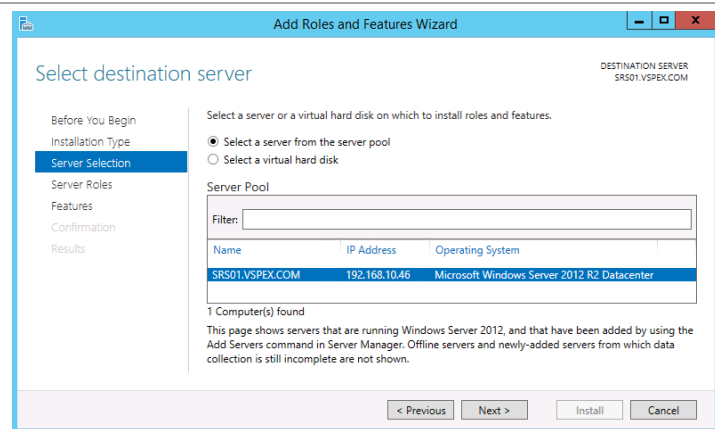
Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features**.



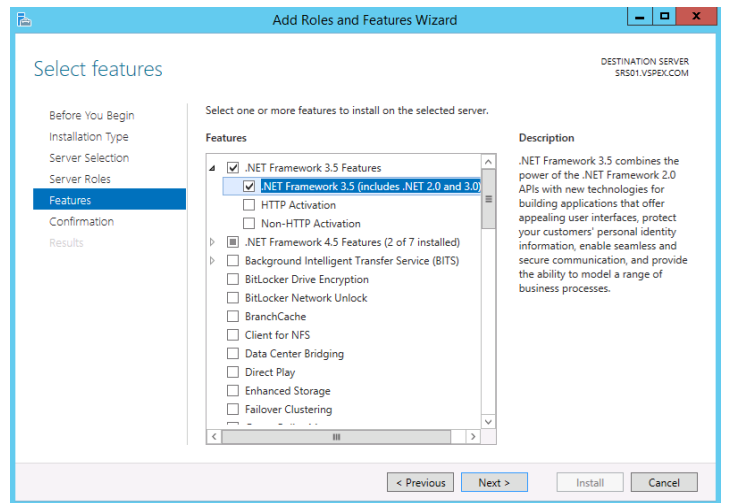
The **Add Roles and Features Wizard** starts. On the **Before You Begin** page, click **Server Selection** in the left pane. (Do not click **Next**.)



On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server and then click **Features** in the left pane. (Do not click **Next**.)

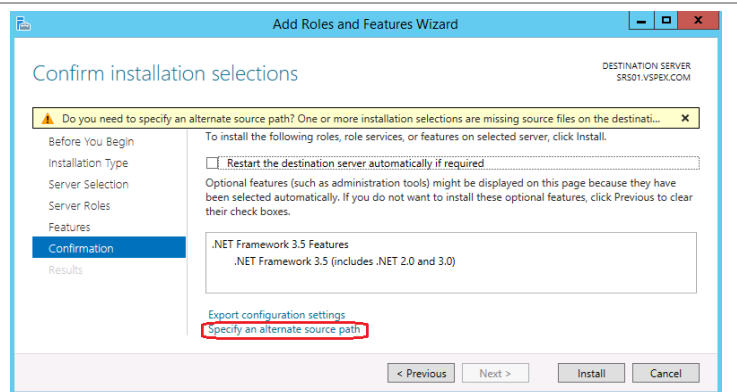


On the **Select Features** page, in the **Features** pane. Select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.

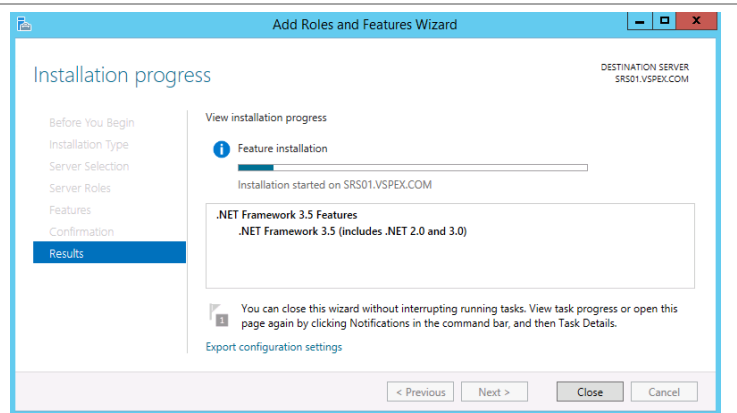


On the **Confirm installation selections** page, verify that **.NET Framework 3.5 Features** is listed. Ensure that the **Restart each destination server automatically** if required is not selected. Click **Install** to begin installation.

**Note:** Unlike other roles and features, the source for **.NET 3.5** is not stored locally. If your system is connected to the internet, the installation will find the source from Microsoft's web site. Otherwise, you need to specify a location where the **\sources\sxs** directory from the installation media is available.



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

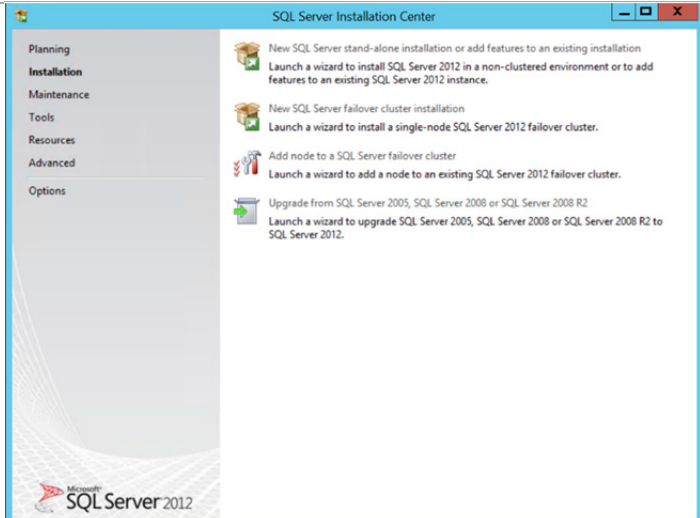


Although this installation was performed interactively, the installation of roles and features can be automated by using the shown PowerShell cmdlet.

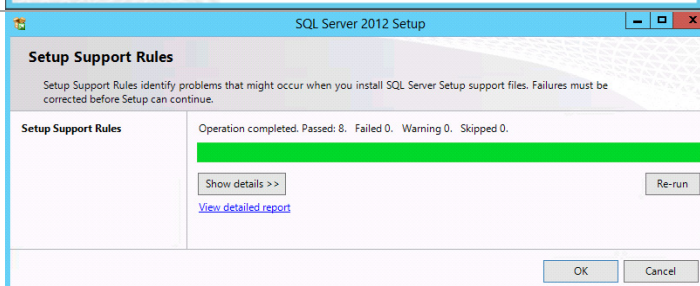
```
Install-WindowsFeature -Name NET-Framework-Core -Source E:\sources\sxs
```

## Install SQL Server 2012 SP2

From the SQL Server 2012 SP1 installation media source, right-click setup.exe and click **Run as administrator** to begin setup. The **SQL Server Installation Center** will appear. Click **Installation** in the left pane. Then click **New SQL Server stand-alone installation or add features to an existing installation**.

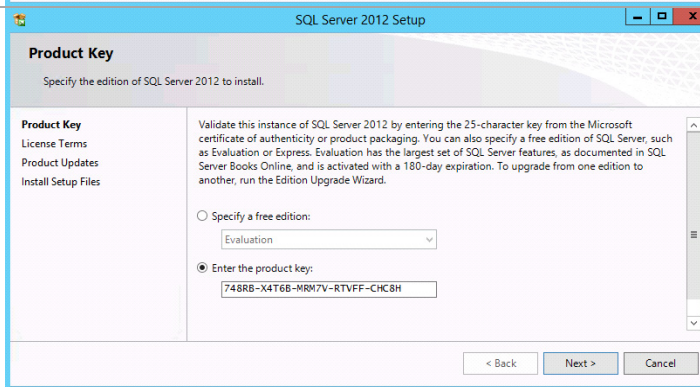


The Setup Support Rules Wizard will appear. Click **OK** to continue.

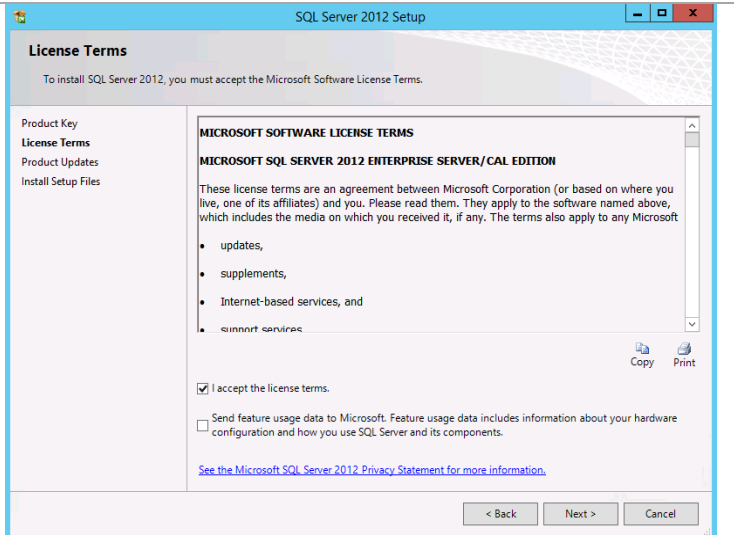


On the **Product Key** page, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

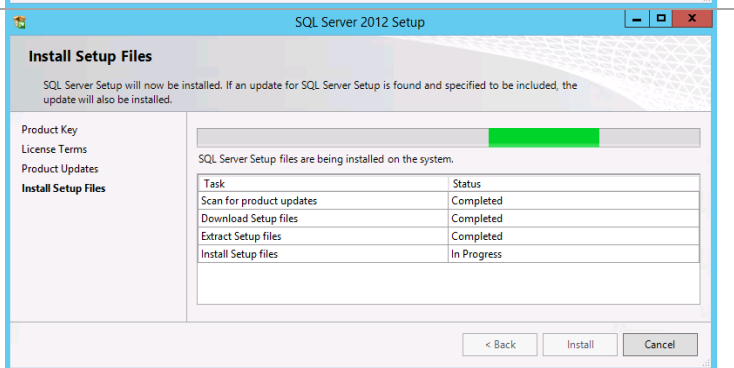
**Note:** If you do not have a product key, select the **Specify a free edition** option, and then click **Evaluation** from the drop-down list for a 180-day evaluation period.



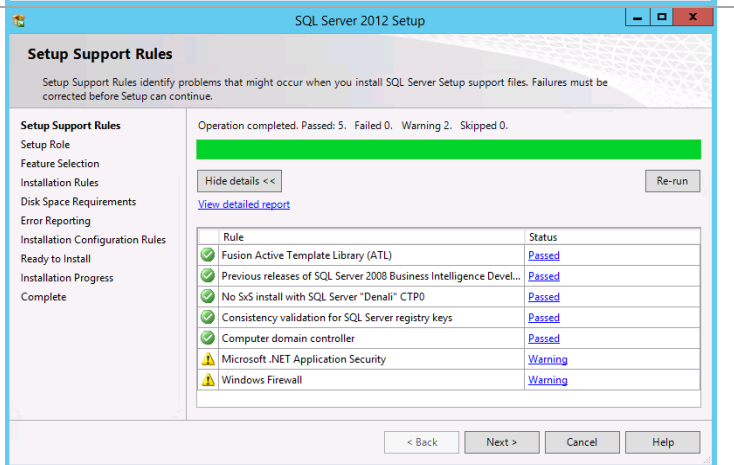
On the **License Terms** page, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box, based on your organization's policies, and click **Next** to continue.



The setup files will be installed. No action required.

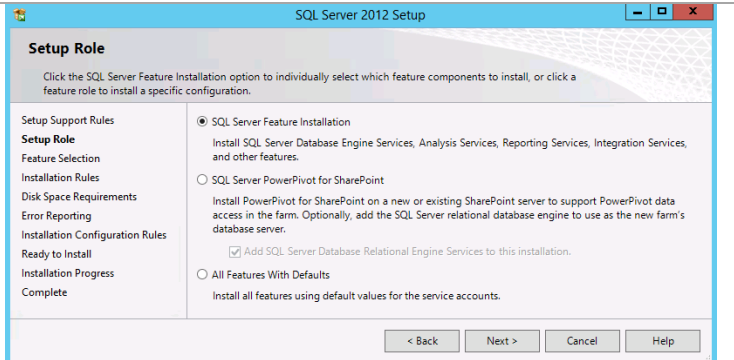


The Setup Support Rules Wizard will appear. Click **OK** to continue.





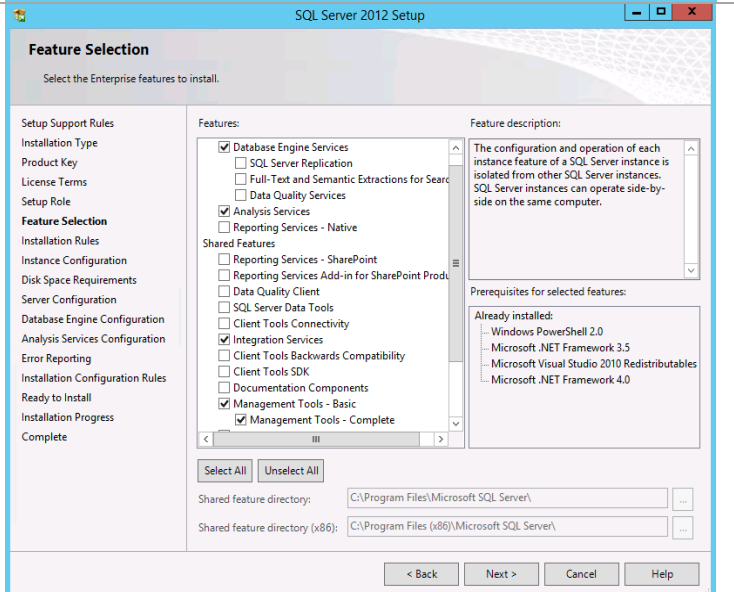
On the **Setup Role** page, select **SQL Server Feature Installation**, and click **Next** to continue.



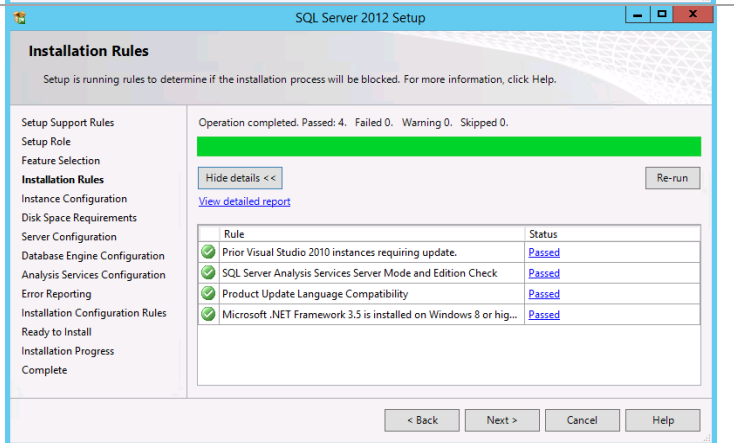
On the **Feature Selection** page, make the following selections:

- Database Engine Services
- Analysis Services
- Integration Services
- Management Tools-Basic
- Management Tools- Complete

When all selections are made, click **Next** to continue.



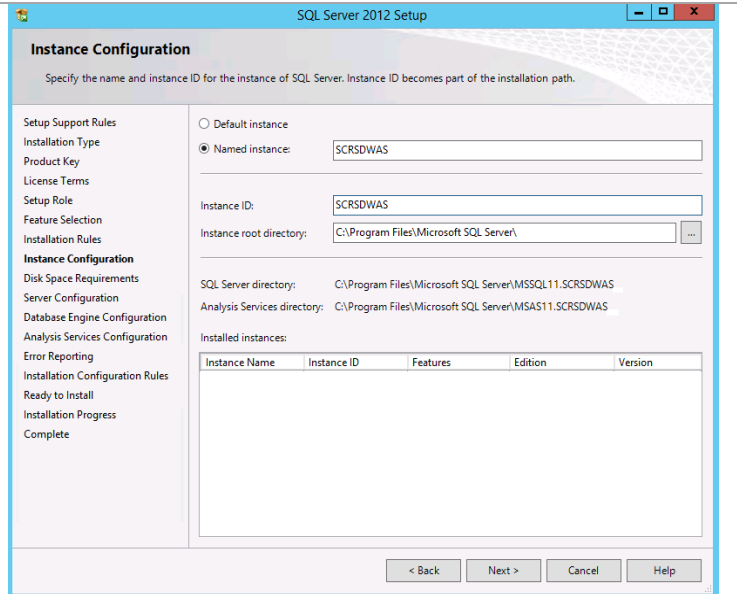
On the **Installation Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



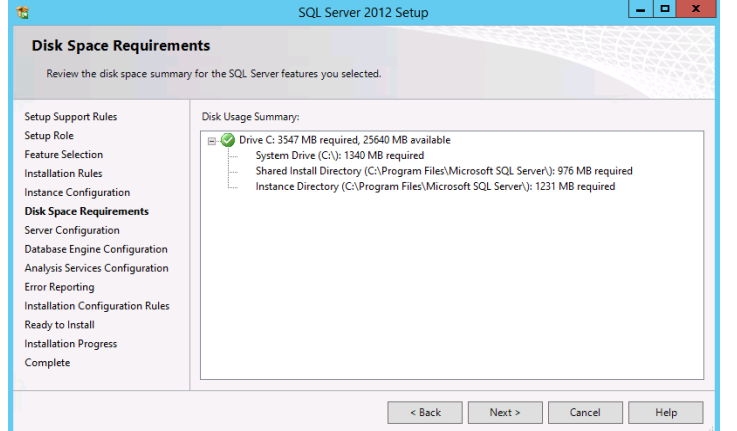
On the **Instance Configuration**, select the **Named instance** option. In the provided text box, specify the instance name being installed:

- **Instance ID** – Specify the instance name being installed. Verify that it matches the **Named instance** value.
- **Instance root directory** – Accept the default location of %ProgramFiles%\Microsoft SQL Server.

Click **Next** to continue.

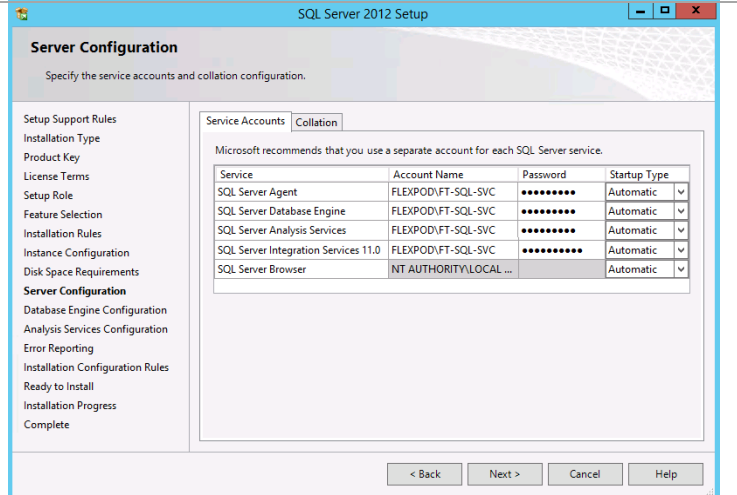


On the **Disk Space Requirements** page, verify that you have sufficient disk space, and click **Next** to continue.

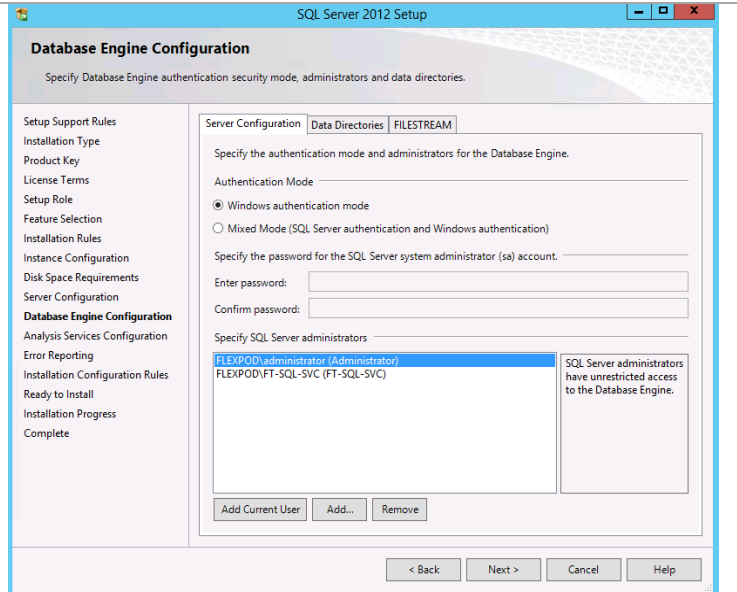


On the **Server Configuration** page, click the **Service Accounts** tab. Specify the SQL Server Service Account and an associated password for the SQL Server Agent, SQL Server Database Engine, SQL Server Analysis Services and SQL Server Integration Services 11.0 services.

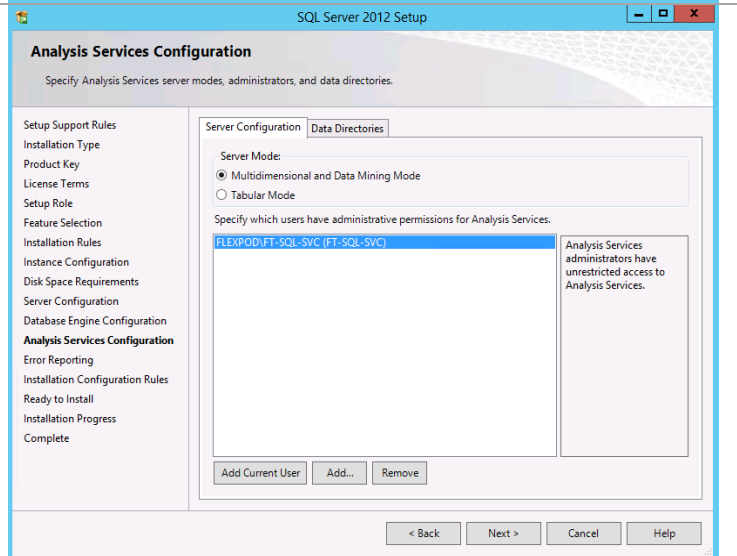
**Note:** For the SQL Server Agent set the Startup Type to **Automatic**.



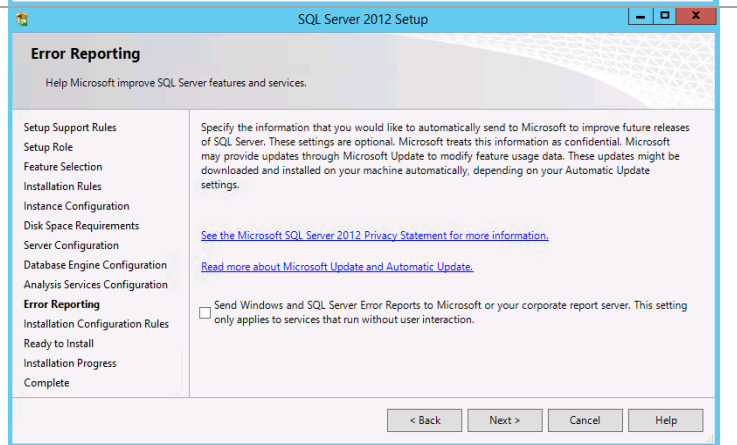
On the **Database Engine Configuration** page, click the **Server Configuration** tab. In the **Authentication Mode** section, select the **Windows authentication mode** option. In the **Specify SQL Server administrators** section, click the **Add...** button to add SQL Server Service Account. Click the **Add Current User** to add the installation account. Click **Next** to continue.



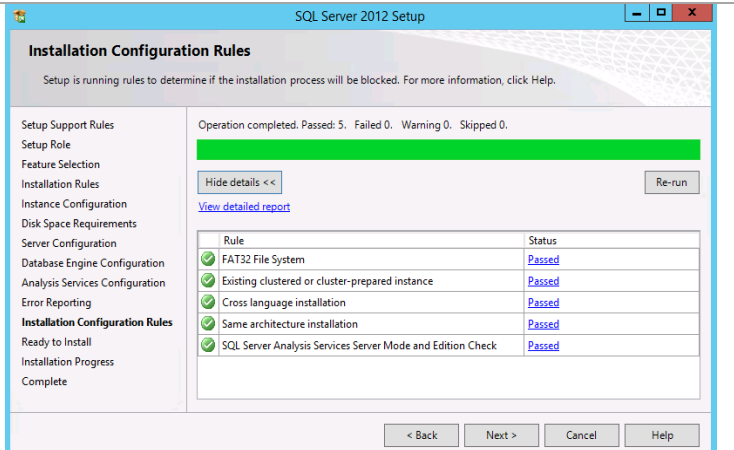
On the **Analysis Services Configuration** page, click the **Server Configuration** tab. In the **Specify which users have administrative permissions for Analysis Services** section, click **Add...** to add the SQL Server Service account. Click **Next** to continue.



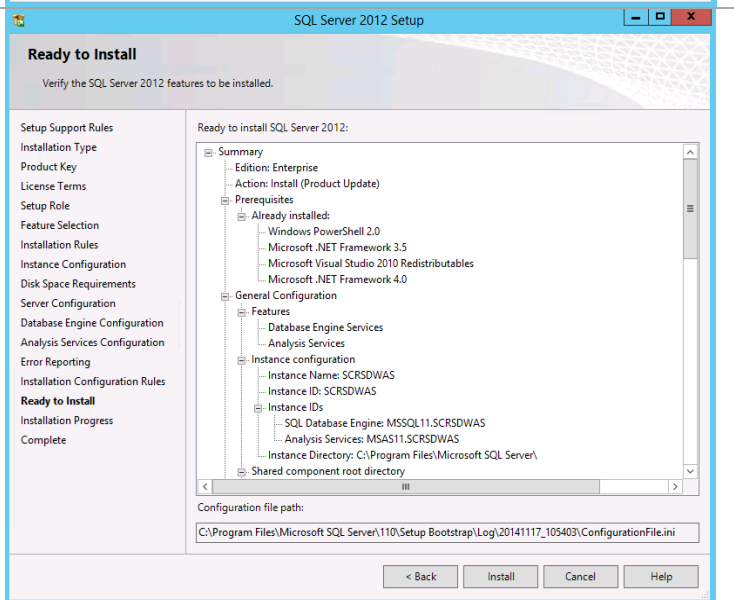
On the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies, and click **Next** to continue.



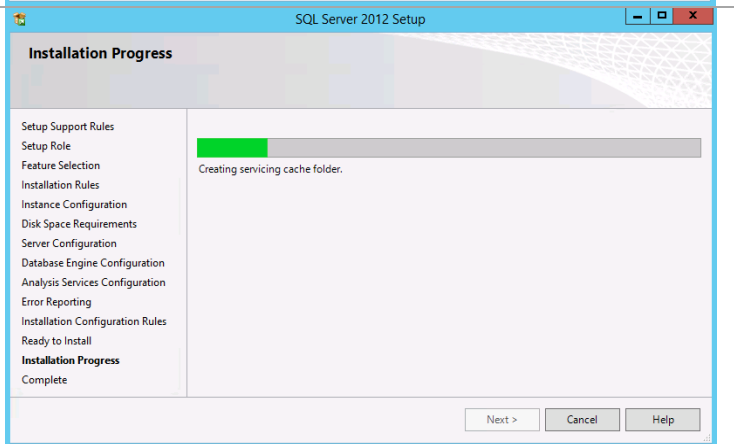
The installation configuration rules check will be run. Click **Next** to continue.



