



FlexPod Data Center with Microsoft Private Cloud FT 3.0 Enterprise

Deployment Guide for FlexPod with Microsoft Private Cloud
Fast Track 3.0 Enterprise with Clustered Data ONTAP

November 2013

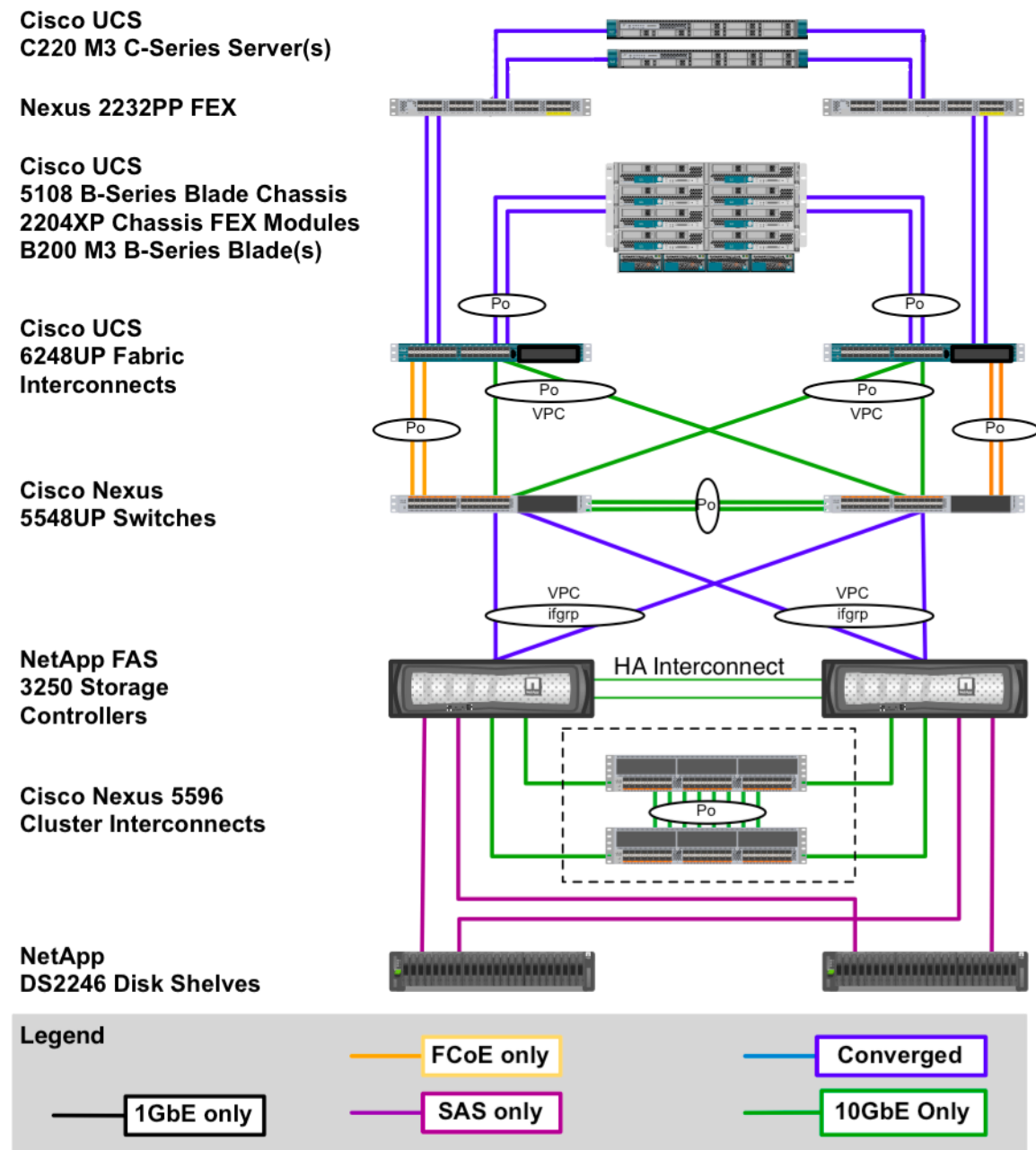


1 Reference Architecture

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

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated foundation for all virtualization solutions. FlexPod with Microsoft Private Cloud validated with Microsoft Private Cloud Fast Track v3 includes NetApp® FAS storage, Cisco Nexus® 5500 Series network switches, the Cisco Unified Computing Systems™ (Cisco UCS™) platforms, and Microsoft virtualization software in a single package. The computing and storage can fit in one data center rack with networking residing in a separate rack or deployed according to a customer's data center design. Due to port density, the networking components can accommodate multiple configurations of this kind.

Figure 1) Architecture overview



The reference configuration shown in Figure 1 includes:

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 5596 fabric interconnects
- Two Cisco Nexus 2232 fabric extenders
- One chassis of Cisco UCS blades with two fabric extenders per chassis
- Four Cisco USC C220M3 Servers
- One FAS3250A (HA pair)

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

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

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

2 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 VM's from one physical host to another	1005
SMB	VLAN Designated for SMB access to VHDX files on the NetApp storage array	1003
VM Cluster Comm	VLAN for cluster connectivity	1006
Database	VLAN for database access	1002
MF-Public	VLAN for Management Fabric application access	1001
AF-Public	VLAN for Application Fabric application access	1007

3 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.

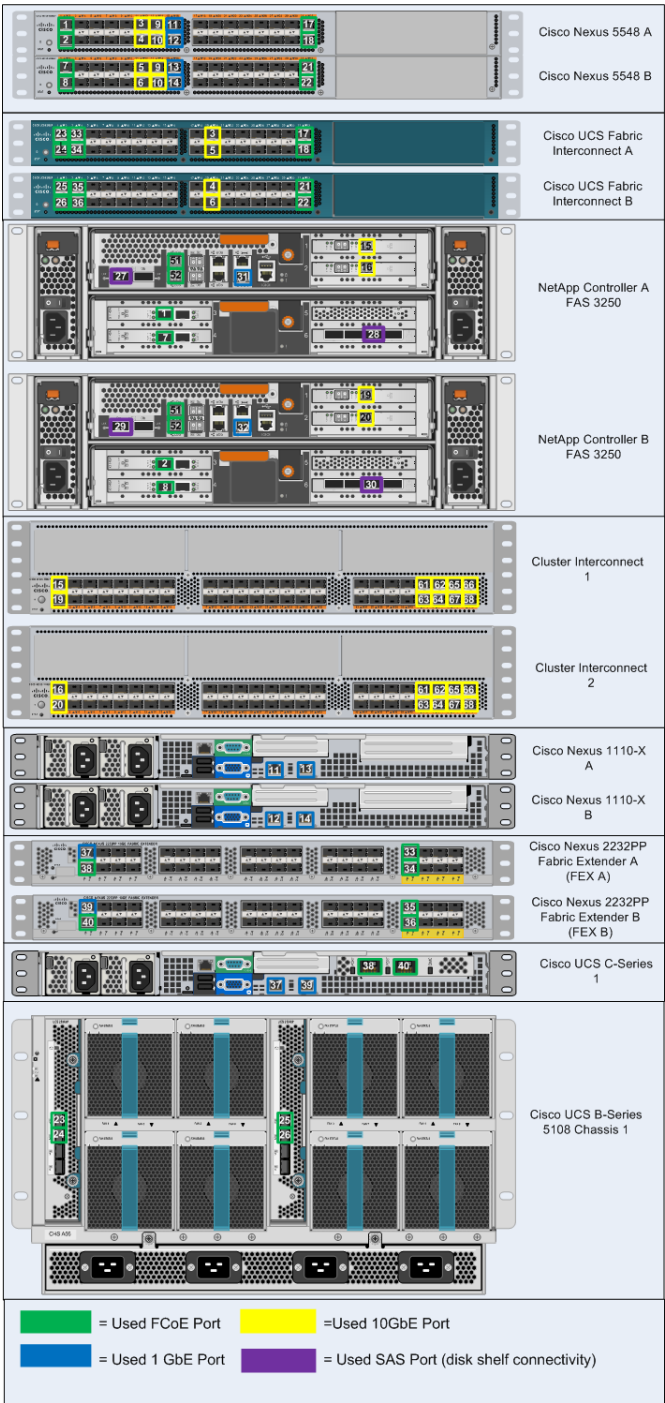
The FlexPod Validated with Microsoft Private Cloud architecture is flexible; therefore, the exact configuration detailed in this section might vary for customer implementations depending on specific requirements. Although customer implementations might deviate from the information that follows, the best 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.

4 Physical Infrastructure

4.1 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



The information provided in Table 2 through
Table 16 corresponds to each connection shown in Figure 2.

Table 2) Cisco Nexus 5548 A cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	Eth1/1	10GbE	NetApp controller 1	e3a
	Eth1/2	10GbE	NetApp controller 2	e3a
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/19
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/19
	Eth1/13	10GbE	Cisco Nexus 5548 B	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 B	Eth1/14
	Eth1/15	GbE	Cisco Nexus 1110-XA	LOM A
	Eth1/16	GbE	Cisco Nexus 1110-XB	LOM A
	Eth1/31	10GbE	Cisco UCS fabric interconnect A	Eth1/31
	Eth1/32	10GbE	Cisco UCS fabric interconnect A	Eth1/32
	MGMT0	GbE	GbE management switch	Any

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

Table 3) Cisco Nexus 5548 B cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B	Eth1/1	10GbE	NetApp controller 1	e4a
	Eth1/2	10GbE	NetApp controller 2	e4a
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/20
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/20
	Eth1/13	10GbE	Cisco Nexus 5548 A	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 A	Eth1/14
	Eth1/15	GbE	Cisco Nexus 1110-XA	LOM B
	Eth1/16	GbE	Cisco Nexus 1110-XB	LOM B
	Eth1/31	10GbE	Cisco UCS fabric interconnect B	Eth1/31

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/32	10GbE	Cisco UCS fabric interconnect B	Eth1/32
	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	e1a
	Eth1/2	10GbE	NetApp controller 2	e1a
	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	e2a
	Eth1/2	10GbE	NetApp controller 2	e2a
	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
	e0a	GbE	GbE management switch	Any
	e0b	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	c0a	10GbE	NetApp controller 2	c0a
	c0b	10GbE	NetApp controller 2	c0b
	e1a	10GbE	Cisco Nexus 5596 A	Eth1/1
	e2a	10GbE	Cisco Nexus 5596 B	Eth1/1
	e3a	10GbE	Cisco Nexus 5548 A	Eth1/1
	e4a	10GbE	Cisco Nexus 5548 B	Eth1/1

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
	e0a	GbE	GbE management switch	Any
	e0b	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	c0a	10GbE	NetApp controller 1	c0a
	c0b	10GbE	NetApp controller 1	c0b
	e1a	10GbE	Cisco Nexus 5596 A	Eth1/2
	e2a	10GbE	Cisco Nexus 5596 B	Eth1/2
	e3a	10GbE	Cisco Nexus 5548 A	Eth1/2
	e4a	10GbE	Cisco Nexus 5548 B	Eth1/2

Table 8) Cisco UCS fabric interconnect A cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/11
	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/11

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/1	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/2	10GbE	Cisco UCS Chassis FEX A/Cisco Nexus 2232PP FEX A	
	Eth1/3	10GbE	Cisco UCS Chassis FEX A/Cisco Nexus 2232PP FEX A	
	Eth1/4	10GbE	Cisco UCS Chassis FEX A/Cisco Nexus 2232PP FEX A	
	Eth1/5	10GbE	Cisco UCS Chassis FEX A/Cisco Nexus 2232PP FEX A	
	Eth1/6	10GbE	Cisco UCS Chassis FEX A/Cisco Nexus 2232PP FEX A	
	Eth1/31	10GbE	Cisco Nexus 5548 A	Eth1/31
	Eth1/32	10GbE	Cisco Nexus 5548 A	Eth1/32
	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	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/12
	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/12
	Eth1/1	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/2	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/3	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/4	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/5	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/6	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/31	10GbE	Cisco Nexus 5548 B	Eth1/31
	Eth1/32	10GbE	Cisco Nexus 5548 B	Eth1/32
	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 Nexus 2232PP FEX A.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX A	Port 1	GbE	Cisco UCS C-Series 1	M1
	Port 2	10GbE	Cisco UCS C-Series 1	Port 0
	Port 3	GbE	Cisco UCS C-Series 2	M1
	Port 4	10GbE	Cisco UCS C-Series 2	Port 0
	Port 5	GbE	Cisco UCS C-Series 3	M1
	Port 6	10GbE	Cisco UCS C-Series 3	Port 0
	Port 7	GbE	Cisco UCS C-Series 4	M1
	Port 8	10GbE	Cisco UCS C-Series 4	Port 0
	Port 2/1	10GbE	Cisco UCS fabric interconnect A	
	Port 2/2	10GbE	Cisco UCS fabric interconnect A	

Table 11) Cisco Nexus 2232PP FEX B.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX B	Port 1	GbE	Cisco UCS C-Series 1	M2
	Port 2	10GbE	Cisco UCS C-Series 1	Port 1
	Port 3	GbE	Cisco UCS C-Series 2	M2
	Port 4	10GbE	Cisco UCS C-Series 2	Port 1
	Port 5	GbE	Cisco UCS C-Series 3	M2
	Port 6	10GbE	Cisco UCS C-Series 3	Port 1
	Port 7	GbE	Cisco UCS C-Series 4	M2
	Port 8	10GbE	Cisco UCS C-Series 4	Port 1

Local Device	Local Port	Connection	Remote Device	Remote Port
	Port 2/1	10GbE	Cisco UCS fabric interconnect B	
	Port 2/2	10GbE	Cisco UCS fabric interconnect B	

Table 12) Cisco UCS C-Series 1.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 1	M1	GbE	Cisco Nexus 2232PP FEX A	Port 1
	M2	GbE	Cisco Nexus 2232PP FEX B	Port 1
	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 2
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 2

Table 13) Cisco UCS C-Series 2.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 2	M1	GbE	Cisco Nexus 2232PP FEX A	Port 3
	M2	GbE	Cisco Nexus 2232PP FEX B	Port 3
	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 4
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 4

Table 14) Cisco UCS C-Series 3.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 3	M1	GbE	Cisco Nexus 2232PP FEX A	Port 5
	M2	GbE	Cisco Nexus 2232PP FEX B	Port 5
	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 6
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 6

Table 15) Cisco UCS C-Series 4.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 4	M1	GbE	Cisco Nexus 2232PP FEX A	Port 7
	M2	GbE	Cisco Nexus 2232PP FEX B	Port 7
	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 8
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 8

Table 16) FAS3250 card layout.

Slot	Part Number	Description
1	X1117A-R6	NIC 2-port 10GbE (ports e1a and e1b)
2	X1117A-R6	NIC 2-port 10GbE (ports e2a and e2b)
3	X1140A-R6	Unified target 2-port 10GbE (ports e3a and e3b)
4	X1140A-R6	Unified target 2-port 10GbE (ports e4a and e4b)
5	X1971A-R5	Flash Cache™ – 512GB
6	X2065A-R6	SAS, 4-port, 6Gb

5 Nexus 5548UP Deployment Procedure

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

Note: The configuration steps detailed in this section provides guidance for configuring the Nexus 5548UP running release Cisco NX-OS Firmware 6.0(2)N1(2)

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.

5.1 Initial Cisco Nexus 5548UP Switch Configuration

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

Nexus 5548 A

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

1. Enter **yes** to enforce secure password standards.
2. Enter the password for the admin user.
3. Enter the password a second time to commit the password.
4. Enter **yes** to enter the basic configuration dialog.
5. Create another login account (yes/no) [n] : Enter.
6. Configure read-only SNMP community string (yes/no) [n] : **Yes** Enter.
7. Enter the SNMP community string : <SNMP community string> Enter
8. Enter the switch name : <Nexus A Switch name> Enter.
9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y] : Enter.
10. Mgmt0 IPv4 address : <Nexus A mgmt0 IP> Enter.
11. Mgmt0 IPv4 netmask : <Nexus A mgmt0 netmask> Enter.

12. Configure the default gateway? (yes/no) [*y*]: Enter.
13. IPv4 address of the default gateway: <*Nexus A mgmt0 gateway*> Enter.
14. Enable the telnet service? (yes/no) [*n*]: Enter.
15. Enable the ssh service? (yes/no) [*y*]: Enter.
16. Type of ssh key you would like to generate (dsa/rsa): **rsa**.
17. Number of key bits <768–2048>:1024 Enter.
18. Configure the ntp server? (yes/no) [*y*]: Enter.
19. NTP server IPv4 address: <*NTP Server IP*> Enter.
20. Enter basic FC configurations (yes/no) [*n*]: Enter.
21. Would you like to edit the configuration? (yes/no) [*n*]: Enter.

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

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

Nexus 5548 B

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

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

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

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

5.2 Enable Appropriate Cisco Nexus Features

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

Nexus A and Nexus B

1. Type `config t` to enter the global configuration mode.
2. Type `feature lacp`.
3. Type `feature fcoe`.
4. Type `feature npiv`.
5. Type `feature vpc`.

5.3 Set Global Configurations

These steps provide details for setting global configurations.

Nexus A and Nexus B

Perform the following configuration procedures on both Nexus switches.

Configure Timezone

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

Configure Spanning Tree

1. From the global configuration mode, type `spanning-tree port type network default` to make sure that, by default, the ports are considered as network ports in regards to spanning-tree.
2. Type `spanning-tree port type edge bpduguard default` to enable bpduguard on all edge ports by default.
3. Type `spanning-tree port type edge bpdufilter default` to enable bpdufilter on all edge ports by default.

Configure Access Control Lists and Cost of Service

1. Type `ip access-list classify_silver`.
2. Type `10 permit ip <SMB net address> any`
Note: where the variable is the network address of the SMB VLAN used for VHD access in CIDR notation (i.e. 192.168.102.0/24).
3. Type `20 permit ip any <SMB net address>`
4. Type `class-map type qos match-all class-gold`.

5. **Type** match cos 4.
6. **Type** exit.
7. **Type** class-map type qos match-all class-silver.
8. **Type** match cos 2.
9. **Type** match access-group name classify_silver.
10. **Type** exit.
11. **Type** class-map type queuing class-gold.
12. **Type** match qos-group 3.
13. **Type** exit.
14. **Type** class-map type queuing class-silver.
15. **Type** match qos-group 4.
16. **Type** exit.
17. **Type** policy-map type qos system_qos_policy.
18. **Type** class class-gold.
19. **Type** set qos-group 3.
20. **Type** class class-silver.
21. **Type** set qos-group 4.
22. **Type** class class-fcoe.
23. **Type** set qos-group 1.
24. **Type** exit.
25. **Type** exit.
26. **Type** policy-map type queuing system_q_in_policy.
27. **Type** class type queuing class-fcoe.
28. **Type** bandwidth percent 20.
29. **Type** class type queuing class-gold.
30. **Type** bandwidth percent 33.
31. **Type** class type queuing class-silver.
32. **Type** bandwidth percent 29.
33. **Type** class type queuing class-default.
34. **Type** bandwidth percent 18.
35. **Type** exit.
36. **Type** exit.
37. **Type** policy-map type queuing system_q_out_policy.
38. **Type** class type queuing class-fcoe.
39. **Type** bandwidth percent 20.
40. **Type** class type queuing class-gold.
41. **Type** bandwidth percent 33.
42. **Type** class type queuing class-silver.
43. **Type** bandwidth percent 29.

44. Type `class type queuing class-default`.
45. Type `bandwidth percent 18`.
46. Type `exit`.
47. Type `exit`.
48. Type `class-map type n`
49. Type `match qos-group 3`.
50. Type `exit`.
51. Type `class-map type network-qos class-silver`.
52. Type `match qos-group 4`.
53. Type `exit`.
54. Type `policy-map type network-qos system_nq_policy`.
55. Type `class type network-qos class-gold`.
56. Type `set cos 4`.
57. Type `mtu 9000`.
58. Type `class type network-qos class-fcoe`.
59. Type `pause no-drop`.
60. Type `mtu 2158`.
61. Type `class type network-qos class-silver`.
62. Type `set cos 2`.
63. Type `mtu 9000`.
64. Type `class type network-qos class-default`.
65. Type `mtu 9000`.
66. Type `exit`.
67. Type `system qos`.
68. Type `service-policy type qos input system_qos_policy`.
69. Type `service-policy type queuing input system_q_in_policy`.
70. Type `service-policy type queuing output system_q_out_policy`.
71. Type `service-policy type network-qos system_nq_policy`.
72. Type `exit`.
73. Type `copy run start`.
74. Type `show running-config ipqos`.

```
class-map type qos class-fcoe
class-map type qos match-all class-gold
  match cos 4
class-map type qos match-all class-silver
  match access-group name classify_silver
class-map type qos match-all system_qos_policy
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-gold
  match qos-group 3
class-map type queuing class-silver
  match qos-group 4
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
```

```

match qos-group 2
policy-map type qos system_qos_policy
  class class-gold
    set qos-group 3
  class class-silver
    set qos-group 4
  class class-fcoe
    set qos-group 1
  class class-default
policy-map type queuing system_q_in_policy
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-gold
    bandwidth percent 33
  class type queuing class-silver
    bandwidth percent 29
  class type queuing class-default
    bandwidth percent 18
policy-map type queuing system_q_out_policy
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing class-gold
    bandwidth percent 33
  class type queuing class-silver
    bandwidth percent 29
  class type queuing class-default
    bandwidth percent 18
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-gold
  match qos-group 3
class-map type network-qos class-silver
  match qos-group 4
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos system_nq_policy
  class type network-qos class-gold
    set cos 4
    mtu 9000
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-silver
    set cos 2
    mtu 9000
  class type network-qos class-default
    mtu 9000
    multicast-optimize
system qos
  service-policy type qos input system_qos_policy
  service-policy type queuing input system_q_in_policy
  service-policy type queuing output system_q_out_policy
  service-policy type network-qos system_nq_policy

```

5.4 Create Necessary VLANs

These steps provide details for creating the necessary VLANs.

Nexus A

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

Nexus B

4. **Type** `vlan <<Fabric_B_FCoE_VLAN ID>>`.
5. **Type** `name FCoE_Fabric_B`.
6. **Type** `exit`.

Nexus A and Nexus B

1. **Type** `vlan <<Native VLAN ID>>`.
2. **Type** `name Native-VLAN`.
3. **Type** `exit`.
4. **Type** `vlan <<CSV VLAN ID>>`.
5. **Type** `name CSV-VLAN`.
6. **Type** `exit`.
7. **Type** `vlan <<Live Migration VLAN ID>>`.
8. **Type** `name Live-Migration-VLAN`.
9. **Type** `exit`.
10. **Type** `vlan <<SMB VLAN ID>>`.
11. **Type** `name SMB-VLAN`.
12. **Type** `exit`.
13. **Type** `vlan <<MGMT VLAN ID>>`.
14. **Type** `name Mgmt-VLAN`.
15. **Type** `exit`.
16. **Type** `vlan <<VM Database VLAN ID>>`.
17. **Type** `name VM-Database-VLAN`.
18. **Type** `exit`.
19. **Type** `vlan <<VM MF-Public VLAN ID>>`.
20. **Type** `name VM-MF-Public-VLAN`.
21. **Type** `exit`.
22. **Type** `vlan <<VM AF-Public VLAN ID>>`.
23. **Type** `name VM-AF-Public-VLAN`.
24. **Type** `exit`.
25. **Type** `vlan <<VM Cluster Comm VLAN ID>>`.
26. **Type** `name VM-Cluster-Comm-VLAN`.
27. **Type** `exit`.
28. **Type** `copy run start`
29. **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
2	Native-VLAN	active	
10	Mgmt-VLAN	active	
101	FCoE Fabric_A	active	
1001	VM-MF-Public-VLAN	active	
1002	VM-Database-VLAN	active	
1003	SMB-VLAN	active	
1004	CSV-VLAN	active	
1005	Live-Migration-VLAN	active	
1006	VM-App-Cluster-Comm-VLAN		active
1007	VM-AF-Public-VLAN	active	
VLAN Type Vlan-mode			

1	enet	CE	
2	enet	CE	
10	enet	CE	
101	enet	CE	
1001	enet	CE	
1002	enet	CE	
1003	enet	CE	
1004	enet	CE	
1005	enet	CE	
1006	enet	CE	
Primary	Secondary	Type	Ports

5.5 Add Individual Port Descriptions for Troubleshooting

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

Nexus 5548 A

From the global configuration mode, do the following:

1. Type `interface Eth1/1`.
2. Type `description <Controller A:e3a>`.
3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description <Controller B:e3a>`.
6. Type `exit`.
7. Type `interface Eth1/11`.
8. Type `description <UCSM A:Eth1/19>`.
9. Type `exit`.
10. Type `interface Eth1/12`.
11. Type `description <UCSM B:Eth1/19>`.
12. Type `exit`.
13. Type `interface Eth1/13`.
14. Type `description <Nexus B:Eth1/13>-PeerLink`.
15. Type `exit`.
16. Type `interface Eth1/14`.

17. Type description <Nexus B:Eth1/14>-PeerLink.
18. Type exit.
19. Type interface Eth1/31.
20. Type description <UCSM A:Eth1/31>FCoE.
21. Type exit.
22. Type interface Eth1/32.
23. Type description <UCSM A:Eth1/32>FCoE.
24. Type exit.
25. Type show interface description.

Port	Type	Speed	Description
Eth1/1	eth	10G	fascluster01-01:e3a
Eth1/2	eth	10G	fascluster01-02:e3a
Eth1/3	eth	10G	--
Eth1/4	eth	10G	--
Eth1/5	eth	10G	--
Eth1/6	eth	10G	--
Eth1/7	eth	10G	--
Eth1/8	eth	10G	--
Eth1/9	eth	10G	--
Eth1/10	eth	10G	--
Eth1/11	eth	10G	MSPCFT-UCS01-A:Eth1/19
Eth1/12	eth	10G	MSPCFT-UCS01-B:Eth1/20
Eth1/13	eth	10G	MSPCFT-N5548B:eth1/13-PeerLink
Eth1/14	eth	10G	MSPCFT-N5548B:eth1/14-PeerLink
Eth1/15	eth	10G	--
Eth1/16	eth	10G	--
Eth1/17	eth	10G	--
Eth1/18	eth	10G	--
Eth1/19	eth	10G	--
Eth1/20	eth	10G	--
Eth1/21	eth	10G	--
Eth1/22	eth	10G	--
Eth1/23	eth	10G	--
Eth1/24	eth	10G	--
Eth1/25	eth	10G	--
Eth1/26	eth	10G	--
Eth1/27	eth	10G	--
Eth1/28	eth	10G	--
Eth1/29	eth	10G	--
Eth1/30	eth	10G	--
Eth1/31	eth	10G	MSPCFT-UCS01-A:Eth1/31-FCoE
Eth1/32	eth	10G	MSPCFT-UCS01-A:Eth1/32-FCoE

Nexus 5548 B

From the global configuration mode, do the following:

1. Type interface Eth1/1.
2. Type description <Controller A:e4a>.
3. Type exit.
4. Type interface Eth1/2.
5. Type description <Controller B:e4a>.
6. Type exit.
7. Type interface Eth1/11.
8. Type description <UCSM A:Eth1/20>.

9. Type exit.
10. Type interface Eth1/12.
11. Type description <UCSM B:Eth1/20>.
12. Type exit.
13. Type interface Eth1/13.
14. Type description <Nexus A:Eth1/13>-PeerLink.
15. Type exit.
16. Type interface Eth1/14.
17. Type description <Nexus A:Eth1/14>-PeerLink.
18. Type exit.
19. Type interface Eth1/31.
20. Type description <UCSM B:Eth1/31>-FCoE.
21. Type exit.
22. Type interface Eth1/32.
23. Type description <UCSM B:Eth1/32>-FCoE.
24. Type exit.
25. Type show interface description.

Port	Type	Speed	Description
Eth1/1	eth	10G	fascluster01-01:e4a
Eth1/2	eth	10G	fascluster01-02:e4a
Eth1/3	eth	10G	--
Eth1/4	eth	10G	--
Eth1/5	eth	10G	--
Eth1/6	eth	10G	--
Eth1/7	eth	10G	--
Eth1/8	eth	10G	--
Eth1/9	eth	10G	--
Eth1/10	eth	10G	--
Eth1/11	eth	10G	MSPCFT-UCS01-A:Eth1/20
Eth1/12	eth	10G	MSPCFT-UCS01-B:Eth1/19
Eth1/13	eth	10G	MSPCFT-N5548A:eth1/13-PeerLink
Eth1/14	eth	10G	MSPCFT-N5548A:eth1/14-PeerLink
Eth1/15	eth	10G	--
Eth1/16	eth	10G	--
Eth1/17	eth	10G	--
Eth1/18	eth	10G	--
Eth1/19	eth	10G	--
Eth1/20	eth	10G	--
Eth1/21	eth	10G	--
Eth1/22	eth	10G	--
Eth1/23	eth	10G	--
Eth1/24	eth	10G	--
Eth1/25	eth	10G	--
Eth1/26	eth	10G	--
Eth1/27	eth	10G	--
Eth1/28	eth	10G	--
Eth1/29	eth	10G	--
Eth1/30	eth	10G	--
Eth1/31	eth	10G	MSPCFT-UCS01-B:Eth1/31-FCoE
Eth1/32	eth	10G	MSPCFT-UCS01-B:Eth1/32-FCoE

5.6 Create Necessary Port Channels

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

Nexus 5548 A

From the global configuration mode, do the following:

1. Type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.
4. Type `interface Eth1/13-14`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description <Controller A>`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `description <Controller B>`.
17. Type `exit`.
18. Type `interface Eth1/2`.
19. Type `channel-group 12 mode active`.
20. Type `no shutdown`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `description <UCSM A>`.
24. Type `exit`.
25. Type `interface Eth1/11`.
26. Type `channel-group 13 mode active`.
27. Type `no shutdown`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `description <UCSM B>`.
31. Type `exit`.
32. Type `interface Eth1/12`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `interface eth1/31`.
37. Type `switchport description <UCSM A:eth1/31>`.

38. Type `exit`.
39. Type `interface eth1/32`.
40. Type `switchport description <UCSM A:eth1/32>`.
41. Type `exit`.
42. Type `interface Po15`.
43. Type `description <UCSM A>-FCoE`.
44. Type `interface Eth1/31-32`.
45. Type `channel-group 15 mode active`.
46. Type `no shutdown`.
47. Type `exit`
48. Type `copy run start`.
49. Type `show port-channel summary`

Flags: D - Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed S - Switched R - Routed U - Up (port-channel) M - Not in use. Min-links not met					
Group	Port-Channel	Type	Protocol	Member Ports	
10	Po10 (SU)	Eth	LACP	Eth1/13 (P)	Eth1/14 (P)
11	Po11 (SD)	Eth	LACP	Eth1/1 (I)	
12	Po12 (SD)	Eth	LACP	Eth1/2 (I)	
13	Po13 (SD)	Eth	LACP	Eth1/11 (I)	
14	Po14 (SD)	Eth	LACP	Eth1/12 (I)	
15	Po15 (SD)	Eth	LACP	Eth1/31 (I)	Eth1/32 (I)

Nexus 5548 B

1. From the global configuration mode, type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.
4. Type `interface Eth1/13-14`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description <Controller A>`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `description <Controller B>`.

17. Type `exit`.
18. Type `interface Eth1/2`.
19. Type `channel-group 12 mode active`.
20. Type `no shutdown`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `description <UCSM A>`.
24. Type `exit`.
25. Type `interface Eth1/11`.
26. Type `channel-group 13 mode active`.
27. Type `no shutdown`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `description <UCSM B>`.
31. Type `exit`.
32. Type `interface Eth1/12`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `interface Po16`.
37. Type `description <UCSM B>-FCoE`.
38. Type `interface eth1/31-32`.
39. Type `channel-group 16 mode active`.
40. Type `no shutdown`.
41. Type `exit`.
42. Type `copy run start`.
43. Type `show port-channel summary`

```

Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
10    Po10(SU)    Eth       LACP      Eth1/13(P)  Eth1/14(P)
11    Po11(SD)    Eth       LACP      Eth1/1(I)
12    Po12(SD)    Eth       LACP      Eth1/2(I)
13    Po13(SD)    Eth       LACP      Eth1/11(I)
14    Po14(SD)    Eth       LACP      Eth1/12(I)
16    Po16(SD)    Eth       LACP      Eth1/31(I)  Eth1/32(I)

```

5.7 Add Port Channel Configurations

These steps provide details for adding Port Channel configurations.

Nexus 5548 A

From the global configuration mode, do the following:

1. **Type** interface Po10.
2. **Type** switchport mode trunk.
3. **Type** switchport trunk native vlan <<Native VLAN ID>>.
4. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>, <<SMB VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, >>, <<VM AF-Public VLAN ID>> <<VM APP Cluster Comm VLAN ID>>.
5. **Type** spanning-tree port type network.
6. **Type** no shutdown.
7. **Type** exit.
8. **Type** interface Po11.
9. **Type** switchport mode trunk.
10. **Type** switchport trunk native vlan <<Native VLAN ID>>.
11. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<SMB A VLAN ID>>, <<Fabric A FCoE VLAN ID>>.
12. **Type** spanning-tree port type edge trunk.
13. **Type** no shut.
14. **Type** exit.
15. **Type** interface Po12.
16. **Type** switchport mode trunk.
17. **Type** switchport trunk native vlan <<Native VLAN ID>>.
18. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<SMB VLAN ID>>, <<Fabric A FCoE VLAN ID>>.
19. **Type** spanning-tree port type edge trunk.
20. **Type** no shut.
21. **Type** exit.
22. **Type** interface Po13.
23. **Type** switchport mode trunk.
24. **Type** switchport trunk native vlan <<Native VLAN ID>>.
25. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>, <<SMB VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, >>, <<VM AF-Public VLAN ID>> <<VM Cluster Comm VLAN ID>>.
26. **Type** spanning-tree port type edge trunk.
27. **Type** no shut.
28. **Type** exit.
29. **Type** interface Po14
30. **Type** switchport mode trunk
31. **Type** switchport trunk native vlan <<Native VLAN ID>>.

32. Type `switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>,<<SMB VLAN ID>>, <<Live Migration VLAN ID>>, >>,<<VM MF-Public VLAN ID>>, <<VM AF-Public VLAN ID>>, <<VM Cluster Comm VLAN ID>>.`
33. Type `spanning-tree port type edge trunk.`
34. Type `no shutdown.`
35. Type `exit.`
36. Type `interface Po15.`
37. Type `switchport mode trunk.`
38. Type `switchport trunk allowed vlan <Fabric A FCoE VLAN ID>`
39. Type `no shutdown`
40. Type `exit.`
41. Type `copy run start.`
42. Type `show running-configuration port-channel 10-15`

```
interface port-channel10
  description vPC Peer-Link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  spanning-tree port type network

interface port-channel11
  description fascluster01-01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,101,1003
  spanning-tree port type edge trunk

interface port-channel12
  description fascluster01-02
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,101,1003
  spanning-tree port type edge trunk

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

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

interface port-channel15
  description MSPCFT-UCS01-A-FCoE
  switchport mode trunk
  switchport trunk allowed vlan 101
  speed 10000
```

Nexus 5548 B

From the global configuration mode, do the following:

1. Type `interface Po10.`
2. Type `switchport mode trunk.`

3. **Type** switchport trunk native vlan <<Native VLAN ID>>.
4. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<SMB VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, <<VM AF-Public VLAN ID>>, <<VM APP Cluster Comm VLAN ID>>.
5. **Type** spanning-tree port type network.
6. **Type** no shutdown.
7. **Type** exit.
8. **Type** interface Po11.
9. **Type** switchport mode trunk.
10. **Type** switchport trunk native vlan <<Native VLAN ID>>.
11. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<SMB VLAN ID>>, <<Fabric B FCoE VLAN ID>>.
12. **Type** spanning-tree port type edge trunk.
13. **Type** no shut.
14. **Type** exit.
15. **Type** interface Po12.
16. **Type** switchport mode trunk.
17. **Type** switchport trunk native vlan <<Native VLAN ID>>.
18. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<SMB VLAN ID>>, <<Fabric B FCoE VLAN ID>>.
19. **Type** spanning-tree port type edge trunk.
20. **Type** no shut.
21. **Type** exit.
22. **Type** interface Po13.
23. **Type** switchport mode trunk.
24. **Type** switchport trunk native vlan <Native VLAN ID>.
25. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<SMB VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, <<VM AF-Public VLAN ID>>, <<VM APP Cluster Comm VLAN ID>>.
26. **Type** spanning-tree port type edge trunk.
27. **Type** no shut.
28. **Type** exit.
29. **Type** interface Po14.
30. **Type** switchport mode trunk.
31. **Type** switchport trunk native vlan <Native VLAN ID>.
32. **Type** switchport trunk allowed vlan <<MGMT VLAN ID>>, <<CSV VLAN ID>>, <<SMB VLAN ID>>, <<Live Migration VLAN ID>>, <<VM Database VLAN ID>>, <<VM MF-Public VLAN ID>>, <<VM AF-Public VLAN ID>>, <<VM APP Cluster Comm VLAN ID>>.
33. **Type** spanning-tree port type edge trunk.
34. **Type** no shut.

35. Type `exit`.
36. Type `interface Po16`.
37. Type `switchport mode trunk`.
38. Type `switchport trunk allowed vlan <Fabric B FCoE VLAN ID>`
39. Type `no shutdown`.
40. Type `exit`.
41. Type `copy run start`.
42. Type `show running-configuration port-channel 10-14`

```
interface port-channel10
  description vPC Peer-Link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,1001-1007
  spanning-tree port type network

interface port-channel11
  description fascluster01-01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,102,1003
  spanning-tree port type edge trunk

interface port-channel12
  description fascluster01-02
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 10,102,1003
  spanning-tree port type edge trunk

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

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
```

43. Type `show running-configuration port-channel 16`

```
interface port-channel16
  description MSPCFT-UCS01-B-FCoE
  switchport mode trunk
  switchport trunk allowed vlan 102
```

5.8 Configure Virtual Port Channels

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

Nexus 5548 A

From the global configuration mode, do the following:

1. Type `vpc domain <Nexus vPC domain ID>`.
2. Type `role priority 10`.

3. **Type** peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0 IP> vrf management.
4. **Type** exit.
5. **Type** interface Po10.
6. **Type** vpc peer-link.
7. **Type** exit.
8. **Type** interface Po11.
9. **Type** vpc 11.
10. **Type** exit.
11. **Type** interface Po12.
12. **Type** vpc 12.
13. **Type** exit.
14. **Type** interface Po13.
15. **Type** vpc 13.
16. **Type** exit.
17. **Type** interface Po14.
18. **Type** vpc 14.
19. **Type** exit.
20. **Type** copy run start.
21. **Type** show vpc brief.

Legend:

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

```
vPC domain id          : 100
Peer status            : peer link is down
                       (peer-keepalive not operational,
                       peer never alive)
vPC keep-alive status  : Suspended (Destination IP not reachable)
Configuration consistency status : failed
Per-vlan consistency status : success
Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason  : Consistency Check Not Performed
vPC role               : none established
Number of vPCs configured : 4
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status    : Disabled
```

vPC Peer-link status

id	Port	Status	Active vlans
1	Po10	up	-

vPC status

id	Port	Status	Consistency	Reason	Active vlans
11	Po11	down	Not Applicable	Consistency Check Not Performed	-
12	Po12	down	Not Applicable	Consistency Check Not Performed	-
13	Po13	down	Not Applicable	Consistency Check Not Performed	-

14	Pol4	down	Not Applicable	Consistency Check Not Performed	-
----	------	------	-------------------	------------------------------------	---

Nexus 5548 B

From the global configuration mode, do the following:

1. Type `vpc domain <Nexus vPC domain ID>`.
2. Type `role priority 20`.
3. Type `peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0 IP> vrf management`.
4. Type `exit`.
5. Type `interface Po10`.
6. Type `vpc peer-link`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `vpc 11`.
10. Type `exit`.
11. Type `interface Po12`.
12. Type `vpc 12`.
13. Type `exit`.
14. Type `interface Po13`.
15. Type `vpc 13`.
16. Type `exit`.
17. Type `interface Po14`.
18. Type `vpc 14`.
19. Type `exit`.
20. Type `copy run start`.
21. Type `show vpc brief`.

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            : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Disabled
```

vPC Peer-link status

```
-----
id  Port  Status Active vlans
--  ---  -
1   Po10  up    10,1001-1006
```

vPC status

id	Port	Status	Consistency	Reason	Active vlans
11	Po11	down*	Not Applicable	Consistency Check Not Performed	-
12	Po12	down*	Not Applicable	Consistency Check Not Performed	-
13	Po13	down*	Not Applicable	Consistency Check Not Performed	-
14	Po14	down*	Not Applicable	Consistency Check Not Performed	-

5.9 Configure FCoE Fabric

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

Nexus 5548 A

1. Type `interface vfc11`.
2. Type `bind interface po11`.
3. Type `no shutdown`.
4. Type `exit`.
5. Type `interface vfc12`.
6. Type `bind interface po12`.
7. Type `no shutdown`.
8. Type `exit`.
9. Type `interface vfc15`.
10. Type `bind interface po15`.
11. Type `switchport trunk allowed vsan 101`
12. Type `no shutdown`.
13. Type `exit`.
14. Type `vsan database`.
15. Type `vsan <VSAN A ID>`
16. Type `vsan <VSAN A ID> name Fabric_A`.
17. Type `vsan <VSAN A ID> interface vfc11`.
18. Type `vsan <VSAN A ID> interface vfc12`.
19. Type `vsan <VSAN A ID> interface vfc15`.
20. Type `exit`.
21. Type `vlan <<Fabric_A_FCoE_VLAN ID>>`
22. Type `fcoe vsan <VSAN A ID>`.
23. Type `exit`.
24. Type `copy run start`
25. Type `show vsan 101`.

```
vsan 101 information
  name:Fabric_A  state:active
  interoperability mode:default
  loadbalancing:src-id/dst-id/oxid
  operational state:down
```

26. Type show vsan 101 membership.

```
vsan 101 interfaces:
    vfc11          vfc12          vfc15
```

27. Type show port-channel database interface po11,po12,po15.

```
port-channel11
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:54m:02s
  Time since last bundle is 1d:22h:52m:42s
  Last bundled member is Ethernet1/1
  Ports:   Ethernet1/1      [active ] [individual]

port-channel12
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:52m:17s
  Time since last bundle is 1d:22h:51m:38s
  Last bundled member is Ethernet1/2
  Ports:   Ethernet1/2      [active ] [individual]

port-channel15
  Last membership update is successful
  2 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:44m:47s
  Time since last bundle is 1d:22h:07m:26s
  Last bundled member is Ethernet1/32
  Time since last unbundle is 1d:22h:07m:39s
  Last unbundled member is Ethernet1/32
  Ports:   Ethernet1/31      [active ] [down]
           Ethernet1/32      [active ] [down]
```

Nexus 5548 B

1. Type interface vfc11.
2. Type bind interface po11.
3. Type no shutdown.
4. Type exit.
5. Type interface vfc12.
6. Type bind interface po12.
7. Type no shutdown
8. Type exit.
9. Type interface vfc16
10. Type bind interface po16
11. Type switchport trunk allowed vsan 102
12. Type no shutdown
13. Type exit.
14. Type vsan database.
15. Type vsan <VSAN B ID>
16. Type vsan <VSAN B ID> name Fabric_B.
17. Type vsan <VSAN B ID> interface vfc11.
18. Type vsan <VSAN B ID> interface vfc12.
19. Type vsan <VSAN B ID> interface vfc16

20. Type `exit`.
21. Type `vlan <<Fabric_B_FCoE_VLAN ID>>`
22. Type `fcoe vsan <VSAN B ID>`.
23. Type `exit`.
24. Type `copy run start`.
25. Type `show vsan 102`.

```
vsan 102 information
  name:Fabric_B  state:active
  interoperability mode:default
  loadbalancing:src-id/dst-id/oxid
  operational state:down
```

26. Type `show vsan 101 membership`.

```
vsan 102 interfaces:
  vfc11          vfc12          vfc16
```

27. Type `show port-channel database interface po11,po12,po16`.

```
port-channel11
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:35m:03s
  Time since last bundle is 1d:22h:34m:09s
  Last bundled member is Ethernet1/1
  Ports:  Ethernet1/1      [active ] [individual]

port-channel12
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:32m:25s
  Time since last bundle is 1d:22h:31m:42s
  Last bundled member is Ethernet1/2
  Ports:  Ethernet1/2      [active ] [individual]

port-channel16
  Last membership update is successful
  2 ports in total, 0 ports up
  Age of the port-channel is 1d:22h:27m:50s
  Time since last bundle is 1d:22h:14m:47s
  Last bundled member is Ethernet1/32
  Time since last unbundle is 1d:22h:14m:52s
  Last unbundled member is Ethernet1/32
  Ports:  Ethernet1/31      [active ] [down]
          Ethernet1/32      [active ] [down]
```

5.10 Link into Existing Network Infrastructure

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

6 Storage Configuration

6.1 Controller FAS32xx Series

Table 17) Controller FAS32XX series prerequisites.

Requirement	Reference	Comments
Physical site where storage system needs to be installed must be ready	Site Requirements Guide	Refer to the “Site Preparation” section.
Storage system connectivity requirements	Site Requirements Guide	Refer to the “System Connectivity Requirements” section.
Storage system general power requirements	Site Requirements Guide	Refer to the “Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements” section.
Storage system model-specific requirements	Site Requirements Guide	Refer to the “FAS32xx/V32xx Series Systems” section.

System Configuration Guides

System configuration guides provide supported hardware and software components for the specific Data ONTAP version. These online guides provide configuration information for all NetApp storage appliances currently supported by the Data ONTAP software. They also provide 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 [System Configuration Guides](#) at the [NetApp Support](#) site.
2. Click the appropriate NetApp storage appliance and then click the component you want to view. Alternatively, to compare components by storage appliance, click a component and then click the NetApp storage appliance you want to view.

Controllers

Follow the physical installation procedures for the controllers in the [FAS32xx documentation](#) at the [NetApp Support](#) site.

6.2 Disk Shelves DS2246 Series

DS2246 Disk Shelves

Follow the procedures in the [Disk Shelf Installation and Setup section of the DS2246 Disk Shelf Overview](#) to install a disk shelf for a new storage system.

Follow procedures for proper cabling with the controller model as described in [SAS Disk Shelves Universal SAS and ACP Cabling Guide](#).

The following information applies to DS2246 disk shelves:

- SAS disk drives use software-based disk ownership. Ownership of a disk drive is assigned to a specific storage system by writing software ownership information on the disk drive rather than by using the topography of the storage system's physical connections.
- Connectivity terms used: shelf-to-shelf (daisy-chain), controller-to-shelf (top connections), and shelf-to controller (bottom connections).
- Unique disk shelf IDs must be set per storage system (a number from 0 through 98).
- Disk shelf power must be turned on to change the digital display shelf ID. The digital display is on the front of the disk shelf.
- Disk shelves must be power-cycled after the shelf ID is changed for it to take effect.
- Changing the shelf ID on a disk shelf that is part of an existing storage system running Data ONTAP requires that you wait at least 30 seconds before turning the power back on so that Data ONTAP can properly delete the old disk shelf address and update the copy of the new disk shelf address.
- Changing the shelf ID on a disk shelf that is part of a new storage system installation (the disk shelf is not yet running Data ONTAP) requires no wait; you can immediately power-cycle the disk shelf.

6.3 Cisco NX5596 Cluster Network Switch Configuration

Table 18) Cisco Nexus 5596 cluster network switch configuration prerequisites.

Description
<ul style="list-style-type: none">• Rack and connect power to the new Cisco Nexus 5596 switches• Provide a terminal session that connects to the switch's serial console port (9600, 8, n, 1)• Connect the <code>mgmt 0</code> port to the management network and be prepared to provide IP address information• Obtain password for admin• Determine switch name• Identify SSH key type (dsa, rsa, or rsa1)• Set up an e-mail server for Cisco Smart Call Home and IP connectivity between the switch and the e-mail server• Provide SNMP contact information for Cisco Smart Call Home (name, phone, street address)• Identify a CCO ID associated with an appropriate Cisco SMARTnet® Service contract for Cisco Smart Call Home• Enable Cisco SMARTnet Service for the device to be registered for Cisco Smart Call home

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, 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

```
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
```

6.4 Clustered Data ONTAP 8.2

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, proceed to step 4 to load Data ONTAP 8.2 software. If Data ONTAP 8.2 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 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2 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.bsdportname 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...
```

23. From the Loader-A prompt, enter:

```
printenv
```

24. If the last-OS-booted-ver parameter is not set to 8.2, proceed to step 4 to load Data ONTAP 8.2 software. If Data ONTAP 8.2 is already loaded, proceed to step 16.

25. Allow the system to boot up.

```
boot_ontap
```

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

```
Ctrl-C
```

Note: If Data ONTAP 8.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2 is the version being booted, then select option 8 and yes to reboot the node. Then proceed with step 15.

27. To install new software first select option 7.

```
7
```

28. Answer yes to perform a nondisruptive upgrade.

```
y
```

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

```
e0M
```

30. Select yes to reboot now.

```
y
```

31. 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>>
```

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

Note: This Web server must be pingable.

```
<<var_url_boot_software>>
```

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

```
Enter
```

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

y

35. 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.

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

Starting AUTOBOOT press Ctrl-C to abort...

37. 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.

38. 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
```

39. At the LOADER-A prompt, enter:

autoboot

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

Ctrl - C

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

4

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

y

43. 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.

6.5 Cluster Create in Clustered Data ONTAP

Table 19) 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 Detail	Cluster Detail Value
Cluster management port	<<var_clustermgmt_port>>
Cluster management gateway	<<var_clustermgmt_gateway>>
ClusterNode01 IP address	<<var_node01_mgmt_ip>>
ClusterNode01 netmask	<<var_node01_mgmt_mask>>
ClusterNode01 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]:
```

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

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

6. 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®, CIFS, FCP, FlexClone®, and SnapManager® 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>>
```

44. 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.

45. 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.

46. Press Enter to accept the AutoSupport™ message.

47. Reboot node 01.

```
system node reboot <<var_node01>>
y
```

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

```
Ctrl - C
```

49. Select 5 to boot into maintenance mode.

```
5
```

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

51. 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.

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

```
disk show -a
```

Note: No disks should be owned in this list.

53. 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>>
```

54. Reboot the controller.

```
halt
```

55. At the LOADER-A prompt, enter:

```
autoboot
```

6.6 Cluster Join in Clustered Data ONTAP

Table 20) 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.

56. 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
```

57. 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.

58. Press Enter to accept the AutoSupport message.

59. Log in to the Cluster Interface with the admin user id and <<var_password>>.

60. Reboot node 02.

```
system          node          reboot          <<var_node02>>
y
```

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

```
Ctrl - C
```

6. Select 5 to boot into maintenance mode.

```
5
```

62. At the question, Continue with boot? enter:

```
y
```

63. 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
```

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

```
disk show -a
```

65. 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>>
```

66. Reboot the controller:

```
halt
```

67. At the LOADER-A prompt, enter:

```
autoboot
```

68. Press Ctrl-C for boot menu when prompted.

```
Ctrl-C
```

6.7 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.

6.8 Zero All Spare Disks

Zero all spare disks in the cluster.

```
disk zerospares
```

6.9 Set Auto-Revert on Cluster Management

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

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

6.10 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
```

6.11 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
```

6.12 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
```

6.13 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
```

6.14 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.

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

6.16 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

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

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

3. 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>>
```

6.17 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>>
```

6.18 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.

6.19 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>>
```

6.20 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
```

6.21 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 <ccyyymmddhhmm>
```

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>>
```

6.22 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>>
```

6.23 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.

6.24 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.

6.25 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>>
```

6.26 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
```

6.27 Vserver

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

```
vserversetup

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
```

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

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

5. Add the two data aggregates to the Infra_vs1 aggregate list for NetApp Virtual Console.

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

6.28 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
```

6.29 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>>
```

6.30 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>>
```

6.31 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
```

6.32 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.

```
fcv create -vserver Infra_vs1
```

6.33 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
```

6.34 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_vsl -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.

6.35 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_vsl -domains <<var_dnsdomain>> -name-servers
<<var_ip_dnsserver>> -state enabled
```

6.36 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_vsl -policyname default -ruleindex 1 -
rorule never -rwrule never -superuser never

vserver export-policy create -vserver Infra_vsl 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!

6.37 FlexVol in Clustered Data ONTAP

1. The following information is required to create a FlexVol® 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 scvmm_lib -aggregate aggr01_n1 -size 1TB -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

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

6.38 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
```

6.39 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
```

6.40 NetApp SAN Configuration Create Device Aliases

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

Gather Necessary Information

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

Table 21) FC Port Names for the infrastructure Vserver

NetApp Controller	FC Lif	FC Portname
Controller A	fcp_lif01a	
	fcp_lif01b	
Controller B	fcp_lif02a	
	fcp_lif02b	

Note: To gather the information in the table above, run `network interface show`.

Nexus 5548 A

- Using the information in Table 21 Create device alias.

```
device-alias database
  device-alias name Infra_vs1_lif01a pwnn <fcp_lif01a WWPN>
  device-alias name Infra_vs1_lif02a pwnn <fcp_lif02a WWPN>
exit
device-alias commit
copy running-config startup-config
```

- Verify device aliase database entries.

```
(config)# show device-alias database
device-alias name Infra_vs1_lif01a pwnn 20:00:00:a0:98:17:4d:5c
device-alias name Infra_vs1_lif02a pwnn 20:02:00:a0:98:17:4d:5c

Total number of entries = 2
(config)# show flog database
-----
INTERFACE      VSAN    FCID      PORT NAME      NODE NAME
-----
vfc11          101     0x130020  50:0a:09:81:8d:13:43:ba 50:0a:09:80:8d:13:43:ba
vfc11          101     0x130021  20:00:00:a0:98:17:4d:5c 20:04:00:a0:98:17:4d:5c
               [Infra_vs1_lif01a]
vfc12          101     0x130040  50:0a:09:81:8d:d3:42:07 50:0a:09:80:8d:d3:42:07
vfc12          101     0x130041  20:02:00:a0:98:17:4d:5c 20:04:00:a0:98:17:4d:5c
               [Infra_vs1_lif02a]
vfc15          101     0x130000  22:db:54:7f:ee:1c:04:bf 20:65:54:7f:ee:1c:04:81

Total number of flogi = 5.
```

Nexus 5548 B

- Using the information in Table 21 Create device alias.

```

device-alias database
  device-alias name Infra_vs1_lif01b pwwn <fcplif01b WWPN>
  device-alias name Infra_vs1_lif02b pwwn <fcplif02b WWPN>
exit
device-alias commit
copy running-config startup-config

```

2. Verify device aliase database entries.

```

(config)# show device-alias database
device-alias name Infra_vs1_liv01b pwwn 20:01:00:a0:98:17:4d:5c
device-alias name Infra_vs1_liv02b pwwn 20:03:00:a0:98:17:4d:5c

Total number of entries = 2
(config)# show flogi database
-----
INTERFACE      VSAN    FCID      PORT NAME      NODE NAME
-----
vfc11           102     0xc90020   50:0a:09:83:8d:13:43:ba 50:0a:09:80:8d:13:43:ba
vfc11           102     0xc90021   20:01:00:a0:98:17:4d:5c 20:04:00:a0:98:17:4d:5c
                  [Infra_vs1_liv01b]
vfc12           102     0xc90040   50:0a:09:83:8d:d3:42:07 50:0a:09:80:8d:d3:42:07
vfc12           102     0xc90041   20:03:00:a0:98:17:4d:5c 20:04:00:a0:98:17:4d:5c
                  [Infra_vs1_liv02b]
vfc16           102     0xc90000   22:dc:54:7f:ee:19:f3:3f 20:66:54:7f:ee:19:f3:01