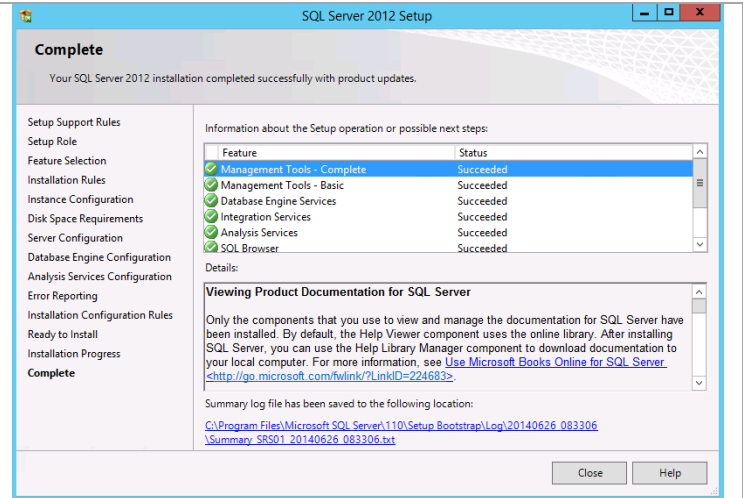
On the **Ready to Install** page, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



On the **Installation Progress** page, the installation progress will be displayed.



When the installation is complete, the **Complete** page will appear. Click **Close**.



## 26.3 Installation

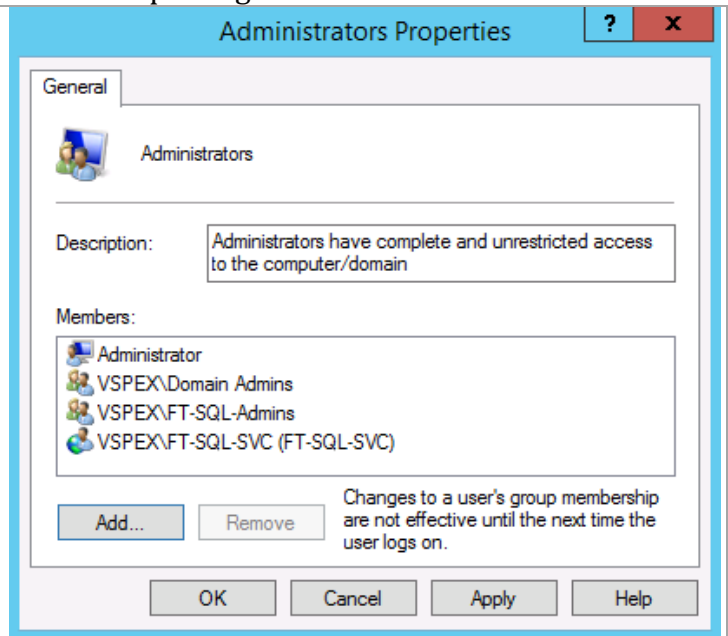
### Install Service Reporting

Complete the following steps to install Service Reporting.

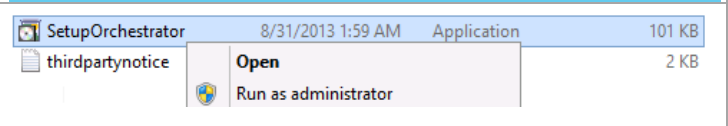
Log on to the Service Reporting virtual machine as a user with local administrator rights.

Verify the following accounts or groups are members of the local Administrators group on the App Controller portal virtual machine:

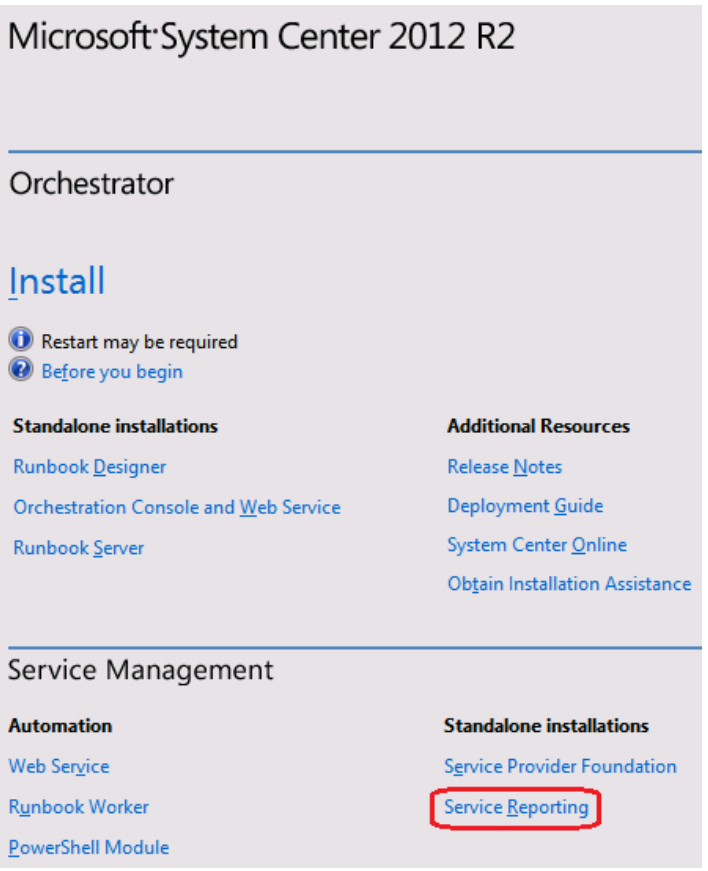
- SQL service account
- SQL Admins group



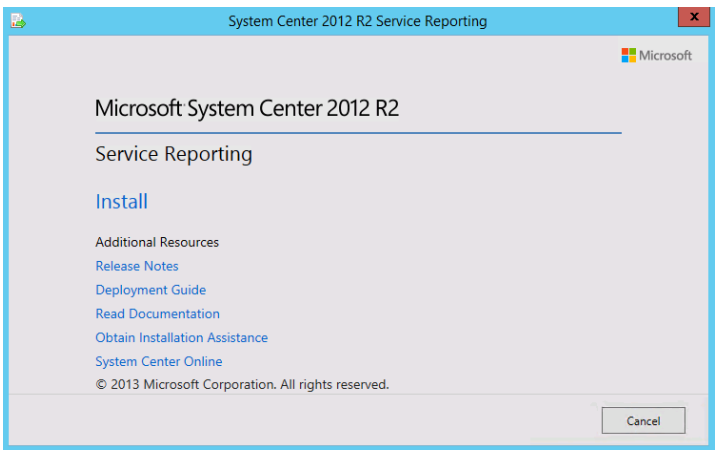
From the **System Center Orchestrator** installation media source, right-click **setupOrchestrator.exe** and select **Run as administrator** to begin setup.



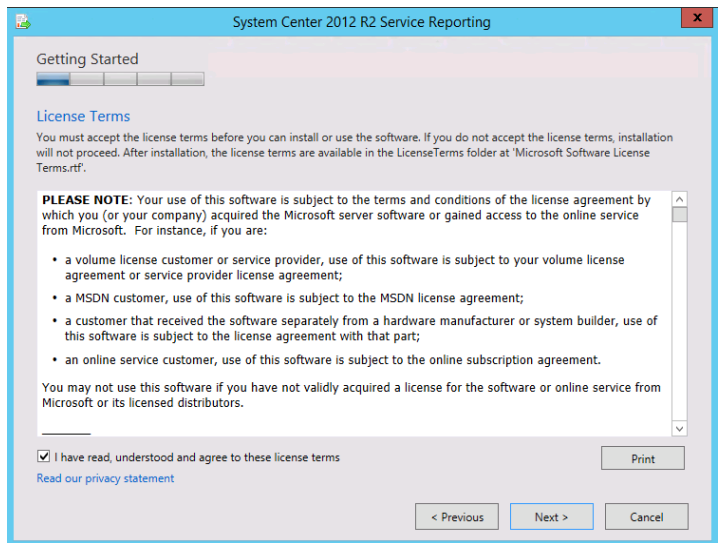
The Orchestrator Setup Wizard will appear. Under Standalone Installation click **Service Reporting** to begin the Service Reporting server installation Wizard.



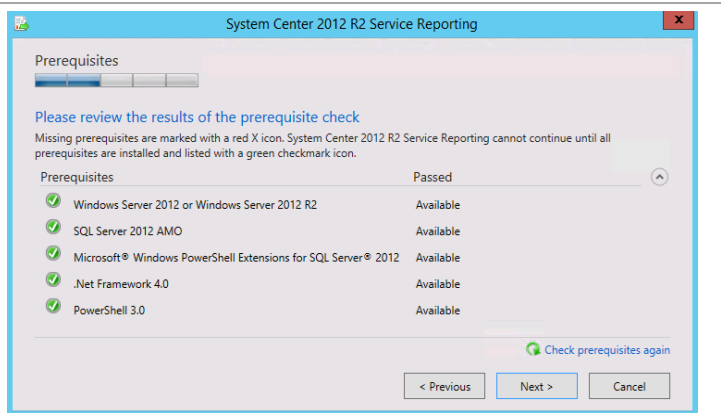
The Service Reporting Setup Wizard will appear. Click **Install** to begin the Service Reporting server installation.



On the **License Terms** page, 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.



On the **Prerequisites** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Installation location** page, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Service Reporting for the installation. Click **Next** to continue.



On the **Configure Service Reporting Data Warehouse** page, specify the following information in the provided text boxes:

- **Database server** – Specify the name of the Service Reporting Server.
- **SQL Server instance** – Specify the name of the SQL Server database instance created for the Service Reporting installation.

Select the **Create a new database** option, and specify the following information in the provided text boxes:

- **ETLRepository DB** – Specify the name of the ETL Repository database. In most cases, use the default value.
- **Staging DB** – Specify the name of the Staging database. In most cases, use the default value.
- **Data Warehouse DB** – Specify the name of the Data Warehouse database. In most cases, use the default value.

Click **Next** to continue.

System Center 2012 R2 Service Reporting

Configuration

Configure Service Reporting Data Warehouse

First, specify the name of the server that hosts the instance of SQL Server 2008 R2 or SQL Server 2012 that contains or will contain the Service Reporting data warehouse. Then, select whether to create a new data warehouse or use an existing Service Reporting Data Warehouse.

Only supported instances are listed.

Database server: SRS01 SQL Server instance: SRS01\SCSRDWAS

Create a new database  
 Use an existing database

ETLRepository DB: UsageETLRepositoryDB

Staging DB: UsageStagingDB

Data Warehouse DB: UsageDatawarehouseDB

< Previous Next > Cancel

On the **Configure Analysis Server** page, specify the following information in the provided text boxes:

- **Database server** – Specify the name of the Service Reporting Server.
- **SQL Server instance** – Specify the name of the SQL Server database instance created for the Service Reporting installation.

Select the **Create a new database** option, and specify the following information in the provided text boxes:

- **Analysis DB** – Specify the name of the Analysis database. In most cases, use the default value.

Click **Next** to continue.

System Center 2012 R2 Service Reporting

Configuration

Configure Analysis Server

Specify the location of the SQL Server Analysis Server.

Only supported instances are listed.

Database server: SRS01 SQL Server instance: SRS01\SCSRDWAS

Create a new database  
 Use an existing database

Analysis DB: UsageAnalysisDB

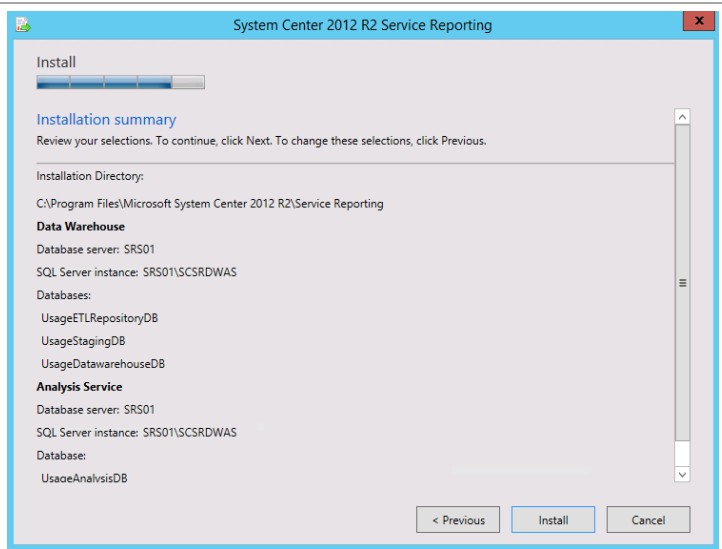
< Previous Next > Cancel



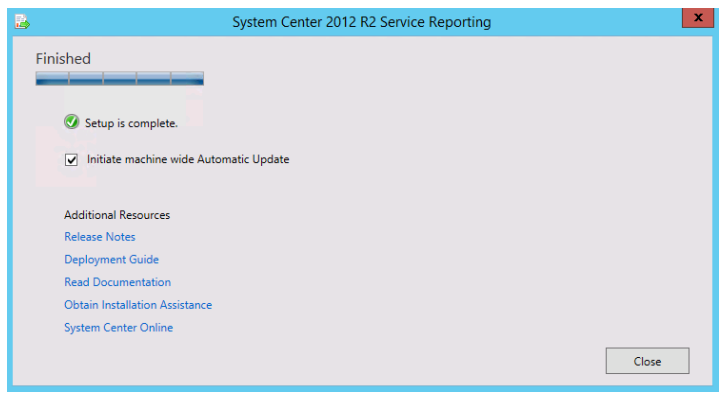
On the **Help improve Microsoft System Center Service Reporting** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft. Under the **Microsoft Update** portion of the page. Select the appropriate option to participate or not participate in automatic updating. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.



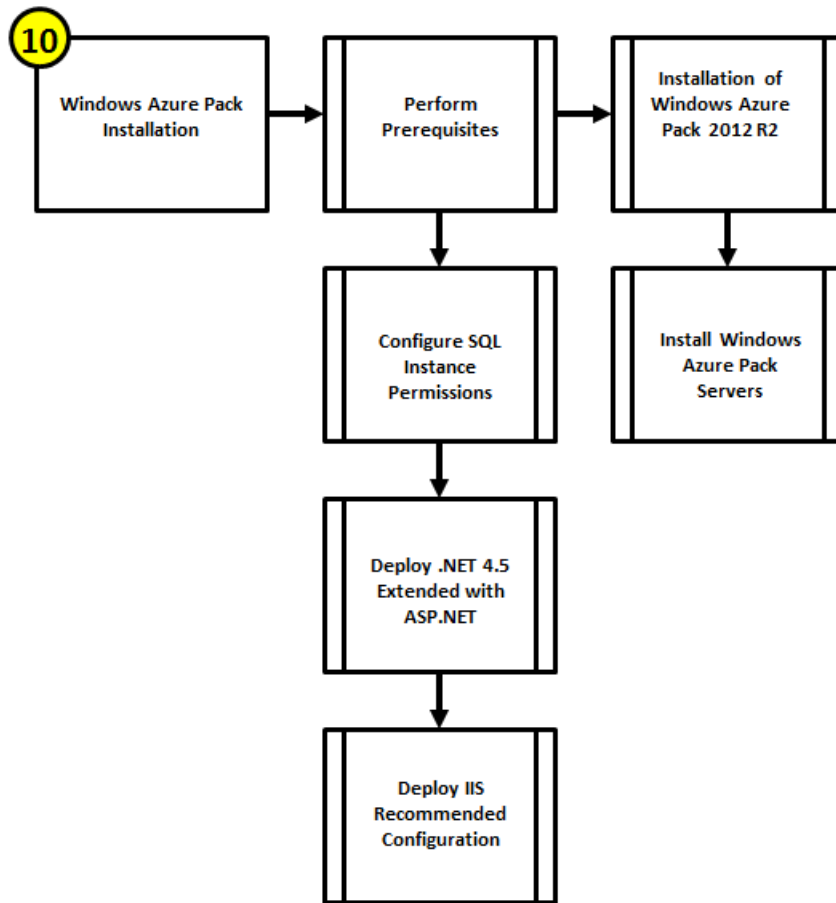
When the installation completes, the wizard will display the **Finished** page. Check the **Initiate machine wide Automatic Update** box. Click **Close** to complete the installation.



## 27 Windows Azure Pack

The Windows Azure Pack installation process includes the high-level steps shown in the following figure.

Figure 5 Windows Azure Pack Installation Process



## 27.1 Overview

Windows Azure Pack (WAP) for Windows Server is a collection of Windows Azure technologies, available to Microsoft customers at no additional cost for installation into your data center. It runs on top of Windows Server 2012 R2 and System Center 2012 R2 and, through the use of the Windows Azure technologies, enables you to offer a rich, self-service, multi-tenant cloud, consistent with the public Windows Azure experience.

WAP is designed to be very scalable. It comprises seven modules.

- Administration Site – A portal for administrators to configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In this portal, administrators create Web Site clouds, virtual machine private clouds, create plans, and manage user subscriptions.
- Administration Authentication Site – By default, Windows Azure Pack uses Windows authentication for the administration portal. You also have the option to use Windows Azure Active Directory Federation Services (AD FS) to authenticate users.
- Administration API – exposes functionality to complete administrative tasks from the management portal for administrators or through the use of Windows PowerShell cmdlets.

- Tenant Site – A customizable self-service portal to provision, monitor, and manage services, such as Windows Azure Pack: Web Sites, Windows Azure Virtual Machines, and Windows Azure Pack: Service Bus. In this portal, users sign up for services and create services, virtual machines, and databases.
- Tenant Authentication Site – uses an ASP.NET Membership provider to provide authentication for the management portal for tenants.
- Tenant Public API – enables end users to manage and configure cloud services that are included in the plans that they subscribe to. The Tenant Public API is designed to serve all the requirements of end users that subscribe to the various services that a hosting service provider provides.
- Tenant API – enables users, or tenants, to manage and configure cloud services that are included in the plans that they subscribe to.

All modules can be installed into a single VM, in separate VMs, or in combinations of VMs. As need for capacity increases, additional VMs can be deployed with the same combination of modules in a network load balanced configuration.

This deployment guide show five modules deployed in pairs of load balanced VMs and two, the Administration Site and the Administration Authorization Site, deployed as single VMs. These two administration sites generally do not require scaling.

- Administration Site – WAP06
- Administration Authentication Site – WAP07
- Administration API – WAP05, WAP05b
- Tenant Site – WAP01, WAP01b
- Tenant Authentication Site – WAP02, WAP02b
- Tenant Public API – WAP03, WAP03b
- Tenant API – WAP04, WAP04b

## 27.2 Prerequisites

The following environment prerequisites must be met before proceeding.

### Accounts

Verify that the following service accounts have been created:

User name	Purpose	Permissions
<DOMAIN>\ FT-WAP-SVC	Windows Azure Pack service account. Account used to run Web Sites and Portal services.	N/A

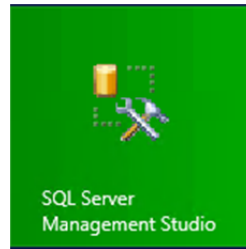
### Groups

No specific groups are required for this component.

## Configure SQL Instance Permissions

Perform the following steps on a SQL Server cluster virtual machine.

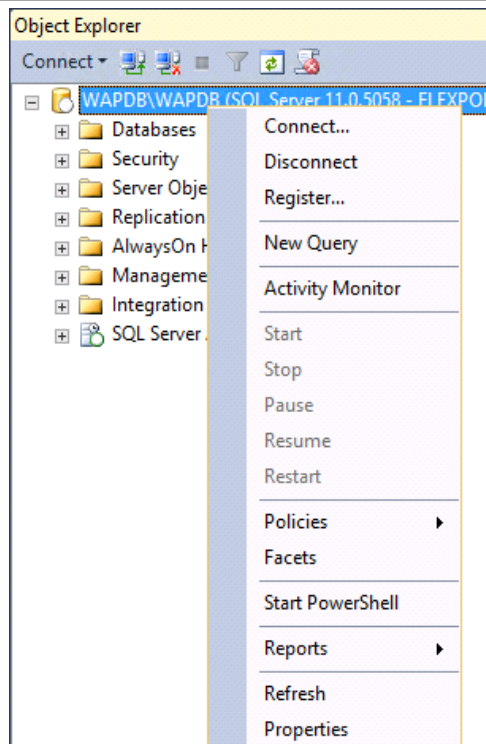
Open the SQL Server Management Studio.



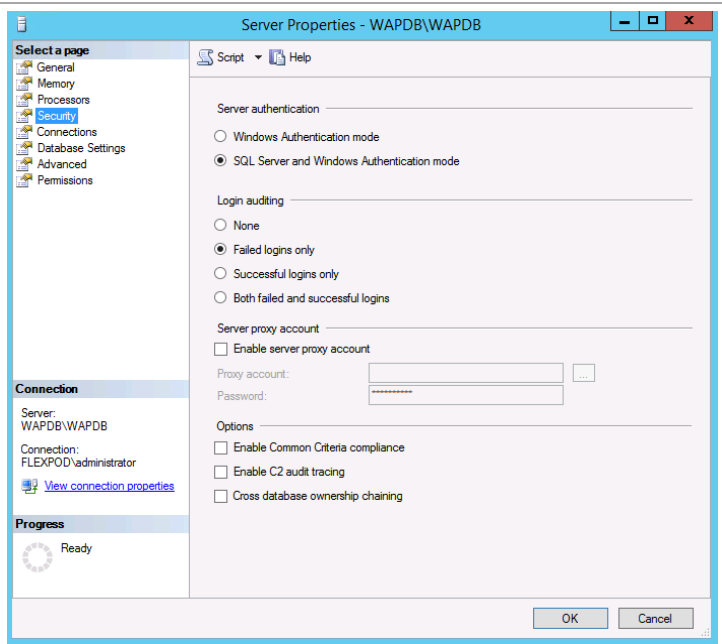
On the **Connect to Server** page, input the connection values for the WAPDB instance. Select **Connect** to connect to the instance.



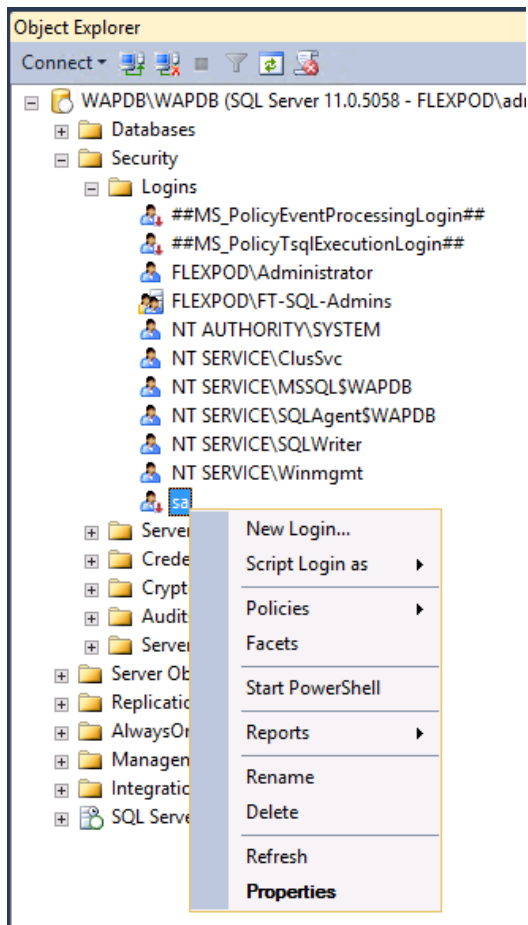
Right-click the WAPDB instance, and select **Properties**.



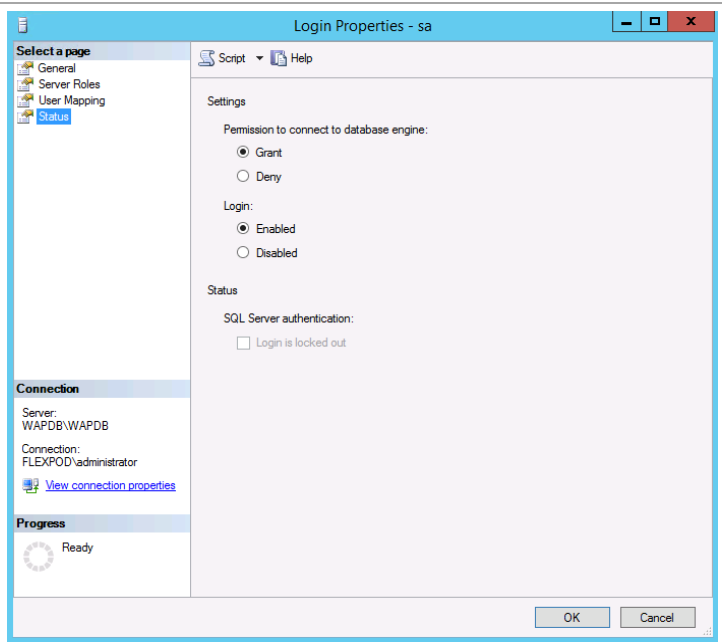
In the **Server Properties** window, select **Security**. Ensure that **SQL Server and Windows Authentication** radio button is selected. Click **OK**.



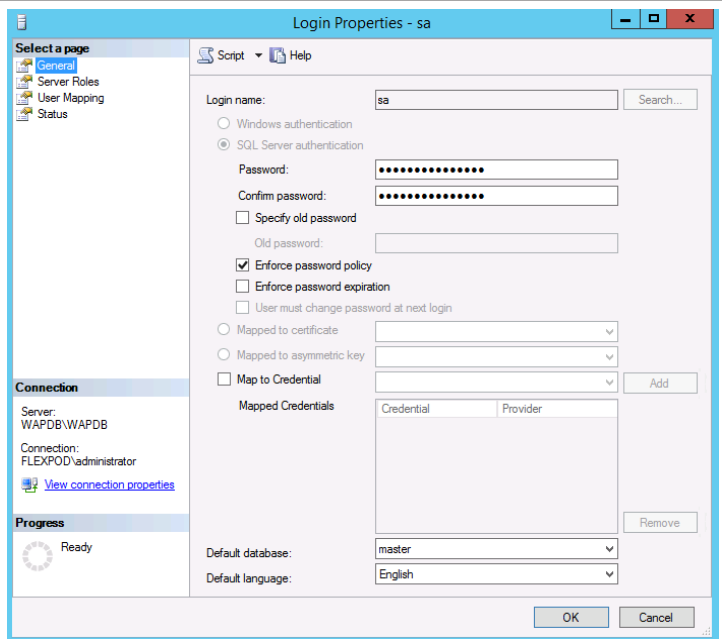
Expand **Security > Logins**. Right-click on the **sa** account and select **Properties**.



In the **Login Properties** window, select **Status** on the left-hand side. Under **Login**, ensure **Enabled** is selected.



Select **General**. Enter a **password** and confirm it. Click **OK** to continue.