Total number of flogi = 5.

```


7 Cisco Unified Computing System Deployment Procedure

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

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

7.1 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.

7.2 Add a Block of IP Addresses for KVM Access

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

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

7.3 Synchronize Cisco UCS to NTP

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

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

7.4 Chassis Discovery Policy

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

1. Navigate to the Equipment tab in the left pane and select the Equipment top-node object.
2. In the right pane, click the Policies tab.

- 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.
- Keep Link Grouping Preference set to Port Channel
- Select Manual Blade Level Cap for the Global Power Allocation Policy
- Click Save Changes in the bottom right corner.

The screenshot shows the 'Equipment' configuration window with the 'Policies' tab selected. The 'Global Policies' sub-tab is active, displaying several policy configuration sections:

- Chassis/FEX Discovery Policy:** Action is set to '4 Link'. Link Grouping Preference has radio buttons for 'None' and 'Port Channel' (selected).
- Rack Server Discovery Policy:** Action has radio buttons for 'Immediate' (selected) and 'User Acknowledged'. Scrub Policy is set to '<not set>'.
- Rack Management Connection Policy:** Action has radio buttons for 'Auto Acknowledged' (selected) and 'User Acknowledged'.
- Power Policy:** Redundancy has radio buttons for 'Non Redundant', 'N+1' (selected), and 'Grid'.
- MAC Address Table Aging:** Aging Time has radio buttons for 'Never', 'Mode Default' (selected), and 'other'.
- Global Power Allocation Policy:** Allocation Method has radio buttons for 'Manual Blade Level Cap' (selected) and 'Policy Driven Chassis Group Cap'.

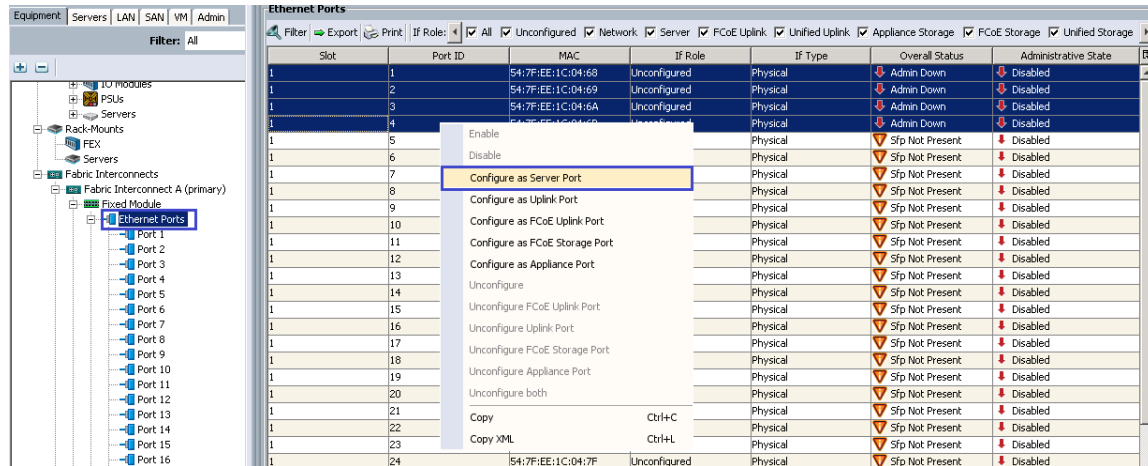
At the bottom right, there are two buttons: 'Save Changes' and 'Reset Values'.

7.5 Enable Server and Uplink Ports

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

- Select the **Equipment** tab on the top left of the window.
- Select **Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module**.
- Expand the **Ethernet Ports** object.
- 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**.
- Click **Yes** to confirm the server ports, and then click **OK**.

- The ports connected to the chassis or to the Cisco 2232 FEX are now configured as server ports.

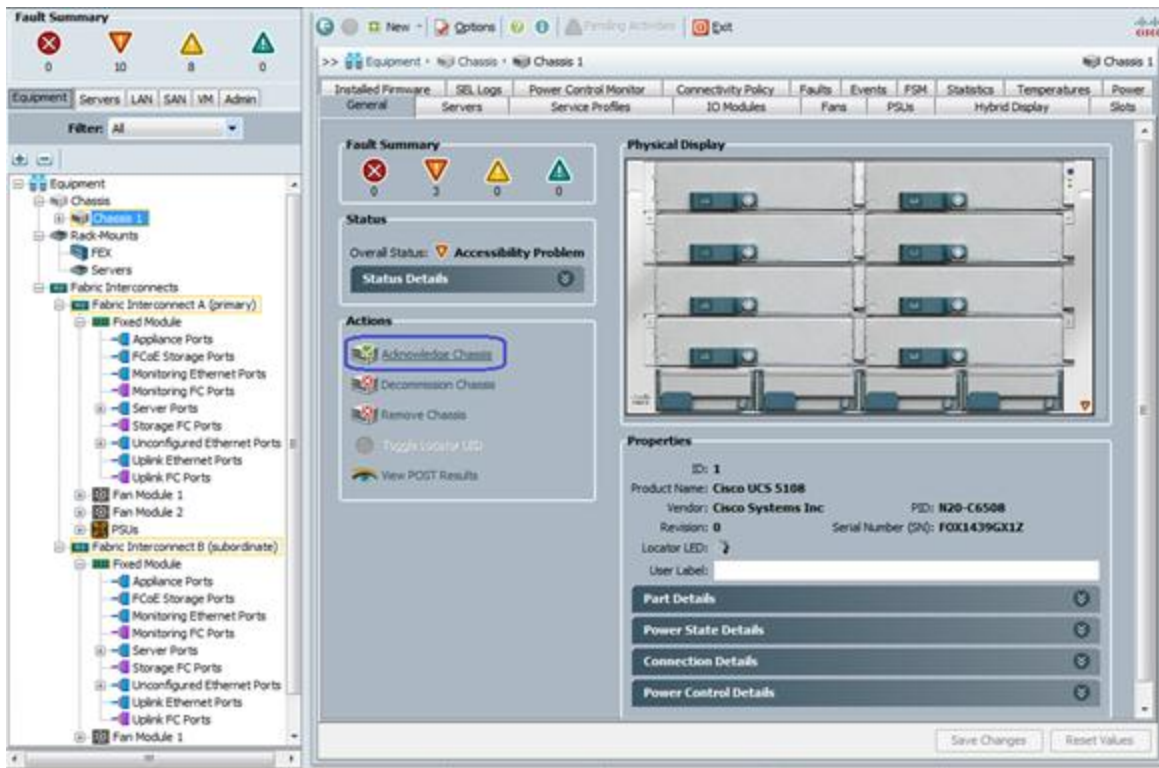


- A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue.
- Select ports the number of ports that are connected to the Cisco UCS chassis (4 per chassis), right-click them, and select **Configure as Uplink Port**.
- A prompt displays asking if this is what you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

7.6 Acknowledge the Cisco UCS Chassis

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

- Select **Chassis 1** in the left pane.
- Click **Acknowledge Chassis**.



7.7 Create Uplink Port Channels to the Cisco Nexus 5548 Switches

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

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

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

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

Unified Computing System Manager

Create Port Channel

1. [Set Port Channel Name](#)
2. [Add Ports](#)

Set Port Channel Name

ID:

Name:

8. Select the port with slot ID: 1 and port: 19 and also the port with slot ID: 1 and port 20 to be added to the Port Channel.
9. Click >> to add the ports to the Port Channel.
10. Click Finish to create the Port Channel.
11. Select the check box for Show navigator for Port-Channel 13 (Fabric A)
12. Click OK to continue.
13. Wait until the overall status of the Port Channel is up.

Equipment Servers LAN SAN VM Admin

Filter: All

LAN

LAN Cloud

Fabric A

Port Channels

Port-Channel 13 (vPC-13-N5548)

Uplink Eth Interfaces

VLAN Optimization Sets

VLANs

Fabric B

QoS System Class

LAN Pin Groups

General Ports Faults Events Statistics

Status

Overall Status: Up

Additional Info:

Actions

Enable Port Channel

Disable Port Channel

Add Ports

Properties

ID: 13

Fabric ID: A

Port Type: Aggregation

Transport Type: Ether

Name: vPC-13-N5548

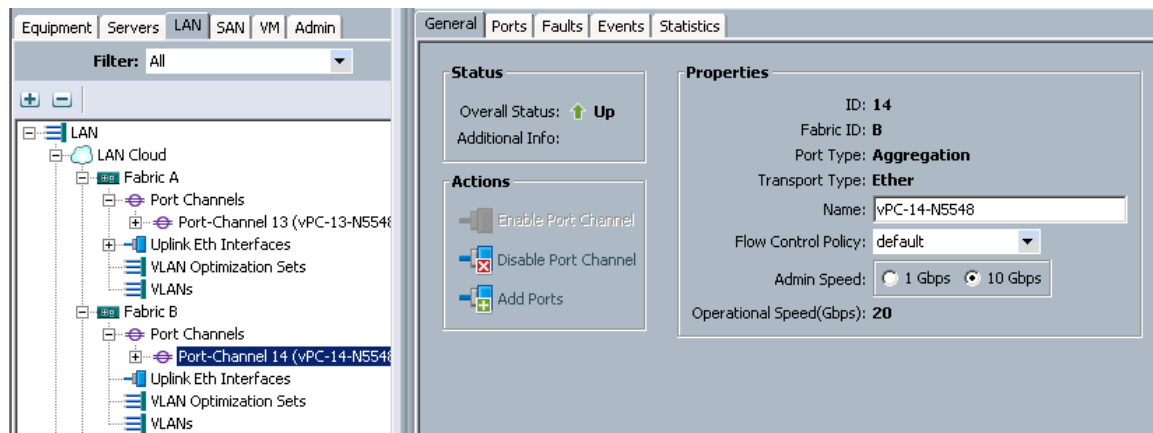
Flow Control Policy: default

Admin Speed: ☐ 1 Gbps ☒ 10 Gbps

Operational Speed(Gbps): 20

14. Click OK to close the Navigator.
15. Under LAN Cloud, expand the Fabric B tree.
16. Right-click Port Channels.
17. Select Create Port Channel.
18. Enter 14 as the unique ID of the Port Channel.
19. Enter vPC-14-N5548 as the name of the Port Channel.
20. Click Next.

21. Select the port with slot ID: 1 and port: 19 and also the port with slot ID: 1 and port 20 to be added to the Port Channel.
22. Click >> to add the ports to the Port Channel.
23. Click **Finish** to create the Port Channel.
24. Select Check box for Show navigator for Port-Channel 14 (Fabric B) .
25. Click **OK** to continue.
26. Wait until the overall status of the Port Channel is up
27. Click **OK** to close the Navigator.



7.8 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.

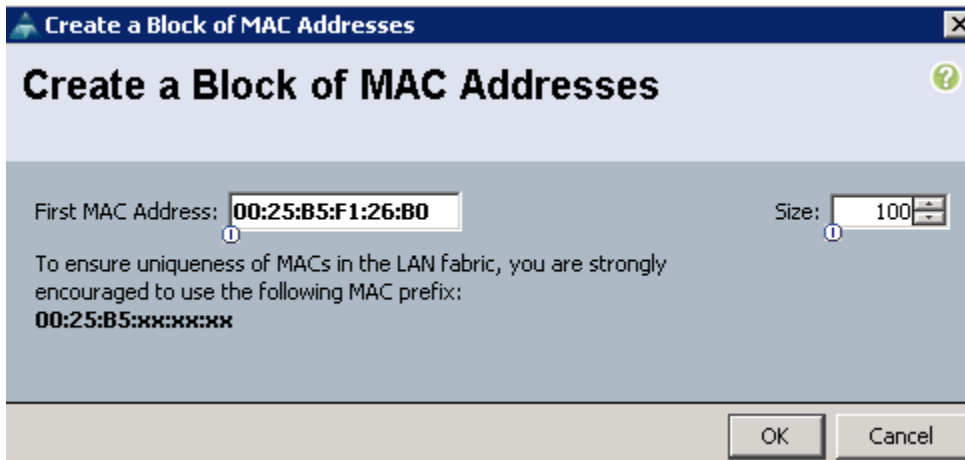
1. Navigate to the Server Tab.
2. Expand Servers and expand Service Profiles
3. Select Service Profiles in the right tree view and click **Create Organization** in the left main view.
4. Enter a name for the organization.
5. Enter a description for the organization (optional).
6. Click **OK**.
7. In the message box that displays, click **OK**.

7.9 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.



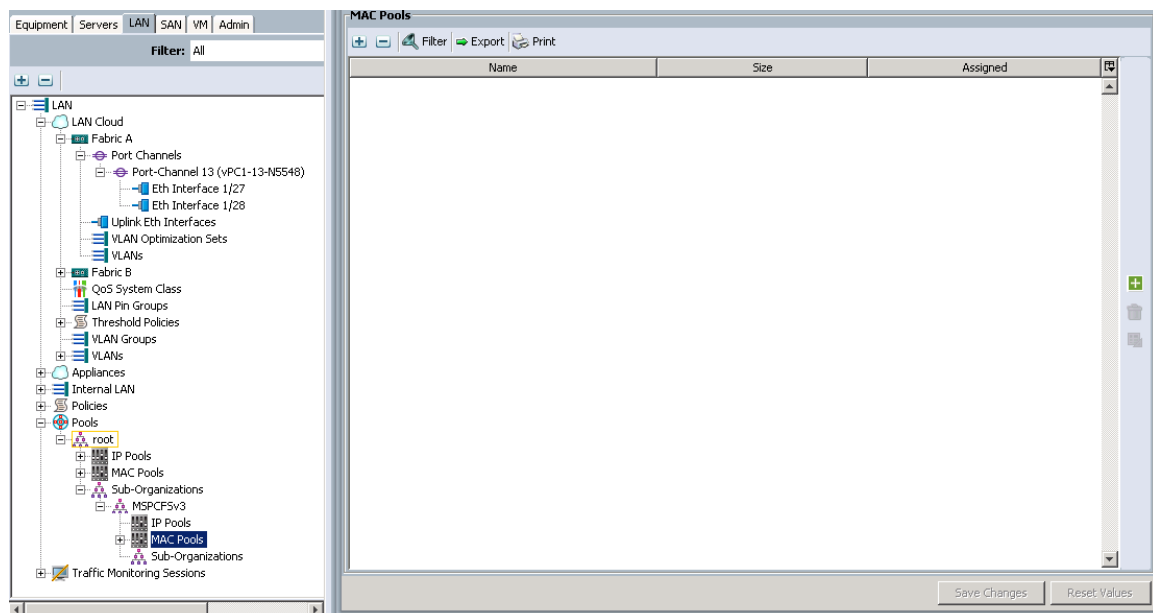
Create a Block of MAC Addresses

First MAC Address: Size:

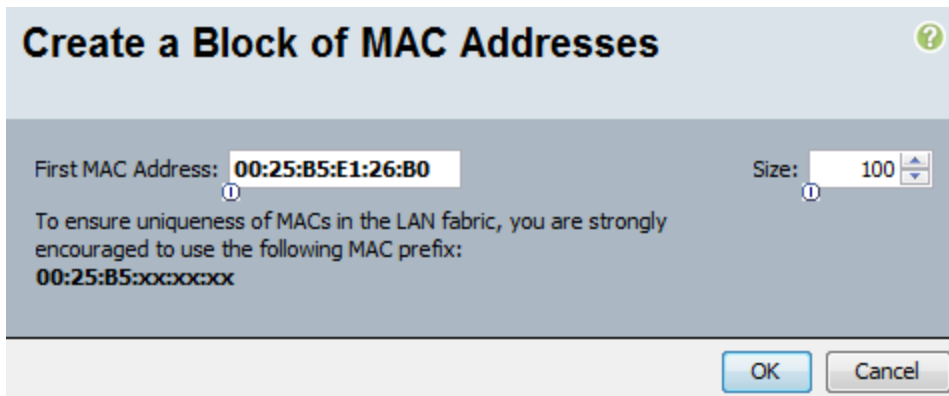
To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:
00:25:B5:xx:xx:xx

OK Cancel

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 MSPCMAC_Pool for 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.



Create a Block of MAC Addresses

First MAC Address: **00:25:B5:E1:26:B0** Size: **100**

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:
00:25:B5:xx:xx:xx

OK Cancel

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


7.10 Create WWNN Pools

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

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

Note: The default is appropriate for most configurations, modify if necessary.

9. Specify a size of the WWNN block sufficient to support the available blade resources.



Create WWN Block


From: **20:00:00:25:B5:B8:08:FF** Size: **100**

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

10. Click **OK** to proceed.
11. Click **Finish** to proceed.
12. Click **OK** to finish.
13. Select **Pools > root >** and the previously created sub organization.

14. Right click WWNN and select Create WWN Pool
15. Enter `WWNN_Pool` as the name of the WWNN pool.
16. (Optional) Add a description for the WWNN pool.
17. Click `Next` to continue.
18. Click `Add` to add a block of WWNN's.
19. Specify a size of the WWPN block sufficient to support the available server resources.



Create WWN Block ?

From: Size:

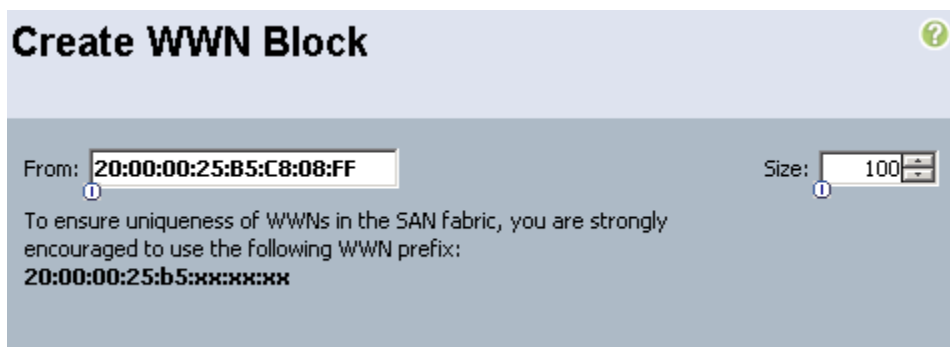
To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:
20:00:00:25:b5:xx:xx:xx

20. Click `OK`.
21. Click `Finish` to create the WWPN pool.
22. Click `OK`.

7.11 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.



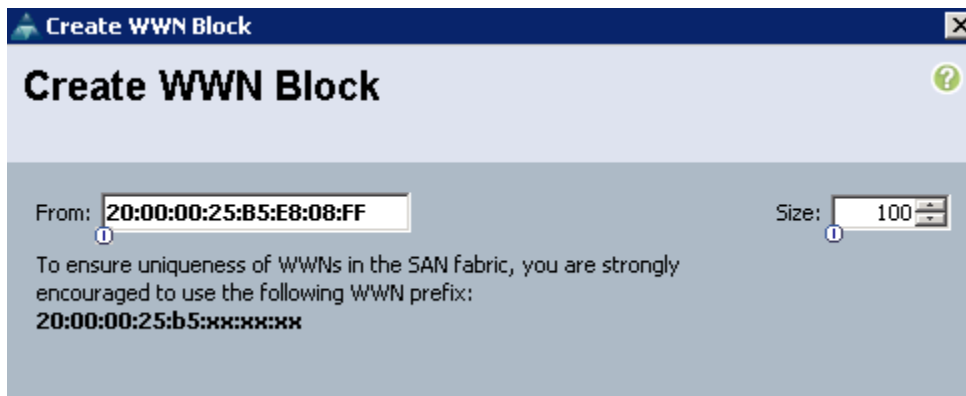
Create WWN Block ?

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

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.



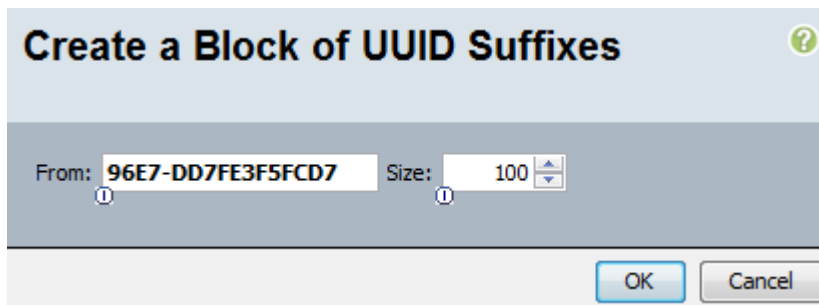
The image shows a dialog box titled "Create WWN Block". It has a blue header bar with the title and a close button. Below the header, there is a text input field for "From:" containing the value "20:00:00:25:B5:E8:08:FF" and a spin box for "Size:" set to "100". Below these fields, there is a message: "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".

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

7.12 Create UUID Suffix Pools

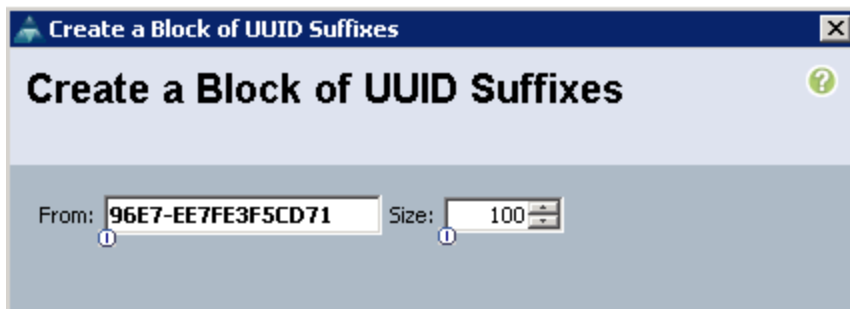
These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

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.



The image shows a dialog box titled "Create a Block of UUID Suffixes". It has a blue header bar with the title and a close button. Below the header, there is a text input field for "From:" containing the value "96E7-DD7FE3F5FCD7" and a spin box for "Size:" set to "100". At the bottom of the dialog, there are "OK" and "Cancel" buttons.

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.

7.13 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 **Infra_Pool**.
6. (Optional) Give the server pool a description.
7. Click **Next** to continue to add servers.
8. Select two server to be used for the infrastructure cluster and Click **>>** to add them to the pool.
9. Click **Finish**.
10. Select **OK** to finish.

7.14 Create VLANs

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

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

Note: Eight VLANs are created.

11. Select **LAN Cloud**.
12. Right-click **VLANs**.
13. Select **Create VLANs**.
14. Enter **Mgmt-VLAN** as the name of the VLAN to be used for management traffic.
15. Keep the **Common/Global** option selected for the scope of the VLAN.
16. Enter the VLAN ID for the management VLAN. Keep the sharing type as **none**.
17. Click **OK**.

Create VLANs

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

18. Right-click VLANs .
19. Select Create VLANs.
20. Enter CSV-VLAN as the name of the VLAN to be used for the CSV VLAN.
21. Keep the Common/Global option selected for the scope of the VLAN.
22. Enter the VLAN ID for the CSV VLAN.
23. Click OK.

Create VLANs

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

24. Right-click VLANs .
25. Select Create VLANs.
26. Enter SMB-VLAN as the name of the VLAN to be used for the VHD access LAN.
27. Keep the Common/Global option selected for the scope of the VLAN.

28. Enter the VLAN ID for the first iSCSI VLAN .
29. Click OK.

Create VLANs

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

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

Create VLANs

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

36. Right click VLANs
37. Select Create VLANs .

38. Enter `VM-App-Cluster-Comm-VLAN` as the name of the VLAN to be used for the VM Cluster VLAN.
39. Keep the `Common/Global` option selected for the scope of the VLAN.
40. Enter the VLAN ID for the VM Cluster VLAN.
41. Click `OK`.

Create VLANs

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

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

Create VLANs ?

VLAN Name/Prefix:

Multicast Policy Name: + Create Multicast Policy

☒ 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

48. Right-click VLANs .
49. Select Create VLANs.
50. Enter VM-MF-Public-VLAN as the name of the VLAN to be used for the VM data VLAN.
51. Keep the Common/Global option selected for the scope of the VLAN.
52. Enter the VLAN ID for the Management Fabric Public VLAN.
53. Click OK.

Create VLANs ?

VLAN Name/Prefix:

Multicast Policy Name: + Create Multicast Policy

☒ 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

54. Right-click VLANs .

55. Select **Create VLANs**.
56. Enter **VM-AF-Public-VLAN** as the name of the VLAN to be used for the VM data VLAN.
57. Keep the **Common/Global** option selected for the scope of the VLAN.
58. Enter the VLAN ID for the Application Fabric Public VLAN.
59. Click **OK**.

Create VLANs

VLAN Name/Prefix: **VM-AF-Public-VLAN**

Multicast Policy Name: **<not set>** + Create Multicast Policy

☒ 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: **1007**

Sharing Type: ☒ None ☐ Primary ☐ Isolated

60. Right-click **VLANs**.
61. Select **Create VLANs**.
62. Enter **Native-VLAN** as the name of the VLAN to be used for the Native VLAN.
63. Keep the **Common/Global** option selected for the scope of the VLAN.
64. Enter the VLAN ID for the Native VLAN.
65. Click **OK**.

Create VLANs

VLAN Name/Prefix: **Native**

Multicast Policy Name: **<not set>** + Create Multicast Policy

☒ 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: **2**

Sharing Type: ☒ None ☐ Primary ☐ Isolated

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

7.15 Create VSANs and FCoE Port Channels

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

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

Create VSAN

Name:

Default Zoning: ☒ Disabled ☐ Enabled

☐ 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.

VSAN ID:

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.

FCoE VLAN:

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

Create VSAN

Name:

Default Zoning: ☒ Disabled ☐ Enabled

☐ 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.

VSAN ID:

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.

FCoE VLAN:

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

Unified Computing System Manager

Create FCoE Port Channel

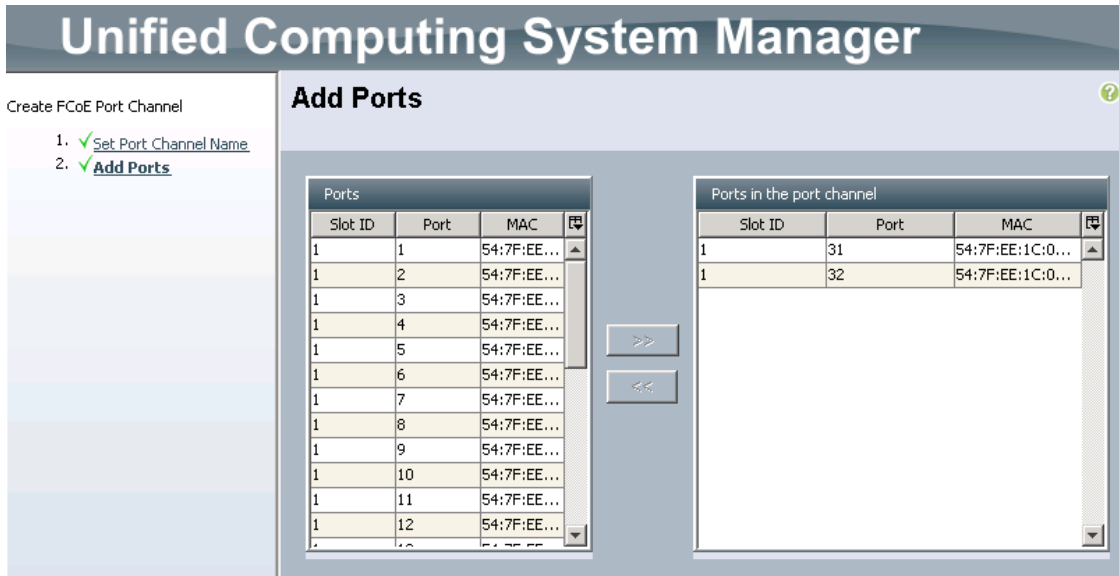
1. ☒ **Set Port Channel Name**
2. ☐ Add Ports

Set Port Channel Name

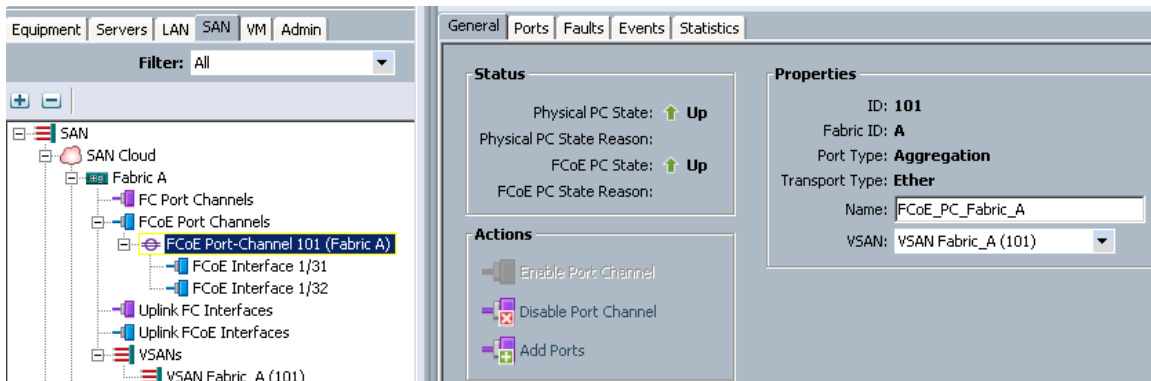
ID:

Name:

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



26. Select the Check box for Show navigator for FCoE Port-Channel 101 (Fabric A) .
27. Click OK to complete creating the FCoE Port Channel.
28. In the tree view, select the newly created FCoE port-channel.
29. Change the VSAN to VSAN Fabric_A (101).
30. Click Save Changes button.



31. Click OK to Close the Navigator.
- Note:** The FCoE Port Channel may take a few seconds to come up. The operational speed will be displayed when the link speed is negotiated. This may take approximately 30 seconds.
- Note:** If the Overall State results in an error condition and does not clear after 30 seconds the FC uplink ports on the Nexus 5548UP will need to shut down and brought back up in order to establish the link.
32. Under SAN Cloud, expand the Fabric B tree.
 33. Right-click FCoE Port Channels
 34. Select Create FCoE Port Channel.
 35. Click Yes, and then enter 102 for the Port Channel ID and FCoE_PC_Fabric_B for the Port Channel name.
 36. Click Next.

Unified Computing System Manager

Create FCoE Port Channel

- ✓ **Set Port Channel Name**
- 📄 [Add Ports](#)

Set Port Channel Name

ID:

Name:

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

Unified Computing System Manager

Create FCoE Port Channel

- ✓ [Set Port Channel Name](#)
- ✓ **Add Ports**

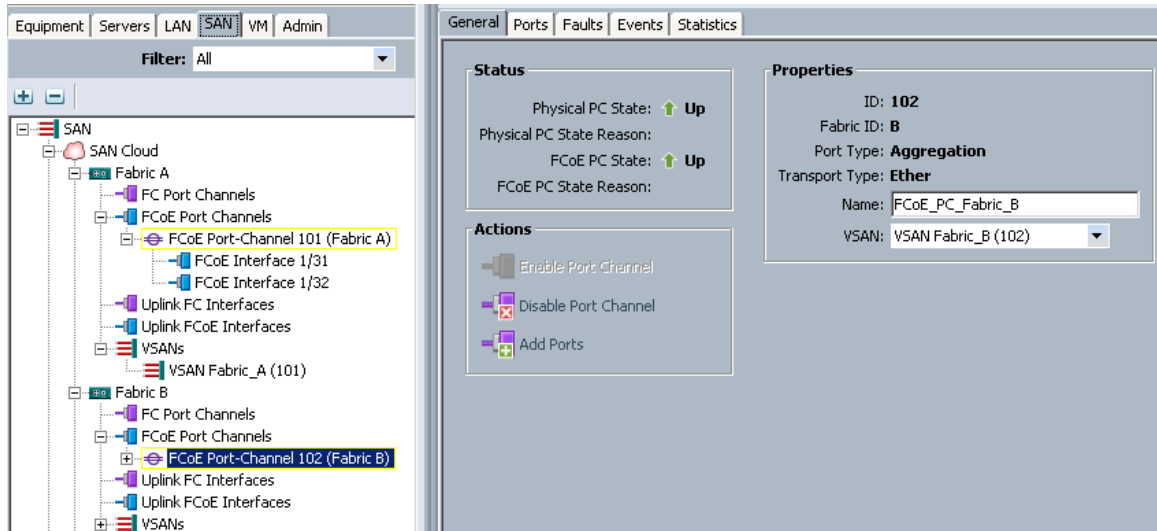
Add Ports

Ports		
Slot ID	Port	MAC
1	1	54:7F:EE:...
1	2	54:7F:EE:...
1	3	54:7F:EE:...
1	4	54:7F:EE:...
1	5	54:7F:EE:...
1	6	54:7F:EE:...
1	7	54:7F:EE:...
1	8	54:7F:EE:...
1	9	54:7F:EE:...
1	10	54:7F:EE:...
1	11	54:7F:EE:...
1	12	54:7F:EE:...

>>
 <<

Ports in the port channel		
Slot ID	Port	MAC
1	31	54:7F:EE:1C:0...
1	32	54:7F:EE:1C:0...

39. Select Check box for Show navigator for FCoE Port-Channel 102 (Fabric B) .
40. Click OK to complete creating the Port Channel.
41. Click OK to complete creating the FCoE Port Channel.
42. In the tree view, select the newly created FCoE port-channel.
43. Change the VSAN to VSAN Fabric_B (102).
44. Click Save Changes button.



45. Click OK to Close the Navigator.

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

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

7.16 Create a FC Adapter Policy for NetApp Storage Arrays

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

1. Select to the SAN tab at the top of the left window.
2. Go to SAN > Policies > root > 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]

Plogi Retries: [0-255]

Plogi 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: [1-1024]

Max LUNs Per Target: [1-1024]

Interrupt Mode: ☒ Msi X ☐ Msi ☐ Intx

7.17 Create Host Firmware Package Policy

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

1. Select the **Servers** tab at the top left of the window.
2. Select **Policies > root** or a suborganization.
3. Right Click **Host Firmware Packages**.
4. Select **Create Host Firmware Package**.

5. Enter the name of the host firmware package for the corresponding server configuration and an optional description.
6. Two 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.

Create Host Firmware Package

Name:

Description:

How would you like to configure the Host Firmware Package? ☒ Simple ☐ Advanced

Blade Package:

Rack Package:

OK Cancel

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

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

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

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input checked="" type="checkbox"/>	4	<input checked="" type="checkbox"/>	9	33	9000	<input type="checkbox"/>
Silver	<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	29	9000	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	18	9000	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	20	fc	N/A

7. Select the LAN tab on the left of the window.

8. Go to LAN > Policies > Root > and the previously created sub organization .
9. Right-click QoS Policies.
10. Select Create QoS Policy.
11. Enter LiveMigration as the QoS Policy name.
12. Change the Priority to Silver. 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.

Create QoS Policy

Name:

Egress

Priority:

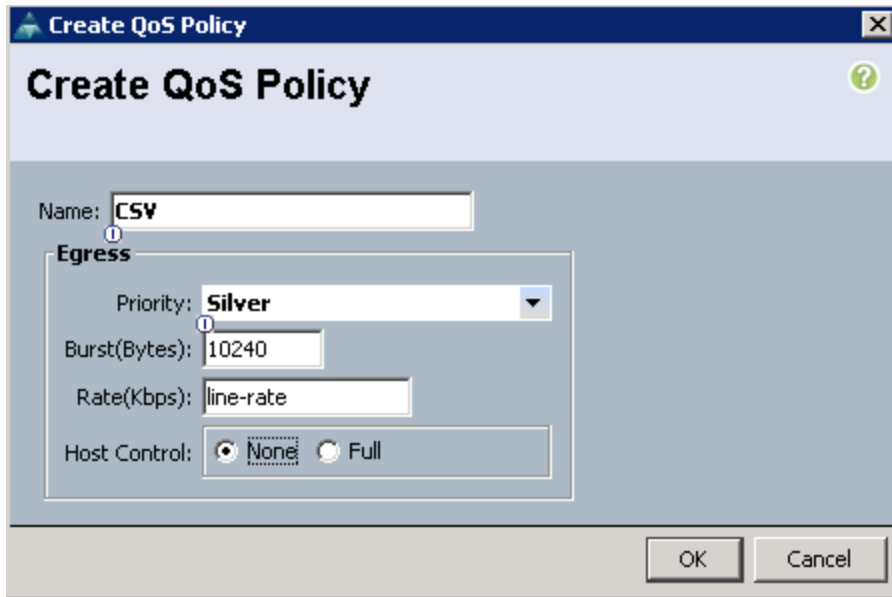
Burst(Bytes):

Rate(Kbps):

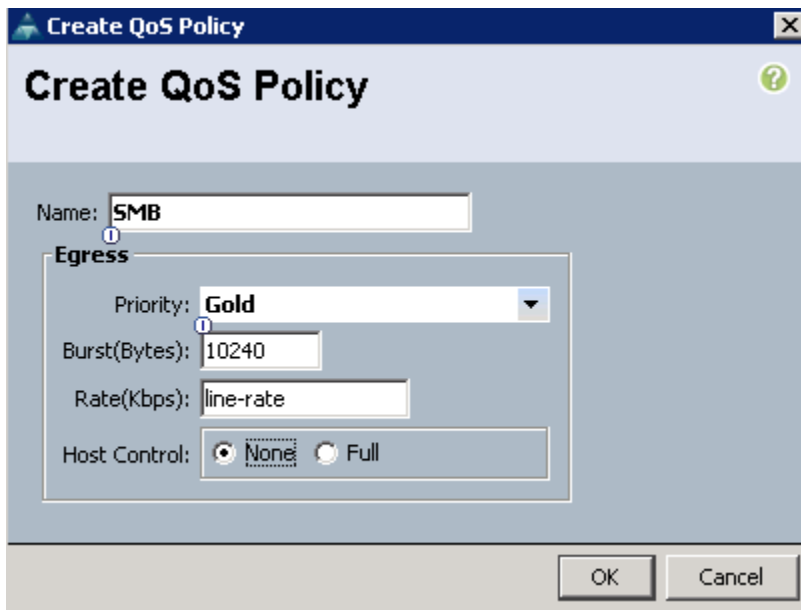
Host Control: ☒ None ☐ Full

OK Cancel

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



19. Right-click QoS Policies.
20. Select Create QoS Policy.
21. Enter SMB as the QoS Policy name.
22. Change the Priority to Gold. 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.



7.19 Create a Power Control Policy

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

1. Select the Servers tab at the top left of the window.

2. Go to Policies > root > 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: **No-Power-Cap**

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

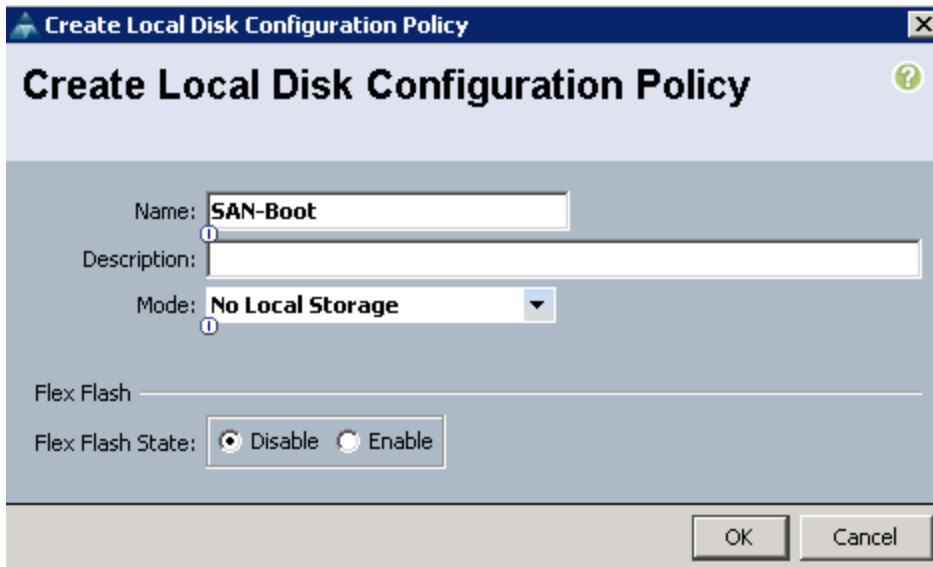
Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

7.20 Create a Local Disk Configuration Policy

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

Note: This policy should not be used on blades that contain local disks.

1. Select the Servers tab on the left of the window.
2. Go to Policies > root > 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:

Flex Flash

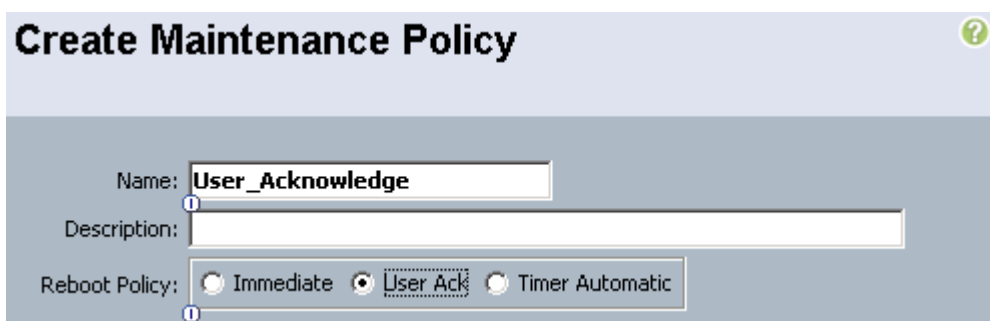
Flex Flash State: ☒ Disable ☐ Enable

OK Cancel

7.21 Create a Maintenance Policy

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

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



Create Maintenance Policy

Name:

Description:

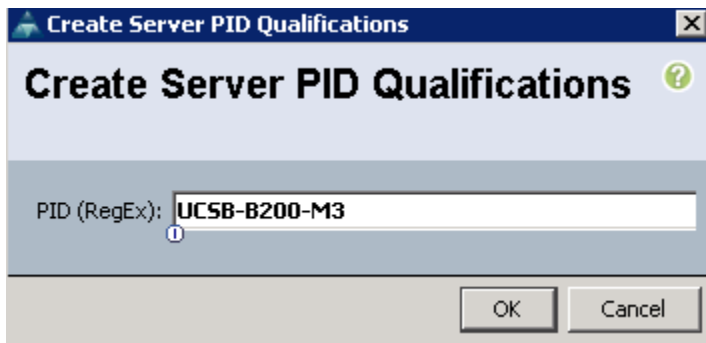
Reboot Policy: ☐ Immediate ☒ User Ack ☐ Timer Automatic

7.22 Create a Server Pool Qualification Policy

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

1. Select the `Servers` tab on the left of the window
2. Go to `Policies > root >` 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-M3 or UCSC-C220-M3S as the Model (RegEx) .
8. Click OK to complete creating the host firmware package.
9. Click OK .



7.23 Create a Server BIOS Policy

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

1. Select the Servers tab on the left of the window.
2. Go to Policies > root > and the previously created sub organization .
3. Right-click BIOS Policies .
4. Select Create BIOS Policy .
5. Enter VMHost-Infra as the BIOS policy name.
6. Make the following changes to optimize Hyper-V support:

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

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:

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

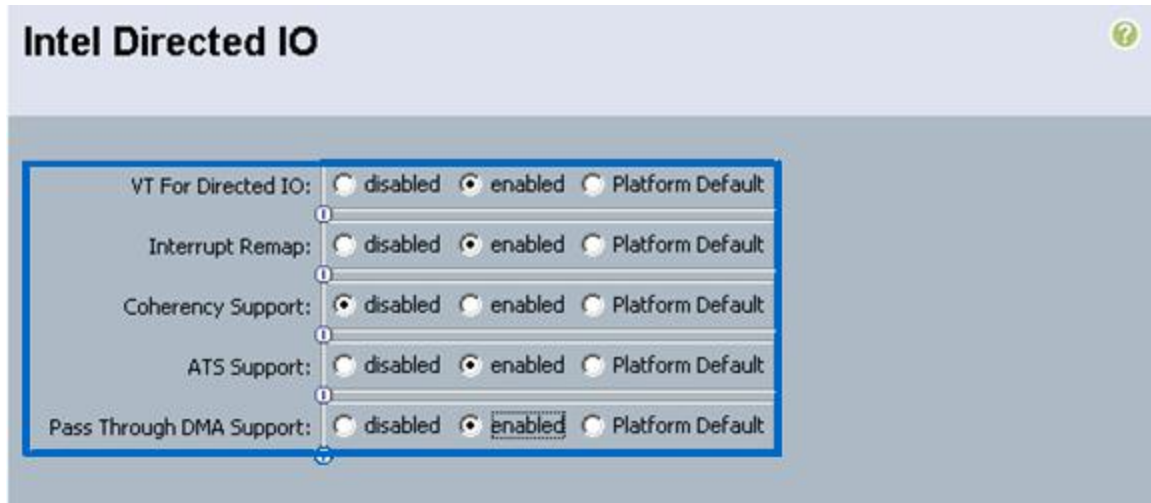
Processor C3 Report: ☐ disabled ☐ acpi-c2 ☐ acpi-c3 ☒ Platform Default

Processor C6 Report: ☐ disabled ☐ enabled ☒ Platform Default

Processor C7 Report: ☐ disabled ☐ enabled ☒ Platform Default

CPU Performance: ☒ enterprise ☐ high-throughput ☐ hpc ☐ Platform Default

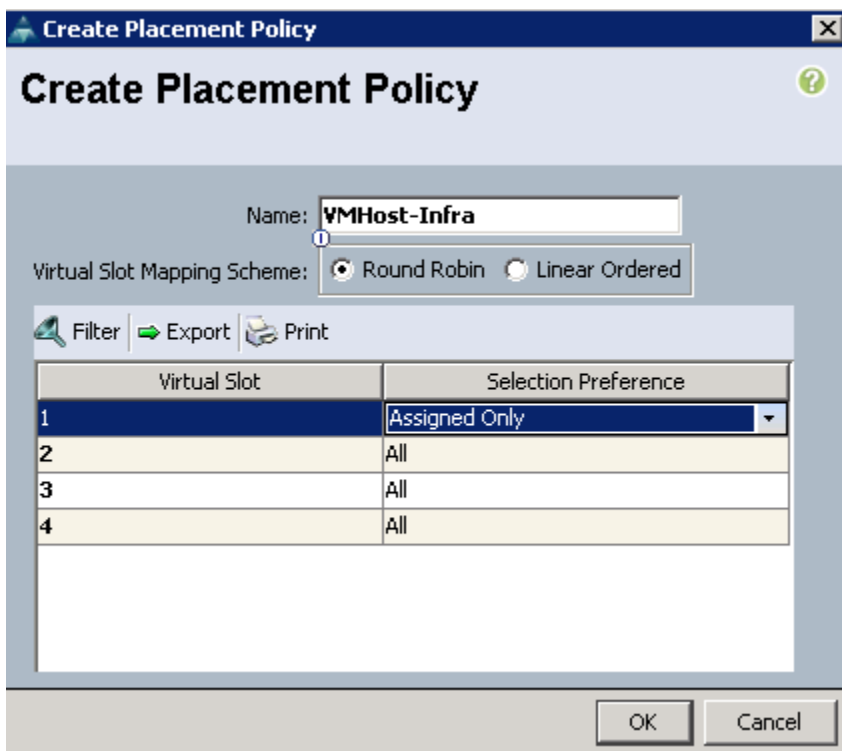
Max Variable MTRR Setting: ☐ auto-max ☐ 8 ☒ Platform Default



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

7.24 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**.



7.25 Create a vNIC Template

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

1. Select the **LAN** tab on the left of the window.
2. Go to **Policies > root >** 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. Leave **Fabric A** checked. Check the **Enable Failover** box. Under target, unselect the **VM** box. Select **Updating Template** as the Template Type. Under **VLANs**, select **CSV VLAN** and set as **Native VLAN**. Under **MTU**, enter 9000. Under **MAC Pool**:, select the MAC pool created earlier. Under **QoS Policy**: select **CSV**.
7. Click **OK** to complete creating the vNIC template.
8. Click **OK**.

Create vNIC Template

Name: **CSV**

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 checked="" type="checkbox"/>	CSV-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input type="checkbox"/>	Mgmt-VLAN	<input type="radio"/>
<input type="checkbox"/>	Fabric A VLAN	<input type="radio"/>

+ Create VLAN

MTU: **9000**

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: **MSPCFT_MAC_Pool(100/1...**

QoS Policy: **CSV**

Network Control Policy: **<not set>**

Pin Group: **<not set>**

Stats Threshold Policy: **default**

Dynamic vNIC Connection Policy: **<not set>**

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. Check Fabric B. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select Live-Migration-VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool:, select the MAC pool created earlier. Under QoS Policy, select Live-Migration.
15. Click OK to complete creating the vNIC template.
16. Click OK.

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"/>	CSV-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	LiveMigration-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	Mgmt-VLAN	<input type="radio"/>
<input type="checkbox"/>	...	<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:

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. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select MGMT-

VLAN. Set as Native VLAN. Under MAC Pool: select the MAC pool created earlier.

23. Click OK to complete creating the vNIC template.

24. Click OK .

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"/>	CSV-VLAN	<input type="radio"/>
<input type="checkbox"/>	LiveMigration-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Mgmt-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	...	<input type="radio"/>

[+ Create VLAN](#)

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

Dynamic vNIC Connection Policy:

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 VM-Cluster-Comm as the vNIC template name.

30. Check Fabric B. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select App-Cluster-Comm. Do not set a Native VLAN. Under MTU, enter 1500. Under MAC Pool, select the MAC pool created earlier.

31. Click OK to complete creating the vNIC template.

32. Click OK .

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"/>	SMB-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	VM-App-Cluster-Comm-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Database-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-MF-Public-VLAN	<input type="radio"/>

[+ Create VLAN](#)

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

Dynamic vNIC Connection Policy:

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

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"/>	SMB-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-Cluster-Comm-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Database-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	VM-MF-Public-VLAN	<input type="radio"/>

[+ Create VLAN](#)

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

Dynamic vNIC Connection Policy:

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

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"/>	SMB-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-Cluster-Comm-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	VM-Database-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-MF-Public-VLAN	<input type="radio"/>

Create VLAN

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

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 as the vNIC template name.
54. Check Fabric B. Check the Enable Failover box. Under target, select Adapter box. Select Updating Template as the Template Type. Under VLANs, select SMB-VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool, select the MAC pool created earlier. Under QoS Policy, select SMB.
55. Click OK to complete creating the vNIC template.
56. 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 checked="" type="checkbox"/>	SMB-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	VM-App-Cluster-Comm-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Database-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-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:

Dynamic vNIC Connection Policy:

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. Check **Fabric B**. Check the **Enable Failover** box. Under **target**, unselect the **VM** box. Select **Updating Template** as the **Template Type**. Under **VLANs**, select **VM-AF-Public**. Do not set a **Native VLAN**. Under **MAC Pool**, select the MAC pool created earlier.
63. Click **OK** to complete creating the vNIC template.
64. 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 checked="" type="checkbox"/>	VM-AF-Public-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-App-Cluster-Comm-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Database-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-MF-Public-VLAN	<input type="radio"/>

Create VLAN

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

Dynamic vNIC Connection Policy:

7.26 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 vNIC Template**.
5. Enter **Fabric-A** as the vHBA template name.
6. Select **Fabric A**. Under **Select VSAN**, select **VSAN_A**. Under **WWN Pool**, select the previously created **WWN pool**.
7. Click **OK** to complete creating the vHBA template.
8. Click **OK**.

Create vHBA Template



Name:

Description:

Fabric ID: ☒ A ☐ B

Select VSAN: + Create 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 VSAN_B. Under WWN Pool, select the previously created WWN pool.
15. Click OK to complete creating the vHBA template.
16. Click OK.

Create vHBA Template

Name:

Description:

Fabric ID: ☐ A ☒ B

Select VSAN: + Create VSAN

Template Type: ☐ Initial Template ☒ Updating Template

Max Data Field Size:

WWPN Pool:

QoS Policy:

Pin Group:

Stats Threshold Policy:

7.27 Create Boot Policies

These steps provide details for creating boot policie 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 oneach 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).

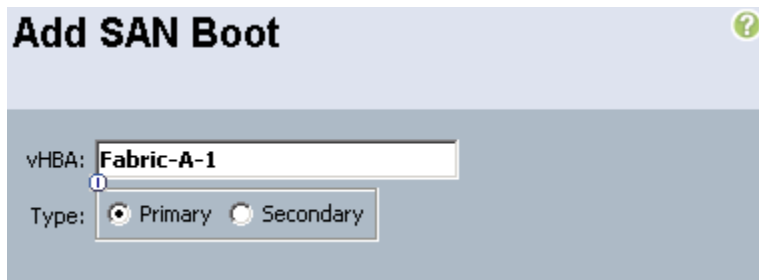
Note: To obtain the WWPN information for the FAS cluster lifs, log in to the FAS cluster and run the fcp portname show command.

Vserver	Logical Interface	WWPN
Infra_vs1	fcp_lif01a	20:00:00:a0:98:17:4d:5c
Infra_vs1	fcp_lif01b	20:01:00:a0:98:17:4d:5c
Infra_vs1	fcp_lif02a	20:02:00:a0:98:17:4d:5c
Infra_vs1	fcp_lif02b	20:03:00:a0:98:17:4d:5c

4 entries were displayed.

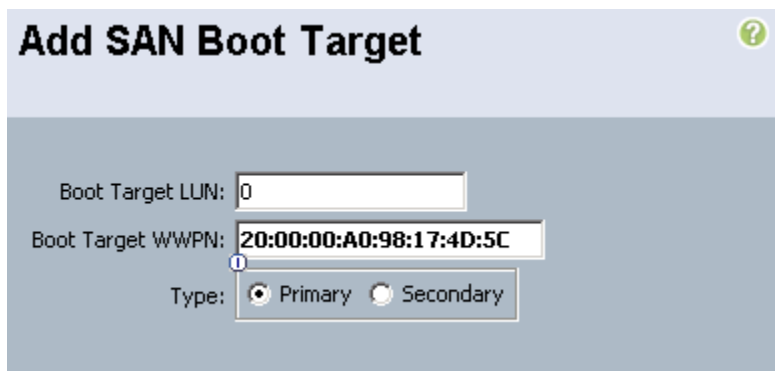
1. Select the Servers tab at the top left of the window.
2. Go to Policies > root > and the previously created sub organization .
3. Right-click Boot Policies .
4. Select Create Boot Policy.
5. Name the boot policy Infra_vs1_n01.
6. (Optional) Give the boot policy a description.
7. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
8. Expand the Local Devices drop-down menu and select Add CD-ROM.
9. Expand the vHBAs drop-down menu and select Add SAN Boot.

10. Enter `Fabric-A-1` in the vHBA field in the Add SAN Boot window that displays.
11. Make sure that Primary is selected as the type.
12. Click OK to add the SAN boot initiator.



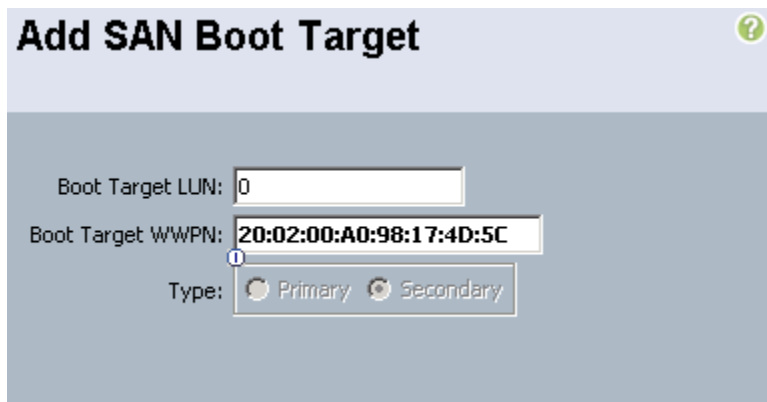
The screenshot shows the 'Add SAN Boot' window. The title bar is light blue with a green question mark icon. The main area has a light blue header with the title 'Add SAN Boot'. Below the header, there is a form with two fields: 'vHBA:' and 'Type:'. The 'vHBA:' field contains the text 'Fabric-A-1'. The 'Type:' field has two radio buttons: 'Primary' (which is selected) and 'Secondary'. There is a small blue 'i' icon next to the 'vHBA:' field.

13. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as 0.
14. Enter the WWPN for the primary FCoE adapter interface `lif01a` of node-1. To obtain this information, log in to the FAS cluster and run the `fcportname show` command.
15. Be sure to use the FC portname for `lif01a` and not the FC node name.
16. Keep the type as `Primary`.
17. Click OK to add the SAN boot target.



The screenshot shows the 'Add SAN Boot Target' window. The title bar is light blue with a green question mark icon. The main area has a light blue header with the title 'Add SAN Boot Target'. Below the header, there is a form with three fields: 'Boot Target LUN:', 'Boot Target WWPN:', and 'Type:'. The 'Boot Target LUN:' field contains the value '0'. The 'Boot Target WWPN:' field contains the value '20:00:00:A0:98:17:4D:5C'. The 'Type:' field has two radio buttons: 'Primary' (which is selected) and 'Secondary'. There is a small blue 'i' icon next to the 'Boot Target WWPN:' field.

18. Under the vHBA drop-down menu, select `Add SAN Boot Target`. Keep the value for Boot Target LUN as 0.
19. Enter the WWPN for the primary FCoE adapter interface `lif02a` of node-2. To obtain this information, log in to the FAS cluster and run the `fcportname show` command.
20. Be sure to use the FC portname for port `lif02a` and not the FC node name.
21. Click OK to add the SAN boot target.



The screenshot shows the 'Add SAN Boot Target' window. The title bar is light blue with a green question mark icon. The main area has a light blue header with the title 'Add SAN Boot Target'. Below the header, there is a form with three fields: 'Boot Target LUN:', 'Boot Target WWPN:', and 'Type:'. The 'Boot Target LUN:' field contains the value '0'. The 'Boot Target WWPN:' field contains the value '20:02:00:A0:98:17:4D:5C'. The 'Type:' field has two radio buttons: 'Primary' and 'Secondary' (which is selected). There is a small blue 'i' icon next to the 'Boot Target WWPN:' field.

22. Select **Add SAN Boot** under the vHBA drop-down menu.
23. Enter **Fabric-B-1** in the vHBA field in the Add SAN Boot window that displays.
24. The type should automatically be set to **Secondary** and it should be grayed out. This is fine.
25. Click **OK** to add the SAN boot target.

Add SAN Boot

vHBA: **Fabric-B-1**

Type: ☒ Primary ☐ Secondary

26. Select **Add SAN Boot Target** under the vHBA drop-down menu.
27. The Add SAN Boot Target window displays. Keep the value for **Boot Target LUN** as **0**.
28. Enter the WWPN for the primary FCoE adapter interface **lif01b** of the node-1. To obtain this information, log in to FAS cluster and run the `fcportname show` command.
29. Be sure to use the FC portname for **portli02b** and not the FC node name.
30. Keep the type as **Primary**.
31. Click **OK** to add the SAN boot target.

Add SAN Boot Target

Boot Target LUN: **0**

Boot Target WWPN: **20:01:00:A0:98:17:4D:5C**

Type: ☒ Primary ☐ Secondary

32. Under the vHBA drop-down menu, select **Add SAN Boot Target**. Keep the value for **Boot Target LUN** as **0**.
33. Enter the WWPN for the primary FCoE adapter interface **lif02b** of node-2. To obtain this information, log in to controller A and run the `fcportname show` command.
34. Be sure to use the FC portname for port **lif01b** and not the FC node name.
35. Click **OK** to add the SAN boot target.

Add SAN Boot Target

Boot Target LUN: **0**

Boot Target WWPN: **20:03:00:A0:98:17:4D:5C**

Type: ☒ Primary ☐ Secondary

36. Click Save Changes .

7.28 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`.
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

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

Networking ?

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by defa... + 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 ⌵

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

Create vNIC ?

Name: ?

Use vNIC Template: ☒ ?

+ Create vNIC Template

vNIC Template: CSV ⌵ ?

Adapter Performance Profile

Adapter Policy: Windows ⌵ + Create Ethernet Adapter Policy

9. Click **Add** to add a vNIC to the template.
10. The **Create vNIC** window displays. Name the vNIC **LiveMigration**.
11. Check the **Use LAN Connectivity Template** checkbox.

12. Select `LiveMigration` for the vNIC Template field.
13. Select `Windows` in the Adapter Policy field.
14. Click `OK` to add the vNIC to the template.

Create vNIC ?

Name:

Use vNIC Template: ☒

+ Create vNIC Template

vNIC Template:

Adapter Performance Profile

Adapter Policy: + Create Ethernet Adapter Policy

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

Create vNIC ?

Name:

Use vNIC Template: ☒

+ Create vNIC Template

vNIC Template:

Adapter Performance Profile

Adapter Policy: + Create Ethernet Adapter Policy

21. Click `Add` to add a vNIC to the template.

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

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 VM-Database.
29. Check the Use LAN Connectivity Template checkbox.
30. Select VM-Database for the vNIC Template field.
31. Select Windows in the Adapter Policy field.
32. Click OK to add the vNIC to the template.

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 VM-MF-Public.
35. Check the Use LAN Connectivity Template checkbox.
36. Select VM-MF-Public for the vNIC Template field.
37. Select Windows in the Adapter Policy field.
38. Click OK to add the vNIC to the template.

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
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

Storage section

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

Create vHBA

The screenshot shows the 'Create vHBA' window with the following configuration:

- Name:** Fabric-A-1
- Use vHBA Template:** ☒
- + Create vHBA Template** (button)
- vHBA Template:** Fabric-A (dropdown menu)
- Adapter Performance Profile** (section header)
- Adapter Policy:** Windows-NetApp (dropdown menu)
- + Create Fibre Channel Adapter Policy** (button)

14. Click the Add button at the bottom of the window to add vHBAs to the template.
15. The Create vHBA window displays. Name the vHBA Fabric-A-2.
16. Check the box for Use vHBA Template.
17. Select Fabric-A in the vHBA Template field.
18. Select Windows-NetApp in the Adapter Policy field.
19. Click OK to add the vHBA to the template.

Create vHBA

The screenshot shows the 'Create vHBA' window with the following configuration:

- Name:** Fabric-A-2
- Use vHBA Template:** ☒
- + Create vHBA Template** (button)
- vHBA Template:** Fabric-A (dropdown menu)
- Adapter Performance Profile** (section header)
- Adapter Policy:** Windows-NetApp (dropdown menu)
- + Create Fibre Channel Adapter Policy** (button)


20. Click the Add button at the bottom of the window to add vHBAs to the template.
21. The Create vHBA window displays. Name the vHBA Fabric-B-1.
22. Check the box for Use vHBA Template.
23. Select Fabric-B in the vHBA Template field.
24. Select Windows-NetApp in the Adapter Policy field.

25. 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

26. Click the **Add** button at the bottom of the window to add vHBAs to the template.

27. The **Create vHBA** window displays. Name the vHBA **Fabric-B-2**.

28. Check the box for **Use vHBA Template**.

29. Select **Fabric-B** in the vHBA Template field.


30. Select **Windows-NetApp** in the Adapter Policy field.

31. 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

32. **Verify** – Review the table to make sure that all four vHBAs were created.

Create Service Profile Template

1. ☒ Identify Service Profile Template
2. ☒ Networking
3. ☒ **Storage**
4. ☐ Zoning
5. ☐ vNIC/vHBA Placement
6. ☐ Server Boot Order
7. ☐ Maintenance Policy
8. ☐ Server Assignment
9. ☐ Operational Policies

Storage

Optionally specify disk policies and SAN configuration information.

Select a local disk configuration policy.

Local Storage: SAN-Boot Mode: **No Local Storage**

Create Local Disk Configuration Policy

Protect Configuration: **Yes**
If **Protect Configuration** is set, the local disk configuration is preserved if the service profile is disassociated with the

How would you like to configure SAN connectivity? ☐ Simple ☒ Expert ☐ No vHBAs ☐ Use Connectivity Policy

A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

World Wide Node Name

WWNN Assignment: node-default(99/100)

The WWNN will be assigned from the selected pool.
The available/total WWNNs are displayed after the pool name.

Name	WWPN
<input type="checkbox"/> vHBA Fabric-A-1	Derived
<input type="checkbox"/> vHBA IF	
<input type="checkbox"/> vHBA Fabric-A-2	Derived
<input type="checkbox"/> vHBA IF	
<input type="checkbox"/> vHBA Fabric-B-1	Derived
<input type="checkbox"/> vHBA IF	

Add

33. Click Next to continue to the next section.

Zoning Section

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

Create Service Profile Template

1. ☒ Identify Service Profile Template
2. ☒ Networking
3. ☒ Storage
4. ☒ **Zoning**
5. ☐ vNIC/vHBA Placement
6. ☐ Server Boot Order
7. ☐ Maintenance Policy
8. ☐ Server Assignment
9. ☐ Operational Policies

Zoning

Specify zoning information

WARNING: Switch in end-host mode. In end-host mode, zoning configuration will NOT be applied.

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-A-2
Fabric-B-1
Fabric-B-2

Select vHBA Initiator Groups

Name	Storage Connection Policy Name
------	--------------------------------

Add

34. Click Next to continue the next section.

vNIC/vHBA Placement Section

Select the VMHost-InfraPlacement Policy in the Select Placement field.

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: VMHost-Infra

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

Move Up Move Down

vNICs

vHBAs

Name
App-Cluste...
CSV
LiveMigrati...
Mgmt
SMB
VM-Databa...
VM-MF-Pu...

>> assign >>

<< remove <<

1. Select vCon1 assign the vNICs in the following order:
 - Mgmt
 - SMB
 - LiveMigration
 - CSV
 - VM-Database
 - VM-MF-Public
 - App-Cluster-Comm
2. Click the vHBA tab and add the vHBAs in the following order:
 - Fabric-A-1
 - Fabric-B-1
 - Fabric-A-2
 - Fabric-B2

3. Verify: Review the table to make sure that all of the vHBAs and vNICs were created.

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: [+ 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

vNICs vHBAs

Name

>> assign >>
<< remove <<

Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
<input checked="" type="checkbox"/> vCon 1		Assigned Only
<input checked="" type="checkbox"/> vNIC Mgmt	1	
<input checked="" type="checkbox"/> vNIC SMB	2	
<input checked="" type="checkbox"/> vNIC LiveMigration	3	
<input checked="" type="checkbox"/> vNIC CSV	4	
<input checked="" type="checkbox"/> vNIC VM-Database	5	
<input checked="" type="checkbox"/> vNIC VM-MF-Public	6	
<input checked="" type="checkbox"/> vNIC App-Cluster-Comm	7	

▲ Move Up ▼ Move Down

4. Click **Next** to continue to the next section.

Server Boot Order Section

5. Select `Infra_vs1_n1` in the Boot Policy field.
6. 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.
7. 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_n01** + Create Boot Policy

Name: **Infra_vs1_n01**

Description:

Reboot on Boot Order Change: **No**

Enforce vNIC/vHBA/iSCSI Name: **Yes**

WARNINGS:

The type (primary/secondary) does not indicate a boot order precedence.

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	
CD-ROM	1					
Storage	2					
SAN primary		Fabric-A-1	Primary			
SAN Target primary			Primary	0	20:00:00:A0:98:17:4D:5C	
SAN Target secondary			Secondary	0	20:02:00:A0:98:17:4D:5C	
SAN secondary		Fabric-B-1	Secondary			
SAN Target primary			Primary	0	20:01:00:A0:98:17:4D:5C	
SAN Target secondary			Secondary	0	20:03:00:A0:98:17:4D:5C	

Create iSCSI vNIC Set iSCSI Boot Parameters

Maintenance Policy Section

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

Unified Computing System Manager

Create Service Profile Template

1. ✓ [Identify Service Profile Template](#)
2. ✓ [Networking](#)
3. ✓ [Storage](#)
4. ✓ [Zoning](#)
5. ✓ [vNIC/vHBA Placement](#)
6. ✓ [Server Boot Order](#)
7. ✓ [Maintenance Policy](#)
8. [Server Assignment](#)
9. [Operational Policies](#)

Maintenance Policy

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: **User_Acknowledge** + Create Maintenance Policy

Name: **User_Acknowledge**

Description:

Reboot Policy: **User Ack**

Server Assignment Section

1. Select `Infra_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-Infra` in the `Host Firmware` field.
5. Click `Next` to continue to the next section.

The screenshot shows the UCSM web interface. At the top, a banner reads "Unified Computing System Manager". Below it, the "Server Assignment" section is active, indicated by a green question mark icon. On the left, a sidebar titled "Create Service Profile Template" lists nine steps: 1. Identify Service Profile Template (checked), 2. Networking (checked), 3. Storage (checked), 4. Zoning (checked), 5. vNIC/vHBA Placement (checked), 6. Server Boot Order (checked), 7. Maintenance Policy (checked), 8. Server Assignment (checked), and 9. Operational Policies (unchecked). The main content area for "Server Assignment" has the heading "Optionally specify a server pool for this service profile template." It contains a "Pool Assignment" dropdown menu set to "Infra_Pool" and a "+ Create Server Pool" button. Below this is a section for power state selection with the text "Select the power state to be applied when this profile is associated with the server." and two radio buttons: "Up" (selected) and "Down". A paragraph explains that the service profile template will be associated with one of the servers in the selected pool and that a server pool policy qualification can be specified. Below this is a "Server Pool Qualification" dropdown menu set to "VMHost-Infra" and a "Restrict Migration" checkbox (unchecked). At the bottom, a "Firmware Management (BIOS, Disk Controller, Adapter)" section contains a paragraph explaining that selecting a host firmware policy will update the firmware on the server. Below this is a "Host Firmware" dropdown menu set to "VMHost-Infra" and a "+ Create Host Firmware Package" button.

Unified Computing System Manager

Create Service Profile Template

1. ☒ [Identify Service Profile Template](#)
2. ☒ [Networking](#)
3. ☒ [Storage](#)
4. ☒ [Zoning](#)
5. ☒ [vNIC/vHBA Placement](#)
6. ☒ [Server Boot Order](#)
7. ☒ [Maintenance Policy](#)
8. ☒ [Server Assignment](#)
9. ☐ [Operational Policies](#)

Server Assignment

Optionally specify a server pool for this service profile template.

Pool Assignment: Infra_Pool + 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: VMHost-Infra

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: VMHost-Infra + Create Host Firmware Package

Operational Policies Section

1. Select `VMHost-Infra` 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.

Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

1. [Identify Service Profile Template](#)

2. [Networking](#)

3. [Storage](#)

4. [Zoning](#)

5. [vNIC/vHBA Placement](#)

6. [Server Boot Order](#)

7. [Maintenance Policy](#)

8. [Server Assignment](#)

9. [Operational Policies](#)

Operational Policies

Optionally specify information that affects how the system operates.

BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy:

VM-Host-Infra

Create BIOS Policy

External IPMI Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy:

No-Power-Cap

Create Power Control Policy

Scrub Policy

< Prev

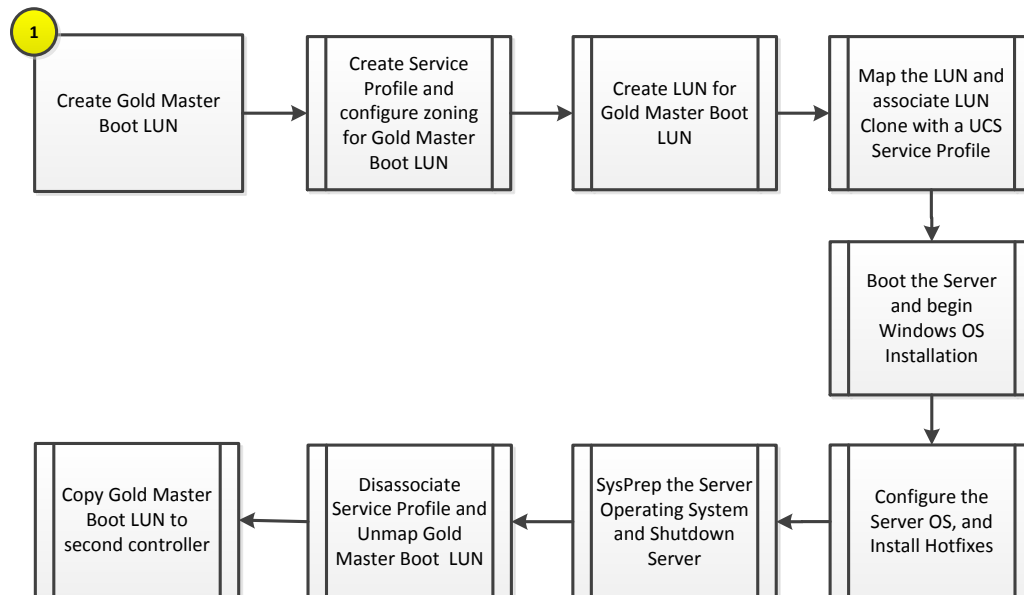
Next >

Finish

Cancel

Create Gold Master Boot LUN

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



8 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.

8.1 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 installation ISO image
- Access to Cisco UCS FCoE driver installation ISO image
- Access to Cisco UCS Ethernet driver installation ISO image

8.2 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.

8.3 Create the GoldMaster boot LUN

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

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

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

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