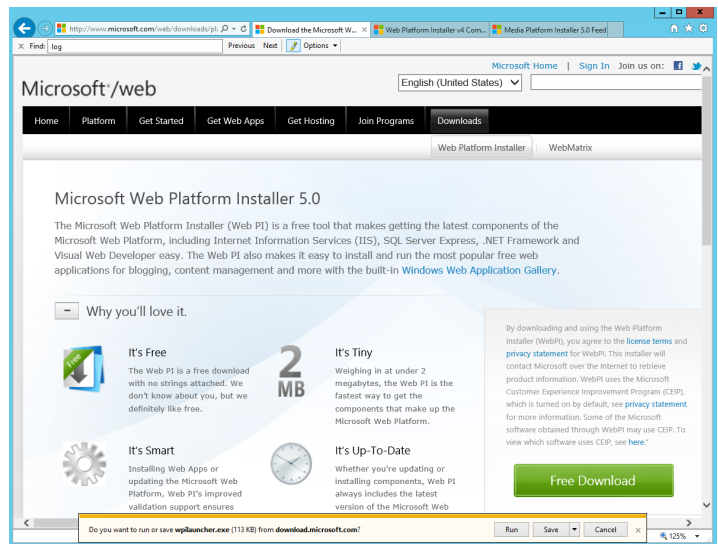


## Download Offline Cache

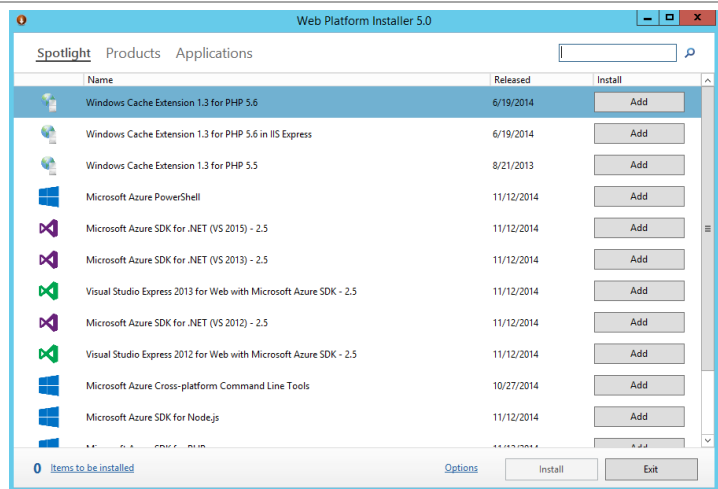
WAP can be installed either via an online GUI or via command line. These instructions assume the use of the command line. Using the command line requires that you first create an offline cache of the components that will be installed. A Windows Server 2012 or 2012 R2 server with internet connectivity is required for obtaining these files. All files should be copied to the same parent directory as they share a subdirectory structure. For ease of installation, this should be a file share accessible by all WAP virtual machines.

Perform the following steps on a Windows Server 2012 or 2012 R2 server.

Open up Internet Explorer and navigate to - <http://www.microsoft.com/web/download/s/platform.aspx>  
Click **Free Download**.  
When the “Do you want to run or save” windows pops up, click **Run**.

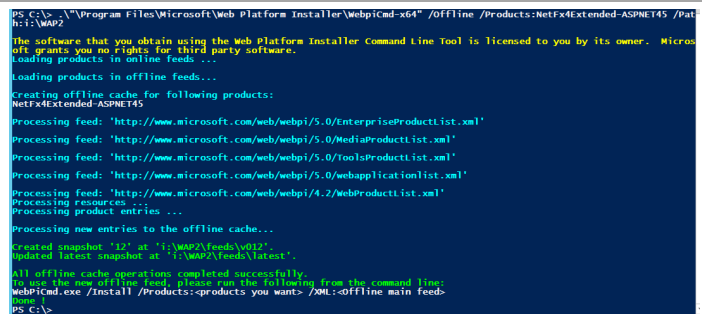


When the installation completes, you will be presented with a window from which you can chose installation options. Click **Exit** to continue.



Download the .NET 4.5 Extended with ASP.NET files with this command:

```
.\ "C:\Program Files\Microsoft\Web Platform Installer\WebPiCmd-x64" /Offline /Products:NetFx4Extended-ASPNET45 /Path:<offline cache directory>
```



Here are the commands to download the other required files to the offline cache directory.

For more information about downloading to the offline cache, see [www.iis.net/learn/install/web-platform-installer/web-platform-installer-v4-command-line-webpicmdexe-rtw-release](http://www.iis.net/learn/install/web-platform-installer/web-platform-installer-v4-command-line-webpicmdexe-rtw-release)

```
.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:IIS7 /Path:<offline cache
directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_AdminSite /Path:<offline
cache directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_WindowsAuthSite
/Path:<offline cache directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_AdminAPIAndServiceProviders_B
undle /Path:<offline cache directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_TenantSite /Path:<offline
cache directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_AuthSite /Path:<offline cache
directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_Tenant_PublicAPI
/Path:<offline cache directory>

.\"C:\Program Files\Microsoft\Web Platform
Installer\WebPicmd-x64" /Offline
/Products:WAP_TenantAPI /Path:<offline
cache directory>
```

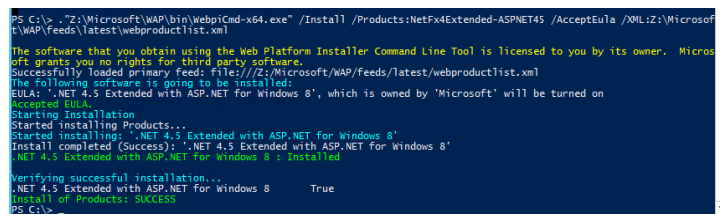
## Deploy .NET 4.5 Extended with ASP.NET

Perform the following steps on all WAP virtual machines.

From an elevated PowerShell window, enter this command:

```
."<offline cache
directory>\bin\Webpicmd-
x64.exe" /Install
/Products:NetFx4Extended-
ASPNET45 /AcceptEula
/XML:<offline cache
directory>\feeds\latest\webprod
uctlist.xml
```

Make sure the component successfully installed.



```
PS C:\> "Z:\Microsoft\WAP\bin\Webpicmd-x64.exe" /Install /Products:NetFx4Extended-ASPNET45 /AcceptEula /XML:Z:\Microsof
t\WAP\Feeds\latest\webproductlist.xml

The software that you obtain using the Web Platform Installer Command Line Tool is licensed to you by its owner. Microso
ft grants you no rights for third party software.
Successfully loaded primary feeds: files//Z:/Microsoft/WAP/Feeds/latest/webproductlist.xml
The following software is going to be installed:
EULA: '.NET 4.5 Extended with ASP.NET for Windows 8', which is owned by 'Microsoft' will be turned on
Accepted Eula
Starting Installation
Started installing Products...
Started installing: '.NET 4.5 Extended with ASP.NET for Windows 8'
Install completed (Success): '.NET 4.5 Extended with ASP.NET for Windows 8'
.NET 4.5 Extended with ASP.NET for Windows 8 : Installed

Verifying successful installation...
.NET 4.5 Extended with ASP.NET for Windows 8 True
Install of Products: Success
PS C:\>
```



## Deploy IIS Recommended Configuration

Perform the following steps on all WAP virtual machines.

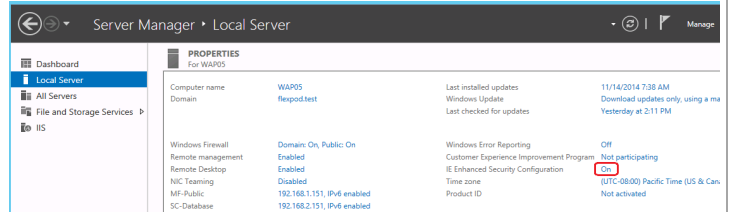
From an elevated PowerShell window, enter this command:

```
."<offline cache
directory>\bin\WebpiCmd-
x64.exe" /Install
/Products:IIS7 /AcceptEula
/XML:<offline cache
directory>\feeds\latest\webprod
uctlist.xml
```

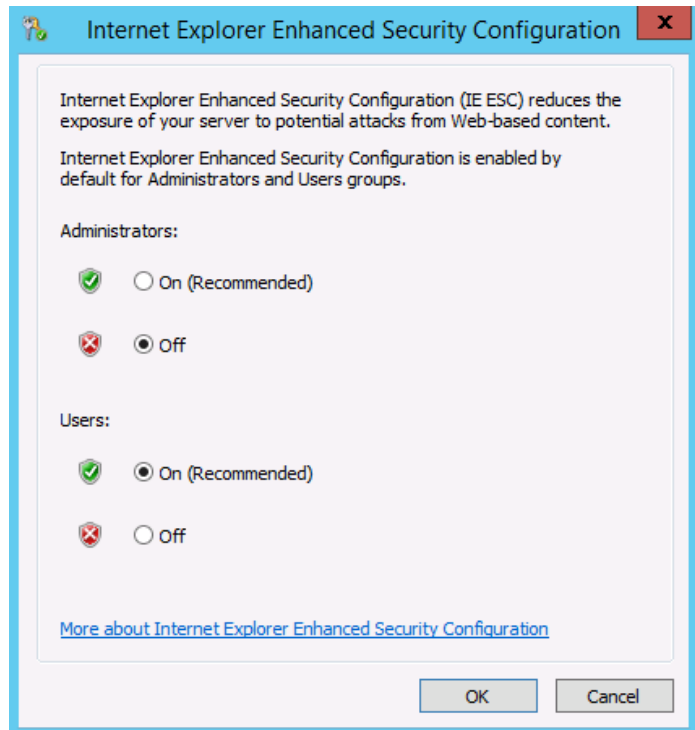
Make sure all components successfully installed.

```
Verifying successful installation...
IIS: WAS Process Model True
IIS: WAS Configuration API True
IIS: WAS .NET Environment True
IIS: Static Content True
IIS: Default Document True
IIS: Directory Browsing True
IIS: HTTP Errors True
IIS: HTTP Logging True
IIS: Logging Tools True
IIS: Request Monitor True
IIS: Request Filtering True
IIS: Static Content Compression True
IIS: ISAPI Extensions True
IIS: ISAPI Filters True
IIS: Management Console True
IIS: .NET Extensibility True
IIS: ASP.NET True
IIS Recommended Configuration True
Install of Products: SUCCESS
PS C:\>
```

On Service Manager, change the **IE Enhanced Security Configuration** for the Administrator from on to off by clicking **On**.



Under **Administrators** click the radio button by **Off**. Click **OK** to continue.



## 27.3 Installation

You can install the components in any order, although you will not be able to open the management portal for administrators or tenants until you have installed and configured the Service Management API and authentication sites. The recommended installation order is:

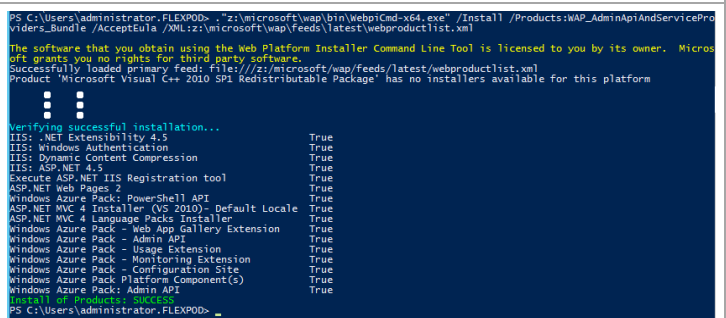
1. Service Management APIs
2. Authentication Sites
3. Management Portals

### Administration API

Perform the following steps on each Administration API virtual machine (WAP05, WAP05b).

From an elevated PowerShell window, enter this command:

```
. "<offline cache
directory>\bin\WebpiCmd-
x64.exe" /Install
/Products:WAP_AdminApiAndService
Providers_Bundle /AcceptEula
/XML:<offline cache
directory>\feeds\latest\webprod
uctlist.xml
```

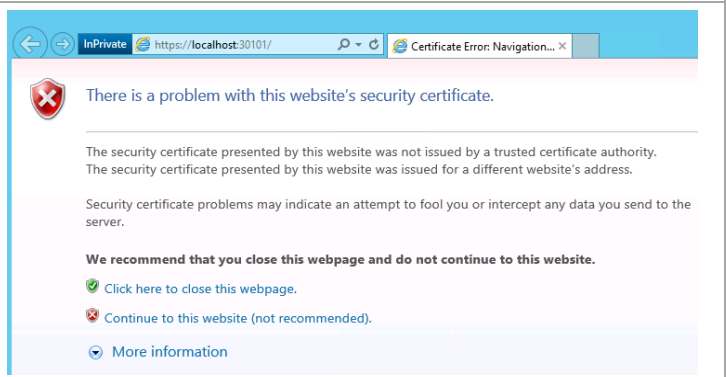


```
PS C:\Users\Administrator.FLEXPOD> . "z:\microsoft\wap\bin\WebpiCmd-x64.exe" /Install /Products:WAP_AdminApiAndServicePro
viders_Bundle /AcceptEula /XML:z:\microsoft\wap\feeds\latest\webproductlist.xml
The software that you obtain using the Web Platform Installer Command Line Tool is licensed to you by its owner. Microso
ft grants you no rights for third party software.
Successfully loaded primary feed: file:///z:/microsoft/wap/feeds/latest/webproductlist.xml
Product 'Microsoft Visual C++ 2010 SP1 Redistributable Package' has no installers available for this platform

Verifying successful installation...
IIS: .NET Extensibility 4.5 True
IIS: Windows Authentication True
IIS: Dynamic Content Compression True
IIS: ASP.NET 4.5 True
Execute ASP.NET IIS Registration tool True
ASP.NET Web Pages 2 True
Windows Azure Pack: PowerShell API True
ASP.NET MVC 4 Installer (VS 2010) - Default Locale True
ASP.NET MVC 4 Language Packs Installer True
Windows Azure Pack - Web App Gallery Extension True
Windows Azure Pack - Admin API True
Windows Azure Pack - Usage Extension True
Windows Azure Pack - Monitoring Extension True
Windows Azure Pack - Configuration Site True
Windows Azure Pack Platform Component(s) True
Windows Azure Pack: Admin API True

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

Internet Explorer will automatically launch and attempt to open the configuration page. Click **Continue to this website (not recommended)**.



On the **Database Server Setup** page enter the following information:

**Server Name** – SQL Server and database instance name for the WAP database

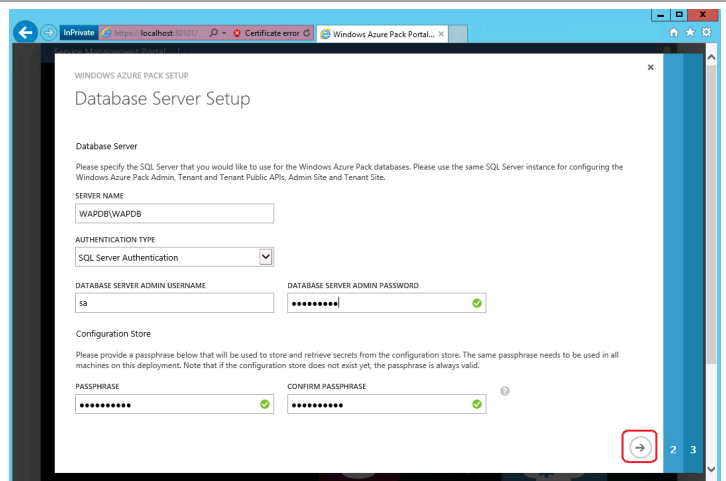
**Authentication Type** – select SQL Server Authentication

**Database Server Admin Username** – enter **sa** as the user name.

**Database Server Admin Password** – enter appropriate password

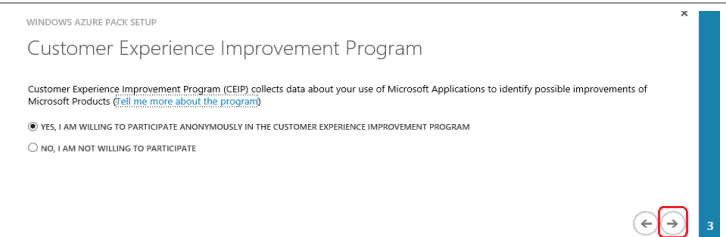
**Passphrase** – enter and confirm a passphrase

Click the **right arrow** to continue.

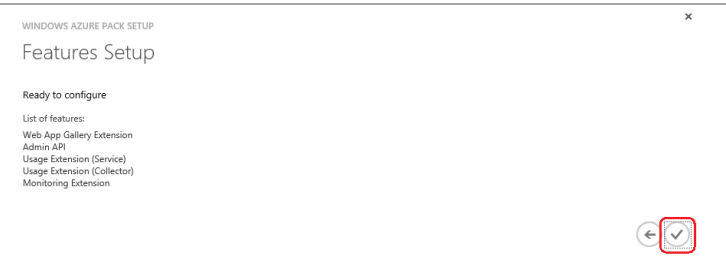


On the **Customer Experience Improvement Program** page select the radio button according to your willingness to participate.

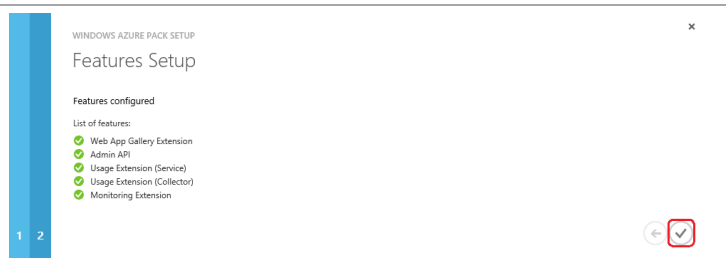
Click the **right arrow** to continue.



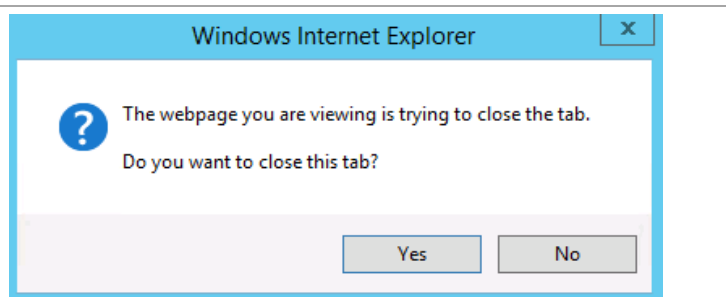
On the **Feature Setup** page review your entries and click the **check mark** to start the configuration.



All features will show a check mark upon successful installation. Click the **check mark** to complete the installation process.



A warning window will display. Click **Yes** to continue. Repeat for additional Administration API virtual machines.



## Tenant API

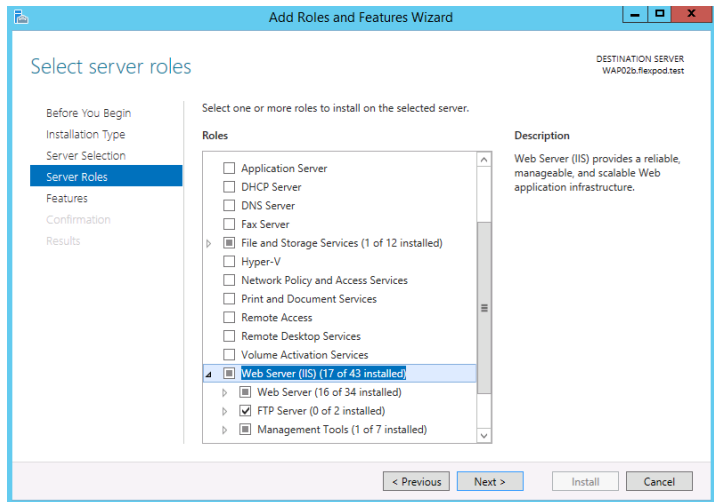
Perform the following steps on each Tenant API virtual machine (WAP04, WAP04b).

From an elevated PowerShell window, enter this command:

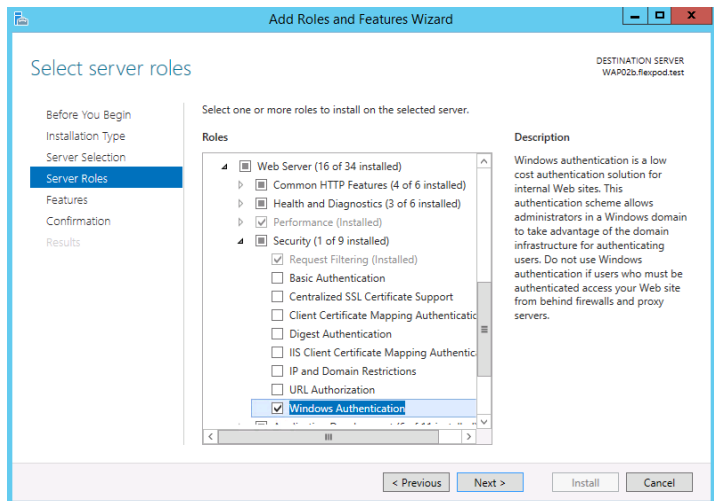
```
. "<offline cache
directory>\bin\WebpiCmd-
x64.exe" /Install
/Products:WAP_TenantAPI
/AcceptEula /XML:<offline cache
directory>\feeds\latest\webprod
uctlist.xml
```

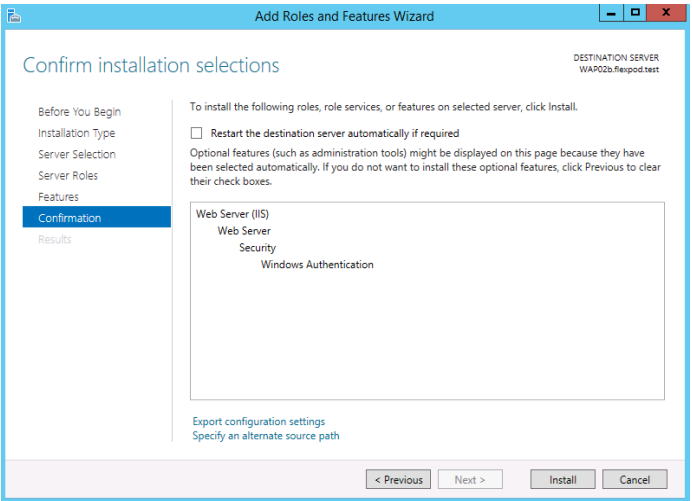
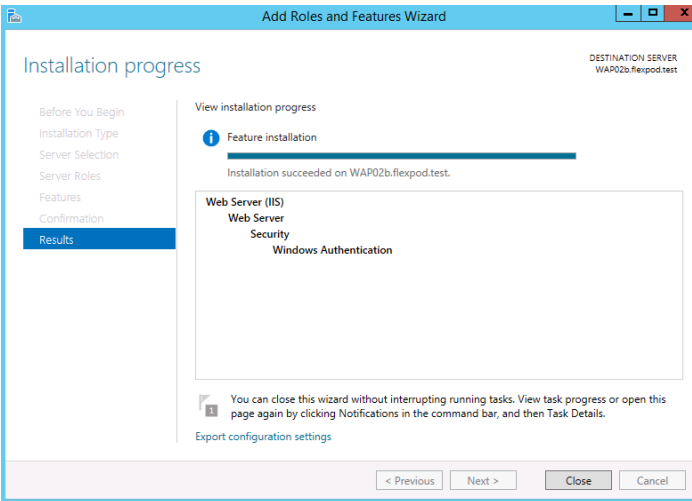
```
PS C:\Users\administrator.FLEXP04> "z:\microsoft\wap\bin\WebpiCmd-x64.exe" /Install /Products:WAP_TenantAPI /AcceptEula
/XML:z:\microsoft\wap\feeds\latest\webproductlist.xml
The software that you obtain using the Web Platform Installer Command Line Tool is licensed to you by its owner. Micros
oft grants you no rights for third party software.
Successfully loaded primary Feeds: File:///z:/microsoft/wap/feeds/latest/webproductlist.xml
Product 'Microsoft Visual C++ 2010 SP1 Redistributable Package' has no installers available for this platform
:
:
:
:
Verifying successful installation...
IIS: .NET Extensibility 4.5 True
IIS: Windows Authentication True
IIS: ASP.NET 4.5 True
Execute ASP.NET IIS Registration tool True
ASP.NET Web Pages 2 True
ASP.NET MVC 4 Installer (VS 2010)- Default Local True
ASP.NET MVC 4 Language Packs Installer True
Windows Azure Pack - Tenant API True
Install of Products: SUCCESS
PS C:\Users\administrator.FLEXP04>
```

From **Server Manager** launch **Manage > Add Roles and Features**. Accept the default responses until you get to **Server Roles**. Scroll down to **Web Server (IIS)** and expand it.



Expand **Web Server**. Expand **Security**. Click the check box by **Windows Authentication**. Click **Next** until you reach the **Confirmation** page.



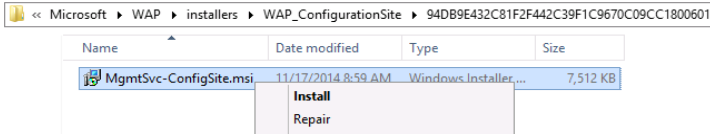
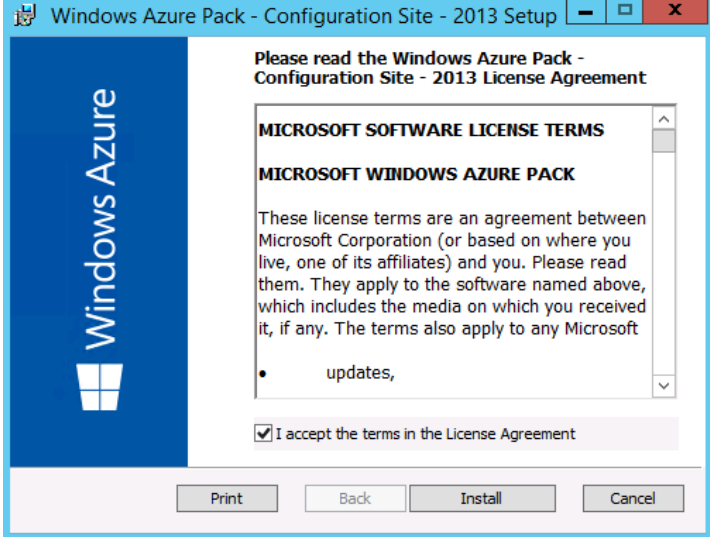
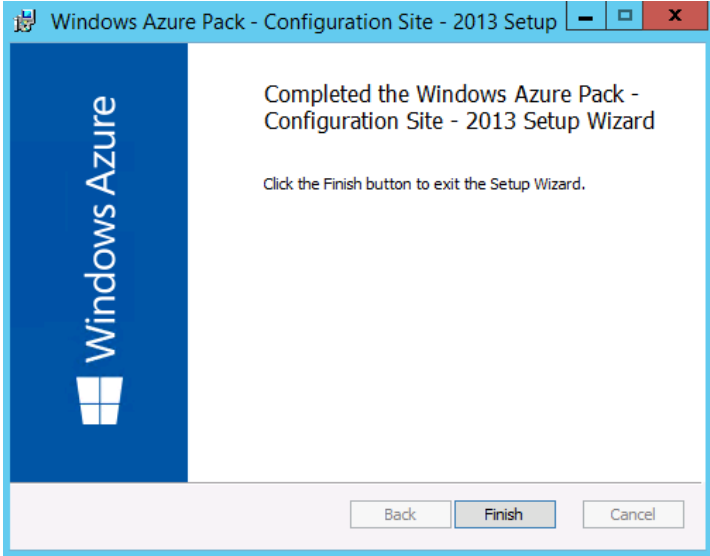
<p>On the <b>Confirmation</b> page, click <b>Install</b>.</p>	
<p>Upon successful installation, click <b>Close</b>.</p>	
<p>Complete the <b>Database Server Setup</b>.</p>	

## Database Server Setup

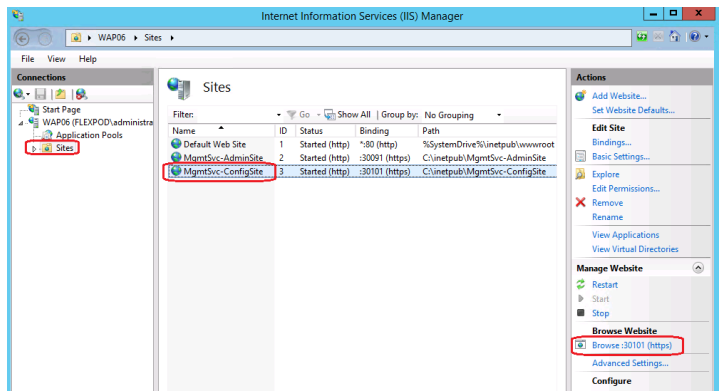
These instructions need to be followed on the following VMs:

- Tenant API
- Tenant Public API
- Administration Authentication
- Tenant Authentication
- Administration Site
- Tenant Site

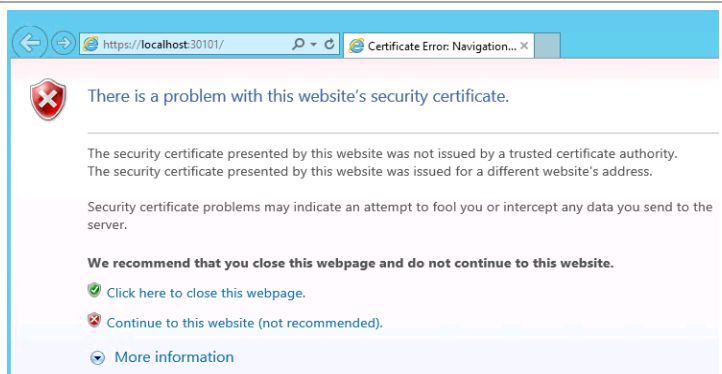
After the respective WAP product has been installed, perform the following steps to configure the connection from the VM to the WAP database.

<p>Navigate to the <b>Installers</b> subdirectory of the offline cache directory. Expand the <b>WAP_ConfigurationSite</b> subdirectory and expand its only subdirectory which is represented by a GUID. Right-click on <b>MgmtSvc-ConfigSite.msi</b> and select <b>Install</b>.</p>	
<p>On the license agreement window select the check box by <b>I accept the terms in the License Agreement</b> and click <b>Install</b>.</p>	
<p>When the installation completes, click <b>Finish</b>.</p>	
<p>Repeat the above steps for the MgmtSvc-PowerShellApi.msi file located at <b>&lt;offline cache directory&gt;\installers\WAP_PowerShellAPI\&lt;GUID&gt;\MgmtSvc-PowerShellAPI.msi</b>.</p>	

Launch the Internet Information Server (IIS) Manager console. Expand the connection and select **Sites**. Click the **AdminSite**. Under **Actions** select **Browse :30101 (https)**.



Internet Explorer will open and a web page saying **There is a problem with this website's security certificate**. Click on **Continue to this website (not recommended)**.



Proceed to the steps to configure the admin web site.

On the **Database Server Setup** page enter the following information:

**Server Name** – SQL Server and database instance name for the WAP database

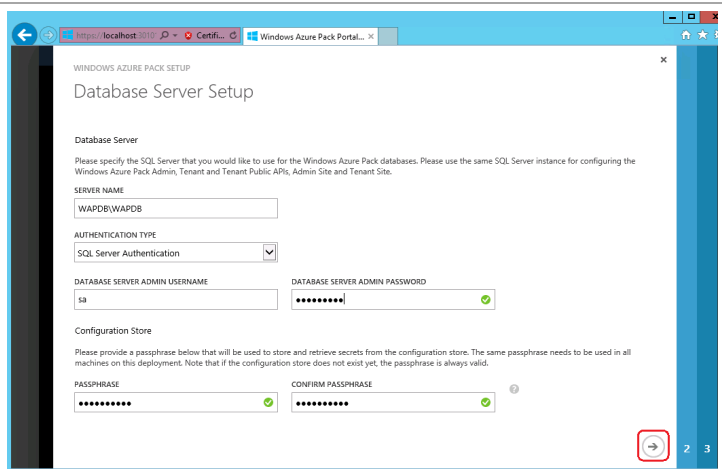
**Authentication Type** – select SQL Server Authentication

**Database Server Admin Username** – enter **sa** as the user name.

**Database Server Admin Password** – enter appropriate password

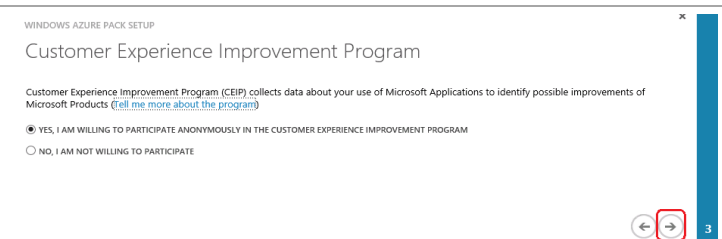
**Passphrase** – enter and confirm a passphrase

Click the **right arrow** to continue.

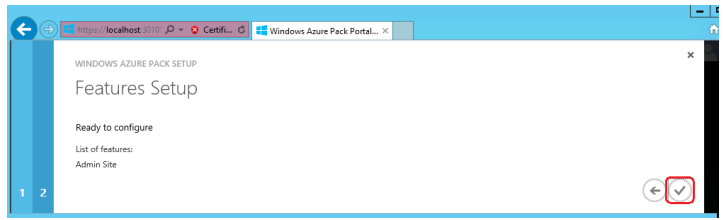


On the **Customer Experience Improvement Program** page select the radio button according to your willingness to participate.

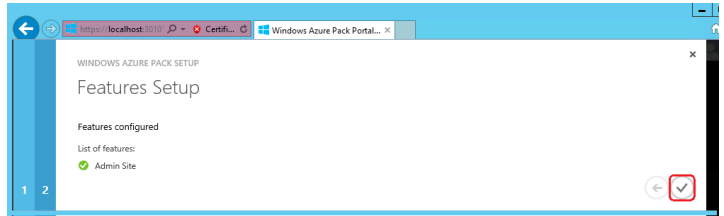
Click the **right arrow** to continue.



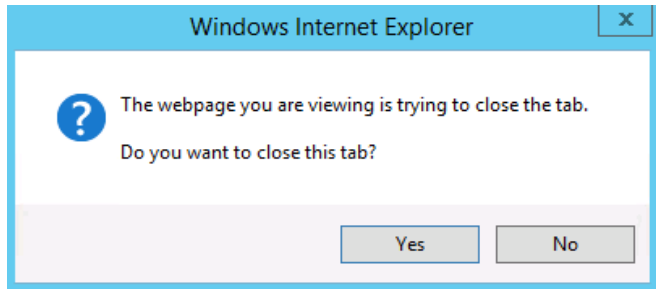
On the **Feature Setup** page review your entries and click the **check mark** to start the configuration.



All features will show a check mark upon successful installation. Click the **check mark** to complete the installation process.



A warning window will display. Click **Yes** to continue. Repeat for additional WAP virtual machines.



## Tenant Public API

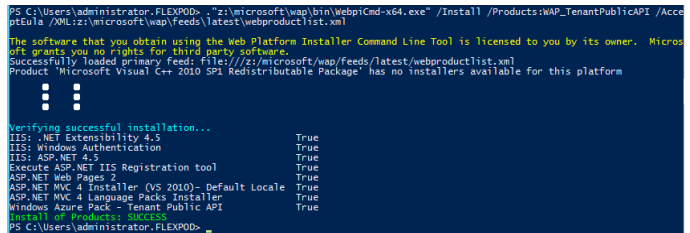
Perform the following steps on each Tenant Public API virtual machine (WAP03, WAP03b).

From an elevated PowerShell window, enter this command:

```

."<offline cache
directory>\bin\WebpiCmd-
x64.exe" /Install
/Product:WAP_TenantPublicAPI
/AcceptEula /XML:<offline cache
directory>\feeds\latest\webprod
uctlist.xml

```



Complete the **Database Server Setup**.





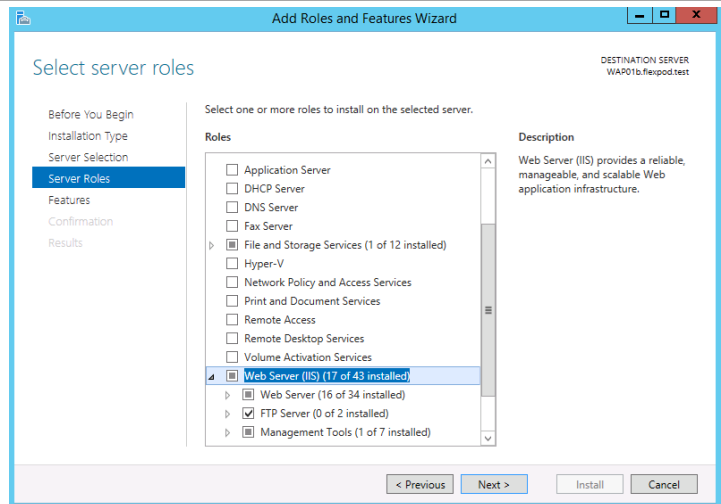
## Tenant Site

Perform the following steps on each Tenant Site virtual machine (WAP01, WAP01b).

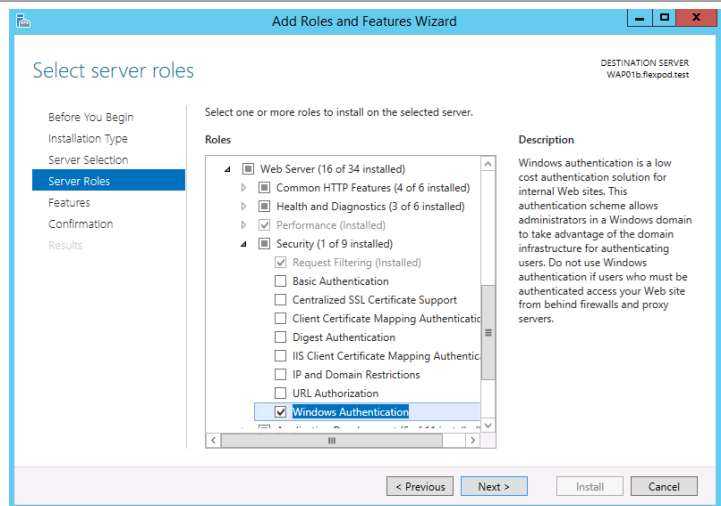
From an elevated PowerShell window, enter this command:  
.`"<offline cache directory>\bin\WebpiCmd-x64.exe" /Install /Products:WAP_TenantSite /AcceptEula /XML:<offline cache directory>\feeds\latest\webproductlist.xml`

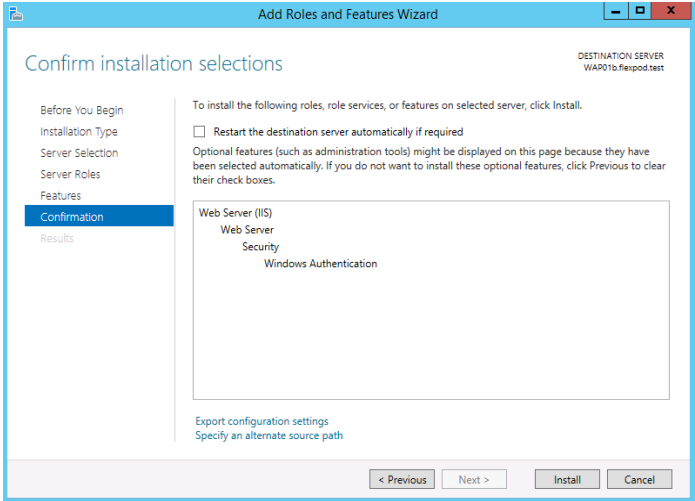
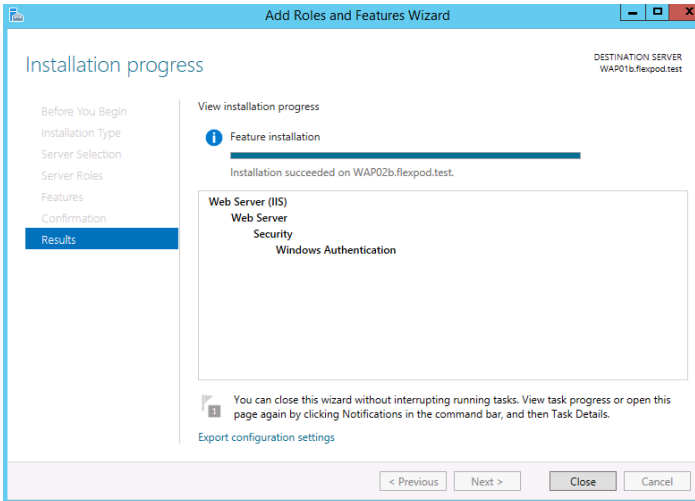
```
PS C:\Users\administrator_FLEXP00> "Z:\Microsoft\WAP\bin\WebpiCmd-x64.exe" /Install /Products:WAP_TenantSite /AcceptEula /XML:Z:\Microsoft\WAP\Feeds\latest\webproductlist.xml
The software that you obtain using the Web Platform Installer Command Line Tool is licensed to you by its owner. Microsoft grants you no rights for third party software.
Successfully loaded primary Feeds Files://Z:\Microsoft\WAP\Feeds\latest\webproductlist.xml
The following software is going to be installed:
:
:
:
:
Verifying successful installation...
IIS: .NET Extensibility 4.5 True
IIS: Basic Authentication True
IIS: Dynamic Content Compression True
IIS: ASP.NET 4.5 True
Execute ASP.NET IIS Registration tool True
ASP.NET Web Pages 2 True
URL Rewrite 2.0 True
ASP.NET MVC 4 Installer (VS 2010) - Default Locale True
ASP.NET MVC 4 Language Packs Installer True
Windows Azure Pack - Tenant Site True
Install of products: WAP01b
PS C:\Users\administrator_FLEXP00>
```

From **Server Manager** launch **Manage > Add Roles and Features**. Accept the default responses until you get to **Server Roles**. Scroll down to **Web Server (IIS)** and expand it.



Expand **Web Server**. Expand **Security**. Click the check box by **Windows Authentication**. Click **Next** until you reach the **Confirmation** page.



<p>On the <b>Confirmation</b> page, click <b>Install</b>.</p>	
<p>On successful installation, click <b>Close</b>.</p>	
<p>Complete the <b>Database Server Setup</b>.</p>	

## 27.4 Post-Installation

Microsoft has several recommended practices that should be followed once installation of the WAP components are completed. They can be found here - <http://msdn.microsoft.com/en-us/library/jj902594.aspx>.

## 28 Complete the NetScaler Network Load Balancer Configuration for the WAP Components

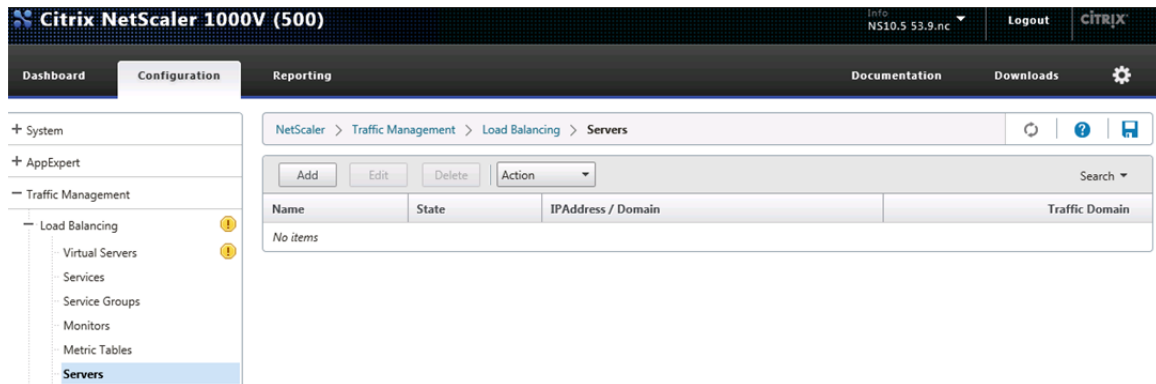
1. Log in to the NetScaler primary server.

## 28.2 Create the Servers that will be Load Balanced

Create Server entries for the following list of WAP component servers

Server Name	IP Address
SCSFP01	192.168.1.51
SCSFP02	192.168.1.52
WAP01A	192.168.1.111
WAP01B	192.168.1.112
WAP02A	192.168.1.121
WAP02B	192.168.1.122
WAP03A	192.168.1.131
WAP03B	192.168.1.132
WAP04A	192.168.1.141
WAP04B	192.168.1.142
WAP05A	192.168.1.151
WAP05B	192.168.1.152

1. Click the Configuration tab, expand Traffic Management tree, expand Load Balancing and select Servers.



2. Click Add. Enter the server name and IP Address of each WAP component server and click Create.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

### Create Server

Server Name\*  
SCSFP01

IP Address  Domain Name

IPAddress\*  
192 . 168 . 1 . 51  IPv6 ?

Traffic Domain  
[Dropdown] + [Edit]

Enable after Creating

Comments  
[Text Area]

Create Close

3. Repeat this procedure for all WAP component servers.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

NetScaler > Traffic Management > Load Balancing > Servers

Add Edit Delete Action Search

Name	State	IPAddress / Domain	Traffic Domain
WAP05B	Enabled	192.168.1.152	0
WAP05A	Enabled	192.168.1.151	0
WAP04B	Enabled	192.168.1.142	0
WAP04A	Enabled	192.168.1.141	0
WAP03B	Enabled	192.168.1.132	0
WAP03A	Enabled	192.168.1.131	0
WAP02B	Enabled	192.168.1.122	0
WAP02A	Enabled	192.168.1.121	0
WAP01B	Enabled	192.168.1.112	0
WAP01A	Enabled	192.168.1.111	0
SCSFP02	Enabled	192.168.1.52	0
SCSFP01	Enabled	192.168.1.51	0

## 28.3 Create the Load Balancing Service Groups

Service Group Name	Port Number	Server Members
SCSPF-Pool	80	SCSFP01
		SCSFP02
WAP01-Pool	80	WAP01A
		WAP01B
WAP02-Pool	80	WAP02A
		WAP02B
WAP03-Pool	80	WAP03A
		WAP03B
WAP04-Pool	80	WAP04A

		WAP04B
WAP05-Pool	80	WAP05A
		WAP05B

1. Click Service Groups.
2. Click the Add button and enter the Service Group Name and click OK.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

Load Balancing Service Group

**Basic Settings** Help

Name\* CSPPF-Pool

Protocol\* HTTP

Traffic Domain

Cache Type\* SERVER

AutoScale Mode

Cacheable  
 State  
 Health Monitoring  
 AppFlow Logging

Number of Active Connections 0

Comments

OK Cancel

3. Click Members in the Advanced options list.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

Load Balancing Service Group

**Basic Settings** Help

Name	SCSPF-Pool	Cache Type	SERVER
Protocol	HTTP	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Traffic Domain	0	AppFlow Logging	ENABLED
		Number of Active Connections	0
		AutoScale Mode	-

Done

**Advanced**

- + Members
- + Thresholds & Timeouts
- + Settings

4. Click the Service Group Members to configure the member properties.

The screenshot shows the Citrix NetScaler 1000V (500) Configuration page for a Load Balancing Service Group. The page is divided into several sections:

- Basic Settings:** A table with the following values:
 

Name	SCSPF-Pool	Cache Type	SERVER
Protocol	HTTP	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Traffic Domain	0	AppFlow Logging	ENABLED
		Number of Active Connections	0
		AutoScale Mode	-
- Service Group Members:** A section showing "No Service Group Member" with a "Done" button below it.
- Advanced Settings:** A sidebar menu with options:
  - Thresholds & Timeouts
  - Settings
  - Profiles
  - Monitors

5. Select the Server Based option and select the servers name from the drop down list. Enter 80 for the port type. Click Create.

The screenshot shows the Citrix NetScaler 1000V (500) Service Group Member configuration page. The page is divided into several sections:

- Service Group Member:** A section with radio buttons for "IP Based" and "Server Based" (selected).
- Server Name\*:** A dropdown menu with "SCSPF01" selected.
- Port\*:** A text input field with "80" entered.
- Weight:** A text input field with "1" entered.
- Server Id:** A text input field.
- Hash Id:** A text input field.
- State:** A checkbox that is checked.
- Buttons:** "Create" and "Close" buttons at the bottom.

6. Click Service Group Members again to enter the second server for this group.

The screenshot shows the Citrix NetScaler 1000V (500) Configuration page for a Load Balancing Service Group. The page is divided into several sections:

- Basic Settings:**
  - Name: SCSPF-Pool
  - Protocol: HTTP
  - State: ENABLED
  - Traffic Domain: 0
  - Cache Type: SERVER
  - Cacheable: NO
  - Health Monitoring: YES
  - AppFlow Logging: ENABLED
  - Number of Active Connections: 0
  - AutoScale Mode: -
- Service Group Members:**
  - 1 Service Group Member
- Advanced:**
  - Threats & Timeouts
  - Settings
  - Profiles
  - Monitors

Buttons for "Back", "Done", and "Help" are visible.

7. Click Add to enter the second server.

The screenshot shows the Citrix NetScaler 1000V (500) Service Group Members Binding page. The page displays a table of service group members:

IP Address	Server Name	Port	Weight	Server Id	Hash Id	State
192.168.1.51	SCSPF01	80	1	None	0	ENABLED

Buttons for "Add", "Edit", "Unbind", "Monitor Details", and "Close" are visible. A search bar is also present.

8. Select the Server Based option and select the servers name from the drop down list. Enter 80 for the port type. Click Create.

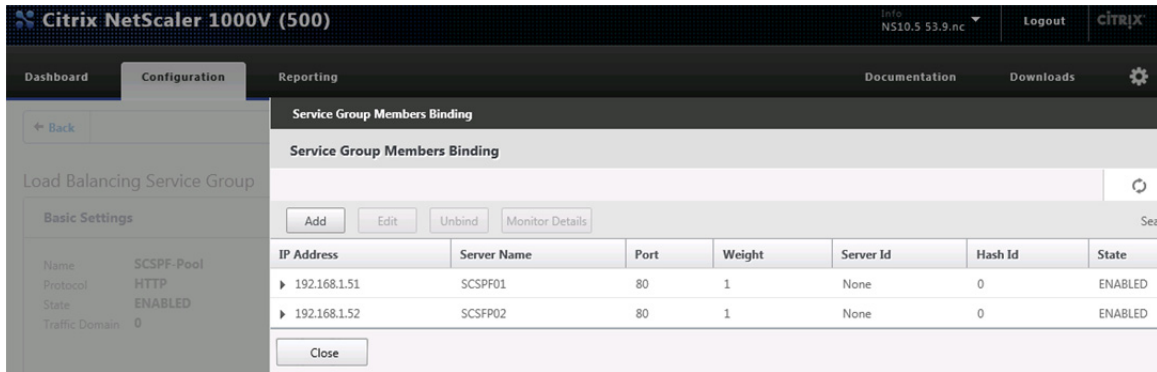
The screenshot shows the Citrix NetScaler 1000V (500) Service Group Member configuration page. The page is divided into several sections:

- Service Group Member:**
  - IP Based  Server Based
  - Server Name\*: SCSPF02
  - Port\*: 80
  - Weight: 1
  - Server Id: [Empty]
  - Hash Id: [Empty]
  - State

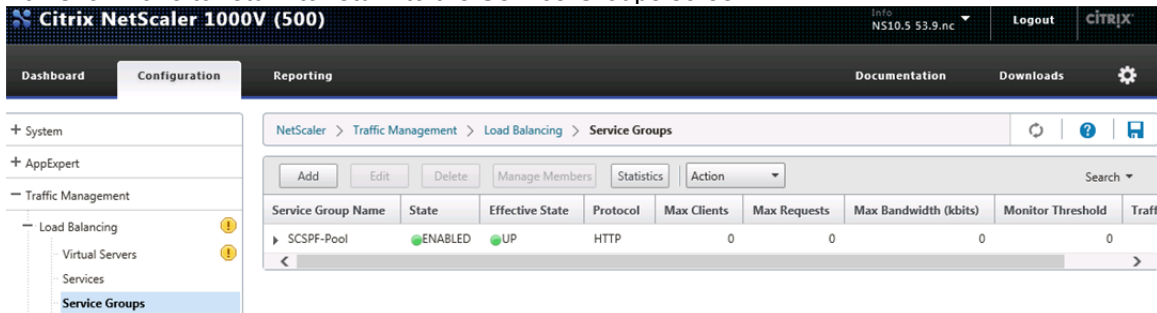
Buttons for "Create" and "Close" are visible.



9. Click Close to return to the Load Balancing Service Group configuration screen.

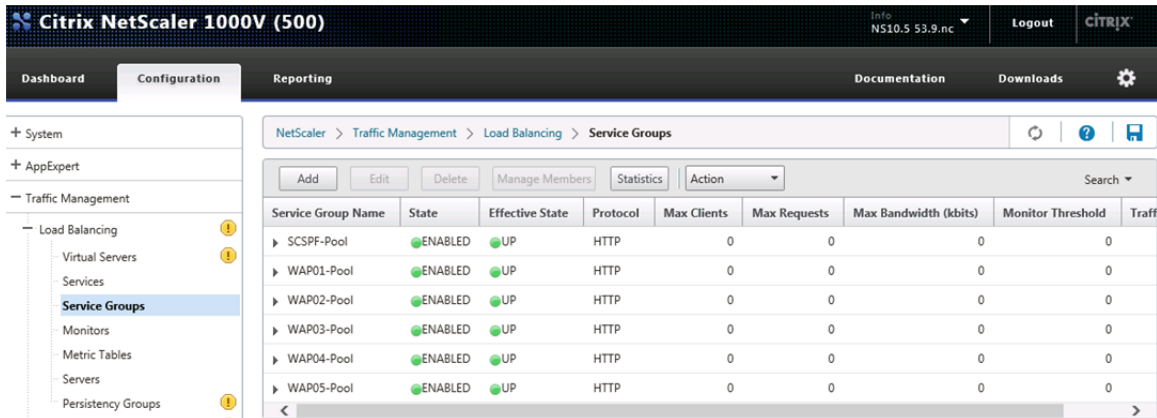


10. Click Done to return to return to the Service Groups screen.



**Note:** Click refresh show the Effective Date of the service group after the service group is created.

**Note:** Repeat this procedure to create the remaining service groups.



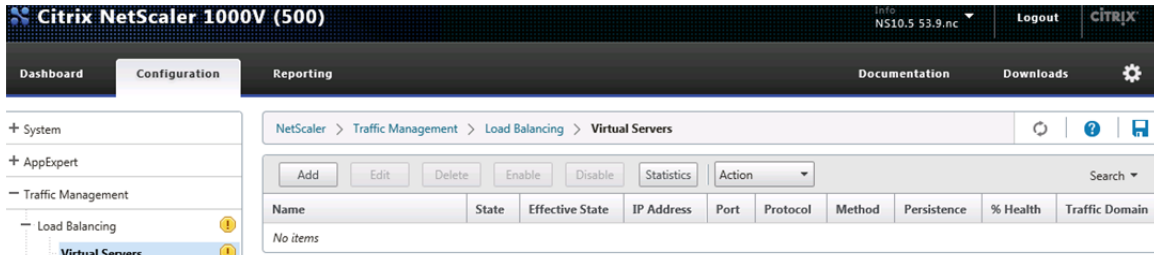
## 28.4 Create Virtual Servers

Create the following Virtual Servers:

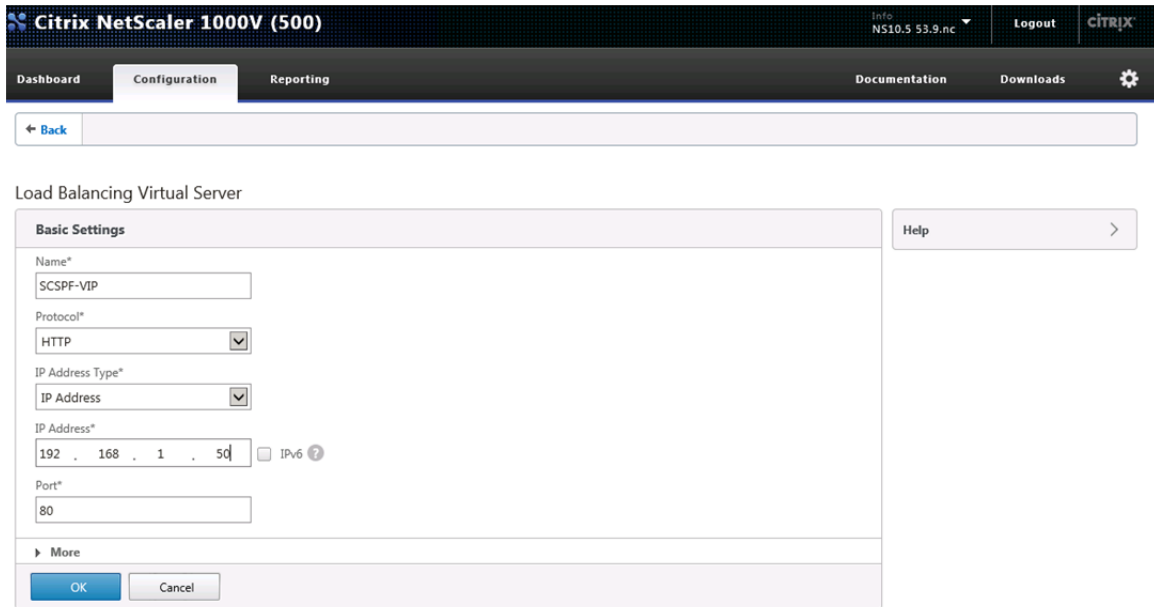
Virtual Server Name	Virtual IP Address	Member Service Groups
SCSPF-VIP	192.168.1.50	SCSPF-Pool
WAP01-VIP	192.168.1.110	WAP01-Pool

WAP02-VIP	192.168.1.120	WAP02-Pool
WAP03-VIP	192.168.1.130	WAP03-Pool
WAP04-VIP	192.168.1.140	WAP04-Pool
WAP05-VIP	192.168.1.150	WAP05-Pool

1. Click Virtual Servers under Load balancing and click Add.



2. Enter the virtual server Name and IP address. Click OK.



3. Click Yes in the confirmation screen to enable the Load Balancing feature.



- Click OK to view the advanced options.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

Load Balancing Virtual Server | [Export as a Template](#)

### Load Balancing Virtual Server

**Basic Settings** Help >

Name: SCSPF-VIP	Listen Priority: -
Protocol: HTTP	Listen Policy Expression: -
State: DOWN	Range: 1
IP Address: 192.168.1.50	Redirection Mode: IP
Port: 80	RHI State: PASSIVE
Traffic Domain: 0	AppFlow Logging: ENABLED

**Service**

No Load Balancing Virtual Server Service Binding >

**OK**

- Click Service Group.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

Load Balancing Virtual Server | [Export as a Template](#)

### Load Balancing Virtual Server

**Basic Settings** Help >

Name: SCSPF-VIP	Listen Priority: -
Protocol: HTTP	Listen Policy Expression: -
State: DOWN	Range: 1
IP Address: 192.168.1.50	Redirection Mode: IP
Port: 80	RHI State: PASSIVE
Traffic Domain: 0	AppFlow Logging: ENABLED

**Service**

No Load Balancing Virtual Server Service Binding >

**Done**

**Advanced**

- [+ Service Group](#)
- [+ Policies](#)
- [+ Method](#)
- [+ Persistence](#)
- [+ Protection](#)

- Click Load Balancing Virtual Server Service Group Binding.

**Citrix NetScaler 1000V (500)** Info NS10.5 53.9.nc Logout citrix

Dashboard Configuration Reporting Documentation Downloads

← Back

Load Balancing Virtual Server | [Export as a Template](#)

### Load Balancing Virtual Server

Basic Settings		Help
Name	SCSPF-VIP	Advanced + Policies + Method + Persistence + Protection + Profiles + Push + Authentication
Protocol	HTTP	
State	DOWN	
IP Address	192.168.1.50	
Port	80	
Traffic Domain	0	
Listen Priority	-	
Listen Policy Expression	-	
Range	1	
Redirection Mode	IP	
RHI State	PASSIVE	
AppFlow Logging	ENABLED	

**Service**

No Load Balancing Virtual Server Service Binding >

**Service Group**

No Load Balancing Virtual Server ServiceGroup Binding >

Done

7. Click “Click to select” to select the Service Group Name for the Virtual Server.

**ServiceGroup Binding**

**ServiceGroup Binding**

Select Service Group Name\*

Click to select > +

Bind Close

8. Select the Service Group Name and click OK.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

ServiceGroup Binding > Service Groups

Service Groups

Add Edit Delete Manage Members Statistics Action

Service Group Name	State	Effective State	Protocol	Max Clients	Max Requests	Max Bandwidth (kbits)	Monitor Threshold
SCSPF-Pool	ENABLED	UP	HTTP	0	0	0	0
WAP01-Pool	ENABLED	UP	HTTP	0	0	0	0
WAP02-Pool	ENABLED	UP	HTTP	0	0	0	0
WAP03-Pool	ENABLED	UP	HTTP	0	0	0	0
WAP04-Pool	ENABLED	UP	HTTP	0	0	0	0
WAP05-Pool	ENABLED	UP	HTTP	0	0	0	0

OK Close

9. Click Bind.

ServiceGroup Binding

ServiceGroup Binding

Select Service Group Name\*

SCSPF-Pool

Bind Close

10. Click Done to complete the Service Group configuration.

Citrix NetScaler 1000V (500) Info NS10.5 53.9.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	SCSPF-VIP	Listen Priority	-
Protocol	HTTP	Listen Policy Expression	-
State	DOWN	Range	1
IP Address	192.168.1.50	Redirection Mode	IP
Port	80	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED

Service

No Load Balancing Virtual Server Service Binding

Service Group

1 Load Balancing Virtual Server ServiceGroup Binding

Done

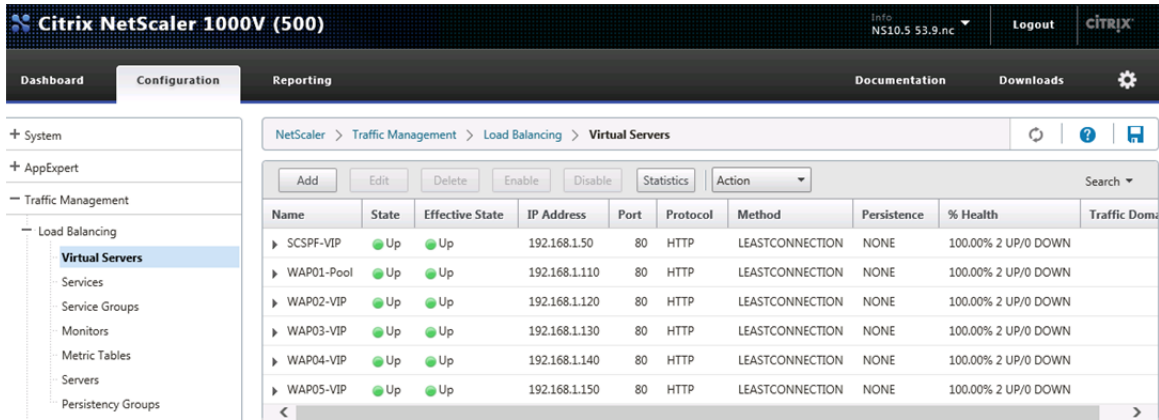
Help

Advanced

- Policies
- Method
- Persistence
- Protection
- Profiles
- Push
- Authentication

11. Click the refresh button to update the status.

**Note:** Repeat this procedure for to create the virtual servers.

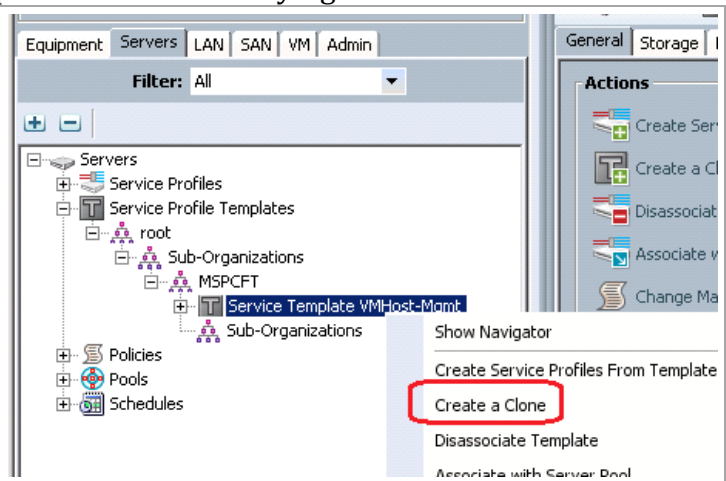


## 29 Deploy App Cluster from Gold Master

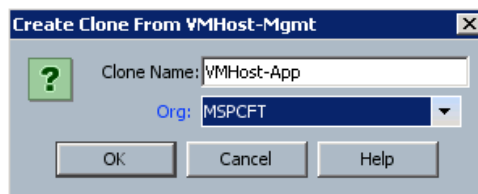
### 29.1 Create Service Profile Template

These steps provide details for creating a service profile template by cloning the previously created service profile template and then modifying it.

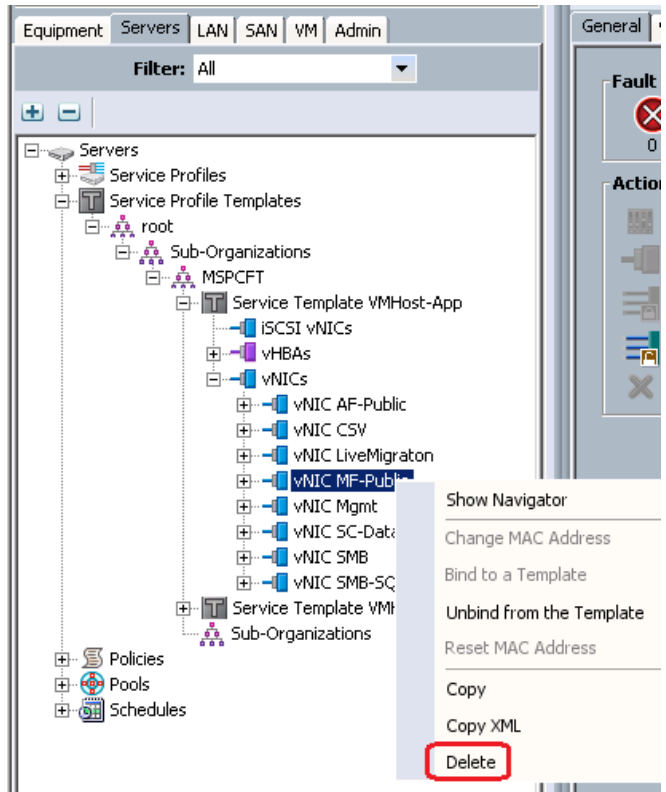
In UCS Manager select the **Servers** tab at the top left window. Select **Servers > Service Profile Templates > root > Sub-Organizations > <suborg> Service Template VMHost-Mgmt**. Right-click and select **Create a Clone**.



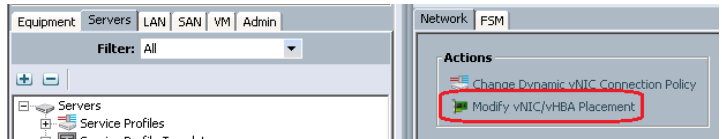
Enter **VMHost-App** for the Clone Name and select the Organization. Click **OK** to create the new Service Profile Template.



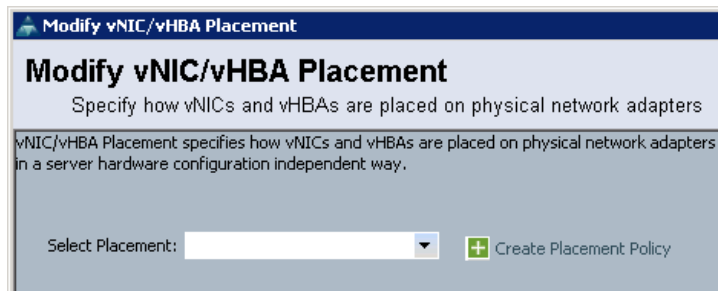
Expand the new template. Expand **vNICs**. Right-click **MF-Public** and select **Delete**. Repeat for the **SC-Database** vNIC.



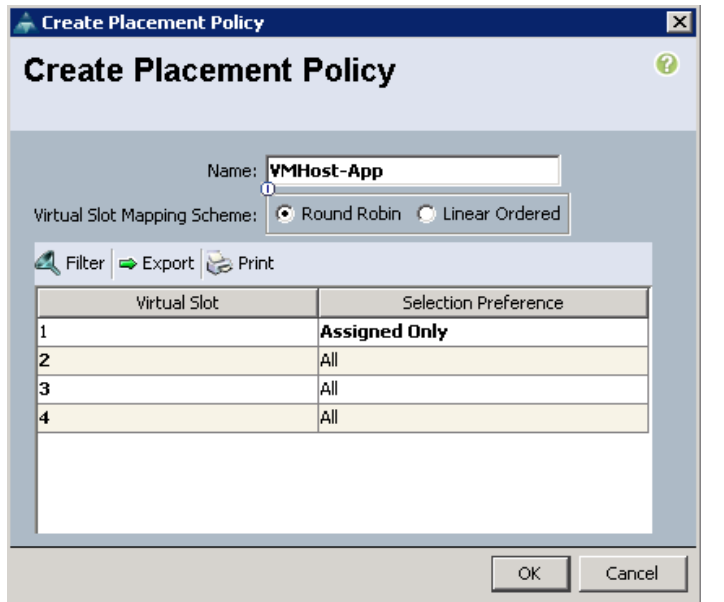
Select **Modify vNIC/vHBA Placement**.



On the Modify vNIC/vHBA Placement page click **Create Placement Policy**.



On the Create Placement Policy page enter a **Name** for the policy. On Virtual Slot 1, select **Assigned Only** for the Selection Preference. Click **OK**.

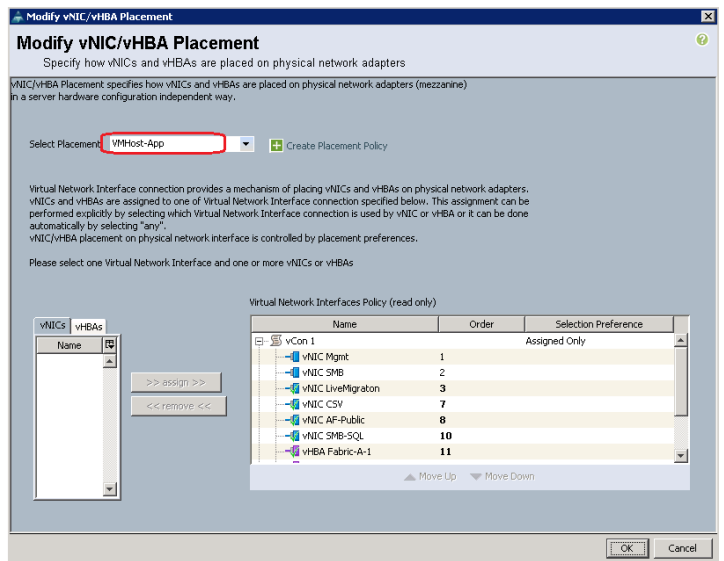


Select the newly created Placement Policy. Select **vCon1** in the Virtual Network Interface Policy. Select the **VM-AF Public** vNIC and click **Assign**.

Place the vNICs in this order:

- Mgmt
- SMB
- LiveMigration
- CSV
- AF-Public
- SMB-SQL

Click **OK**.

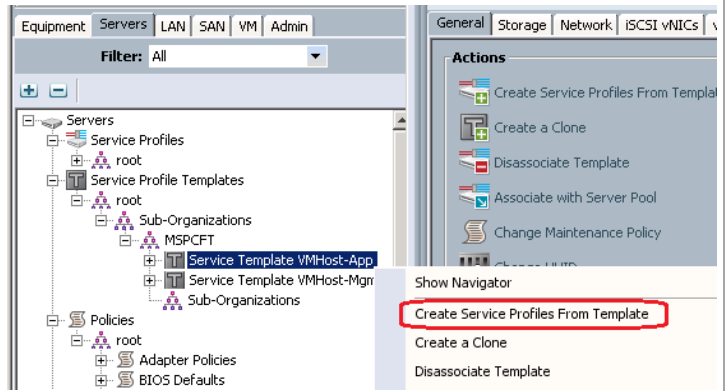


## 29.2 Create Service Profiles

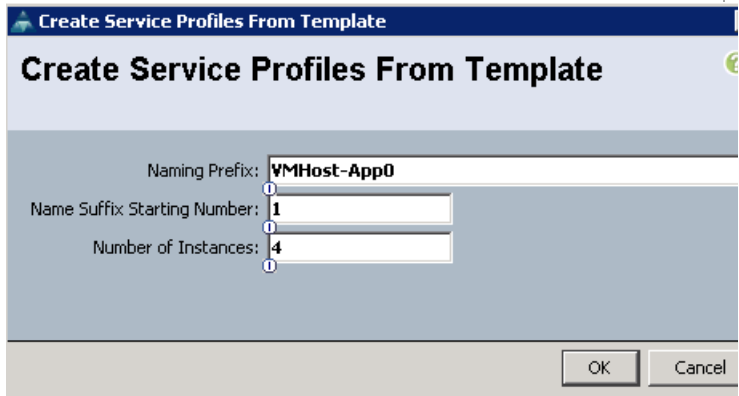
These steps provide details for creating a service profile from a template.



In UCS Manager, Select the **Servers** tab at the top left of the window. Select Service Profile Templates **VMHost-App** in the sub-organization. Right-click and select **Create Service Profile From Template**.



Enter **VMHost-App0** for the service profile prefix. Enter **1** for the Name Suffix Starting Number. Enter **4** for the number of service profile instances to create. Click **OK** to create the service profiles.



### 29.3 Gather the 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 21) vHBA WWPNs for Fabric A and Fabric B

Cisco UCS Service Profile Name	Fabric-A-1 WWPN	Fabric-B-1 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 Sub-Organization> . 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 Fabric-A-1 and vHBA Fabric-B-1 for each service profile in the table above.

## 29.4 FlexClone Boot LUN

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

1. Log into the NetApp Cluster by opening an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Create a new Qtree to hold the boot LUN.