```
New-NcQtree -Volume ucs_boot -Qtree goldmaster
```

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

```
New-NcLun /vol/ucs_boot/goldmaster/boot.lun -Size 200gb -OsType windows_2008 -Unreserved
```

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

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

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

```
Add-NcIgroupInitiator -Igroup goldmaster -Initiator <vHBA_A WWPN>
```

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

```
Add-NcLunMap /vol/ucs_boot/goldmaster/boot.lun goldmaster
```

8.4 Create GoldMaster Zone

Perfrom the following setps to zone the GoldMaster service profile.

1. Create a temporary zone for the goldmaster service profile

```

zone      name      goldmaster_A      vsan      <Fabric      A      VSAN      ID>
  member device-alias infra_vsl_lif01a
  member                                pwnn      <Fabric-A      WWPN>
exit

```

2. Add the new zone to the zoneset.

```

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

```

3. Activate the zoneset.

```

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

```

8.5 Prepare to install Windows Server 2012

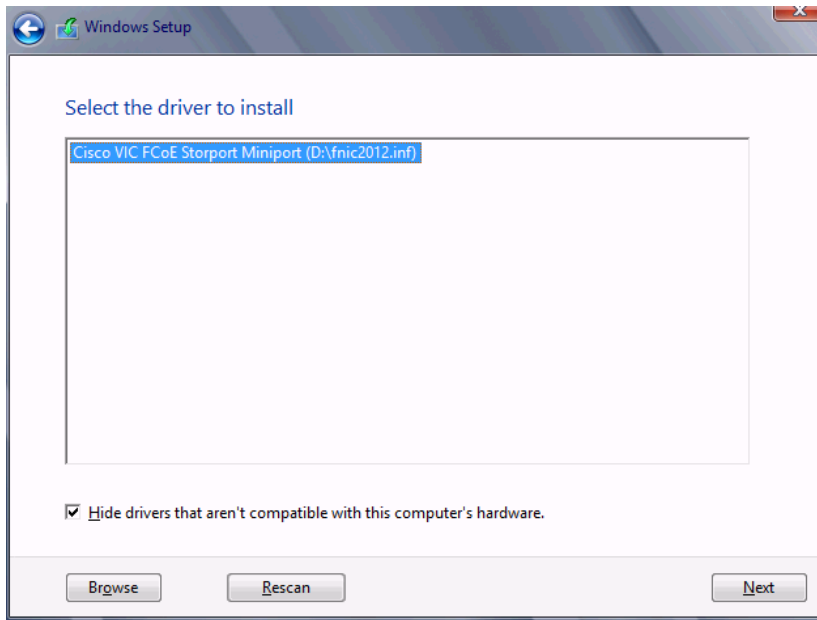
This section details the steps required to prepare the server for OS installation.

1. Right-Click on 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.

8.6 Install Windows Server 2012

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

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 autodetected, Click **Next**.

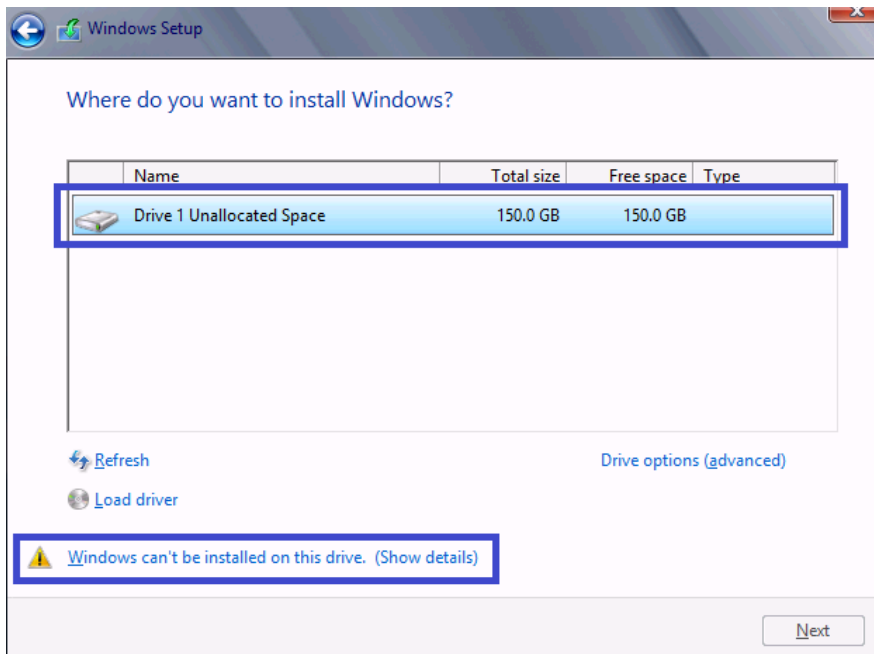


14. You should see a LUN listed in the drive selection screen.

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

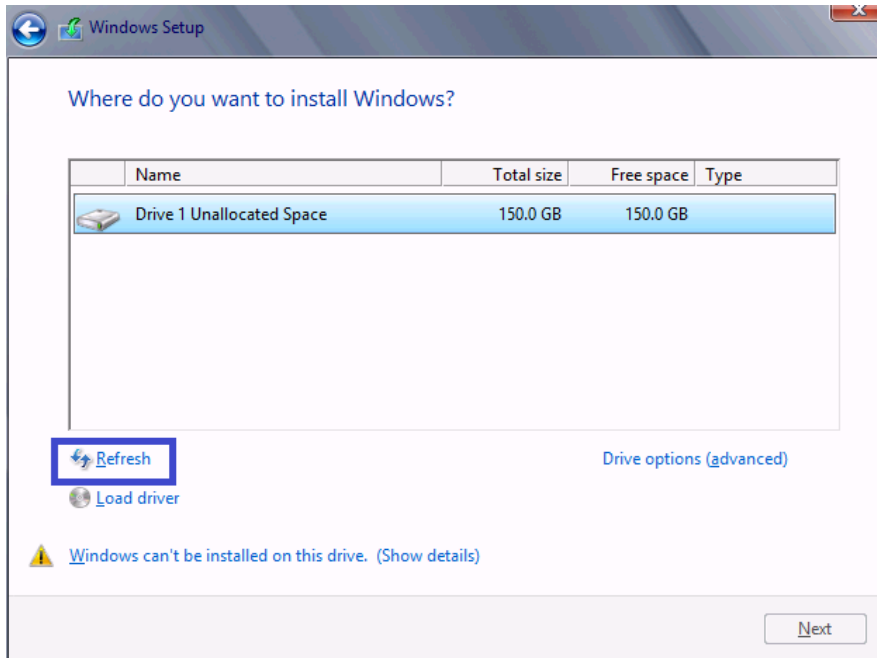
Note: The message "Windows Can't be installed on this drive" appears because the Windows installation ISO image is not mapped at this time.

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



15. In the Virtual Media Session manager clear the Mapped checkbox for the Cisco Driver ISO that you recently added (fNIC driver) and choose yes to acknowledge.

16. Select the **Mapped** checkbox for the Windows ISO in the virtual media session manager.
17. Back in the KVM console click **Refresh** to update the cdrom drive status.



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

8.7 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.

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

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

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

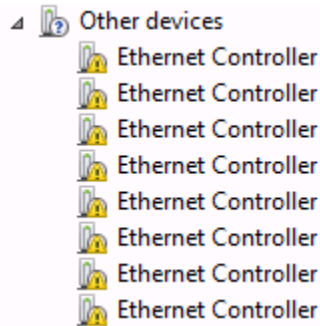
```
Add-WindowsFeature Multipath-IO, Data-Center-Bridging -IncludeManagementTools -Restart
```

8.8 Install Windows eNIC Drivers

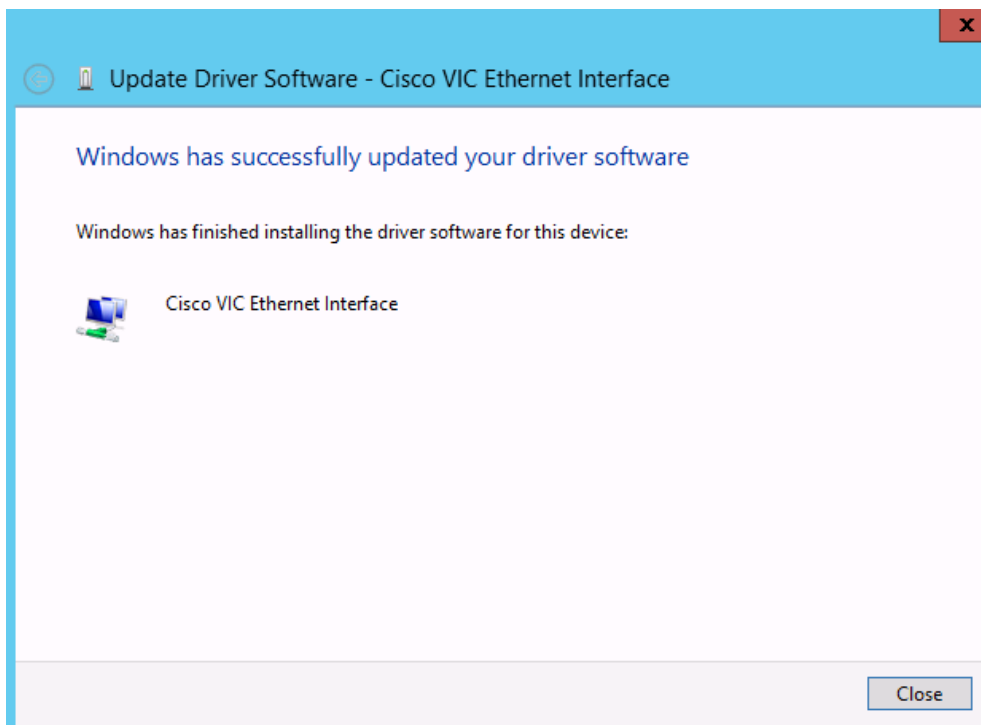
The following steps describe how to install all required network drivers if it was not installed at the same time as the storage driver.

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**



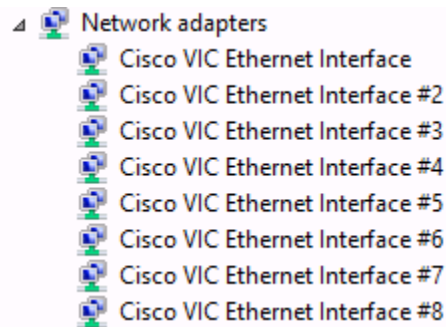
7. Right-click one of the Ethernet Controller, and select **Update Driver Software**.
8. Click **Browse my computer for driver software**.
9. Click Browse, and select the **CDROM drive**, click **OK**.
10. Click **Next > Close**.



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

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

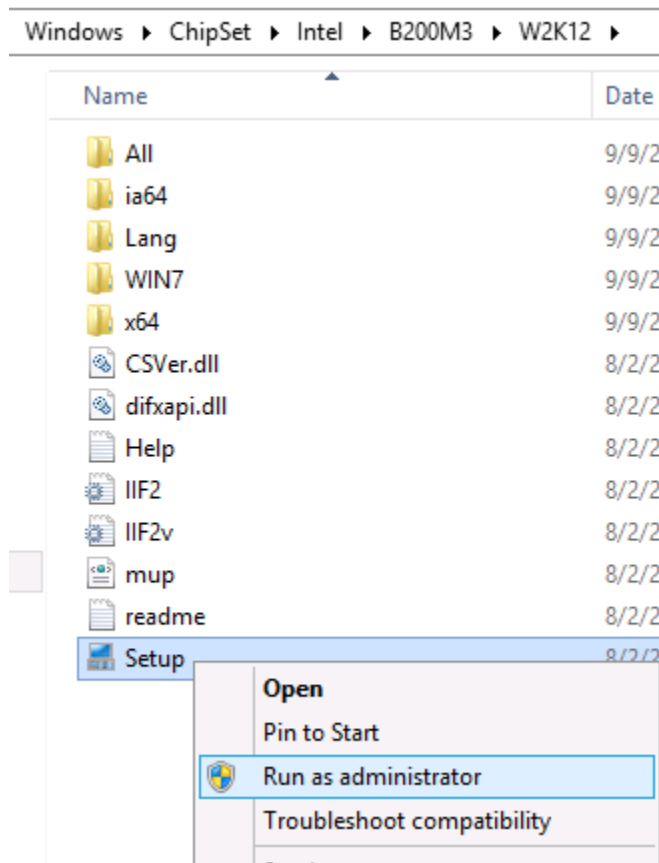
15. All Cisco VIC Ethernet devices will appear under Network Adapters.



16. Configure the TCP/IP settings on the appropriate NIC to provide network access for installing the additional software components.

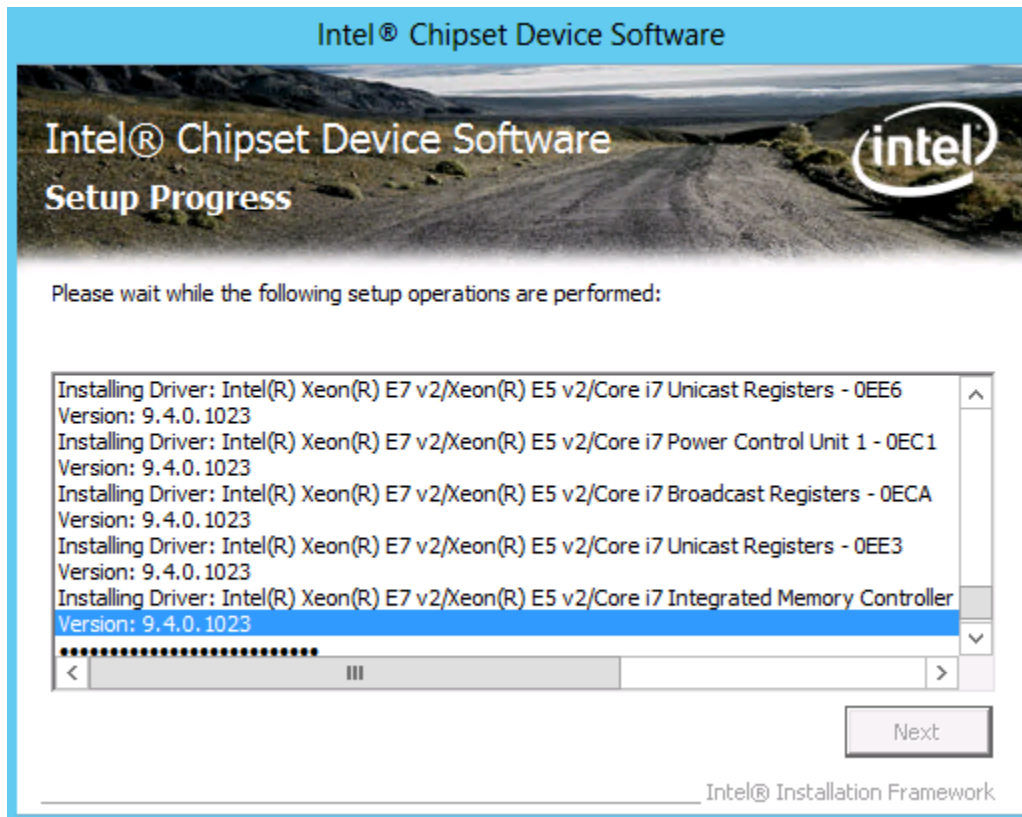
8.9 Install Intel Chipset Device Software for Xeon E5-2600v2 Processors

1. Using the same Cisco drivers ISO image file navigate to the chipset directory (Windows->ChipSet->B200M3->W2K12. Right clic Setup.exe and select Run as Administrator.



2. Click **Next** in the Welcome screen.

3. Review the license agreement and click **Next** to continue.
4. Click **Next** in the Readme File Information screen to begin the installation process.



5. After the installation completes click **Next**.
6. Click Finish to **Exit** the installation wizard.

8.10 Install the Data ONTAP PowerShell Toolkit.

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

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

8.11 Configure Windows MPIO

The following section describes how to configure Windows MPIO to claim NetApp Luns.

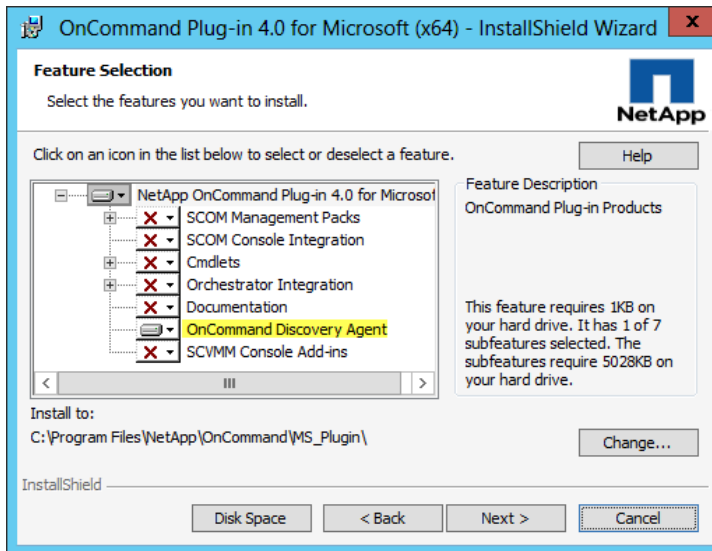
1. Configure Windows Server 2012 MSDSM to claim any NetApp LUNs.

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId LUN
New-MSDSMSupportedHW -VendorId NETAPP -ProductId "LUN C-Mode"
```

Update-MPIOClaimedHW
Restart-Computer

8.12 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.

8.13 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. Once 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 <<var_ntap_A_hostname>> controller with PowerShell.
5. Unmap the goldmaster igroup from the Gold Master Boot LUN.

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

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

9 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 (x64) has been created

9.1 Create Service Profiles

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

37. In UCS Manager, Select the Servers tab at the top left of the window.
38. Select Service Profile Templates VMHost-Mgmt-Fabric-A
39. Right-click and select Create Service Profile From Template.
40. Enter VMHost-Mgmt0 for the service profile prefix.
41. Enter 1 for the Name Suffix Starting Number.
42. Enter 2 for the Number of Instances of the service profiles to create.
43. Click OK to create the service profile.

Create Service Profiles From Template

Naming Prefix:

Name Suffix Starting Number:

Number of Instances:

OK Cancel

44. Click **OK** in the message box.

9.2 Gather Necessary Information

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

Table 22) 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		

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.

9.3 Create Device Aliases

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

Nexus 5548 A

1. Using the information in Table 21 Create device alias.

```
device-alias database
  device-alias name VMHost-Mgmt01-A-1_A pwwn <Fabric-A WWPN>
  device-alias name VMHost-Mgmt02-A-1_A pwwn <Fabric-A WWPN>
  exit
device-alias commit
copy running-config startup-config
```

Nexus 5548 B

1. Using the information in Table 21 Create device alias.

```
device-alias database
  device-alias name VMHost-Mgmt01-B-1_B pwwn <Fabric-B WWPN>
  device-alias name VMHost-Mgmt02-B-1_B pwwn <Fabric-B WWPN>
  exit
device-alias commit
copy running-config startup-config
```

9.4 Create Zones for Each Service Profile

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

Nexus 5548 A

10. Create the Zones and Add Members

```
zone name VMHost-Mgmt01-A-1_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-Mgmt01-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name VMHost-Mgmt02-A-1_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-Mgmt02-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
```

11. Create the Zoneset and Add the Necessary Members

```
zoneset name Flexpod vsan <Fabric A VSAN ID>
  member VMHost-Mgmt01-A-1_A
  member VMHost-Mgmt02-A-1_A
  exit
```

12. Activate the Zoneset

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

Nexus 5548 B

1. Create the Zones and Add Members

```
zone name VMHost-Mgmt01-B-1_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-Mgmt01-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
zone name VMHost-Mgmt02-B-2_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-Mgmt02-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
```

2. Create the Zoneset and Add the Necessary Members

```
zoneset name Flexpod vsan <Fabric B VSAN ID>
```

```
member VMHost-Mgmt-01_B
member VMHost-Mgmt-02_B
exit
```

3. Activate the Zoneset

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

9.5 FlexClone Boot LUN

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

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

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

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

```
New-NcQtree -Volume ucs_boot -Qtree VMHost-Mgmt01
New-NcQtree -Volume ucs_boot -Qtree VMHost-Mgmt02
```

4. Using the information in Table 21, Create igroups

```
New-NcIgroup -Name VMHost-Mgmt01 -Protocol fcp -Type windows |
  Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
  Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-Mgmt02 -Protocol fcp -Type windows |
  Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
  Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
```

5. Clone the boot LUN from the goldmaster boot LUN.

```
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
  -DestinationPath /VMHost-Mgmt01/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
  -DestinationPath /VMHost-Mgmt02/boot.lun
```

6. Map the boot LUN to the new iGroup.

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

9.6 Boot Service Profiles

Complete the following steps to boot each new service profile.

All Hosts

7. Back in USCM right-click on Service profile and select Associate with Server Pool.
8. From the Pool Assignment box, select the Infra_Pool and click OK, and OK again to acknowledge.
9. Right-click the <Hyper-V hostname> and select KVM Console.
10. Click Boot Server, the service profile will then pull a server from the VM-Host-Infra, and configure the hardware per the service profile.
11. Back in USCM right-click <Hyper-V Hostname>, and select KVM Console.

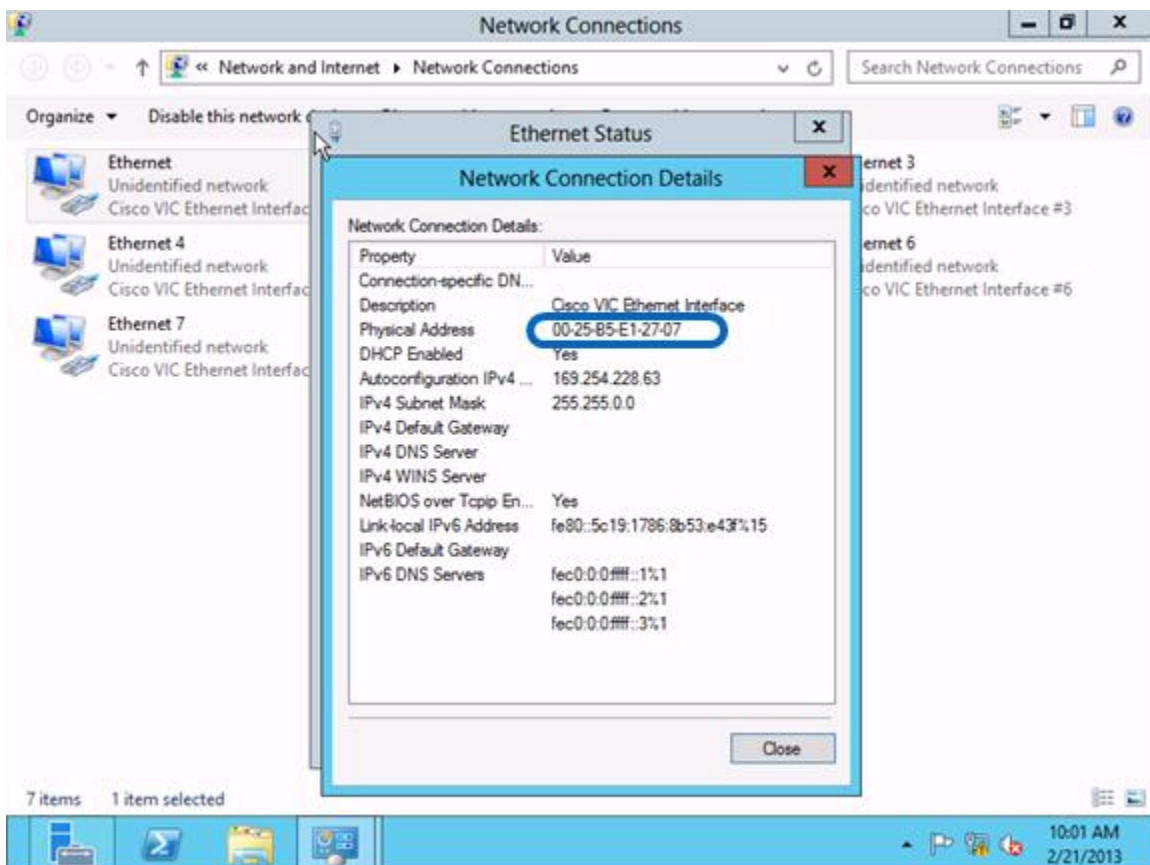
12. Click Boot Server, the service profile will then pull a server from the Infra_Pool, and configure the hardware per the service profile.
13. Once the server has fully booted Windows will enter the out of box experience. Accept the EULA, and click Accept.
14. Enter the region and language settings and Click Next.
15. Enter a new Administrator Password, and click Finish.
16. Repeat for each service profile.

9.7 Configure Windows Networking for FlexPod

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

All Hosts

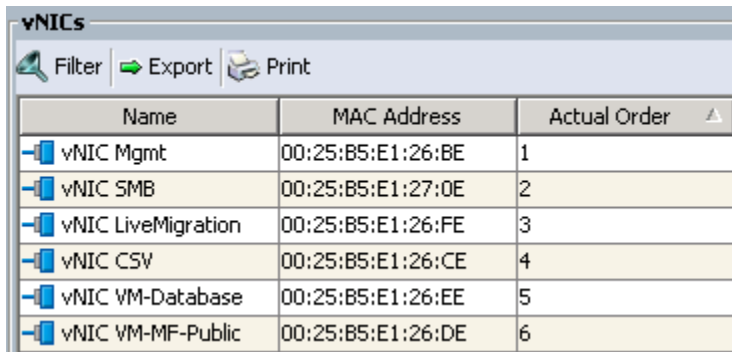
1. In server Manager select Local Server on the left.
2. Click on the IPv4 address assigned by DHCP, IPv6 enabled link to launch the network connections control panel.
3. One at a time right click on each eNIC, and select Status.
4. Click details, and note the Physical Address.



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

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

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



Name	MAC Address	Actual Order
vNIC Mgmt	00:25:B5:E1:26:BE	1
vNIC SMB	00:25:B5:E1:27:0E	2
vNIC LiveMigration	00:25:B5:E1:26:FE	3
vNIC CSV	00:25:B5:E1:26:CE	4
vNIC VM-Database	00:25:B5:E1:26:EE	5
vNIC VM-MF-Public	00:25:B5:E1:26:DE	6

6. Identify the vNIC with the MAC Address noted in step 3.
 7. Back in windows rename the LAN adapter to reflect the network it is associated with.
 8. Set the appropriate IP settings for that adapter.
- Note:** Assign IP Addresses to the LiveMigration, CSV, and Mgmt adapters.
- Note:** Default gateway and DNS entries should be configured for the Mgmt NIC only.
9. Repeat for each eNIC in windows.
 10. In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings
 11. Select the adapter and use the arrows to move it up or down in binding order.
 12. The recommended binding order is:
 - Mgmt
 - SMB
 - LiveMigration
 - CSV
 - VM-Database
 - VM-MF-Public
 - App-Cluster-Comm

9.8 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
VM-Database	External	No	VM-Database	No
App-Cluster-Comm	External	No	App-Cluster-Comm	No

3. Create virtual switch Mgmt


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

4. Create virtual switch VM-Database

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

5. Create virtual switch App-Cluster-Comm

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

9.9 Create Virtual Fibre Channel Switches

Create Hyper-V virtual fibre channel switches and bind them to two unused HBAs on the host. These virtual fibre channel switches will be used by the virtual fibre channel adapter in the SQL Server VMs.

1. Obtain the PWWN for the second pair of HBAs on the Hyper-V hosts.

(Table 23) vHBA WWPNS for Fabric A and Fabric B.

Cisco UCS Service Profile Name	WWNN	Fabric-A-2 WWPN	Fabric-B-2 WWPN
VMHost-Mgmt01			
VMHost-Mgmt02			

All Hosts

1. Create two virtual fibre channel switches.

```
New-VMSan -Name vFabric-A -WorldWideNodeName <vHBA_A WWN> `
-WorldWidePortName <vHBA_A WWPNS>

New-VMSan -Name vFabric-B -WorldWideNodeName <vHBA_B WWN> `
-WorldWidePortName <vHBA_B WWPNS>
```

9.10 Domain Controller Virtual Machines

Most environments will already have an active directory infrastructure and will not require additional domain controllers to be deployed for the Hyper-V FlexPod. 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 C in case active directory domain controller need to be created.

9.11 Prepare nodes for Clustering

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

All Hosts

1. 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.

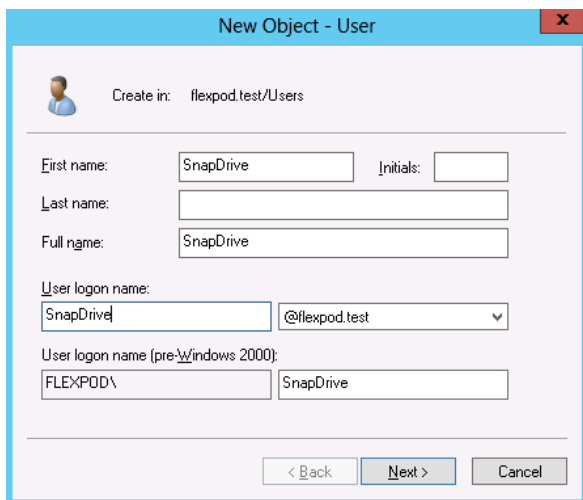
```
Add-Computer -DomainName <domain_name> -Restart
```

9.12 Install NetApp SnapDrive

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

Service Account preparation

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



New Object - User

Create in: flexpod.test/Users

First name: SnapDrive Initials:

Last name:

Full name: SnapDrive

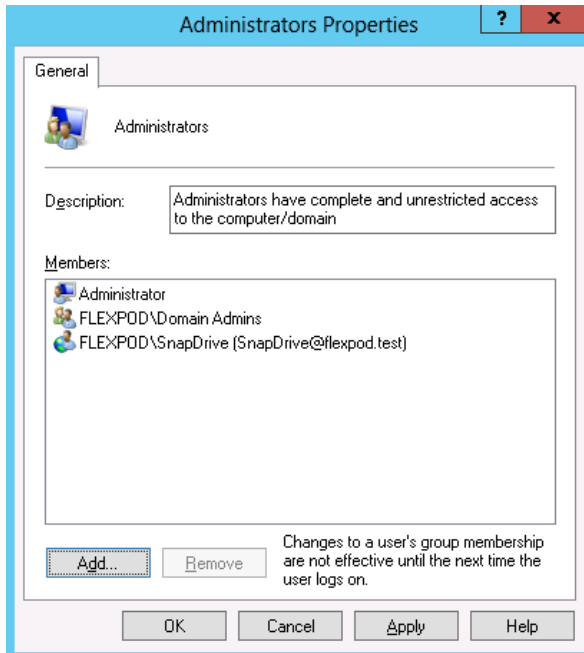
User logon name: SnapDrive @flexpod.test

User logon name (pre-Windows 2000): FLEXPOD\SnapDrive

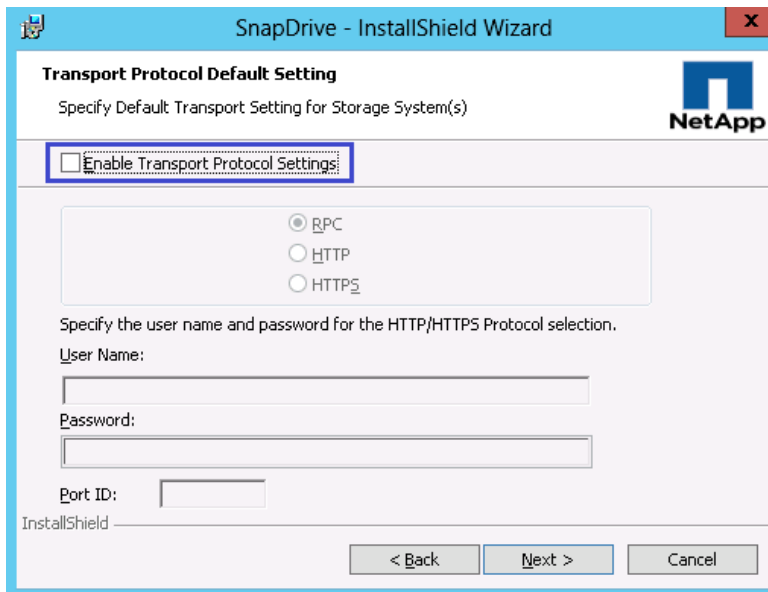
< Back Next > Cancel

All Hosts

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



3. Download SnapDrive installer
http://support.netapp.com/NOW/download/software/snapdrive_win/7.0/SnapDrive7.0_x64.exe
4. Launch the Installer, click **Next**.
5. Select the Storage based Licensing method and click **Next**.
6. Enter your User Name, and Organization information, and click **Next**.
7. Validate the installation path and click **Next**.
8. Check the **Enable SnapDrive to communicate through the Windows Firewall** checkbox and click **Next**.
9. Enter the Account information for the Snapdrive service account, Click **Next**.
10. Click **Next**, through the SnapDrive Web Service Configuration.
11. Uncheck **Enable Preferred storage system IP Address**, and Click **Next**.
12. Uncheck the **Enable Transport Protocol Settings**, and click **Next**



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

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

16. Configure SnapDrive Preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_vserver_mgmt>> -IP << var_vserver_mgmt_ip>>
```

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

```
Set-SdStorageConnectionSetting -StorageSystem <<var_vserver_mgmt>> -protocol https -credential vsadmin
```

9.13 Install NetApp SnapManager for Hyper-V

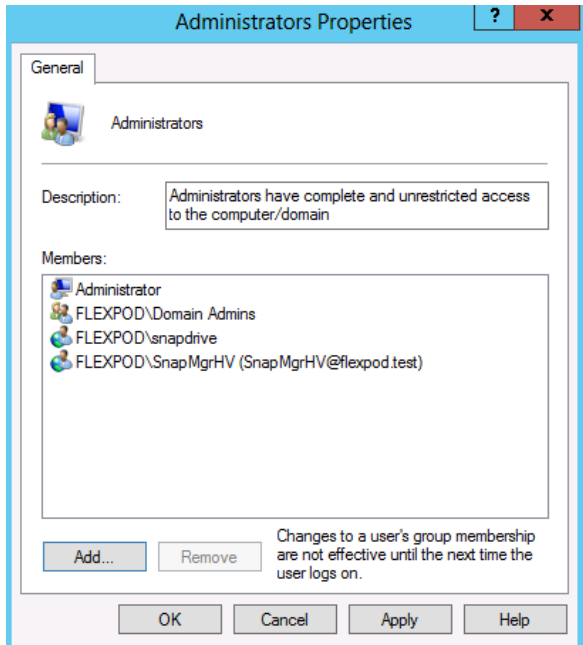
The following section describes how to installation of the NetApp SnapManger for Hyper-V. For detailed information regarding the installation see the Administration and Installation Guide.

Service Account preparation

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

All Hosts

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



All Hosts

1. Download the SnapManger for Hyper-V installer from http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/2.0/SMHV2.0_x64.exe
2. Launch the Installer, click Next.
3. Select the Storage based Licensing method and click Next.
4. Enter your User Name, and Organization information, and click Next.
5. Validate the installation path and click Next.
6. Enter the Account information for the SMHV service account, Click Next.
7. Click Next, through the SMHV Web Service Configuration.
8. Click Install.

9.14 Create a Cluster.

One Host 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> -NoStorage -StaticAddress <cluster_ip_address>
```

3. Rename Cluster Networks

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

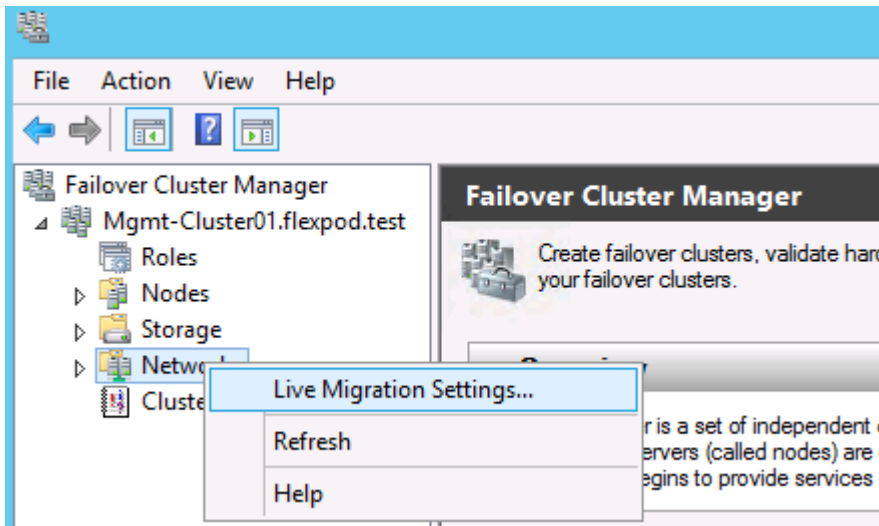
- Designate the CSV network.

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

9.15 Configure Live Migration network.

One Server Only

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



- Deselect all but the LiveMigration network and click OK.

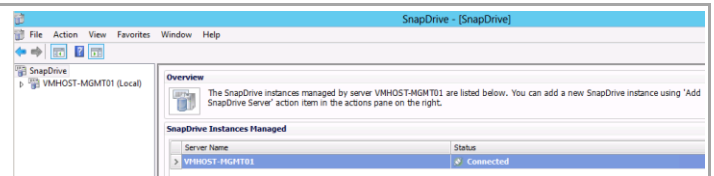
9.16 Create Quorum Witness LUN

One Server Only

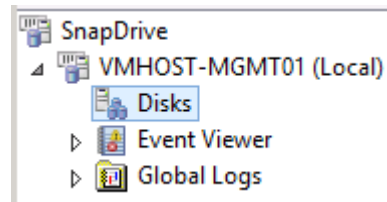
- Open a PowerShell prompt and move the Available Storage cluster group by running.

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

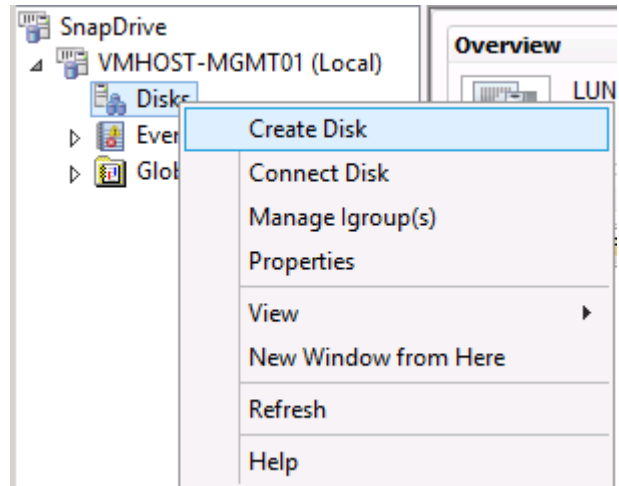
Open SnapDrive from the start screen to configure cluster storage.



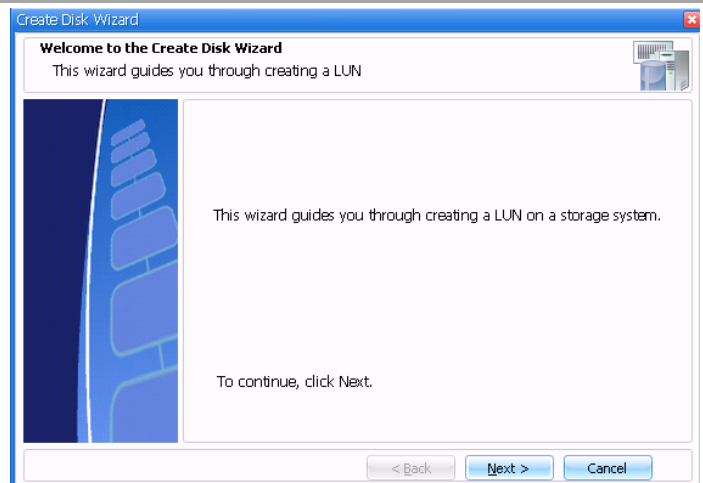
Expand server name object in the left tree view, and select the disk object.



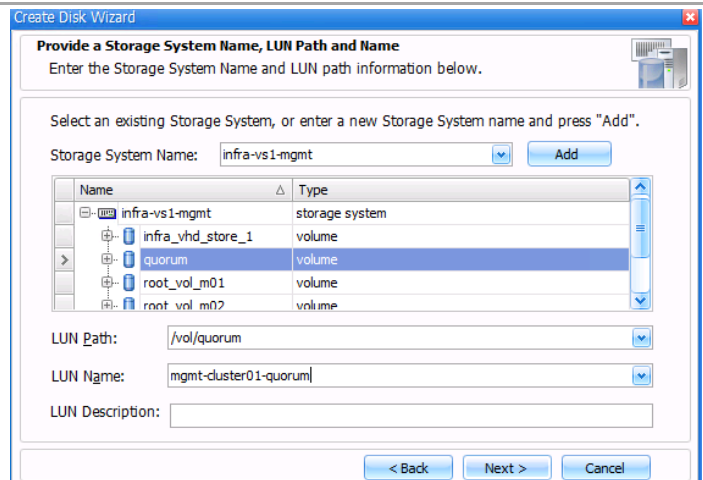
Right-click the Disks Icon and choose to Create Disk.



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.

The screenshot shows the 'Create Disk Wizard' window with the title bar 'Create Disk Wizard'. The main heading is 'Select a LUN Type' with the instruction 'Select whether to create a dedicated or a shared LUN'. Below this, it states 'The LUN can be connected to as a dedicated disk or a shared disk.' There are two radio button options: 'Dedicated' (unselected) and 'Shared (Microsoft Cluster Services only)' (selected). A description for the shared option reads: 'A shared disk is used only with Microsoft® Cluster Services. Select "Shared" if you are using this disk as a Microsoft Cluster Services physical disk resource.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Review the list of cluster nodes and click Next.

The screenshot shows the 'Create Disk Wizard' window with the title bar 'Create Disk Wizard'. The main heading is 'Information about the Microsoft Cluster Services System' with the instruction 'Displays cluster name, active members of the Microsoft Cluster Services System.' Below this, it states 'You are creating a virtual disk to be shared by the active member nodes of a Microsoft Cluster Services system.' It then says 'Following are the Active Nodes for : Mgmt-Cluster01'. A box titled 'Disk devices will be created on each of the active nodes (listed below).' contains a list of two nodes: 'VMHOST-MGMT01' and 'VMHOST-MGMT02'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Select the following parameters:

Driver Parameters

Do not assign a drive letter or Volume Mount Point

Snapshot Copies

Limit

LUN Size:

1GB

The screenshot shows the 'Create Disk Wizard' window with the title bar 'Create Disk Wizard'. The main heading is 'Select LUN Properties' with the instruction 'Provide the drive letter and the size of the LUN to create'. Below this, there are three sections: 'Drive Parameters' with three radio button options: 'Assign a Drive Letter:' (unselected, showing 'D' in a dropdown), 'Use a Volume Mount Point:' (unselected, with an empty text box), and 'Do not assign a Drive letter or Volume Mount Point' (selected); 'Snapshot Copies' with the question 'Do you want to limit the maximum disk size to accommodate at least one snapshot on the volume?' and two radio button options: 'Limit' (selected) and 'Do not limit' (unselected); and 'LUN Size' with a note 'NOTE: Thin provisioning has been configured for the volume hosting this lun', a table showing 'Maximum: 5 GB' and 'Minimum: 64 MB', a 'LUN Size:' section with a dropdown set to '1.0' and a unit dropdown set to 'GB', and a question 'Do you want to allow max lun size for this lun?' with two radio button options: 'Yes' (unselected) and 'No' (selected). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Review the automatic snapshot setting for the target volume and click Next.

Create Disk Wizard

Important Properties of the Storage System Volume.
Settings on the Storage System volume.

SnapDrive will set the following properties for volume name: quorum

Key	Value
snapshot schedule:	OFF

< Back Next > Cancel

In the Select Initiators screen, Select each cluster node and WWPNs for HBAs Fabric-A-1 and Fabric-B-1.

Create Disk Wizard

Select Initiators
Select initiators to be used by this LUN.

Specify a cluster node, and then establish or remove the connection to the LUN for that node by selecting the initiator name from the initiator list.

Select the cluster node name

- Mgmt-Cluster01
 - VMHOST-MGMT01
 - VMHOST-MGMT02

Initiator List for VMHOST-MGMT01

Fiber Channel Initiator(s)

- ☒ 20:00:00:25:b5:e8:09:0e
- ☒ 20:00:00:25:b5:e8:09:3e
- ☐ 20:00:00:25:b5:e8:09:2e
- ☐ 20:00:00:25:b5:e8:09:5e

< Back Next > Cancel

Create Disk Wizard

Select Initiators
Select initiators to be used by this LUN.

Specify a cluster node, and then establish or remove the connection to the LUN for that node by selecting the initiator name from the initiator list.

Select the cluster node name

- Mgmt-Cluster01
 - VMHOST-MGMT01
 - VMHOST-MGMT02

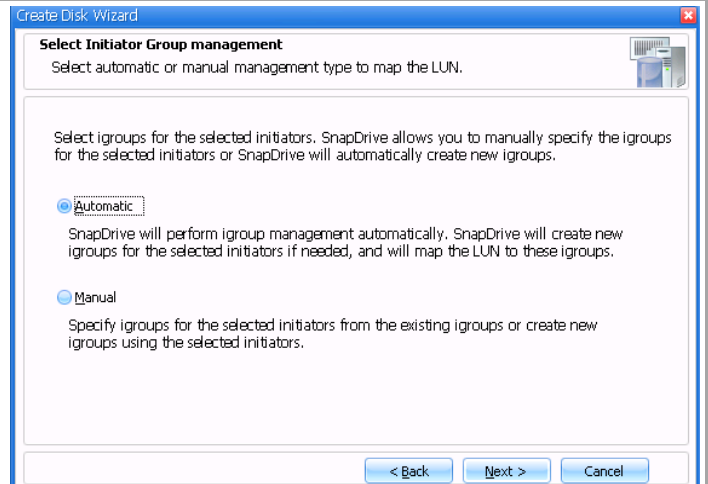
Initiator List for VMHOST-MGMT02

Fiber Channel Initiator(s)

- ☒ 20:00:00:25:b5:e8:09:4e
- ☒ 20:00:00:25:b5:e8:09:1f
- ☐ 20:00:00:25:b5:e8:09:0f
- ☐ 20:00:00:25:b5:e8:09:3f

< Back Next > Cancel

Select Automatic igroup management and Click Next.



Create Disk Wizard

Select Initiator Group management
Select automatic or manual management type to map the LUN.

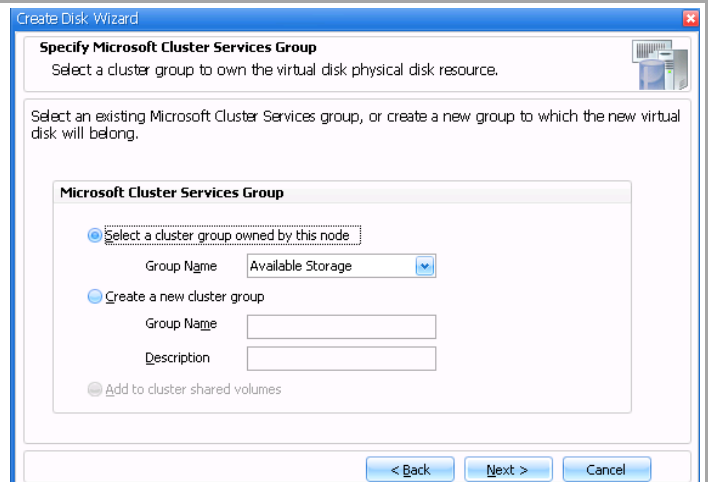
Select igroups for the selected initiators. SnapDrive allows you to manually specify the igroups for the selected initiators or SnapDrive will automatically create new igroups.

☒ Automatic
SnapDrive will perform igroup management automatically. SnapDrive will create new igroups for the selected initiators if needed, and will map the LUN to these igroups.

☐ Manual
Specify igroups for the selected initiators from the existing igroups or create new igroups using the selected initiators.

< Back Next > Cancel

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



Create Disk Wizard

Specify Microsoft Cluster Services Group
Select a cluster group to own the virtual disk physical disk resource.

Select an existing Microsoft Cluster Services group, or create a new group to which the new virtual disk will belong.

Microsoft Cluster Services Group

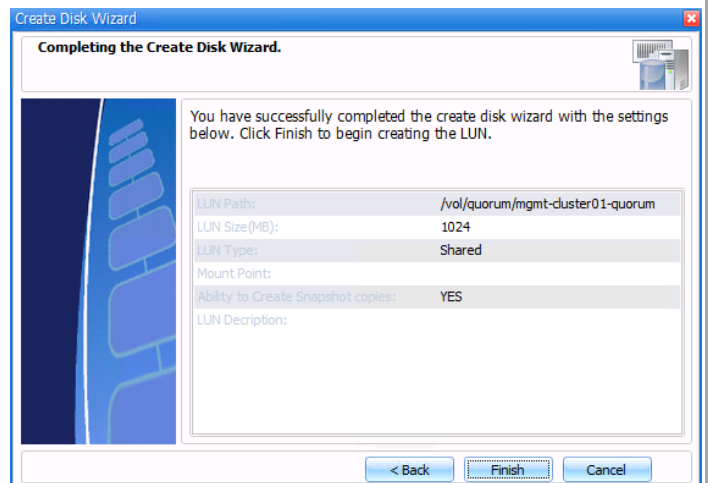
☒ Select a cluster group owned by this node
Group Name: Available Storage

☐ Create a new cluster group
Group Name:
Description:

☐ Add to cluster shared volumes

< Back Next > Cancel

Review the parameters and click Finish.



Create Disk Wizard

Completing the Create Disk Wizard.

You have successfully completed the create disk wizard with the settings below. Click Finish to begin creating the LUN.

LUN Path:	/vol/quorum/mgmt-cluster01-quorum
LUN Size(MB):	1024
LUN Type:	Shared
Mount Point:	
Ability to Create Snapshot copies:	YES
LUN Description:	

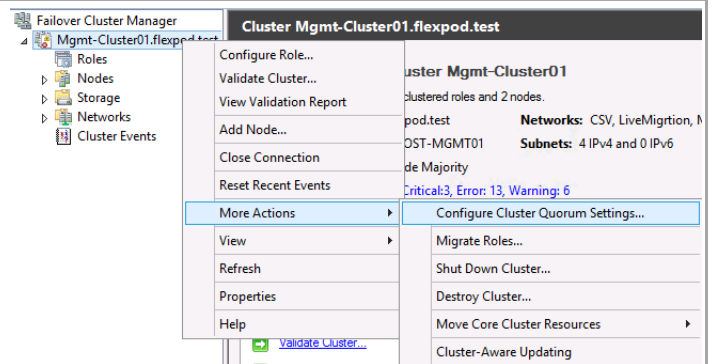
< Back Finish Cancel

Change the Managment Cluster to Use a Quorum Disk

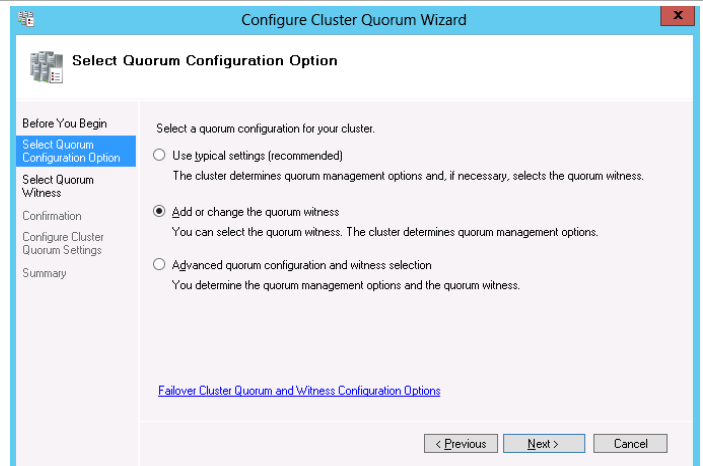
In failover cluster manager, select **More Actions** in the action pane and click **Configure Cluster Quorum Settings...**

The following cmdlet can be used to assign the quorum disk as an alternative to using Failover Cluster Manager.

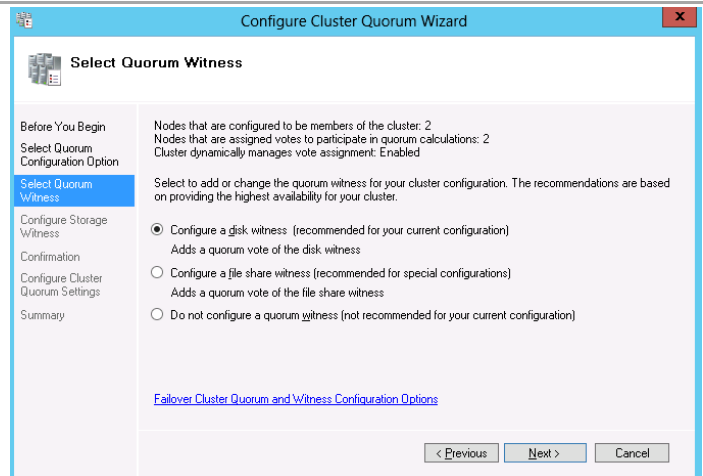
```
Set-ClusterQuorum  
NodeAndDiskMajority  
<ClusterQuorumDisk>
```



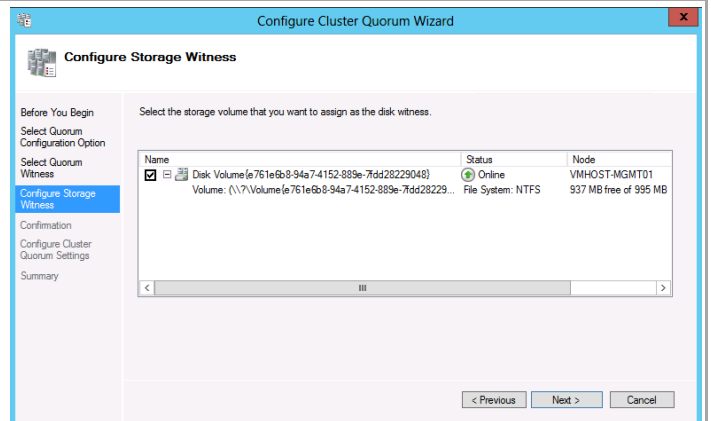
Select **Add or Change the quorum witness**, and click **Next**.



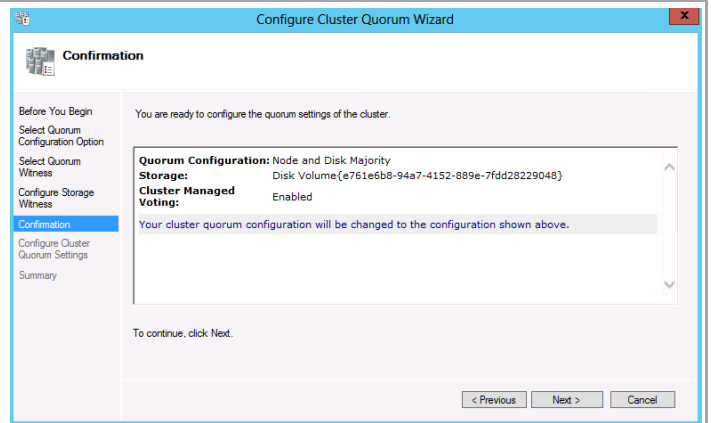
Select **Configure a disk witness** and click **Next**.



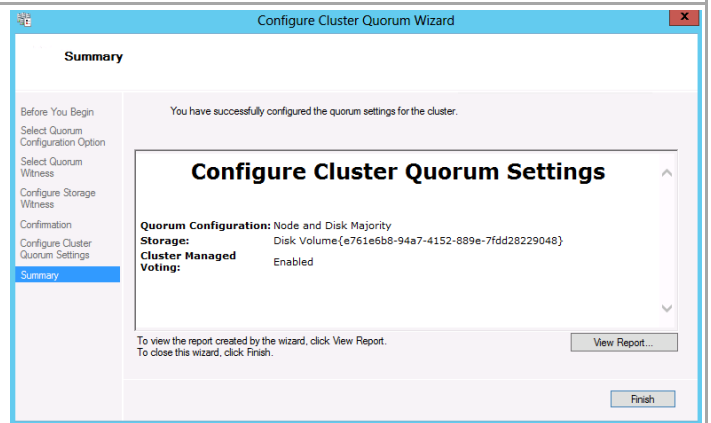
Select the **LUN** without a drive letter that was previously created to be the quorum LUN. Click **Next**.



Confirm the settings and click **Next**.

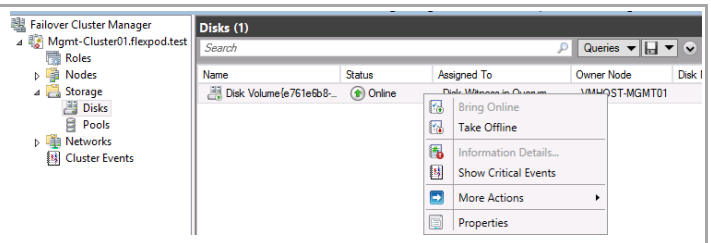


Review the results and click **Finish** to close the wizard screen.

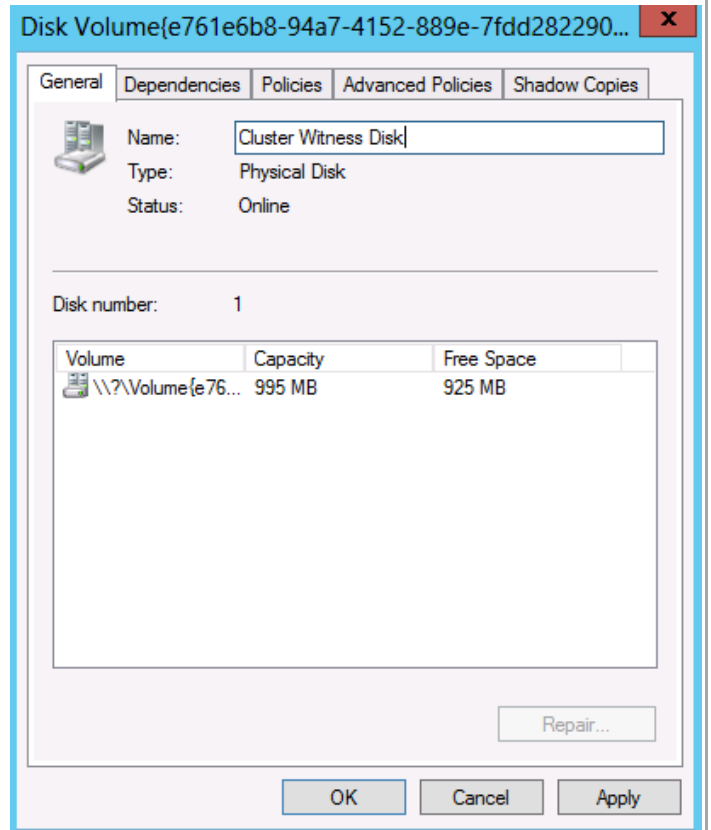


Assign Management Cluster Disk Names

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**.

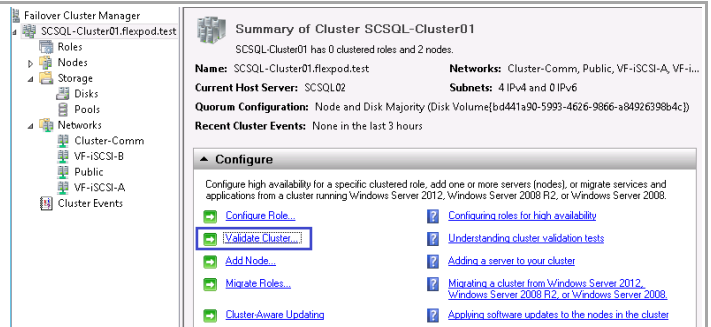


In the Name field, enter a name that reflects the LUN role.



9.17 Validated the Managment Cluster

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



Select **Run all tests** and click Next.

The screenshot shows the 'Testing Options' step of the 'Validate a Configuration Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Testing Options' (selected), 'Review Storage Status', 'Confirmation', 'Validating', and 'Summary'. The main area has a heading 'Testing Options' with a green checkmark icon. Below it, text explains that the tests examine Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration. It also notes that Microsoft supports a cluster solution only if the complete configuration can pass all tests. Two radio buttons are present: 'Run all tests (recommended)' (selected) and 'Run only tests I select'. A link 'More about cluster validation tests' is at the bottom. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Select the shared disks on the cluster and Click Next.

The screenshot shows the 'Review Storage Status' step of the 'Validate a Configuration Wizard'. The left sidebar is the same as the previous screen. The main area has a heading 'Review Storage Status' with a green checkmark icon. Text indicates that additional storage can be selected for validation. A table lists storage items:

Name	Assigned To
<input checked="" type="checkbox"/> Cluster Witness Disk	Disk Witness in Quorum

Below the table, a warning icon and text state: 'To avoid role failures, it is recommended that all roles using this Cluster Shared Volume be stopped before the storage is validated.' Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Confirm the selected options and click **Next**.

The screenshot shows the 'Confirmation' step of the 'Validate a Configuration Wizard'. The left sidebar is the same. The main area has a heading 'Confirmation' with a green checkmark icon. Text states: 'You are ready to start validation. Please confirm that the following settings are correct:'. Two lists are shown:

Servers to Test

- VMHOST-MGMT01.flexpod.test
- VMHost-Mgmt02.flexpod.test

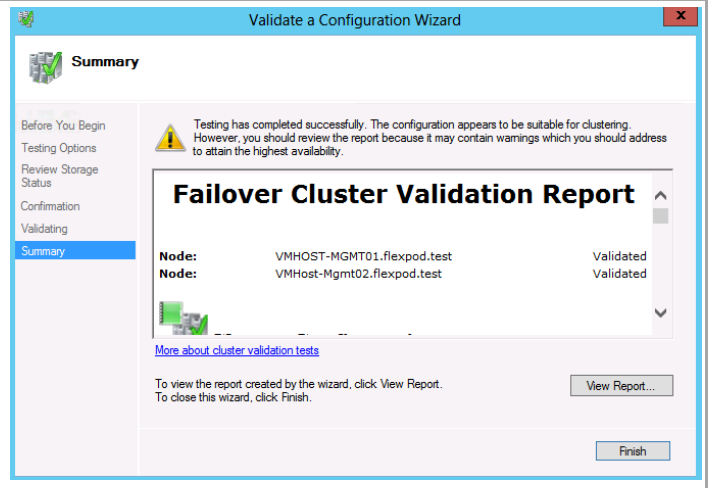
Tests Selected by the User

Tests Selected by the User	Category
List Cluster Core Groups	Cluster Configuration
List Cluster Network Information	Cluster Configuration
List Cluster Resources	Cluster Configuration
List Cluster Volumes	Cluster Configuration
List Clustered Roles	Cluster Configuration

At the bottom, text says 'To continue, click Next.' and a link 'More about cluster validation tests' is provided. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

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

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



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

Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node VMHOST-MGMT01.flexpod.test.

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

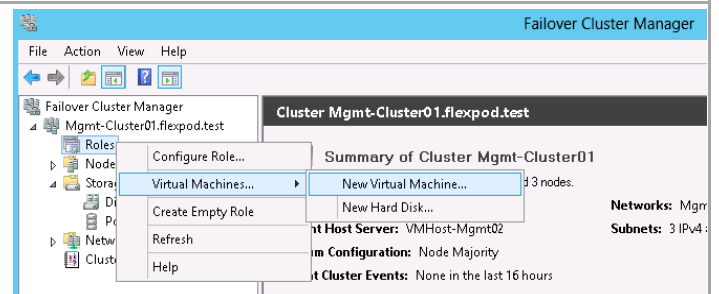
10 Create Gold Master Template VM

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 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 **Services and applications** node, right-click and select **Virtual Machines...**, and then select **New Virtual Machine...** from the context menu.

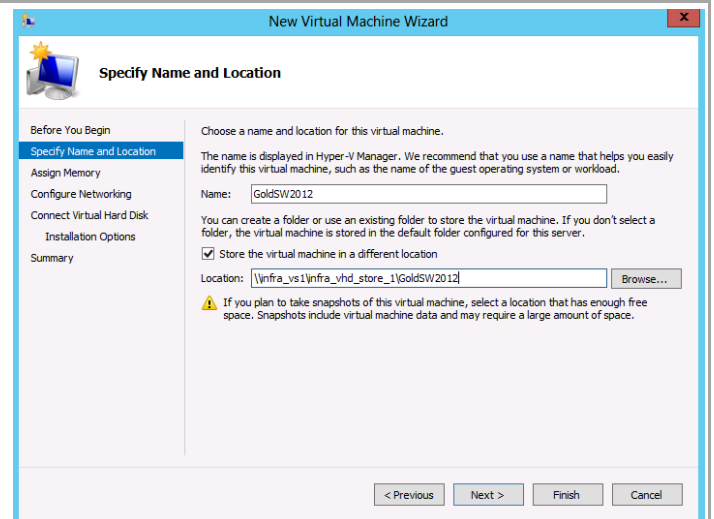


The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:

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

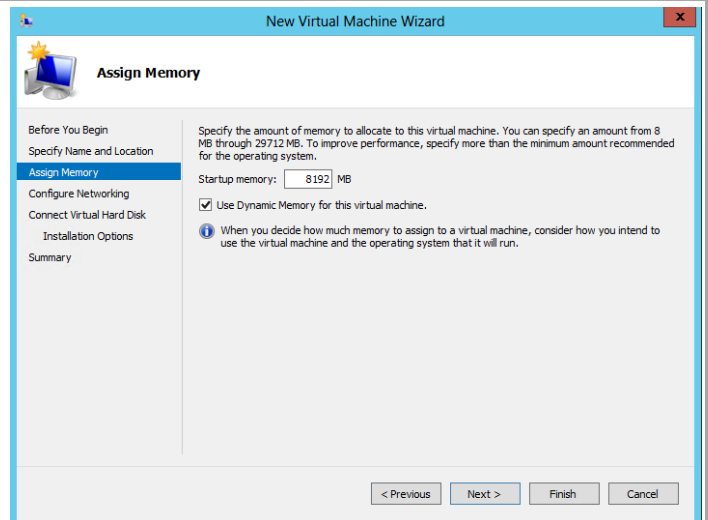
Select the **Store the virtual machine in a different location** check box. In the **Location** text box, specify the location of the vhd share on your storage cluster vserver.

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.

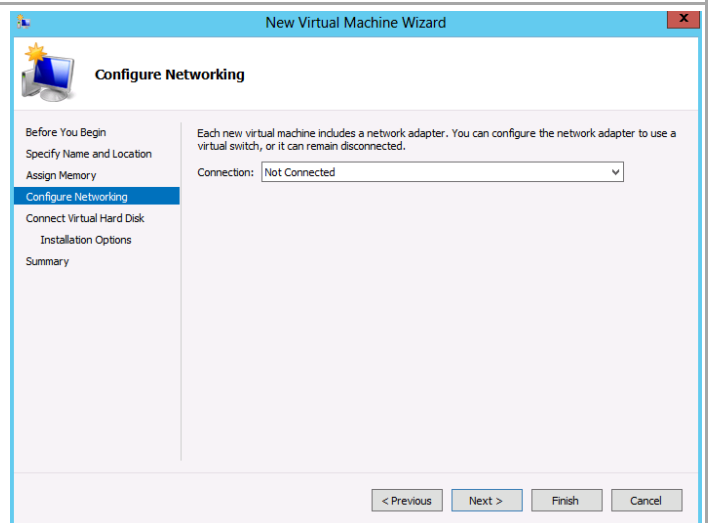


The screenshot shows the 'Assign Memory' step of the 'New Virtual Machine Wizard'. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location', 'Assign Memory' (selected), 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions on specifying memory, a 'Startup memory' field set to '8192 MB', a checked box for 'Use Dynamic Memory for this virtual machine', and an information icon with a note about memory allocation. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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

Connection – specify the Not Connected connection in the drop-down menu.

Click **Next** to continue.



The screenshot shows the 'Configure Networking' step of the 'New Virtual Machine Wizard'. The left sidebar is the same as the previous dialog. The main area explains network adapter configuration and features a 'Connection' dropdown menu set to 'Not Connected'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

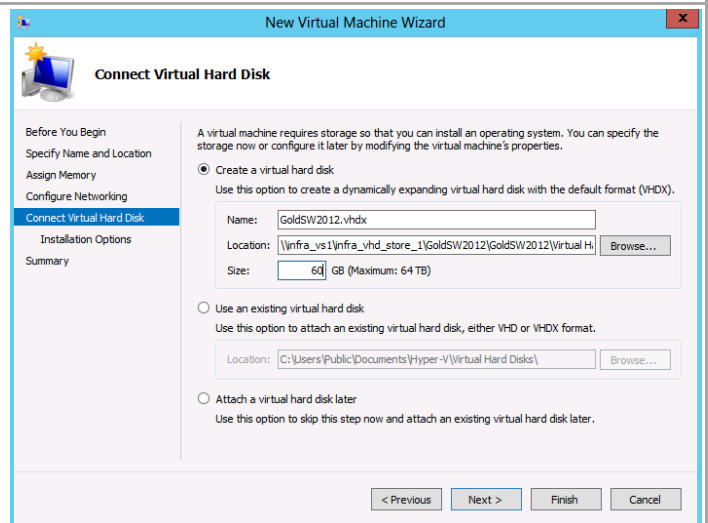
In the **Connect Virtual Hard Disk** dialog, select the **Create a virtual hard disk** option and provide the following values:

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.

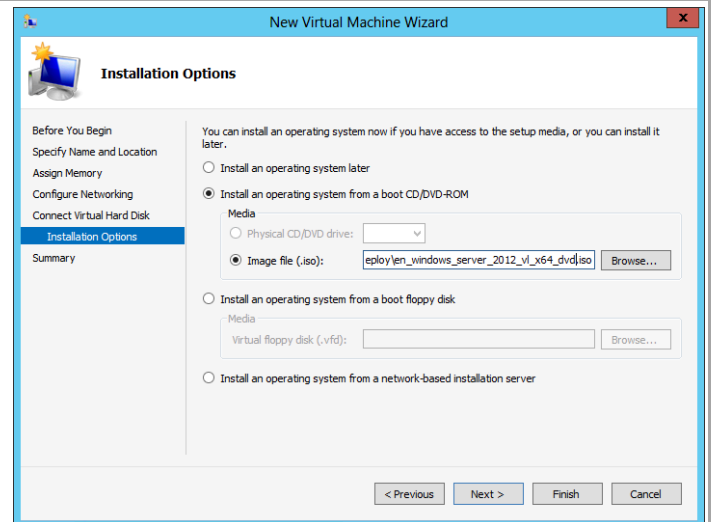


The screenshot shows the 'Connect Virtual Hard Disk' step of the 'New Virtual Machine Wizard'. The left sidebar is the same. The main area offers three options: 'Create a virtual hard disk' (selected), 'Use an existing virtual hard disk', and 'Attach a virtual hard disk later'. The 'Create a virtual hard disk' option includes fields for 'Name' (GoldSW2012.vhdx), 'Location' (\\infra_vs1\infra_vhd_store_1\GoldSW2012\GoldSW2012\Virtual H...), and 'Size' (60 GB). At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

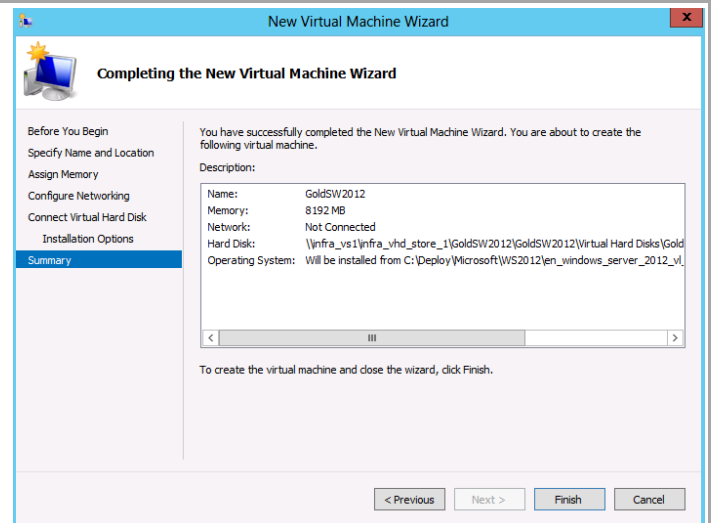
In the **Installation Options** dialog, select the **Install an operating system from a boot CD/DVD-ROM** option and

- **Image file (.iso):** Specify the path the to Windows Server 2012 iso.

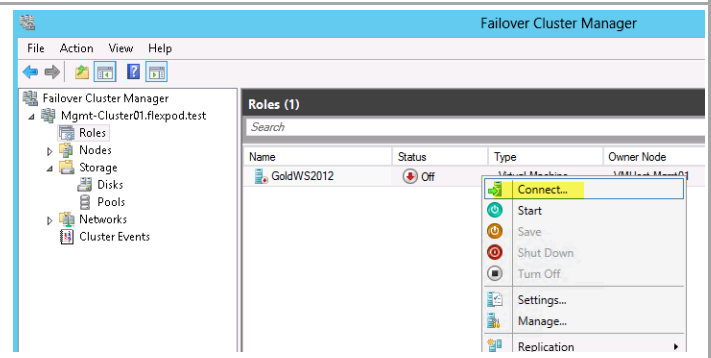
Click **Next** to continue.