```
qtree create -volume ucs_boot -qtree VMHost-App01
qtree create -volume ucs_boot -qtree VMHost-App02
qtree create -volume ucs_boot -qtree VMHost-App03
qtree create -volume ucs_boot -qtree VMHost-App04
```

3. Using the information from above table, Create igroups

```
igroup create -igroup VMHost-App01 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vsriver infra_svm
igroup create -igroup VMHost-App02 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vsriver infra_svm
igroup create -igroup VMHost-App03 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vsriver infra_svm
igroup create -igroup VMHost-App04 -initiator <vHBA_A WWPN>, <vHBA_B WWPN> -ostype
hyper_v -vsriver infra_svm
```

4. Clone the boot LUN from the goldmaster boot LUN.

```
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-App01/boot.lun
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-App02/boot.lun
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-App03/boot.lun
clone create -volume ucs_boot -SourcePath /goldmaster/boot.lun
-DestinationPath /VMHost-App04/boot.lun
```

5. Map the boot LUN to the new iGroup.

```
lun map -Path /vol/ucs_boot/VMHost-App01/boot.lun -InitiatorGroup VMHost-App01 -lun-id 0
-vsriver infra_svm
lun map -Path /vol/ucs_boot/VMHost-App02/boot.lun -InitiatorGroup VMHost-App02 -lun-id 0
-vsriver infra_svm
lun map -Path /vol/ucs_boot/VMHost-App03/boot.lun -InitiatorGroup VMHost-App03 -lun-id 0
-vsriver infra_svm
lun map -Path /vol/ucs_boot/VMHost-App03/boot.lun -InitiatorGroup VMHost-App04 -lun-id 0
-vsriver infra_svm
```

## 29.5 Boot Service Profiles

Complete the following steps to boot each new service profile.

### All Hosts

1. Back in USCM right-click on one of the newly created service profiles and select **Associate with Server Pool**.
2. From the Pool Assignment box, select the App\_Pool and click OK and OK again to acknowledge.

- Right-click the <Hyper-V hostname> and select KVM Console.
- Click Boot Server, the service profile will then pull a server from the App\_Pool pool, and configure the hardware per the service profile.
- Back in USCM right-click <Hyper-V Hostname>, and select KVM Console.
- Click Boot Server, the service profile will then pull a server from the App\_Pool, and configure the hardware per the service profile.
- When the server has fully booted Windows will enter the out of box experience. Accept the EULA, and click Accept.
- Enter the region and language settings and Click Next.
- Enter a new Administrator Password, and click Finish.
- Repeat for each service profile.

## 29.6 Configure Windows Networking for FlexPod

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

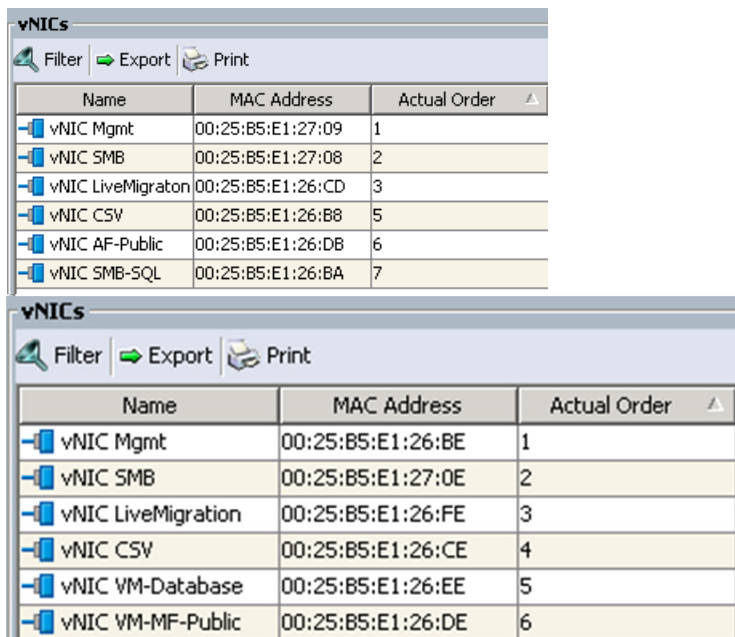
### All Hosts

- In a PowerShell window, type the cmdlet Get-NetAdapter.

```
PS C:\Users\administrator.FLEXPOD> get-netadapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet 6	Cisco VIC Ethernet Interface #6	57	Up	00-25-B5-E1-26-E5	20 Gbps
Ethernet 5	Cisco VIC Ethernet Interface #5	53	Up	00-25-B5-E1-26-C5	20 Gbps
Ethernet 4	Cisco VIC Ethernet Interface #4	49	Up	00-25-B5-E1-27-05	20 Gbps
Ethernet 3	Cisco VIC Ethernet Interface #3	45	Up	00-25-B5-E1-26-B5	20 Gbps
Ethernet 2	Cisco VIC Ethernet Interface #2	21	Up	00-25-B5-E1-26-F5	20 Gbps
Ethernet	Cisco VIC Ethernet Interface	13	Up	00-25-B5-E1-26-D5	20 Gbps

- In the KVM console select Server > Service Profiles > root > Sub-Organizations > MSPCFT > <VMHost-App01> > vNICs.



- Cross-reference the vNICs by MAC address.
- Back in Windows rename the LAN adapter to reflect the network it is associated with.

**Note:** The following PowerShell cmdlet can be used to rename a network adapter

```
2) Rename-NetAdapter "Ethernet" -NewName "Mgmt"
```

5. Set the appropriate IP settings for that adapter.

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

6. Repeat for each eNIC in windows.

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.

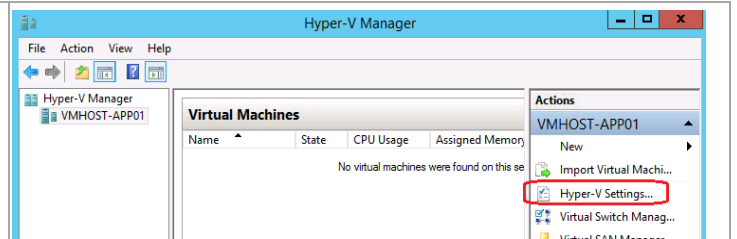
9. The recommended binding order is:

- Mgmt
- SMB
- LiveMigration
- CSV
- AF-Public
- SMB-SQL

## 29.7 Enable Enhanced Session Mode

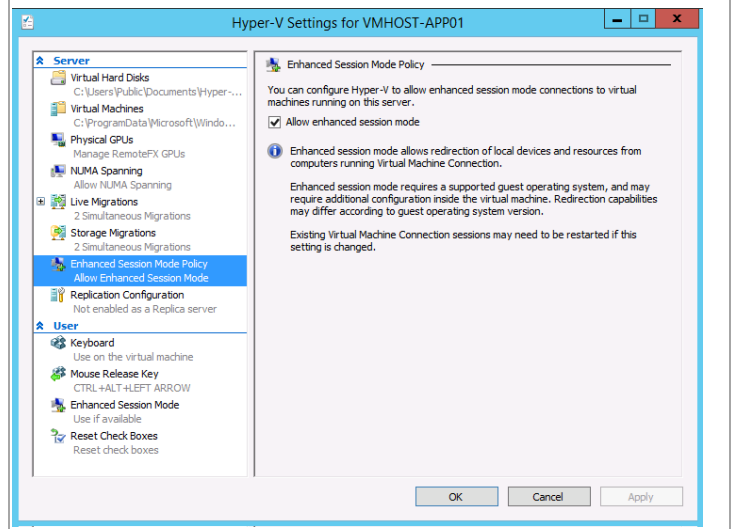
### All Hosts

In the **Hyper-V Manager** console, select **Hyper-V Settings...** under **Actions**.



In the **Hyper-V Settings** page select **Enhanced Session Mode Policy**. Check the box by **Allow enhanced session mode** and click **OK** to accept the change.

Repeat for all Hyper-V Servers.