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**.

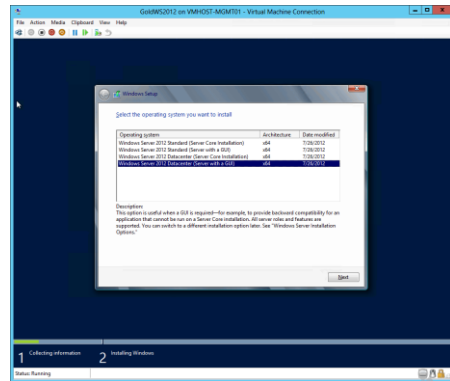
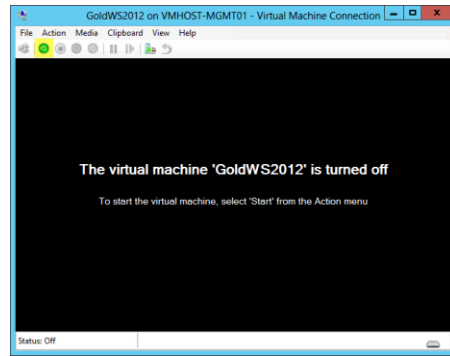


Click the **PowerON** Button to power on the VM and boot into the Windows Server 2012 Installer.

1. After the installer is finished loading, Enter the relevant region information and click **Next**.
2. Click **Install now**.
3. Enter the Product Key and click **Next**.
4. Select **Windows Server 2012 Datacenter (Server with a GUI)** and click **Next**.

Note: You may optionally remove the GUI after the Hyper-V cluster is operational.

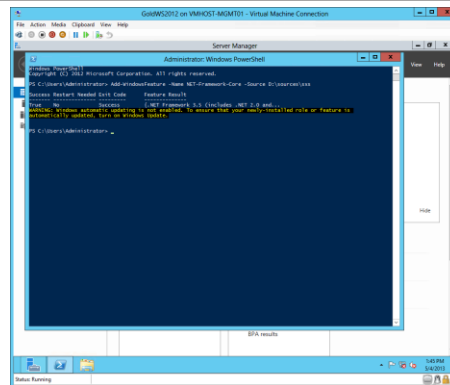
5. After reviewing the EULA, **Check the I accept the license terms**, and click **Next**.
6. Select **Custom: Install Windows only (advanced)**.
7. Select the Drive 0 as the installation location for Windows. Press click **Next** to continue with the install.
8. When Windows is finished installing enter 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:

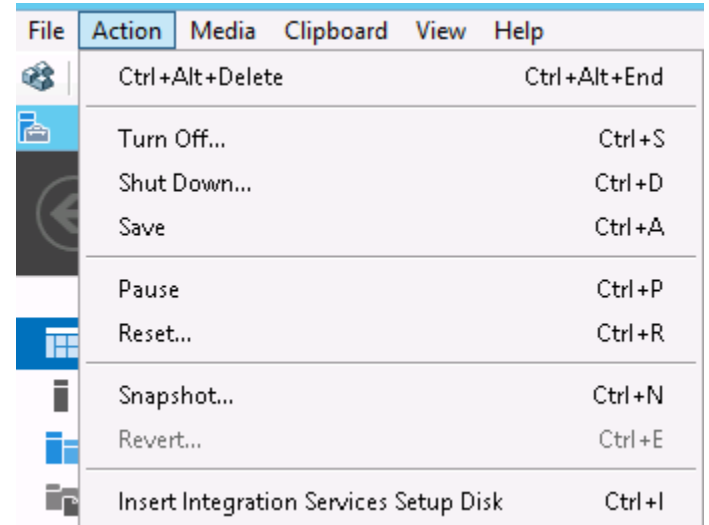
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs

Eject the DVD drive after completeting this operation.



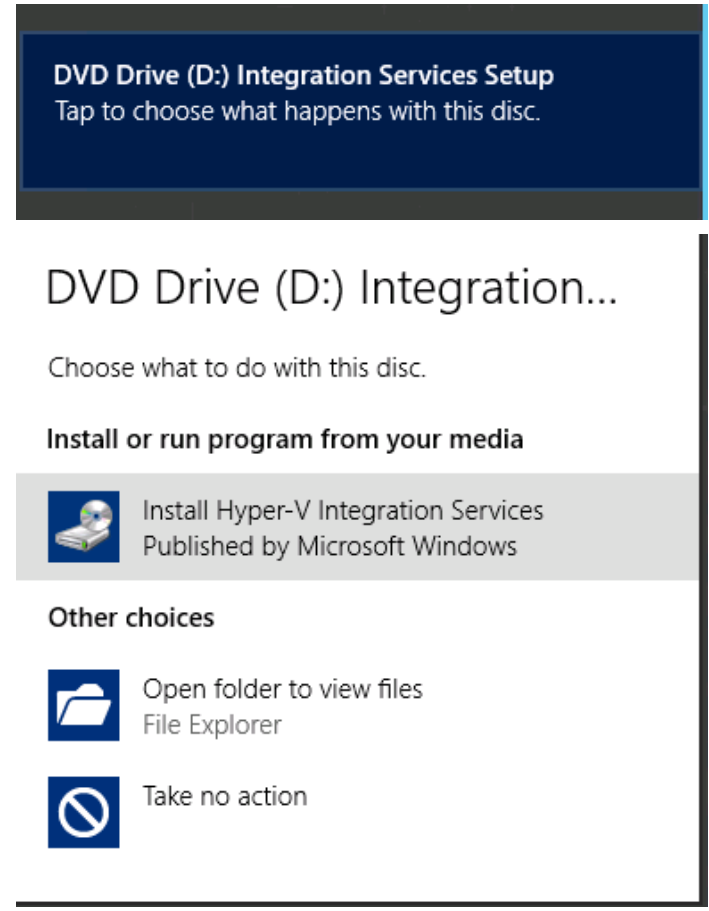
Install important and recommended Windows Updates and reboot .

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.

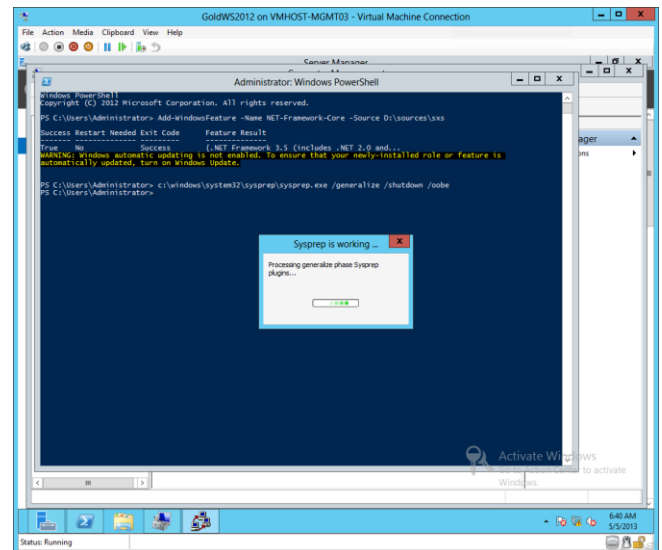
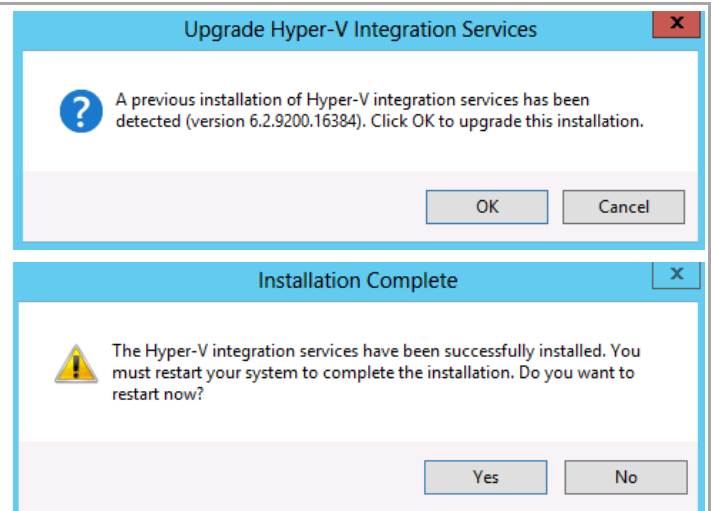


Click **OK** to update the Hyper-V integration services version.

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
```



11 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 two-node Hyper-V failover cluster. These virtual machines serve as the basis for fabric management operations. The following table summarizes the fabric management virtual machine requirements by the System Center component that supports the product or operating system role.

Component Roles	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
SQL Server Cluster Node 1	8	16	60
SQL Server Cluster Node 2	8	16	60
Virtual Machine Manager	4	8	60
Virtual Machine Manager	4	8	60
App Controller	4	8	60
Operations Manager Management Server	8	16	60
Operations Manager Management Server	8	16	60
Operations Manager Reporting Server	8	16	60
Orchestrator Runbook Server	4	8	60
Orchestrator supplemental Runbook Server	4	8	60
Service Manager Management Server	4	16	60
Service Manager portal	4	16	60
Service Manager Data Warehouse	8	16	60
Infrastructure (SMI-S Agent)	2	4	60
Cisco Nexus 1000V VMS 1	1	4	4
Cisco Nexus 1000V VMS 2	1	4	4
Totals	76	164 GB	788 GB

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

11.1 Automated creation and configuration.

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

```
(@{"Name"="SCSQL01";"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCSQL02";"CPU"="8";"memory"="16";"Cluster"=$True},
@{"Name"="SCVMM01";"CPU"="4";"memory"="8";"Cluster"=$True},
@{"Name"="SCVMM02";"CPU"="4";"memory"="8";"Cluster"=$True},
@{"Name"="SCAC01";"CPU"="4";"memory"="8";"Cluster"=$false},
@{"Name"="SCOM01";"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCOM02";"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCOMRS01";"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCOR01";"CPU"="4";"memory"="8";"Cluster"=$false},
@{"Name"="SCOR02";"CPU"="4";"memory"="8";"Cluster"=$false},
@{"Name"="SCSM01";"CPU"="4";"memory"="16";"Cluster"=$false},
@{"Name"="SCSM02";"CPU"="4";"memory"="16";"Cluster"=$false},
@{"Name"="SCSM03";"CPU"="8";"memory"="16";"Cluster"=$false},
@{"Name"="SCInfra";"CPU"="2";"memory"="4";"Cluster"=$false}) | ForEach-Object {
    $Name,$mem,$cpu = $_.Name, $((([int]$_.memory) * 1GB), $_.cpu
    # Use ODX to rapidly provision the New VHDX.
    Copy-Item -Path "\\infra_vsl\infra_vhd_store_1\GoldWS2012.vhdx" `
        -DestinationFile "\\infra_vsl\infra_vhd_store_1\${name}.vhdx"
    # Create the new VM
    $VM = New-VM -BootDevice ide -SwitchName VM-Database `
        -Path "\\infra_vsl\infra_vhd_store_1" -Name $Name `
        -VHDXPath "\\infra_vsl\infra_vhd_store_1\${name}.vhdx"
    # Set the VMs processors
    $VM | Set-VMProcessor -Count $CPU
    # Set the VMs Memory
    $VM | Set-VMemory -DynamicMemoryEnabled $true -StartupBytes $mem -MinimumBytes
($mem/2)
    # Set the VLAN for the vNIC, comment out or change VLAN ID to match your deployment.
    $VM | Get-VMNetworkAdapter | Set-VMNetworkAdapterVlan -VlanId 1001 -Access
    # IF a cluster VM add CLuster-COMm and VM-Fex Nics
    If ($_.Cluster)
    {
        $VM | Add-VMNetworkAdapter -SwitchName VM-Cluster-Comm
        $VM | Add-VMFibreChannelHba -SanName vFabric-A -GenerateWwn
        $VM | Add-VMFibreChannelHba -SanName vFabric-B -GenerateWwn
    }
    # Add VM
    Add-ClusterVirtualMachineRole -Name $Name -VMName $Name
}
```

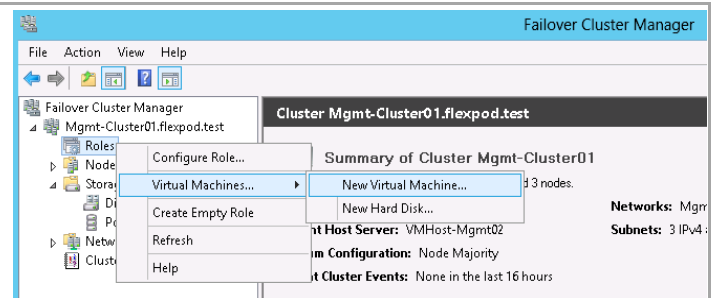
11.2 Manual creation and configuration.

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.

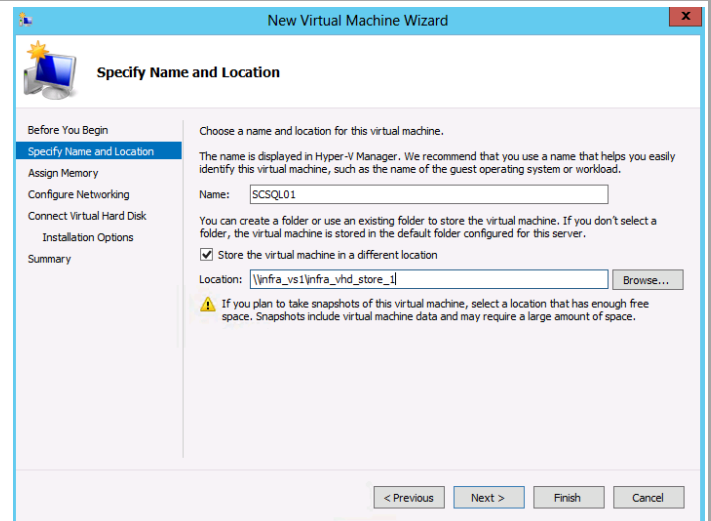


The **New Virtual Machine Wizard** will appear. In the **Specify Name and Location** dialog, provide the following values:

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** checkbox. In the **Location** text box, specify the location of the VHD share of the storage array vServer.

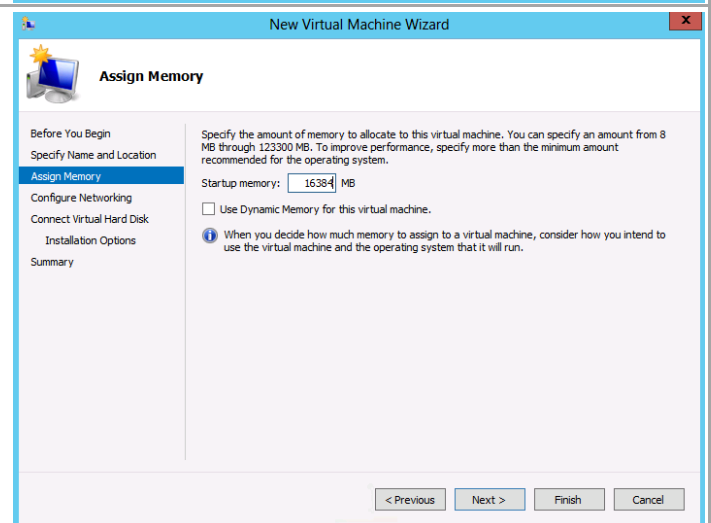
Click **Next** to continue.



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.*

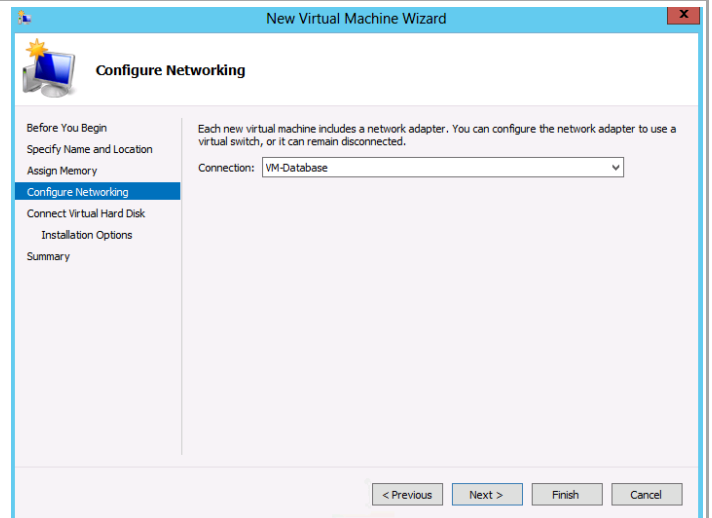
Click **Next** to continue.



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

Connection – specify the VM-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:

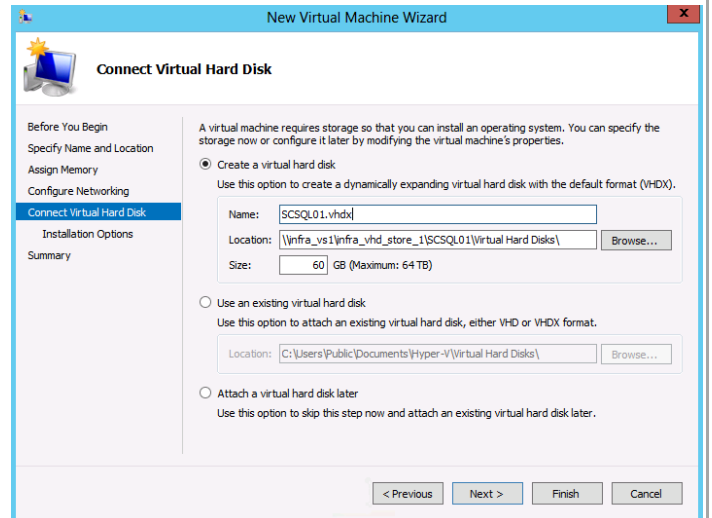
Name – specify the name of the virtual hard disk (VHD). For simplicity this should match the name of the virtual machine.

Location – accept the default location of the CSV on your fabric management host cluster combined with the virtual machine name.

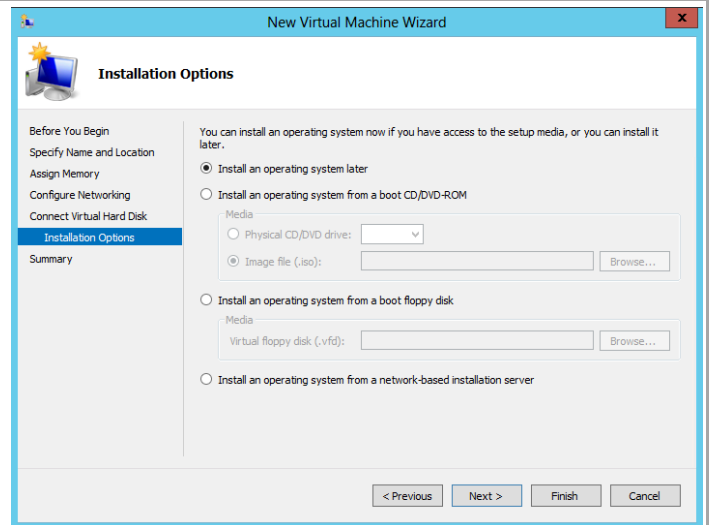
Size – specify the size of the VHD (for operating system partitions this should be 60 GB).

Click **Next** to continue.

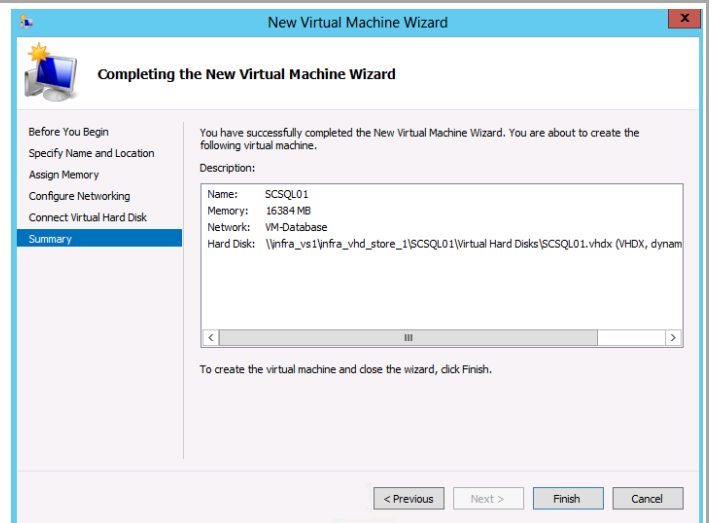
Note: Absent any automated imaging process for the new VMs, a VHD (with Windows Server 2008 R2 or Windows Server 2012 installed and then sysprepped) can be leveraged in place of the new VHD created in this step. This will greatly speed up the provisioning process for the management virtual machines.



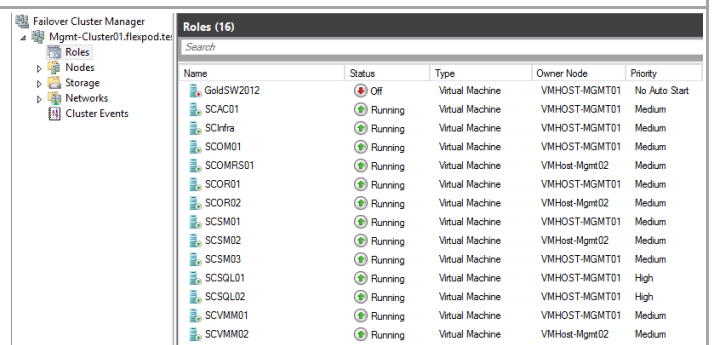
In the **Installation Options** dialog, select the **Install an operating system later** option and click **Next** to continue.



The **Completing the New Virtual Machine Wizard** dialog will display the selections made during the wizard. Click **Finish** to create the virtual machine based on the options selected.
Note: this operation must be completed for each fabric management virtual machine.



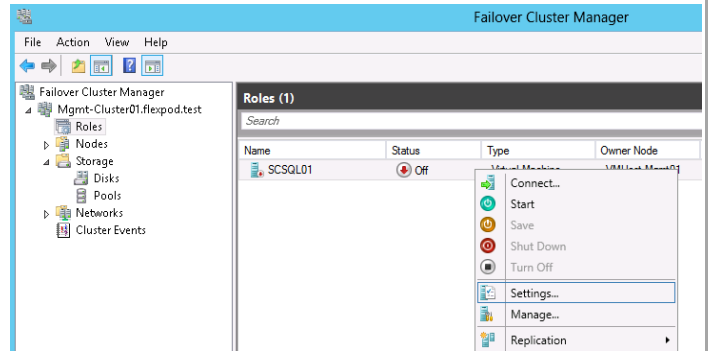
After completion, the virtual machines will be available for management in the **Services and applications** node of the **Failover Cluster Manager**.



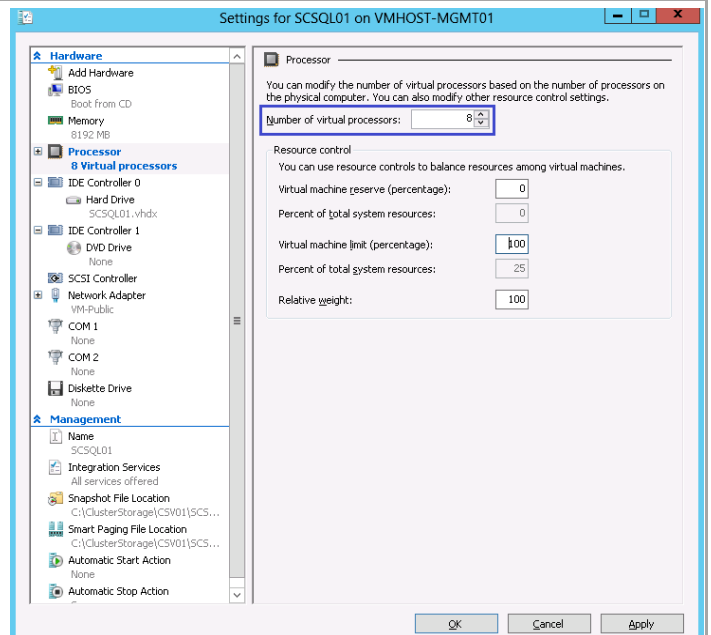
Modify Virtual Machine Settings

Each virtual machine is configured with one virtual processor and one network adapter. The virtual machine configuration must be updated to configure the appropriate number of virtual processors and additional virtual HBA initiator to access LUNs on an FCoE target array.

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

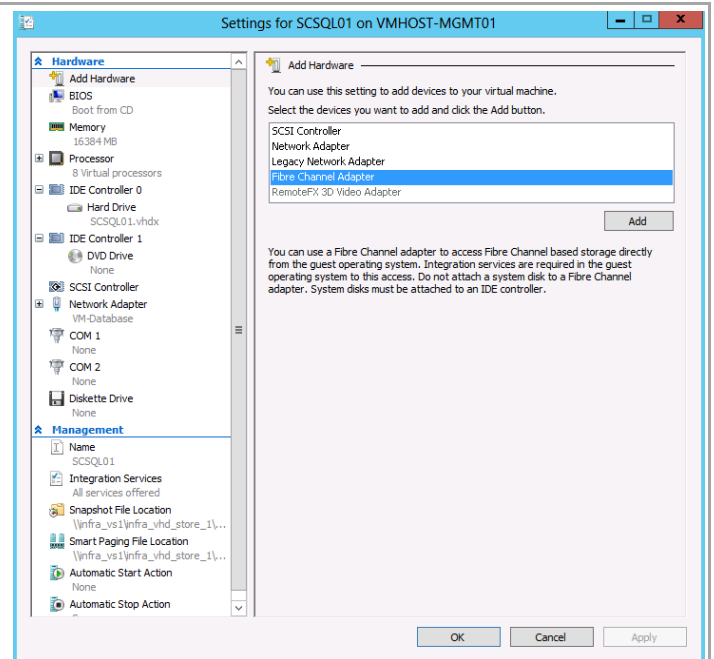


Select **Processor** in the hardware list and set the appropriate number of processors for the specific virtual machine role.

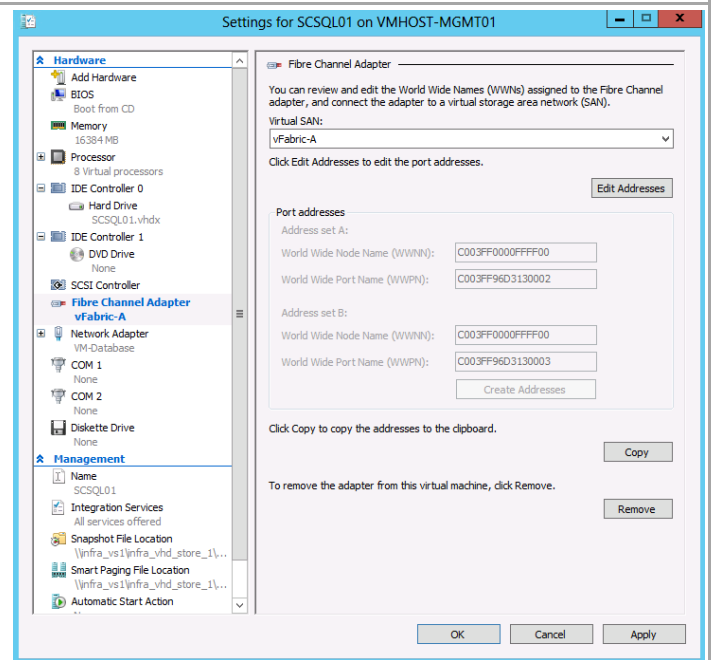


For the SQL Server virtual machines, select **Add Hardware** in the hardware list. Select **Fibre Channel Adapter** in the Add Hardware list and click **Add**.

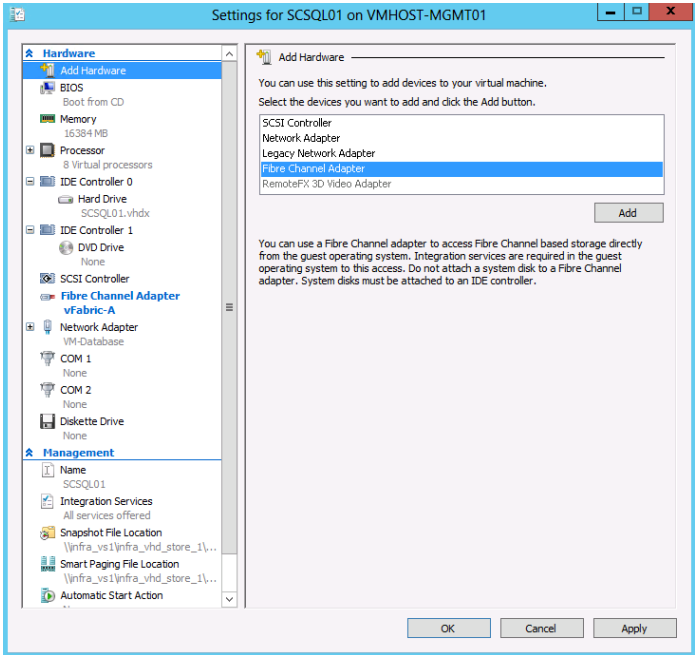
Note: These additional adapters must be added to the SQL Server virtual machines for use as Fibre Channel initiators.



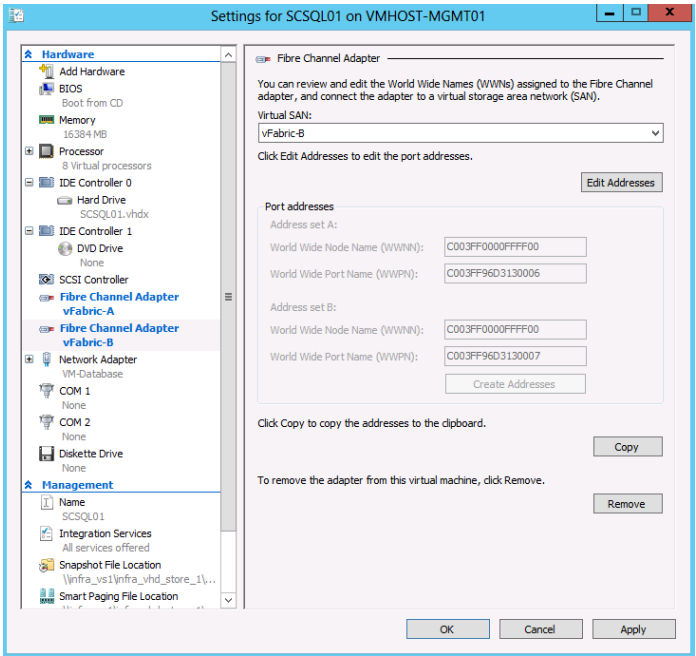
Select **vFabric-A** in the virtual SAN dropdown box.



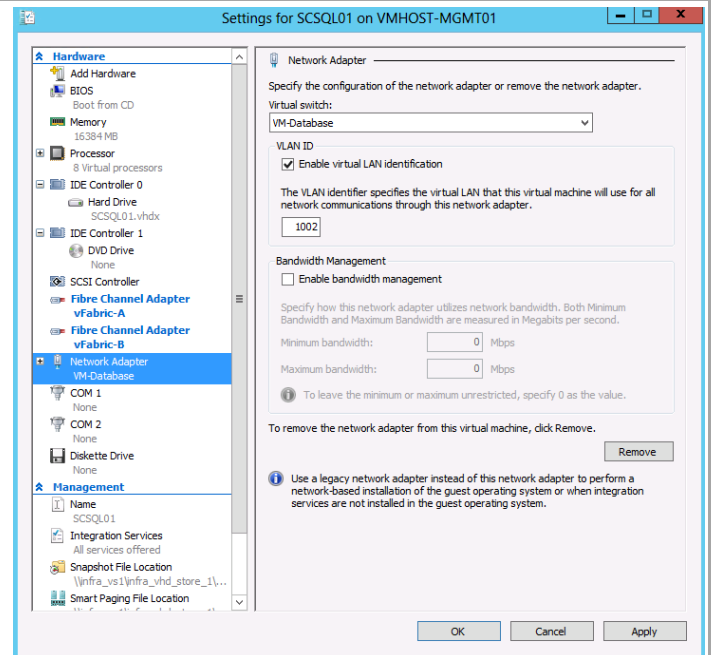
Select **Add Hardware** in the hardware list again.
Select **Fibre Channel Adapter** in the Add Hardware list and click **Add**.



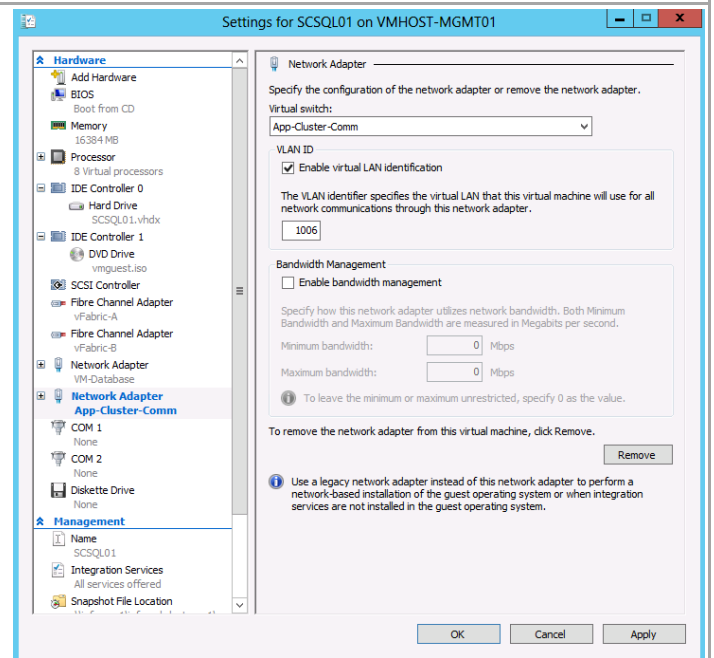
Select **vFabric-B** in the virtual SAN dropdown box.



Select **VM-Database** in the 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.



11.3 Create SAN Zones for the SQL Server Virtual Machines

After the SQL Server virtual machines have been created (in the previous steps), gather the WWPNs of the fibre channel adapters for both virtual machines.

Table 233) vHBA WWPNs for Fabric A and Fabric B.

Virtual Machine Name	vFabric-A WWPNs	vFabric-B WWPNs
SCSQL01		

SCSQL02		
SCVMM01		
SCVMM02		

Note: The WWPNs can be obtained by executing the following powershell command on one of the management cluster nodes.