## 29.8 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.

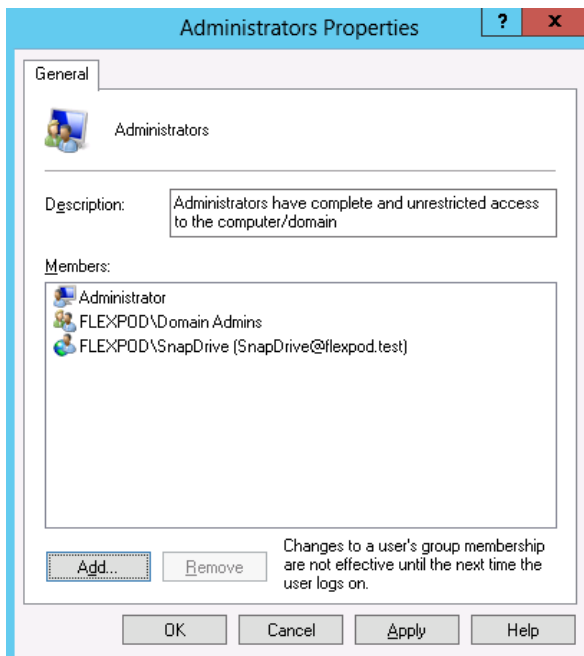
```
Add-Computer -DomainName <domain_name> -Restart
```

## 29.9 Install NetApp SnapDrive

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

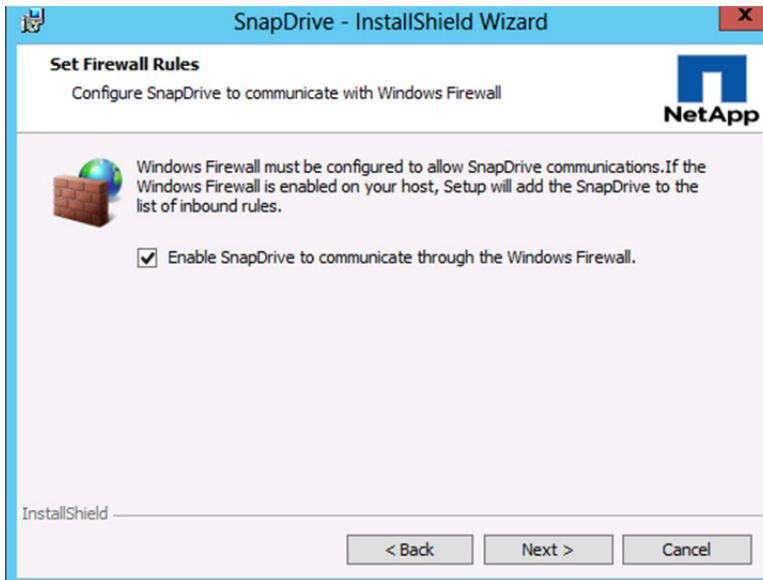
### All App Fabric Hosts

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

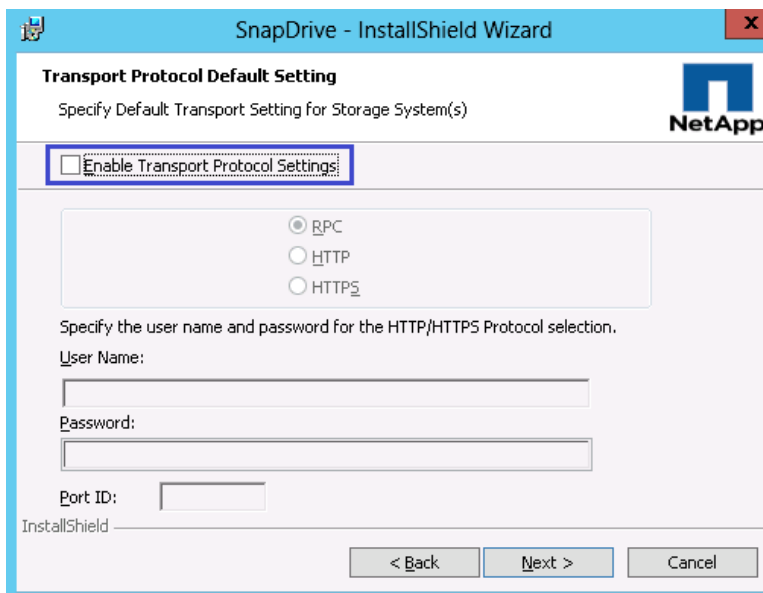


2. Launch the SnapDrive installer - SnapDrive7.0.3\_x64.exe.
3. On the Welcome window click Next.
4. Select the Per Storage System method and click Next.
5. Enter your User Name and Organization information, and click Next.
6. Validate the installation path and click Next.

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 and click Next.
9. Click Next, through the SnapDrive Web Service Configuration.
10. Uncheck Enable Preferred storage system IP Address and click Next.
11. Uncheck the Enable Transport Protocol Settings and click Next.



12. Leave Enable dataset protection integration unchecked and click Next.
13. Click Install.
14. 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.

15. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_vserver_mgmt>> -IP << var_vserver_mgmt_ip>>
```

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

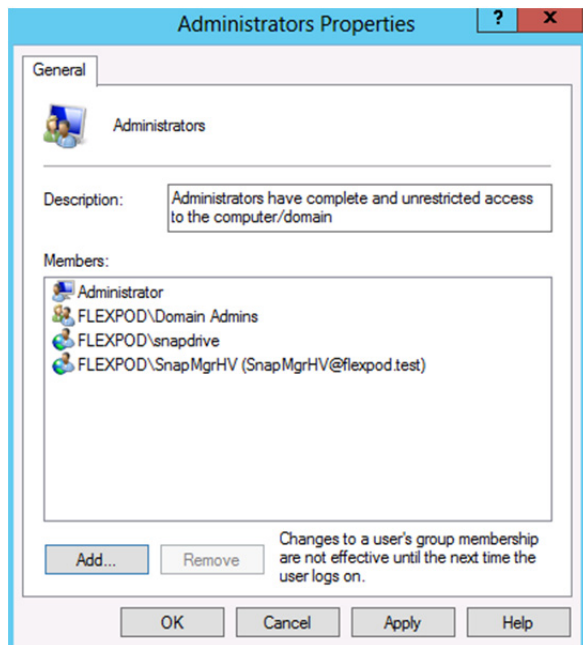
```
Set-SdStorageConnectionSetting -StorageSystem <<var_vserver_mgmt>> -protocol https -  
credential vsadmin
```

## 29.10 Install NetApp SnapManager for Hyper-V

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

### All App Fabric Hosts

1. Add the SMHV service account to the local Administrators group in Windows.



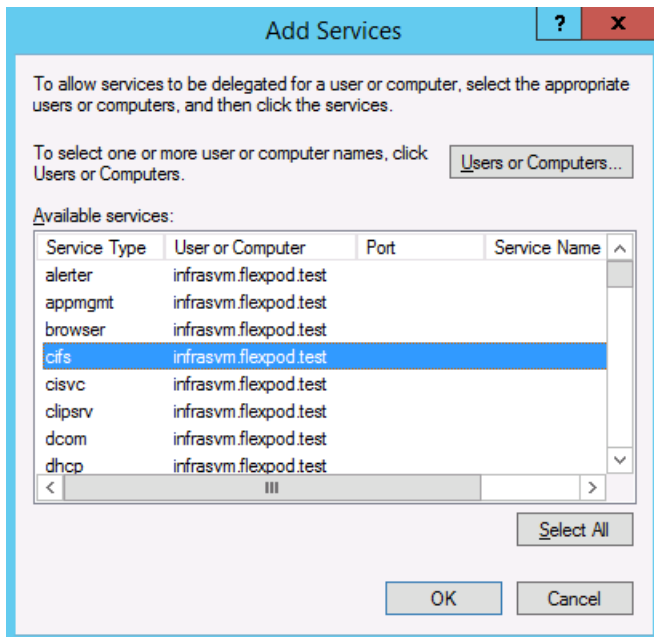
### All App Fabric Hosts

1. Download the SnapManager for Hyper-V installer from [http://support.netapp.com/NOW/download/software/snapmanager\\_hyperv\\_win/2.0/SMHV2.0\\_x64.exe](http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/2.0/SMHV2.0_x64.exe)
2. Launch the Installer and click *Next*.
3. Select the Storage based Licensing method and click *Next*.
4. Validate the installation path and click *Next*.
5. Enter the Account information for the SMHV service account and click *Next*.
6. Accept the default TCP/IP port for the Web Service.
7. Click *Install*.
8. Click *Finish*.

## 29.11 Configure Constrained Delegation for Hyper-V Hosts

While the hosts themselves already have the required permissions to access the SMB share, you will encounter access denied errors when trying to perform remote management functions that access the SMB share. To avoid these issues, configure constrained delegation for the Hyper-V hosts by following these steps.

1. Start Active Directory Users and Computers. Browse to the Computer objects for the Hyper-V hosts.
2. Right click on a Hyper-V host and select Properties
3. Select the Delegation tab.
  - a. Select Trust this computer for delegation to the specified services only
  - b. Select Use Kerberos only
  - c. Click Add
4. Click the Users or Computers... button on the top of the Add Services popup
5. Enter the Name of the Infrastructure Storage Virtual Machine, and click OK
6. Select cifs and click OK



7. Click OK
8. Repeat for each Hyper-V host

## 29.12 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 = 'Live Migration' }
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'Mgmt' }
Get-ClusterNetworkInterface | ? Name -like *SMB* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'SMB' }
```

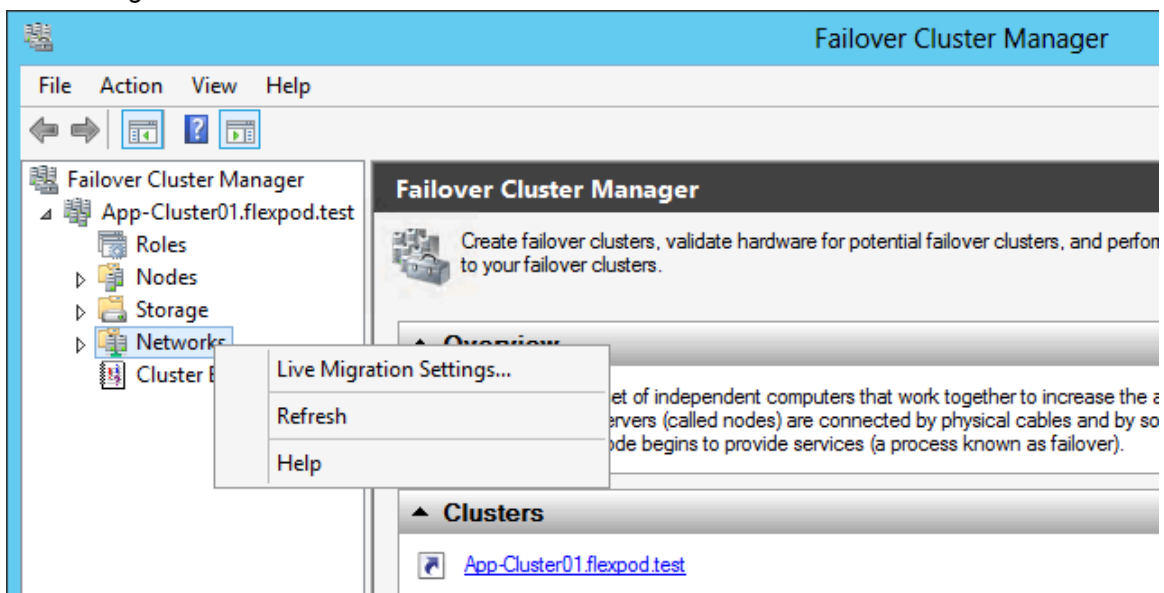
### 4. Designate the CSV network.

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

## 29.13 Configure Live Migration Network

### One Server Only

1. Open Failover Cluster Manager from Server Manager select Tools -> Failover Cluster Manager.
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.

## 29.14 Configure Quorum LUN

The following section will describe How to create the witness disk and configure the cluster to use the witness disk.

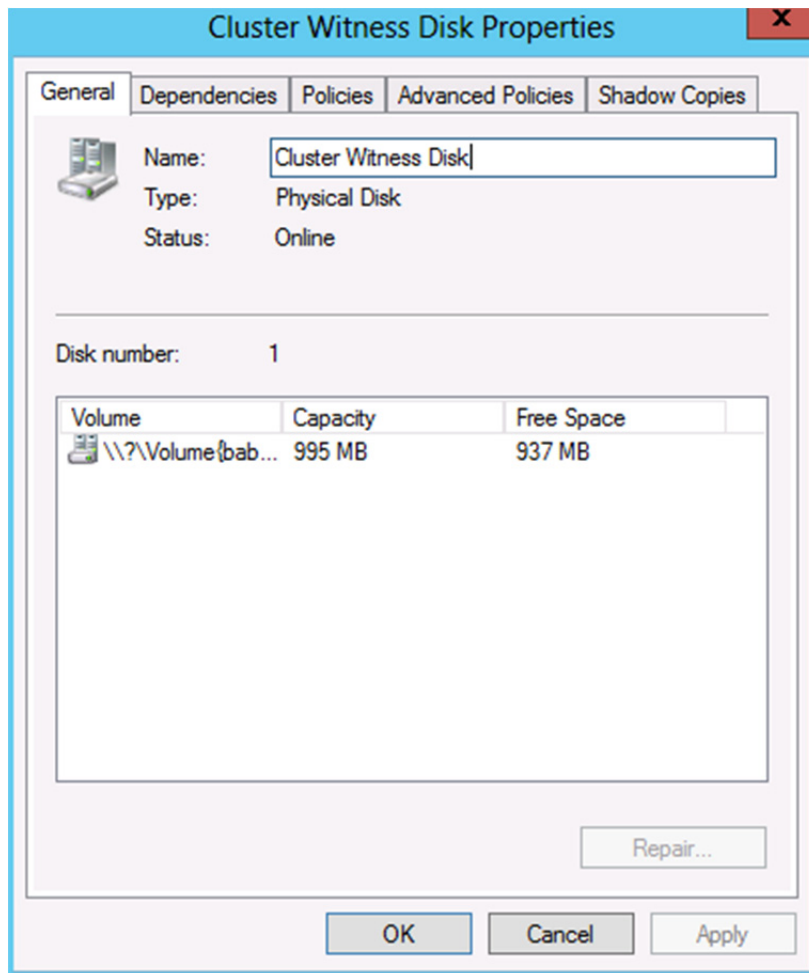
### One Server Only

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

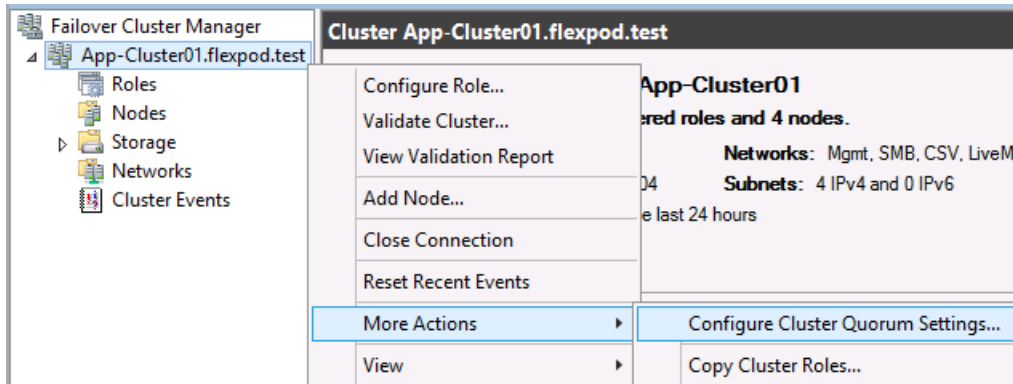
```
Move-ClusterGroup "Available Storage" -Node $env:COMPUTERNAME | Start-ClusterGroup
```

2. Open SnapDrive from the start screen to configure cluster storage.
3. From SnapDrive, Open the Server name, then Open the Disks Icon.

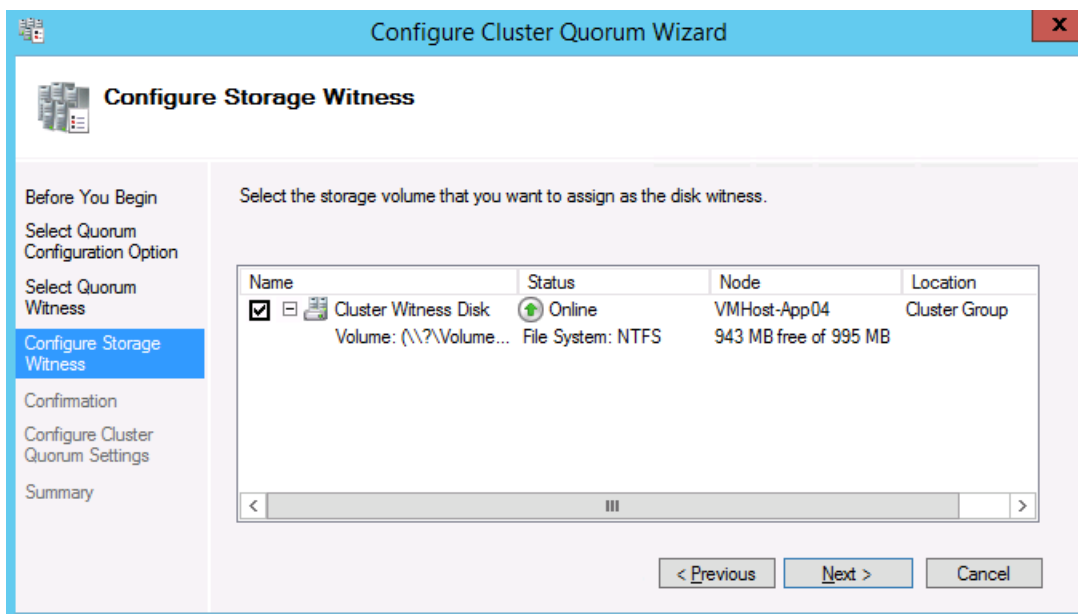
4. Right-click the Disks icon and choose to Create Disk.
5. Type in the IP Address of the controller that contains the quorum Volume.
6. When connected, open the controller tree and select the quorum Volume.
7. Type in the name of the LUN in the LUN NAME box, click Next.
8. Select Shared (Microsoft Cluster Services only) and click Next.
9. Validate that all nodes of the cluster are shown and click Next.
10. Select Do not assign drive letter or volume mount point, 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. Click Select the cluster group Available Storage, and click Next.
15. Click Finish.
16. Select the Management cluster in the left tree view. Expand the Storage object and select Disks. Right click each disk in the middle pane and select properties.
17. In the Name field, enter a name that reflects the LUN role (Cluster Witness Disk).



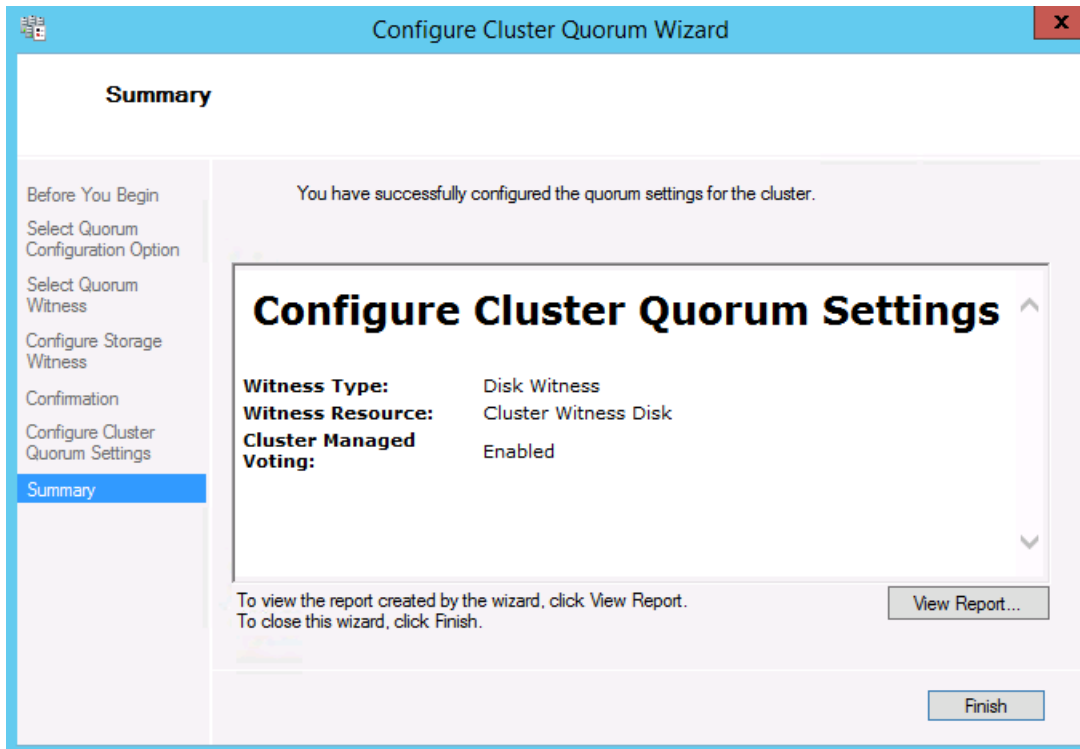
18. In Cluster Manager, click the Cluster object and Select More Actions -> Configure Cluster Quorum Settings.



19. In the Welcome screen Click Next.
20. Click Select the quorum witness, and click Next.
21. Select Configure a disk witness, and click Next.



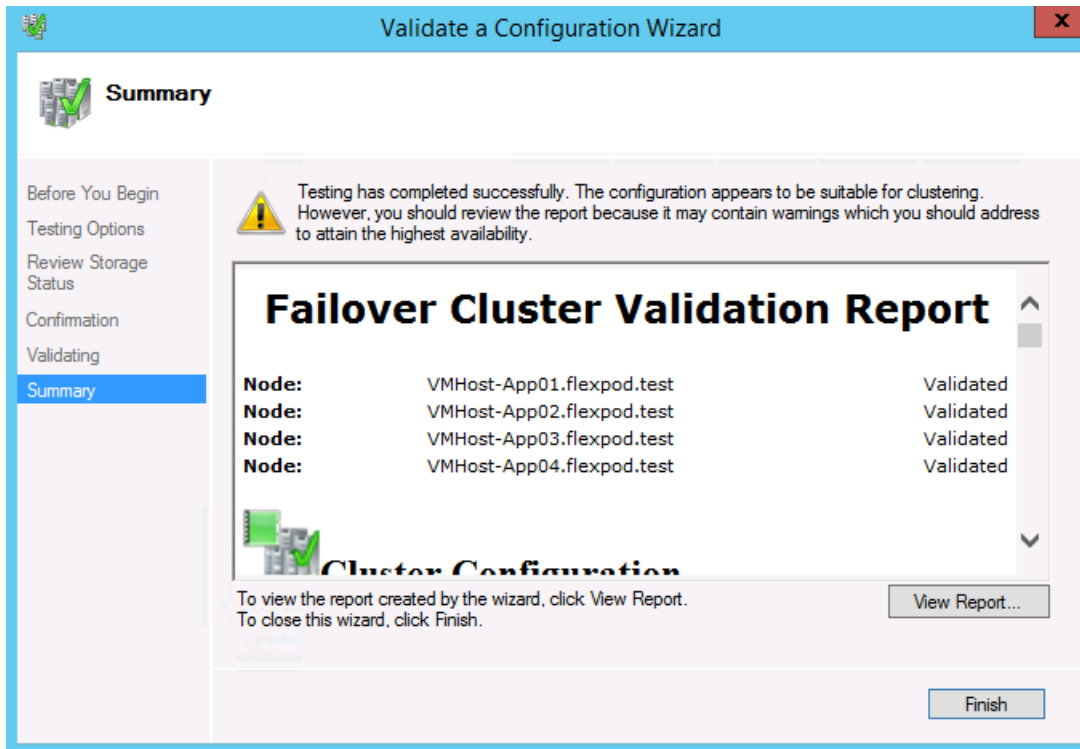
22. Select Cluster Witness Disk, and click Next.
23. Click Next.
24. Click Finish.



## 29.15 Validate 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.

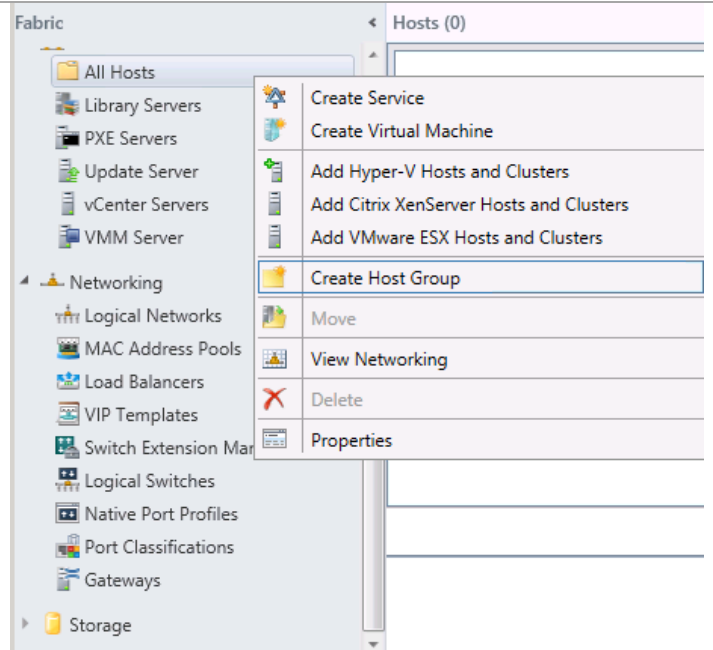
**Note:** Because the CSV, LiveMigration, and SMB networks are non-routed networks, they will not be able to reach other networks defined on the cluster. Therefore you will receive a number of warning messages like the following for each node. You will also receive warnings on the AF-Public network because it is still configured with APIPA addresses. These warnings are expected to be reported by the validation wizard and can safely be disregarded.

*Node vmhost-app02.flexpod.test is reachable from node vmhost-app01.flexpod.test by multiple communication paths, but one or more of these paths experienced more than 10% packet loss.*

## 29.16 Add the Cluster to SCVMM

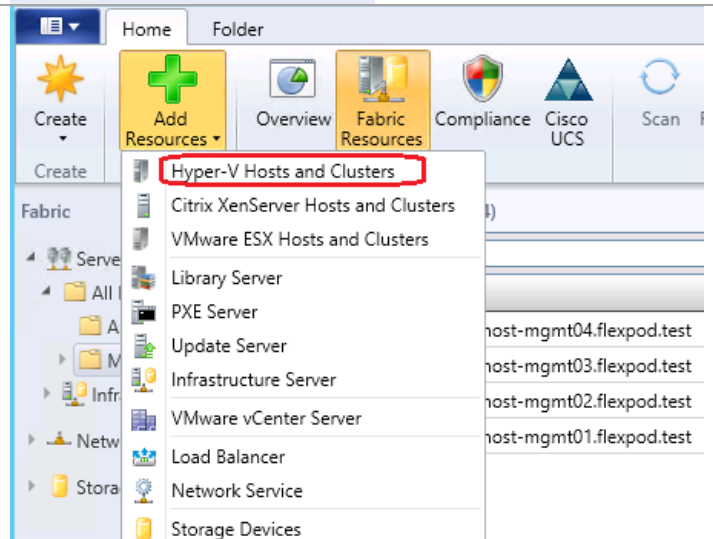
Perform the following steps on the SCVMM server.

Click **Fabric** in the left tree view and right click **All Hosts**. Select **Create Host Group**. Name the new Host Group.

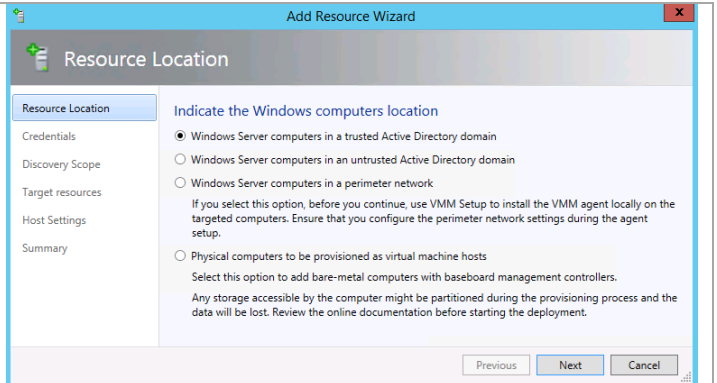


In the **Virtual Machine Manager** console, navigate to the **Fabric** pane.

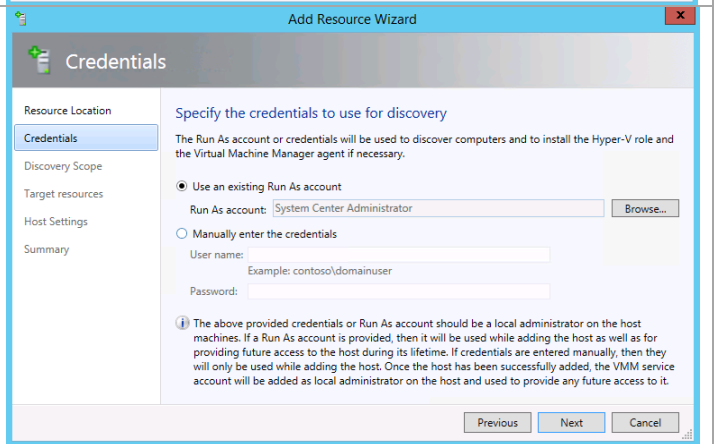
Select Add Resources, Hyper-V Hosts and Clusters.



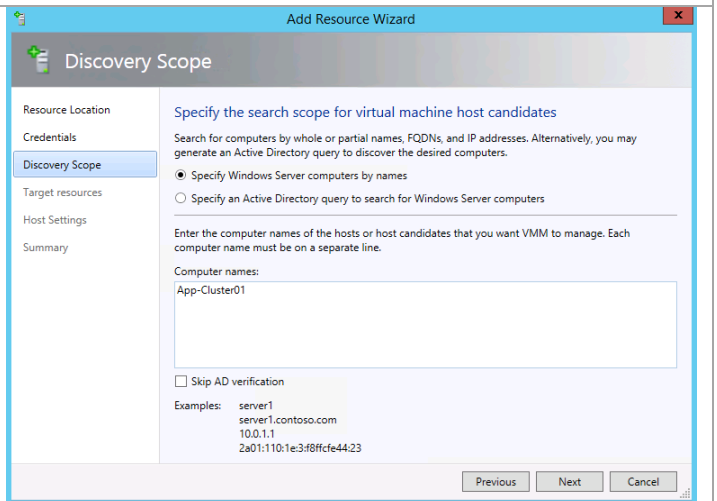
Select Windows Server Computers in a trusted Active Directory domain, and click Next.



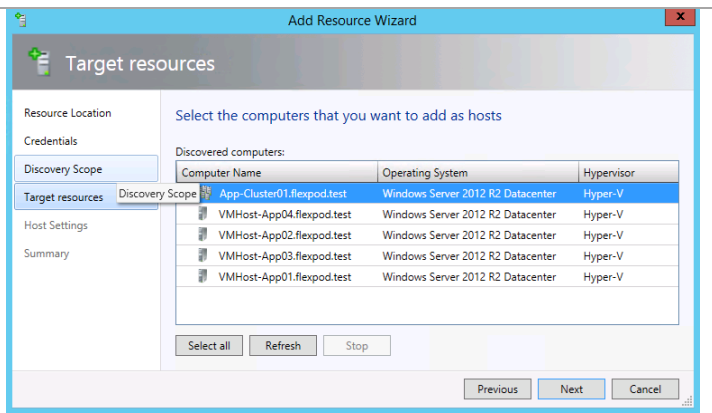
Select the Run As account that was created earlier and click Next.



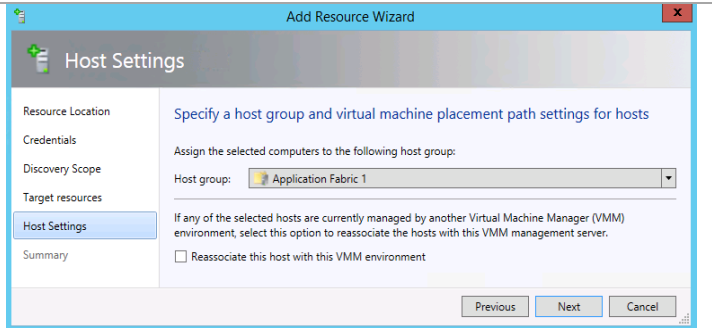
Enter the cluster name and click Next.



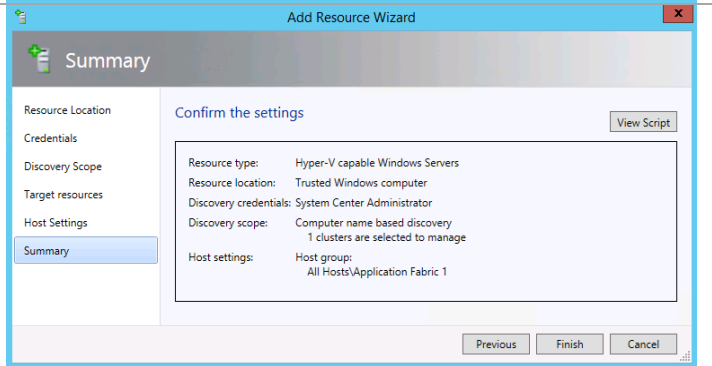
Select the cluster object and click **Next**



Select the Host group **App Fabric** from the dropdown menu and click **Next**



Click **Finish**.



In order to monitor the hosts with SCOM, add the FT-SCOM-Action account to the local Administrators group on each host.

## 29.17 Provision the File Share to the Application Cluster

Complete the following steps to assign VM storage for the Application Cluster.

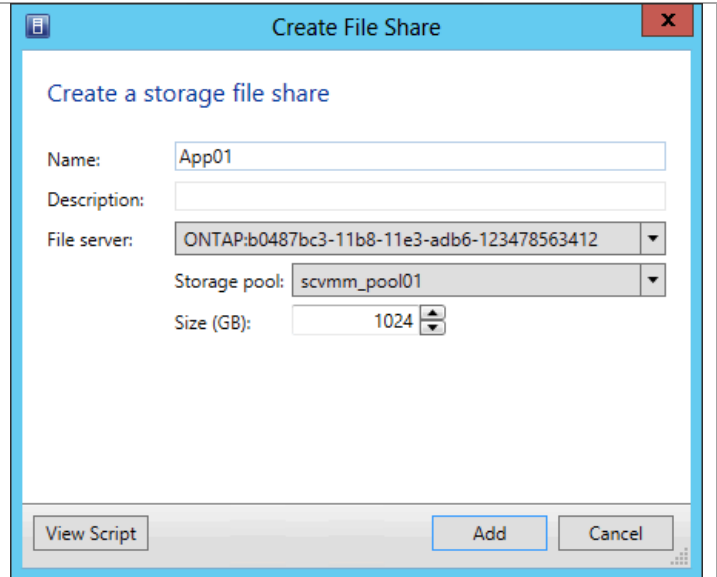
Perform the following steps on the **Virtual Machine Manager** virtual machine.

Click **Fabric** in the left tree view. Navigate to the App-Cluster01, right-click, and select **Properties**.

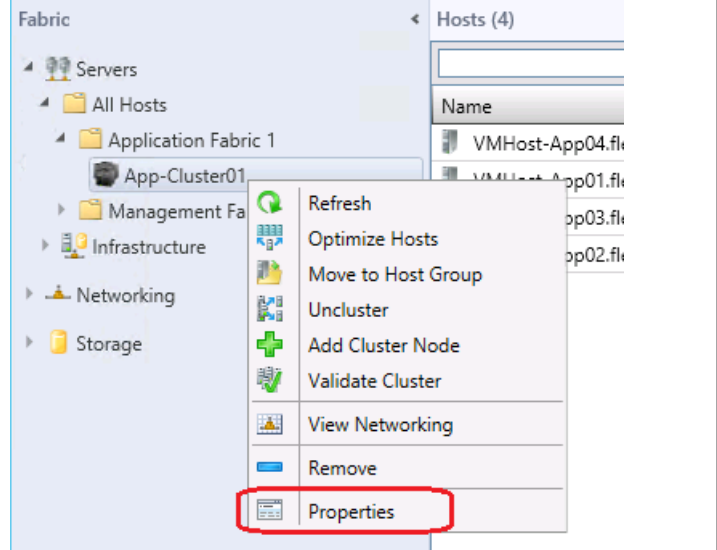


In the Create File Share dialog enter a **Name** for the new share. Select the **Storage Pool** to provision from, and enter the **Size** of the new File Share.

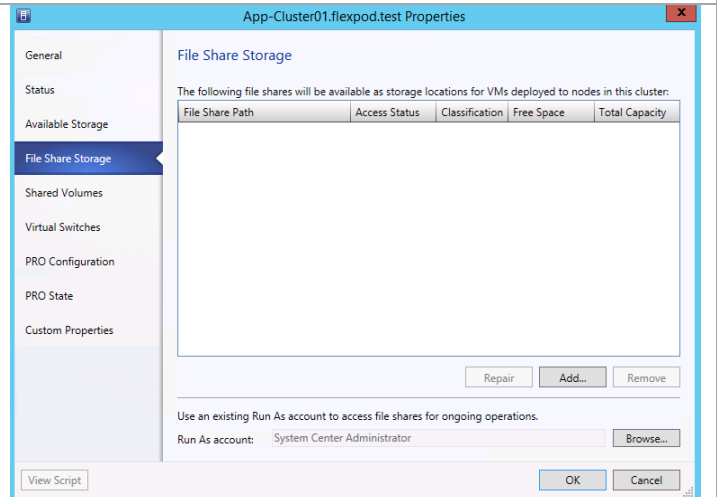
Click **Add**.



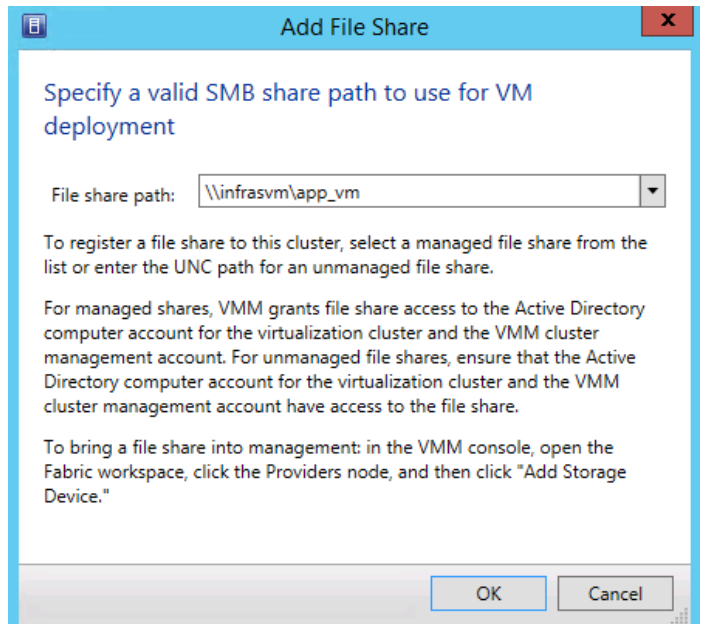
Click **Fabric** in the left tree view. Expand **Servers**, **All Hosts**, and **Application Fabric 1**. Right click the **App Cluster** and select **Properties**.



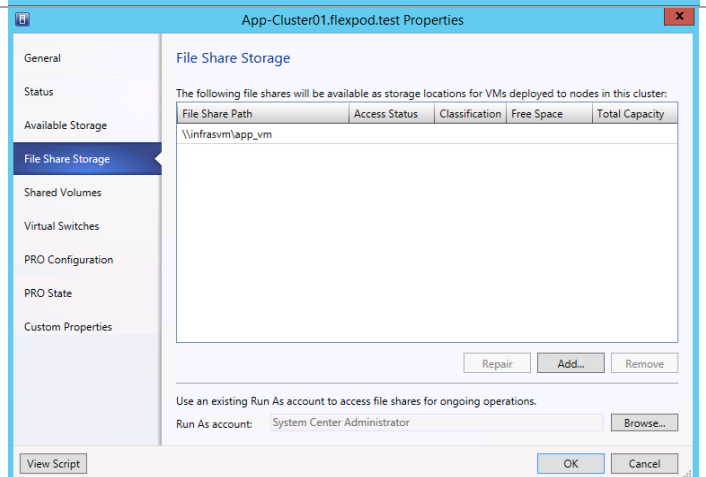
Select **File Share Storage** and click **Add**.



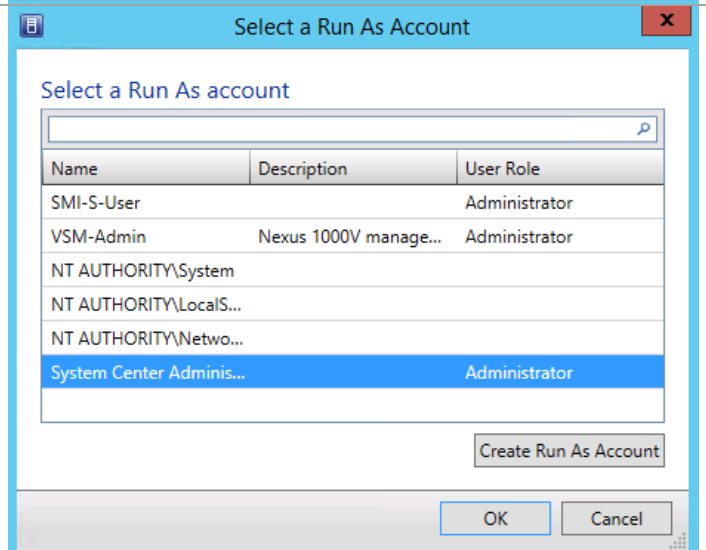
Enter the **File Share Path** and click **OK**.



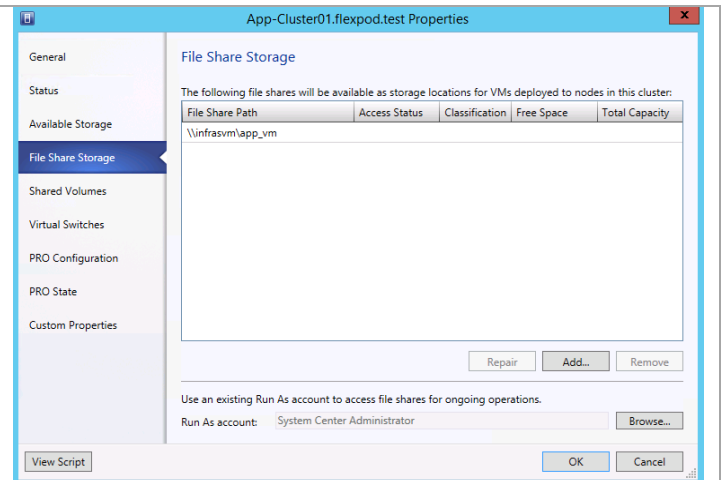
If the Run As account is not already provisioned, click **Browse** to add a **Run As** account.



Select the Run As account and click **OK**.



Click **OK** to register the file share.



## 29.18 Configure App Fabric Network Segment in the Cisco Nexus 1000V VSM

Connect to the Nexus 1000V VSM and enter the following configuration commands.

```
configure terminal

nsm network segment pool App-Fabric
member-of logical network FastTrack
exit

nsm ip pool template N1KV-AF-Public-IP-Pool
ip address 192.168.7.240 192.168.7.249
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
exit

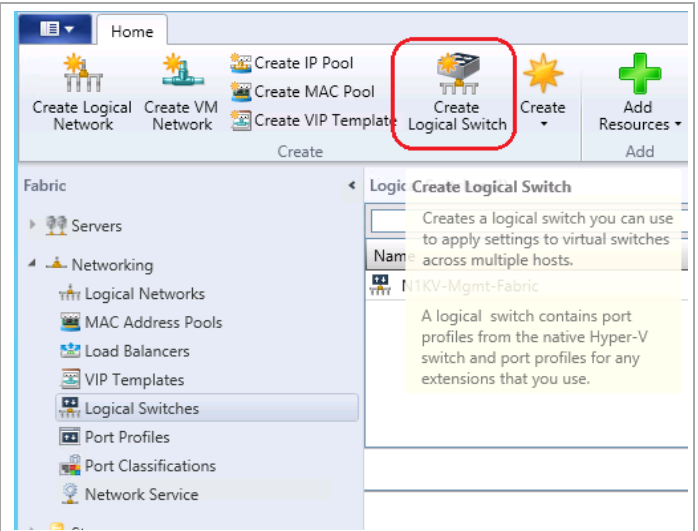
nsm network segment N1KV-AF-Public
member-of network segment pool App-Fabric
switchport access vlan 1007
ip pool import template N1KV-AF-Public-IP-Pool
publish network segment
exit

nsm network uplink N1KV-AF-Uplink
import port-profile N1KV-Uplink-Policy-FastTrack
allow network segment pool App-Fabric
system network uplink
publish network uplink
exit

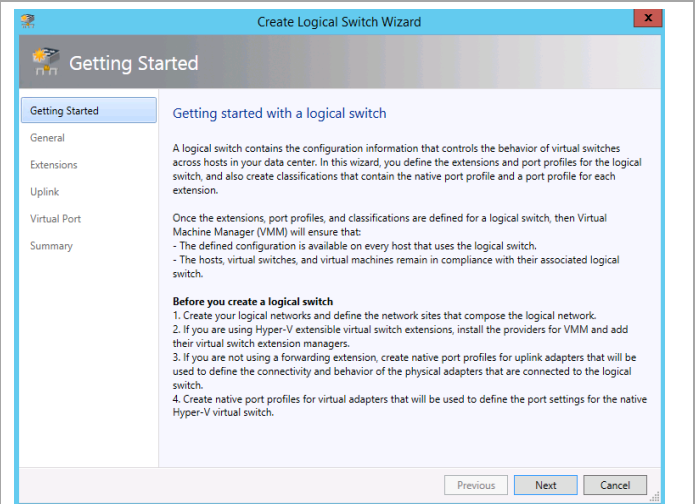
copy running-config startup-config
```

## 29.19 Configure a Logical Switch In Virtual Machine Manager

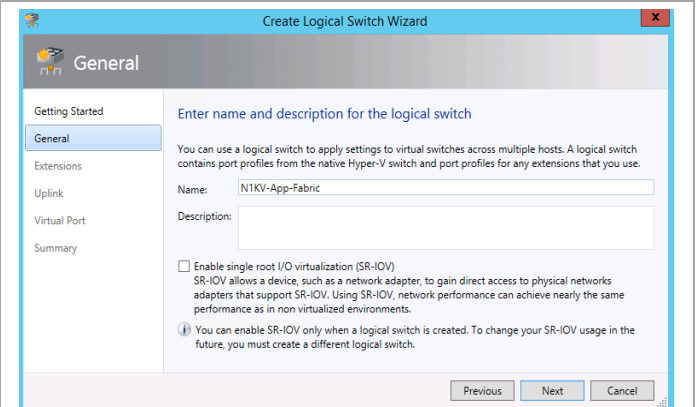
Open the Virtual Machine Manager Console. In the lower left pane select **Fabric > Networking > Logical Switches**. Select **Create Logical Switch**.



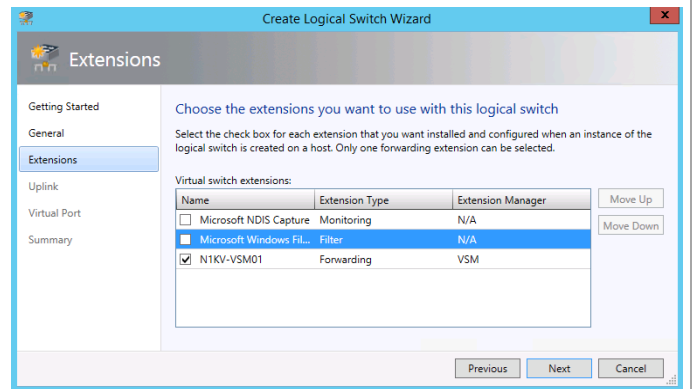
Click **Next** on the Getting Started window.



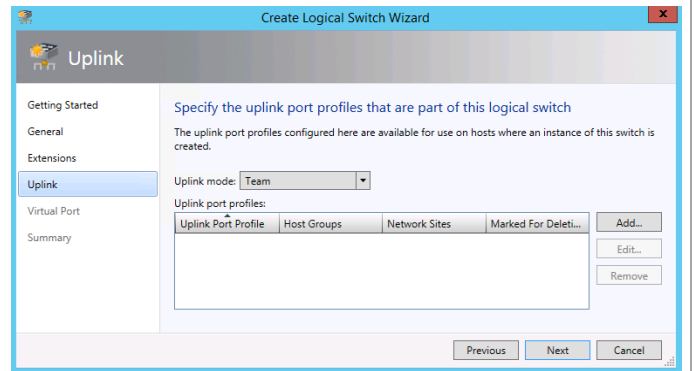
Enter a **logical switch name** for the Nexus 100V and click **Next** to continue.



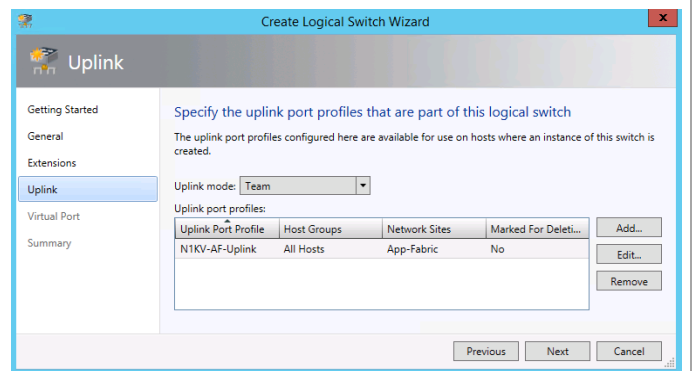
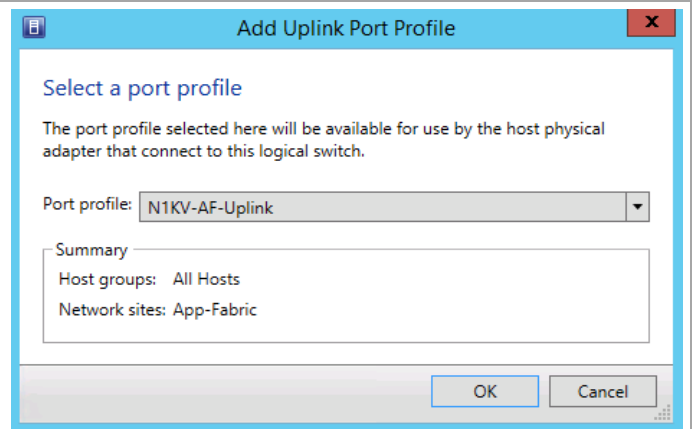
Uncheck **Microsoft Windows Filtering Platform**.  
Check **N1KV-VSM01** forwarding extension type.  
Click **Next** to continue.



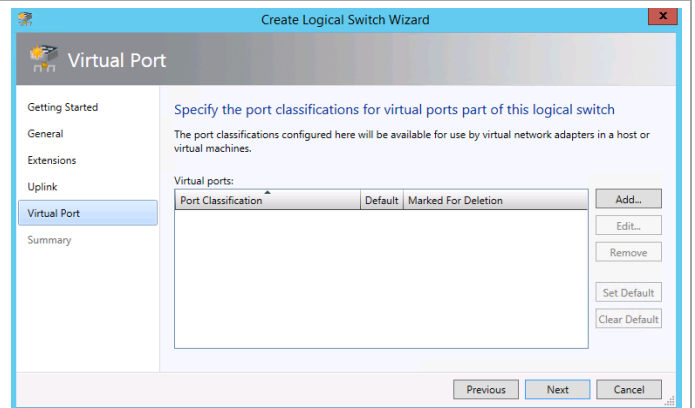
Set **Uplink mode** to **Team** and click **Add**.



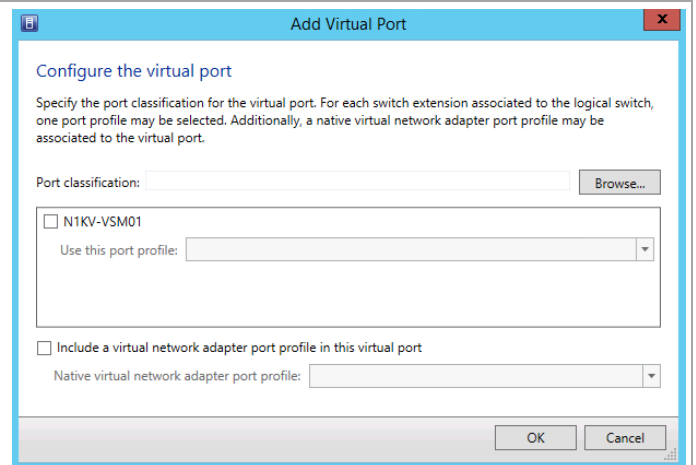
In the pull down menu, select **N1KV-AF-Uplink** port profile. Click **OK**. Back on the Uplink window click **Next**.



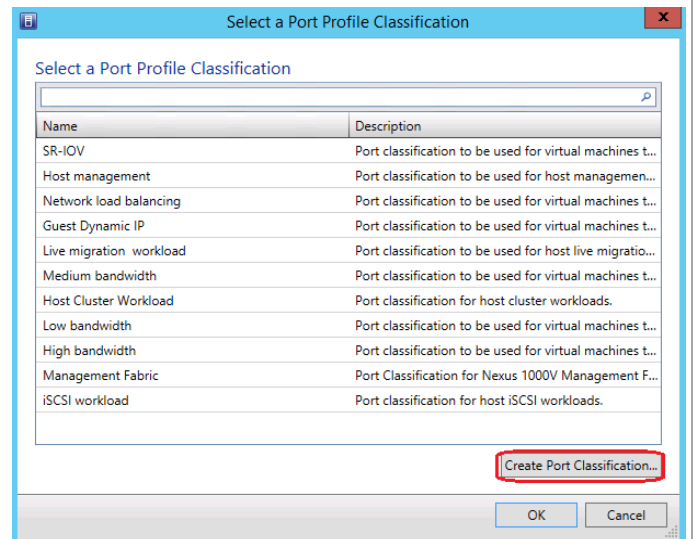
On the Virtual Port window click **Add**.



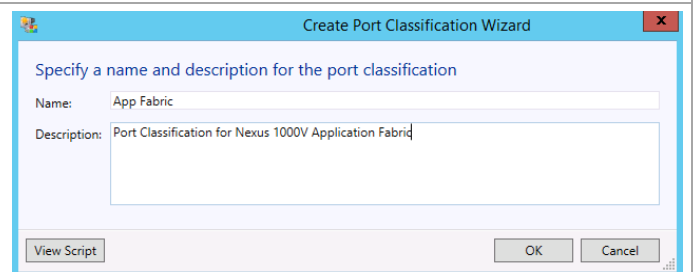
On the Add Virtual Port window click **Browse**.



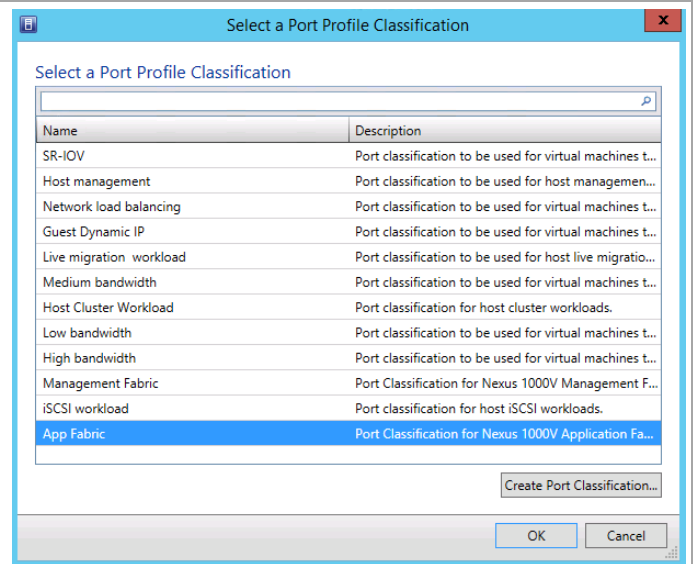
On the Select a Port Profile Classification click **Create Port Classification**.



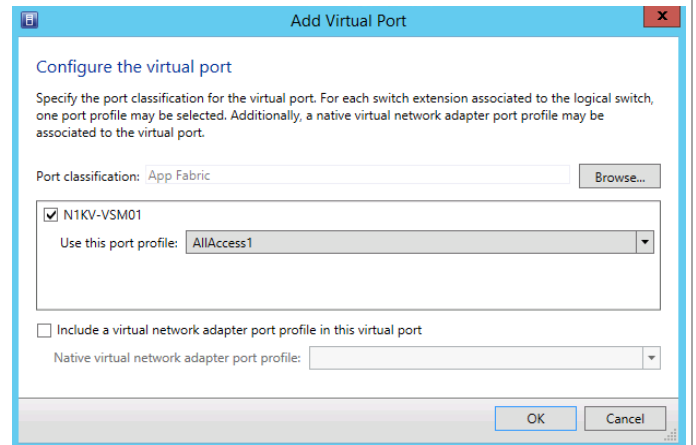
Enter the **Port Classification Name** and optional **Description**. Click **OK**.



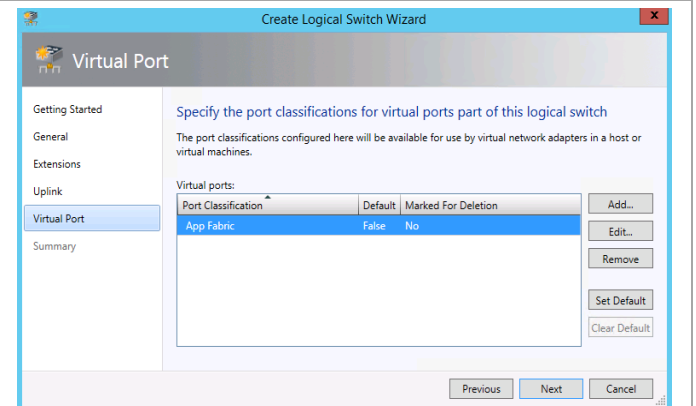
Select the newly created Port Classification and click **OK**.



Check box **N1KV-VSM01**. Select the **Port Profile** and click **OK**.

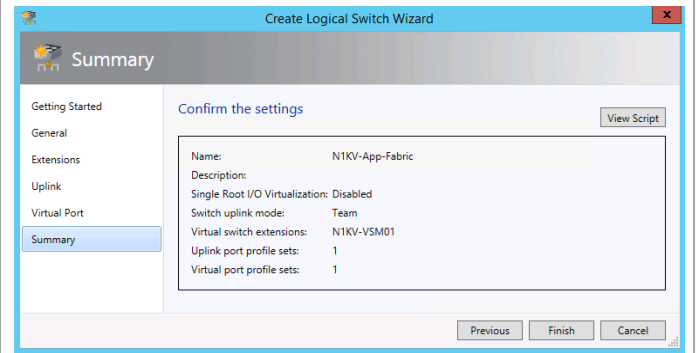


Click **Next** to update the logical switch properties.



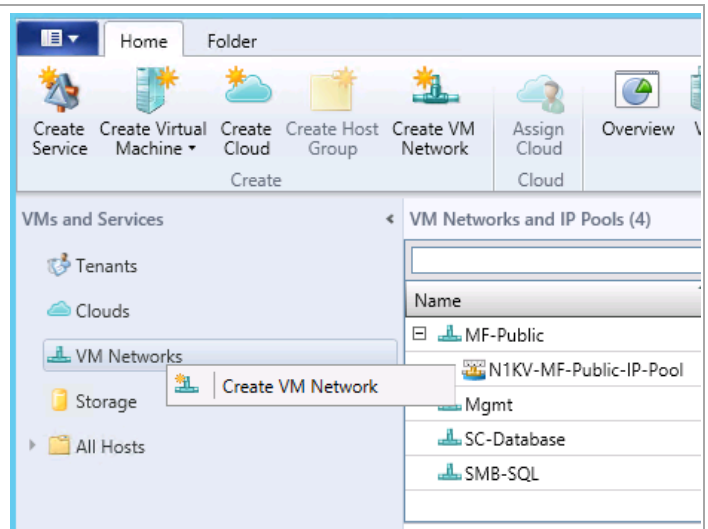


Review the contents of the Summary window and click **Finish** to complete the creation of the logical switch.

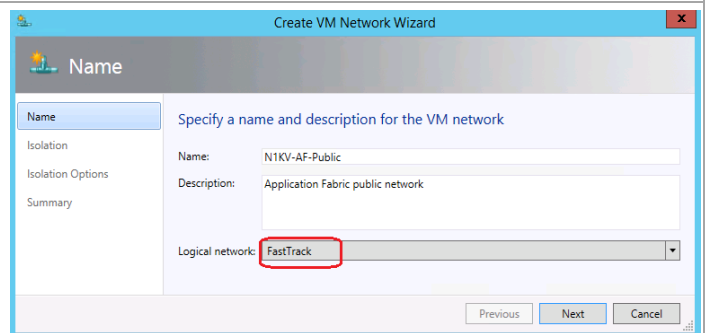


## 29.20 Create App Fabric VM Network

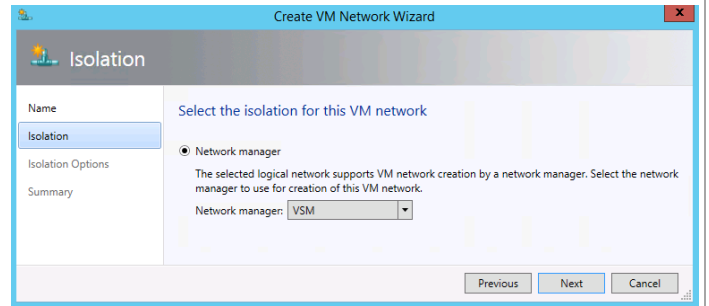
In Virtual Machine Manager, select **VMs and Services**. Right click **VM Networks** and click **Create VM Network**.



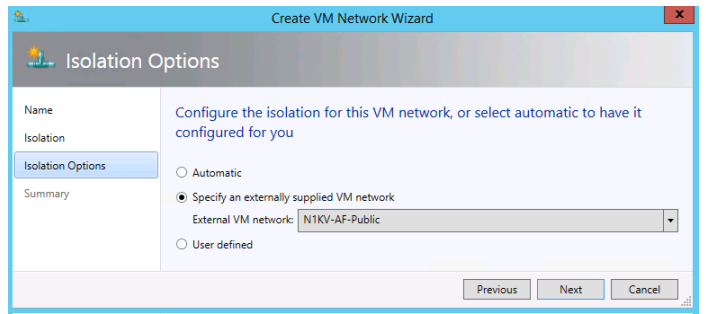
Enter the **network name**. Enter the description. Verify that the logical network **FastTrack** is selected and click **Next**.



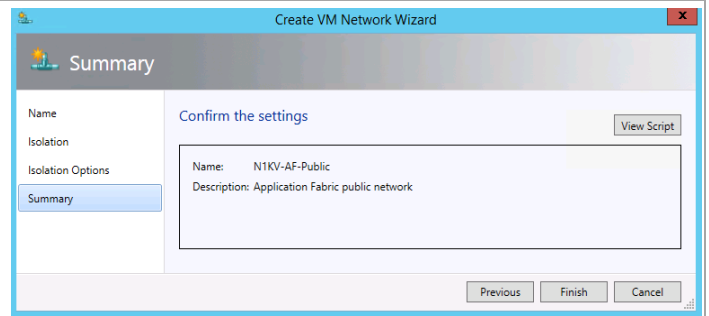
In the Isolation window, ensure the VSM network manager is selected. Click **Next**.



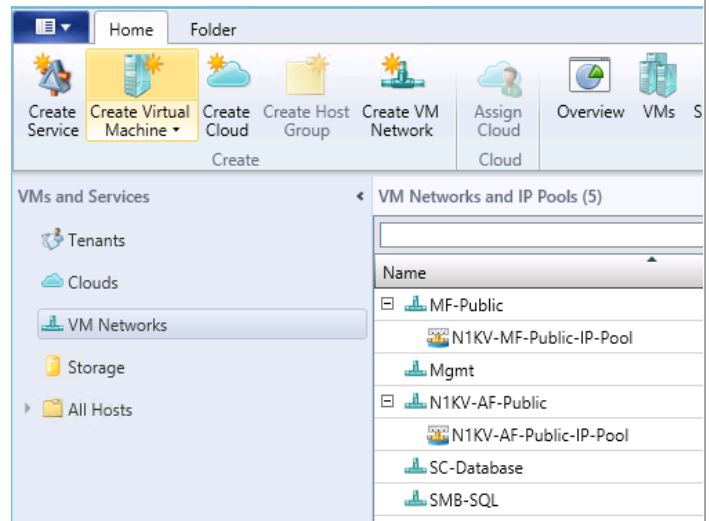
In the Isolation Options window select **Specify an externally supplied VM network** and select the **N1KV-AF-Public** external network. Click **Next** to continue.



In the Summary window, click **Finish**.



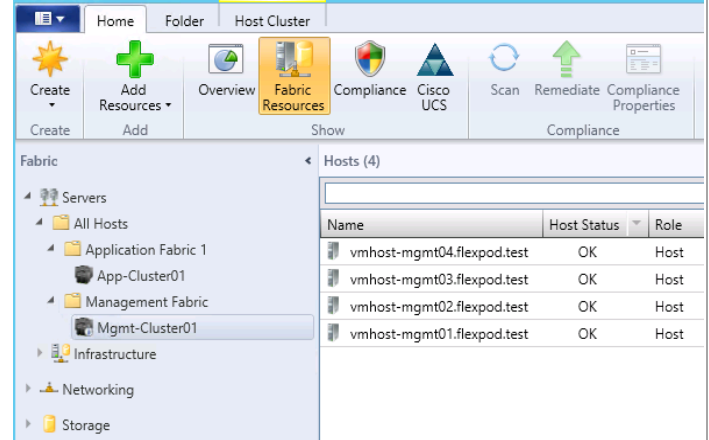
The VM Network is created.



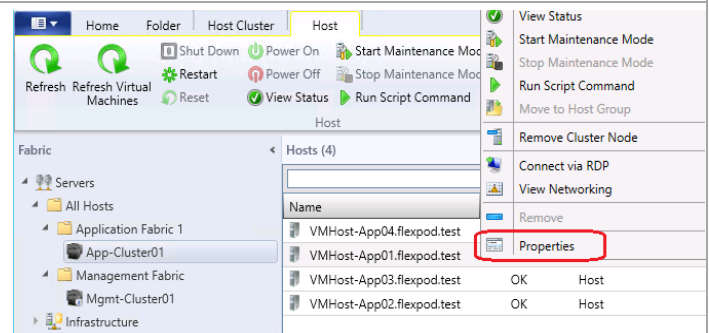
## 29.21 Creating the Logical Switch on the Hyper-V Hosts

Perform the following procedure on each App Fabric Cluster node.

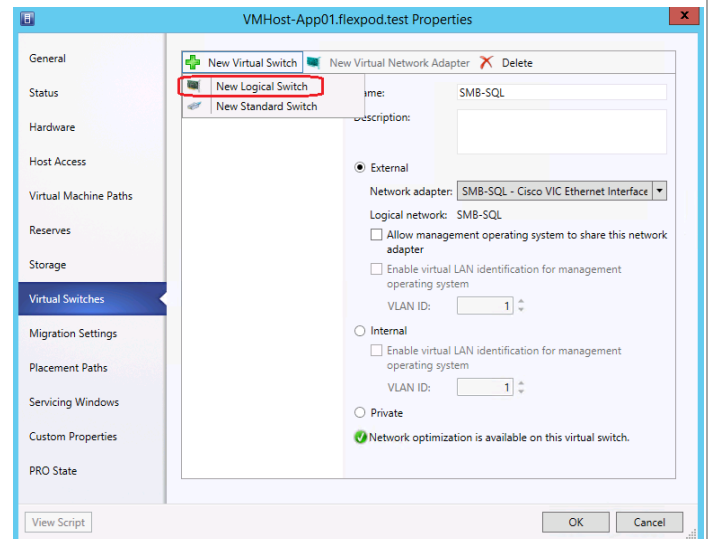
In the active Virtual Machine Manager instance, select **Fabric**. Expand **All Hosts** and **Application Fabric**.



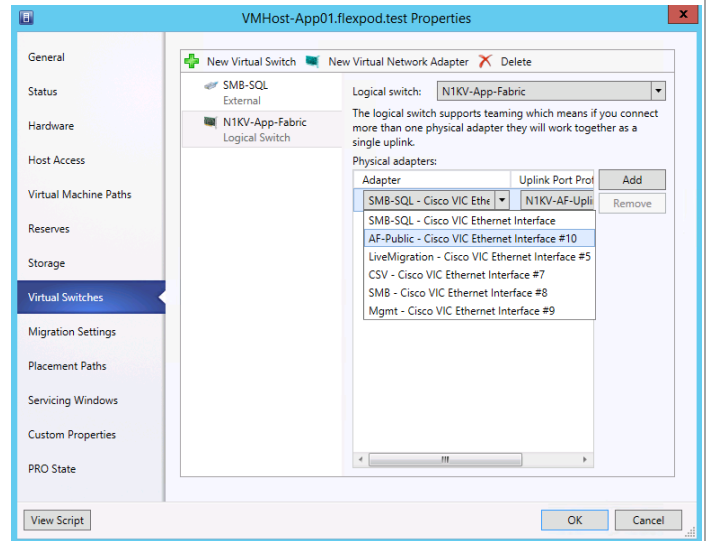
Right-click the first App Fabric host and click **Properties**.



Select **Virtual Switch** in the left pane and **New Virtual Switch**. Select **New Logical Switch**.

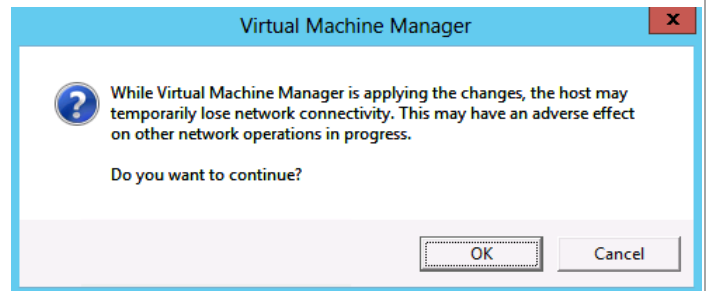


Select the new logical switch in the middle pane and in the right pane select the Ethernet adapter for the AF Public network. Click **OK**.



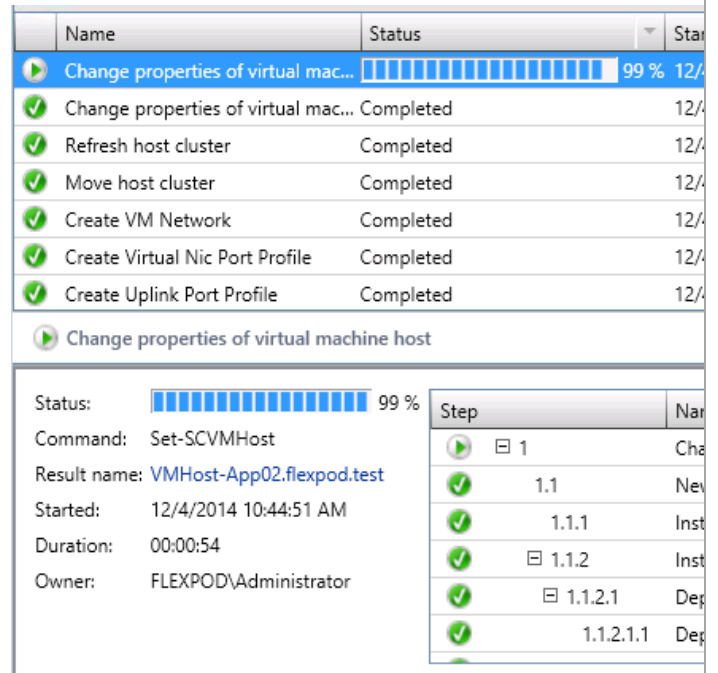
Click **OK** to invoke the configuration change.

Repeat this procedure on the remaining management fabric hosts.

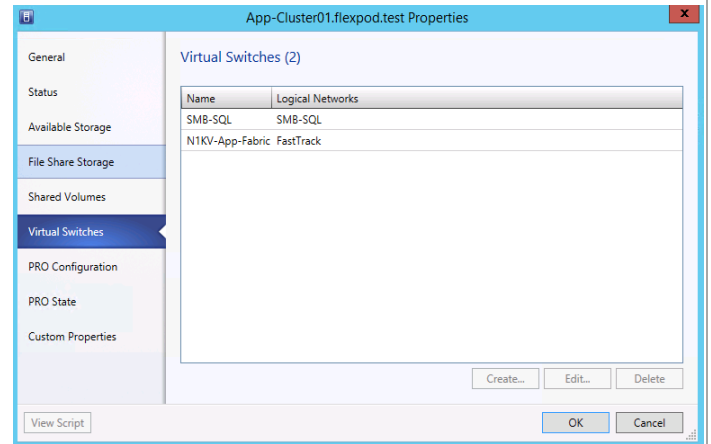


Click Jobs and monitor the job progress. The job will complete with info until the logical switch is installed on all of the hosts in the cluster.

Repeat this procedure on all cluster nodes.



Open the App-Cluster01 properties and verify that the N1KV-Fabric Switch is in the list of switch installed on all cluster nodes.



### 30 Appendix A: Installing Cisco UCS PowerTool

The Cisco UCS PowerTool should be installed on the FlexPod Management server.

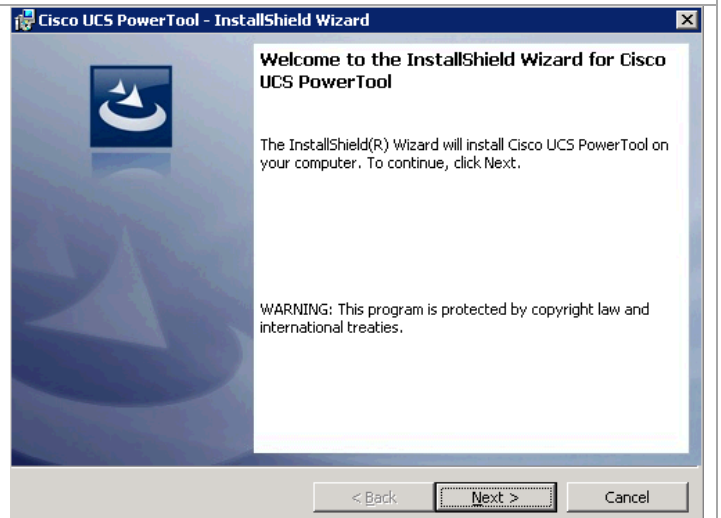
Download the Cisco UCS PowerTool version 1.3.1.0 or newer from the Cisco. It can be found at the following link.

[https://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.3\(1\)&relinid=AVAILABLE&rellifecycle=&reltype=latest](https://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.3(1)&relinid=AVAILABLE&rellifecycle=&reltype=latest)

Extract the zip file and execute the extracted exe file.

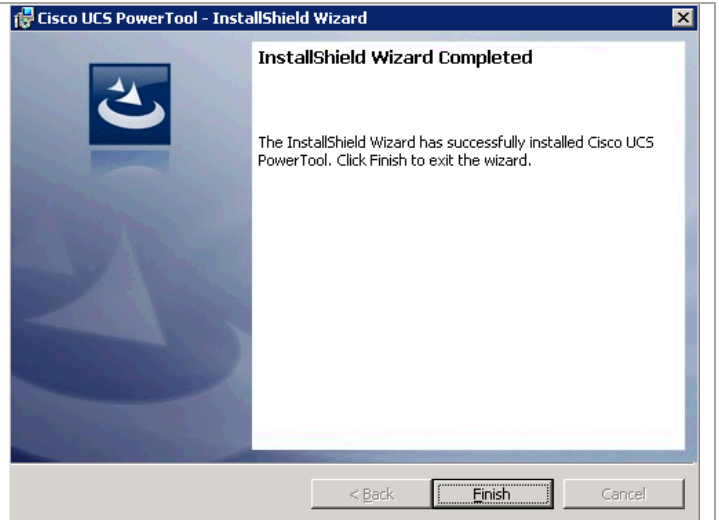
Perform the following steps on the FlexPod management server.

Launch the Cisco UCS PowerTool Installer. The Setup Wizard screen appears.



<p><b>Read and accept</b> the end user license agreement. Click <b>Next</b> to continue.</p>	
<p>Select the <b>Destination Folder</b> and click <b>Next</b> to continue.</p>	
<p>Cisco UCS PowerTool is ready to install. Click <b>Next</b> to complete the installation.</p>	

After the installation completes successfully click **Finish** to close the installation wizard.



## 31 Appendix B: Build of Materials

### 31.1 NetApp Platform Bill of Materials

Product	Description	Qty
DS224628.8TB-0PR6-C	DSK SHLF,24x1.2TB,10K,6G,0P,-	4
X6227-R6-C Chassis	FAS8040/60/80 W/CNTRL Slots,AC PS,-C	1
FAS8040A001-R6	FAS8040 High Availability System	2
SW-2-CLBASE	SW-2,Base,CL,Node	1
SW-2-8040APREMBNDLC	SW-2,Premium BNDL,8040A,-C	2
OS-ONTAPCAP2-0P-C	OS Enable,Per0.1TB,ONTAP,Perf-Stor,0P,-C	1152
X8783A-R6-C	Rail Kit III,Cabinet,-C	5
X5526A-R6-C	Rackmount Kit,4-Post,Universal,-C,R6	1
X6599A-R6-C	SFP+ Optical 10Gb Shortwave,FAS80X0,-C	8
X6589-R6-C	SFP+ Optical 10Gb Shortwave,C	4
X1985-R6-C	12-Node Cluster Cable Label Kit,C	1
X6557-R6-C	Cable,SAS Cntrl-Shelf/ShelfShelf/HA,0.5m,-C	4
X6594-R6-C	Cable,SAS Cntrl-Shelf/Shelf-Shelf/HA,1m,-C	4
X6553-R6-C	Cable,SAS Cntrl-Shelf/Shelf-Shelf/HA,2m,-C	4
X6560-R6-C	Cable,Ethernet,0.5m RJ45 CAT6,-C	4
X6561-R6-C	Cable,Ethernet,2m RJ45 CAT6,-C	1
X6562-R6-C	Cable,Ethernet,5m RJ45 CAT6,-C	4
X800E-R6-C	Power Cable North America,-C,R6	12
DOC-80XX-C	Documents,80XX,-C	1
CS-O2-NOINSTALL-4HR	SupportEdge Premium 4hr Onsite, w/o Install - Mths:36	1
X1974A-R6-C	Flash Cache 1TB PCIe Module 2,-C	2

## 31.2 Cisco Component Bill of Materials

SKU	Description	Qty
UCSB-B200-M4	UCS B200 M4 Blade Server w/o CPU, memory, HDD, mLOM/mezz	8
UCS-CPU-E52660D	2.60 GHz E5-2660 v3/105W 10C/25MB Cache/DDR4 2133MHz	16
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	128
UCSB-MLOM-40G-03	VIC 1340 modular LOM for M4 blade servers	8
N20-BBLKD	UCS 2.5 inch HDD blanking panel	16
UCSB-HS-EP-M4-F	CPU Heat Sink for UCS B200 M4 Socket 1 (Front)	8
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4 Socket 1 (Reat)	8
N20-C6508	UCS 5108 Blade Svr AC Chassis/0 PSU/8 fans/0 fabric extender	1
CAB-C19-CBN	Cabinet Jumper Power Cord, 0 VAC 16A, C20-C19 Connectors	4
UCS-IOM-2208XP	UCS 2208XP I/O Module (8 External, 16 Internal 10Gb Ports)	2
N01-UAC1	Single phase AC power module for UCS 5108	4
N20-CAK	Access. kit for 5108 Blade Chassis including Railkit, KVM dongle	1
N20-FAN5	Fan module for UCS 5108	8
N20-PAC5-00W	00W AC power supply unit for UCS 5108	4
N20-FW010	UCS 5108 Blade Server Chassis FW package	1
UCS-FI-6248UP	UCS 6248UP 1RU Fabric Int/No PSU/32 UP/ 12p LIC	2
UCS-ACC-6248UP	UCS 6248UP Chassis Accessory Kit	2
UCS-PSU-6248UP-AC	UCS 6248UP Power Supply/100-240VAC	4
N10-MGT010	UCS Manager v2.2	2
CAB-9K12A-NA	Power Cord, 1VAC 13A NEMA 5-15 Plug, North America	2
UCS-LIC-10GE	UCS 6200 Series ONLY Fabric Int 1PORT 1/10GE/FC-port license	20
UCS-FAN-6248UP	UCS 6248UP Fan Module	4
UCS-FI-DL2	UCS 6248 Layer 2 Daughter Card	2
N9K-C9396PX	Nexus 9300 with 48p 1/10G SFP+ and 1 uplink module	2
N9K-C9300-RMK	Nexus 9300 Rack Mount Kit	2
N93-LIC-PAK	N9300 License PAK Expansion	2



	Multiple License Keys	
N93-LAN1K9	LAN Enterprise License for Nexus 9300 Platform	
N9K-M12PQ	ACI Uplink Module for Nexus 9300, 12p 40G QSFP	2
QSFP-H40G-CU1M	40GBASE-CR4 Passive Copper Cable, 1m	2
N9K-PAC-650W	Nexus 9300 650W AC PS, Port-side Intake	4
N9K-C9300-FAN2	Nexus 9300 Fan 2, Port-side Intake	4
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	4
N9K-C9300-ACK	Nexus 9300 Accessory Kit	2
N9KDK9-612I2.2A	Nexus 9500/9300/3164PQ Base NX-OS Software Rel 6.1(2)I2(2a) Multiple License Keys	2
SFP-10G-SR	10GBASE-SR SFP Module	4
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter	8
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	8
N1K-1110-X-SSL-5EC	Nexus 1110-X w/ SSL card & 5G enterprise NS1KV (cluster)	1
UCSC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA (Included with above line)	2
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	4