```
PS C:\> Get-VMFibreChannelHba -VMName <VMName> | fl SanName, WorldWidePortNameSetA,
WorldWidePortNameSetB

SanName           : vFabric-A
WorldWidePortNameSetA : C003FF96D3130004
WorldWidePortNameSetB : C003FF96D3130005

SanName           : vFabric-B
WorldWidePortNameSetA : C003FF96D3130006
WorldWidePortNameSetB : C003FF96D3130007
```

11.4 Create Device Aliases

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

Nexus 5548 A

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

```
device-alias database
device-alias name vFC-SCSQL01-A-SetA pwwn <vFC-SCSQL01-A-SetA WWPN>
device-alias name vFC-SCSQL01-A-SetB pwwn <vFC-SCSQL01-A-SetB WWPN>
device-alias name vFC-SCSQL02-A-SetA pwwn <vFC-SCSQL01-A-SetA WWPN>
device-alias name vFC-SCSQL02-A-SetB pwwn <vFC-SCSQL01-A-SetB WWPN>
device-alias name vFC-SCVMM01-A-SetA pwwn <vFC-SCVMM01-A-SetA WWPN>
device-alias name vFC-SCVMM01-A-SetB pwwn <vFC-SCVMM01-A-SetB WWPN>
device-alias name vFC-SCVMM02-A-SetA pwwn <vFC-SCVMM01-A-SetA WWPN>
device-alias name vFC-SCVMM02-A-SetB pwwn <vFC-SCVMM01-A-SetB WWPN>
exit
device-alias commit
copy running-config startup-config
```

Nexus 5548 B

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

```
device-alias database
device-alias name vFC-SCSQL01-B-SetA pwwn <vFC-SCSQL01-B-SetA WWPN>
device-alias name vFC-SCSQL01-B-SetB pwwn <vFC-SCSQL01-A-SetB WWPN>
device-alias name vFC-SCSQL02-B-SetA pwwn <vFC-SCSQL01-B-SetA WWPN>
device-alias name vFC-SCSQL02-B-SetB pwwn <vFC-SCSQL01-B-SetB WWPN>
device-alias name vFC-SCVMM01-B-SetA pwwn <vFC-SCVMM01-B-SetA WWPN>
device-alias name vFC-SCVMM01-B-SetB pwwn <vFC-SCVMM01-A-SetB WWPN>
device-alias name vFC-SCVMM02-B-SetA pwwn <vFC-SCVMM01-B-SetA WWPN>
device-alias name vFC-SCVMM02-B-SetB pwwn <vFC-SCVMM01-B-SetB WWPN>
exit
```

```
device-alias commit
copy running-config startup-config
```

11.5 Create Zones for Each SQL Server

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

Nexus 5548 A

1. Create the Zones and Add Members

```
zone name vFC-SCSQL01-A vsan <Fabric A VSAN ID>
  member          device-alias          vFC-SCSQL01-A-SetA
  member device-alias vFC-SCSQL01-A-SetB
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name vFC-SCSQL02-A vsan <Fabric A VSAN ID>
  member          device-alias          vFC-SCSQL02-A-SetA
  member device-alias vFC-SCSQL02-A-SetB
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name vFC-SCVMM01-A vsan <Fabric A VSAN ID>
  member          device-alias          vFC-SCVMM01-A-SetA
  member device-alias vFC-SCVMM01-A-SetB
  member          device-alias          Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name vFC-SCVMM02-A vsan <Fabric A VSAN ID>
  member          device-alias          vFC-SCVMM02-A-SetA
  member device-alias vFC-SCVMM02-A-SetB
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
```

2. Add members to the Zoneset

```
zoneset name Flexpod vsan <Fabric A VSAN ID>
  member vFC-SCSQL01-A
  member                                vFC-SCSQL02-A
  member vFC-SCVMM01-A
  member vFC-SCVMM02-A
exit
```

3. Activate the Zoneset

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

Nexus 5548 B

1. Create the Zones and Add Members

```
zone name vFC-SCSQL01-B vsan <Fabric B VSAN ID>
```



```

member          device-alias          vFC-SCSQL01-B-SetA
member          device-alias          vFC-SCSQL01-B-SetB
member device-alias Infra_vs1_lif01b
member device-alias Infra_vs1_lif02b
exit
zone name vFC-SCSQL02-B vsan <Fabric B VSAN ID>
member          device-alias          vFC-SCSQL02-B-SetA
member device-alias vFC-SCSQL02-B-SetB
member device-alias Infra_vs1_lif01b
member device-alias Infra_vs1_lif02b
exit
zone name vFC-SCVMM01-B vsan <Fabric B VSAN ID>
member          device-alias          vFC-SCVMM01-B-SetA
member          device-alias          vFC-SCVMM01-B-SetB
member device-alias Infra_vs1_lif01b
member device-alias Infra_vs1_lif02b
exit
zone name vFC-SCVMM02-B vsan <Fabric B VSAN ID>
member          device-alias          vFC-SCVMM02-B-SetA
member device-alias vFC-SCVMM02-B-SetB
member device-alias Infra_vs1_lif01b
member device-alias Infra_vs1_lif02b
exit

```

2. Create the Zoneset and Add the Necessary Members

```

zoneset name Flexpod vsan <Fabric B VSAN ID>
member vFC-SCSQL01-B
member                                     vFC-SCSQL02-B
member vFC-SCVMM01-B
member vFC-SCVMM02-B
exit

```

3. Activate the Zoneset

```

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

```

11.6 Install Windows Server in the Virtual Machines

Windows Server can now be installed into the virtual machines. Windows can be installed using a .ISO file with the installation image . Windows does not need to be installed in each virtual machine if a syspreped 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 address are used instead of DHCP. Each Windows server must be joined to the active directory domain after network connectivity is established.

12 Create Required System Center User Accounts and Security Groups

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

Component	User account	Suggested name	Description
System Center	Component installation account	FT-SCInstall	This optional account is used to install all System Center 2012 components.
SQL Server	SQL Server instance service account	FT-SQL-Service	This account is used as the service account for all instances of SQL Server used in System Center.
Operations Manager	Management server action account	FT-SCOM-Action	This account is used to carry out actions on monitored computers across a network connection.
Operations Manager	System Center Operations Manager configuration service and data access service account	FT-SCOM-SVC	This account is one set of credentials that is used to update and read information in the operational database. Operations Manager verifies that the credentials used for the System Center Operations Manager configuration service and data access service account are assigned to the sdk_user role in the operational database.
Operations Manager	Data Warehouse write account	FT-SCOM-DW	The Data Warehouse write account writes data from the management server to the reporting Data Warehouse and reads data from the operational database.
Operations Manager	Data reader account	FT-SCOM-DR	The data reader account is used to define which account credentials Microsoft SQL Server® 2008 Reporting Services uses to run queries against the Operations Manager reporting Data Warehouse.
Virtual Machine Manager	Virtual Machine Manager service account	FT-VMM-SVC	This account is used to run the Virtual Machine Manager service.
Service Manager	Service Manager services account	FT-SCSM-SVC	This account becomes the operational system account. It is assigned to the logon account for all Service Manager services on all Service Manager servers. This account becomes a member of the sdk_users and configsvc_users database roles for the Service Manager database as part of installation. This account also becomes the Data Warehouse system Run As account. If you change the credentials for these two services, make sure that the new account has a SQL Server login in the Service Manager database and that this account is a member of the Builtin\Administrators group.
Service Manager	Service Manager workflow account	FT-SCSM-WF	This account is used for all workflows and is made a member of the Service Manager workflows user

Component	User account	Suggested name	Description
Service Manager	Service Manager reporting account	FT-SCSM-SSRS	role. This account is used by SQL Server Reporting Services (SSRS) to access the DWDataMart database to get data for reporting. The account becomes a member of the db_datareader database role for the DWDataMart database. Becomes a member of the reportuser database role for the DWDataMart database.
Service Manager	Microsoft SQL Server® 2008 Analysis Services account for OLAP cubes	FT-SCSM-OLAP	This account is used by SQL Server Analysis Services (SSAS) for Service Manager reports.
Service Manager	Operations Manager alert connector	FT-SCSM-OMAlert	This account is used for Service Manager Operations Manager Alert connector operations.
Service Manager	Operations Manager CI connector	FT-SCSM-OMCI	This account is used for Service Manager Operations Manager continuous integration (CI) connector operations.
Service Manager	Active Directory connector	FT-SCSM-ADCI	This account is used for Service Manager Active Domain connector operations.
Service Manager	Virtual Machine Manager CI connector	FT-SCSM-VMMCI	This account is used for Service Manager Virtual Machine manager connector operations.
Service Manager	Orchestrator CI Connector	FT-SCSM-OCI	This account is used for System Center Orchestrator connector operations.
Orchestrator	Orchestrator services account	FT-SCO-SVC	This account is used to run the Orchestrator Management Service, Orchestrator Runbook Service and Orchestrator Runbook Server monitor service.
App Controller	App Controller services account	FT-SCAC-SVC	This account is used to run all App Controller services.

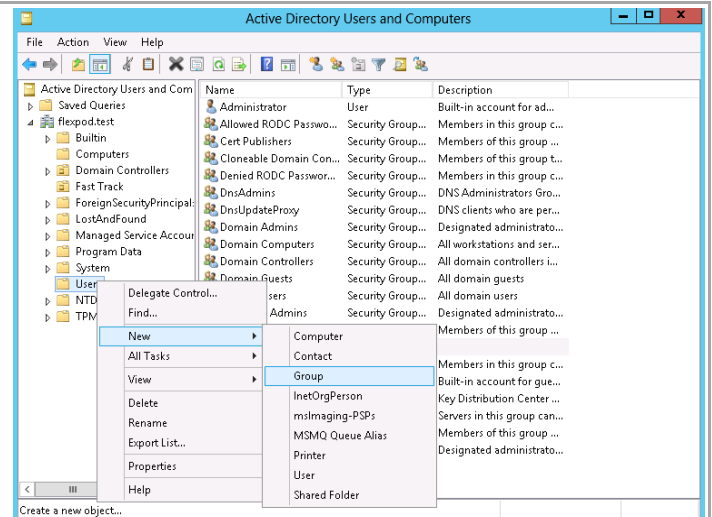
The following Active Directory security groups are required for the Fast Track System Center 2012 SP1 installation:

Component	Group	Name	Group notes
System Center 2012	System Center Administrators	FT-SC-Admins	This group's members are full Admins on all System Center components.
SQL Server	SQL Server Administrators	FT-SQL-Admins	This group's members are sysadmins on all SQL Server instances and local administrators on all SQL Server nodes.
Operations Manager	Operations Manager Administrators	FT-SCOM-Admins	This group's members are administrators for the Operations Manager installation and hold the Administrators role in Operations Manager.
Virtual Machine Manager	Virtual Machine Manager Administrators	FT-SCVMM-Admins	This group's members are administrators for the Virtual Machine Manager installation and hold the Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Delegated Administrators	FT-SCVMM-FabricAdmins	This group's members are delegated administrators for the Virtual Machine Manager installation and hold the Fabric Administrators role in Virtual Machine Manager.

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

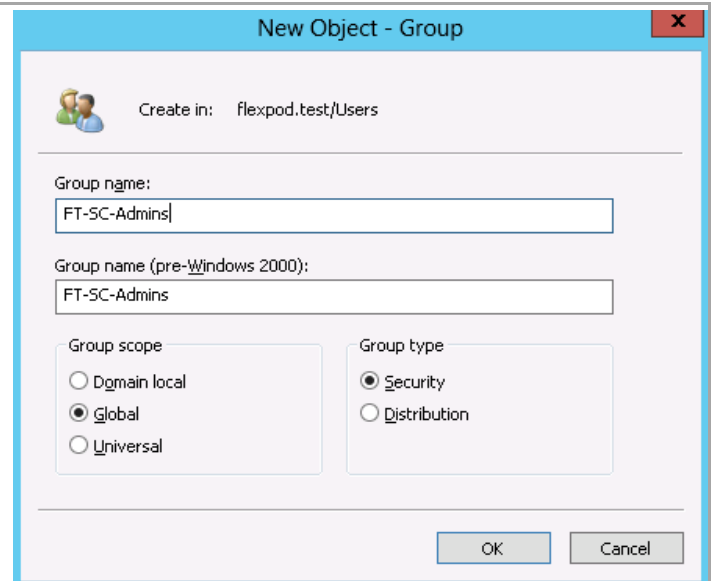
Repeat the following procedure for all user accounts listed in the table above.

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.



New Object - Group

Create in: flexpod.test/Users

Group name:
FT-SC-Admins

Group name (pre-Windows 2000):
FT-SC-Admins

Group scope

☐ Domain local

☒ Global

☐ Universal

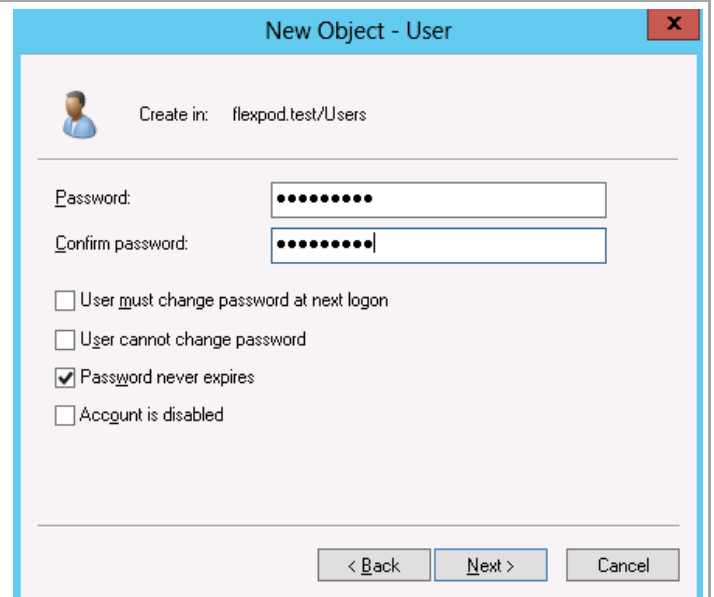
Group type

☒ Security

☐ Distribution

OK Cancel

Enter the password and password confirmation. Click **next**.



New Object - User

Create in: flexpod.test/Users

Password:

Confirm password:

☐ User must change password at next logon

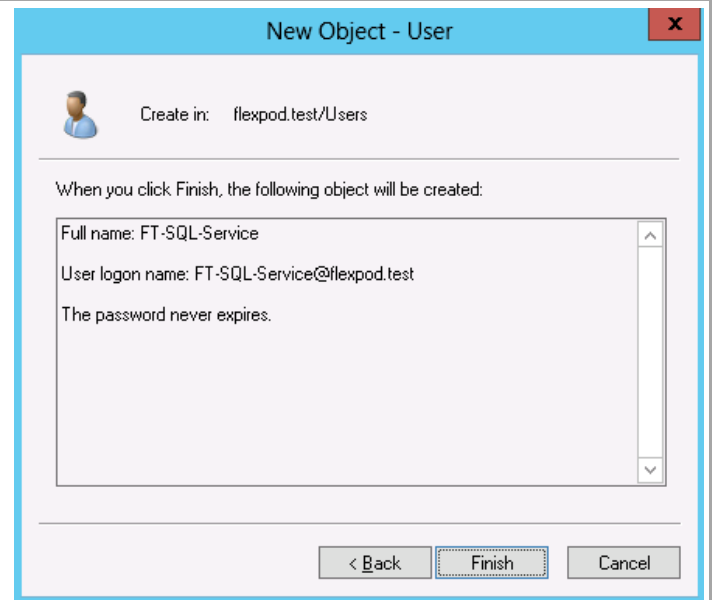
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

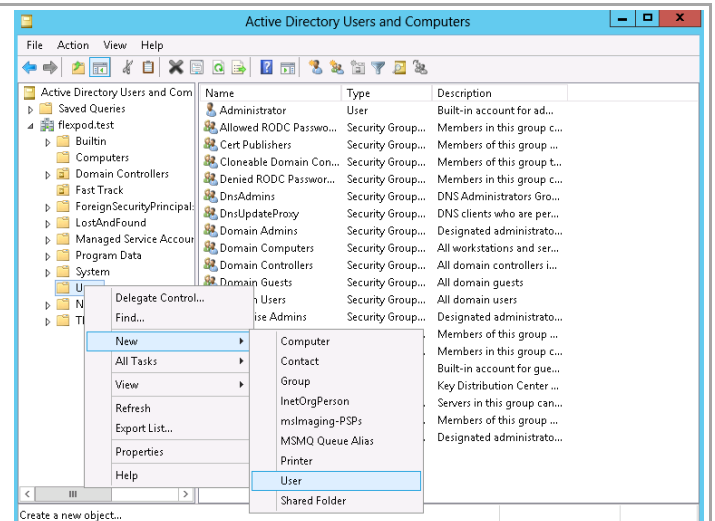
< Back Next > Cancel

Click Finish to create the user account.



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.


The screenshot shows the 'New Object - User' dialog box with the title bar in blue. The main area is light gray. At the top, there is a user icon and the text 'Create in: flexpod.test/Users'. Below this, there are several input fields: 'First name:' (empty), 'Initials:' (empty), 'Last name:' (empty), 'Full name:' (containing 'FT-SQL-Service'), 'User logon name:' (containing 'FT-SQL-Service' and a dropdown menu showing '@flexpod.test'), and 'User logon name (pre-Windows 2000):' (containing 'FLEXPOD\FT-SQL-Service'). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter the password and password policy. Click next.

The screenshot shows the 'New Object - User' dialog box, Step 2. It has the same title bar and 'Create in: flexpod.test/Users' text. Below, there are two password input fields: 'Password:' (filled with dots) and 'Confirm password:' (filled with dots). Below the password fields, there are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom, there are three buttons: '< Back', 'Next >', and '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.

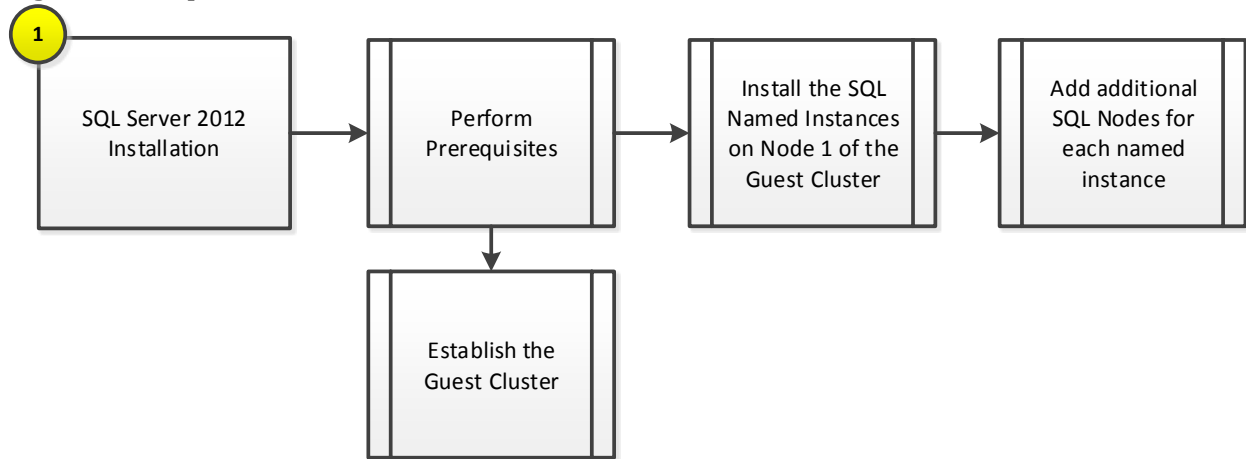
< Back

Finish

Cancel

13 SQL Server 2012 Failover Cluster Installation

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



13.1 Overview

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

This section provides high-level walkthrough on how to install SQL Server 2012 SP1 into the Fast Track fabric management.¹ The following assumptions are made prior to installation:

1. Two to four base virtual machines running Windows Server 2012 have been provisioned for SQL Server.
2. 15 iSCSI LUNs have been assigned to the virtual machine guests.
 - 2.1. One LUN – quorum (1 GB)
 - 2.2. Two LUNs for each fabric management component database (14 LUNs for all components)

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

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

Windows Authentication. The table below outlines the options required for each instance.

Database Instances and Requirements

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

13.2 Pre-Requisites

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

Accounts

Verify that the following accounts have been created:

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

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

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

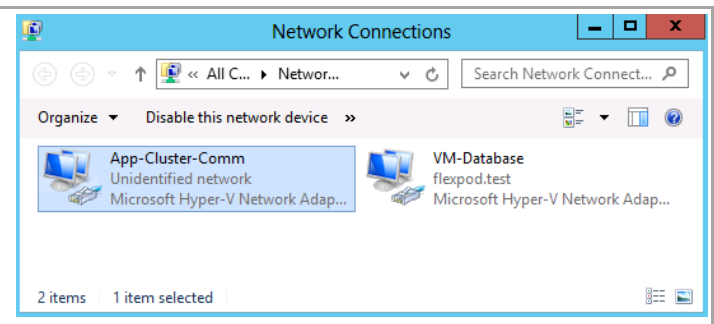
Groups

Verify that the following security groups have been created:

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

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 settings need to be manually configured.

Internet Protocol Version 4 (TCP/IPv4) Properties ? x

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 . 46

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

Internet Protocol Version 4 (TCP/IPv4) Properties ? x

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 . 6 . 46

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

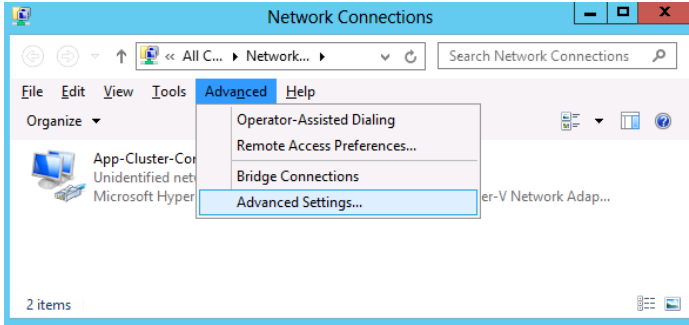
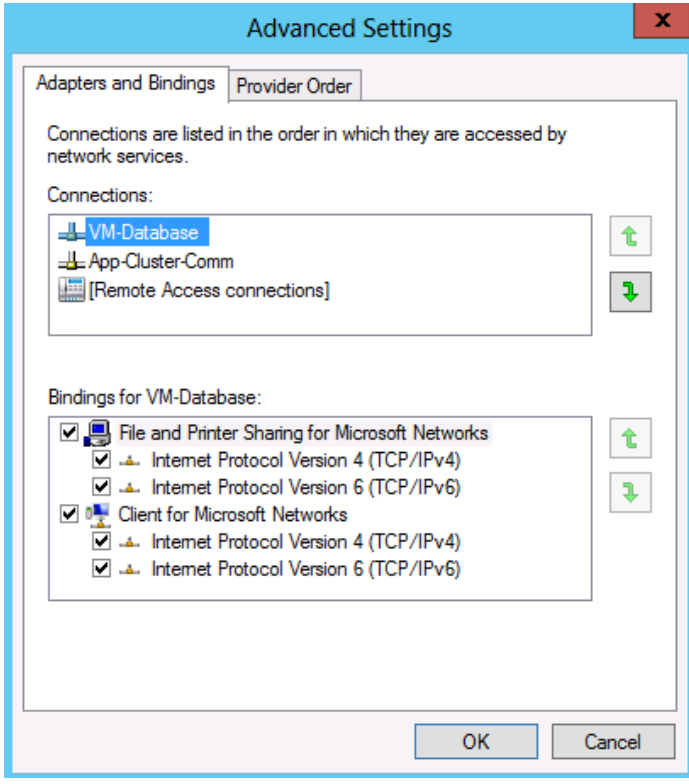
Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

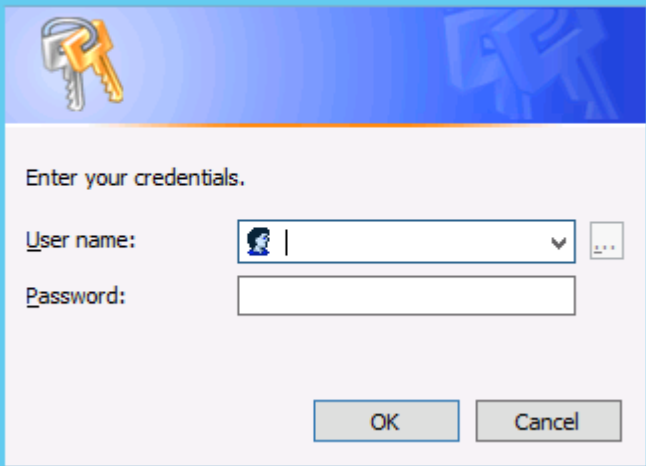
Advanced...

OK Cancel

<p>In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings</p>	
<p>Select the adapter and use the arrows to move it up or down in binding order.</p> <p>The recommended binding order is:</p> <ul style="list-style-type: none">• VM-Database• App-Cluster-Comm	
<p>Open a PowerShell window and rename the computer.</p>	<pre>Rename-Computer -NewName SCSQL01 -Restart</pre>
<p>After the computer reboots, login again, open a Powershell window and join the active directory domain.</p>	<pre>Add-Computer -DomainName flepod.test -Restart</pre>

Enter the account and password with privileges to add a computer to the doman.

Windows PowerShell Credential Re...



Enter your credentials.

User name:

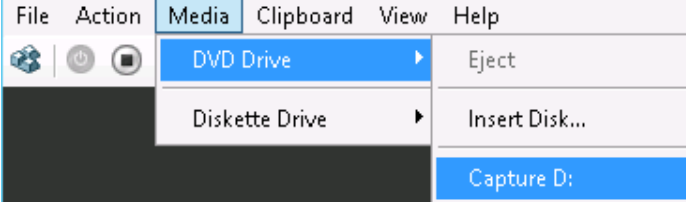
Password:

OK Cancel

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.



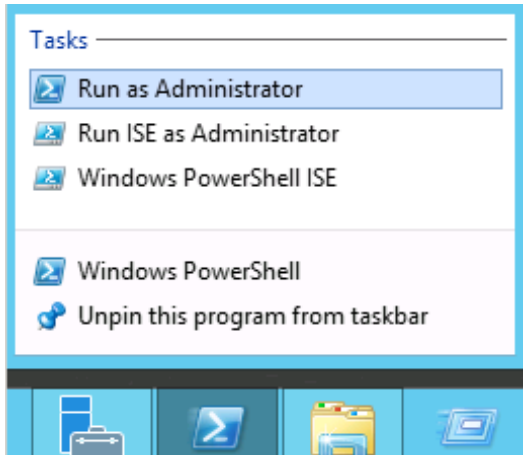
File Action Media Clipboard View Help

DVD Drive Eject

Diskette Drive Insert Disk...

Capture D:

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



Tasks

Run as Administrator

Run ISE as Administrator

Windows PowerShell ISE

Windows PowerShell

Unpin this program from taskbar

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.

```
PS C:\Users\administrator.FLEXP00> Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
Success Restart Needed Exit Code Feature Result
-----
True No Success { .NET Framework 3.5 (includes .NET 2.0 and...
```

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

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

```
PS C:\Users\administrator.FLEXPOD> Add-WindowsFeature failover-clustering, Multipath-IO -IncludeManagementTools  
Success Restart Needed Exit Code Feature Result  
-----  
True No Success {Failover Clustering, Remote Server Admini...  
PS C:\Users\administrator.FLEXPOD>
```

Configure Windows MPIO

The following section describes how to configure Windows MPIO to claim NetApp Luns.

6. Configure Windows Server 2012 MSDSM to claim any NetApp LUNs.

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId LUN  
New-MSDSMSupportedHW -VendorId NETAPP -ProductId "LUN C-Mode"  
Update-MPIOClaimedHW  
Restart-Computer
```

Establish the SQL Server Guest Cluster

This section assumes storage with FCoE interface is available and the customer is implementing a SQL Server guest cluster, the following steps can be followed to create the SQL Server guest cluster. Note that the SQL Server guest cluster can also use fibre channel storage for clustering the virtual fibre channel adapter in Windows Server 2012 Hyper-V. While SMB shares can be used for SQL Server failover clusters, SQL Server Analysis Services is a requirement for the Fast Track design and is not compatible with SMB shares.

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

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

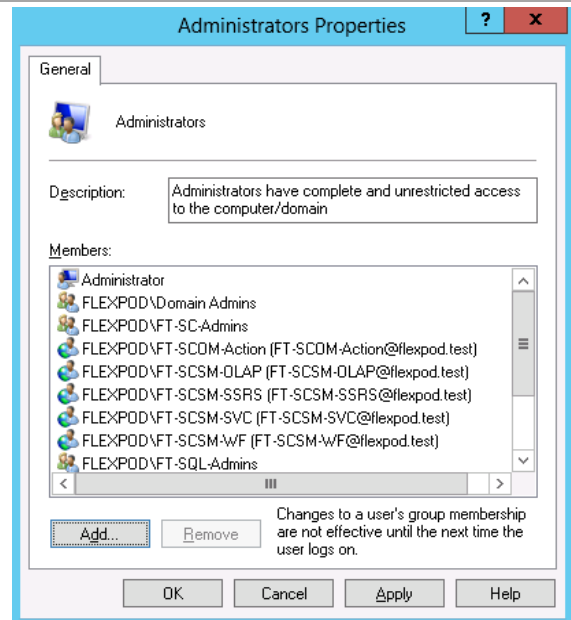
During the provisioning process, two virtual machines were built to the specifications outlined in the Fast Track Reference Architecture Guide to support SQL Server operations for fabric management. Once created, the FCoE targets must be configured within each virtual machine to make them accessible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

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

Log on to the first node in the SQL Server cluster as a user with local admin rights.

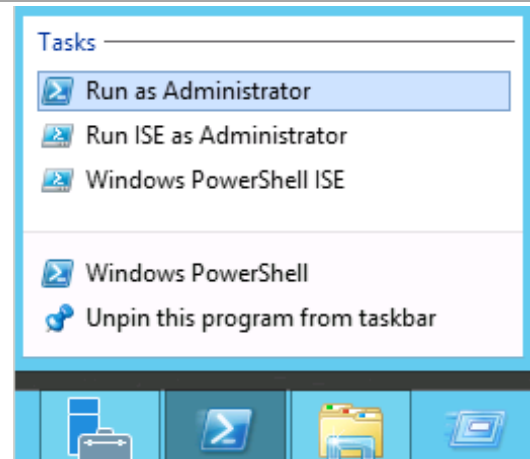
Verify that the following accounts and/or groups are members of the Local Administrators group on the first and second SQL Server nodes:

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 in the two 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>, -NoStorage -StaticAddress <cluster_ip_address>
```

```
PS C:\Users\administrator.FLEXPOD> new-cluster -Name SCSQL-Cluster01 -Node SCSQL01, SCSQL02 -NoStorage -StaticAddress 192.168.1.50
Report File Location: c:\Windows\cluster\Reports\Create Cluster Wizard SCSQL-Cluster01 on 2013.04.23 At 16:34:57.mht
Name
----
SCSQL-Cluster01
PS C:\Users\administrator.FLEXPOD>
```

Rename the cluster networks to match there function.

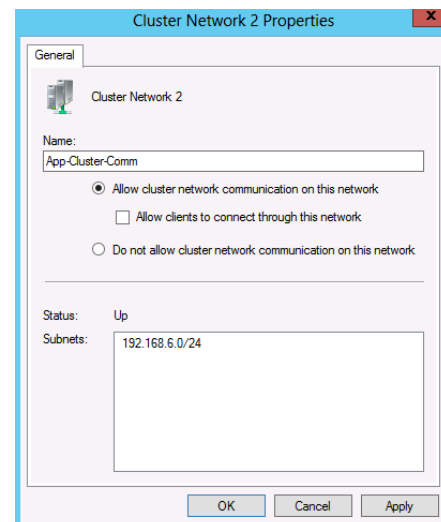
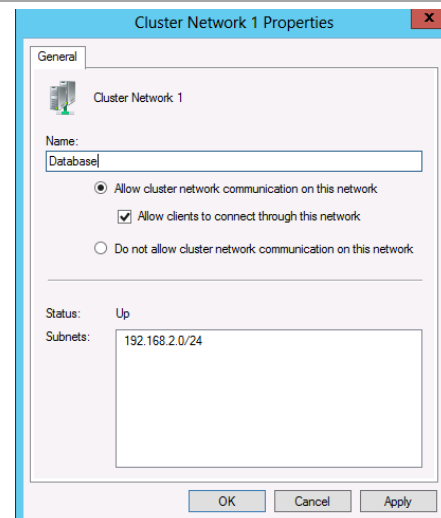
```
Get-ClusterNetworkInterface | ? Name -like *Public* | Group Network| %{ (Get-ClusterNetwork $_.Name).Name = 'Database'}
```

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

Using Failover Cluster Manager, expand the Networks object in the left tree view. Right click each network and select properties.

Check Allow clients to comment through this network for the Database network.

Uncheck Allow clients to comment through this network for the App-Cluster-Comm network.



Create and Map LUNs for SQL Server

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

SQL Server Database and Quorum LUNs

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

Note that 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 LUNs.

1. Start a Windows PowerShell session on the SQL Server node and import the Data ONTAP PowerShell Toolkit module.

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

3. Create a new Qtree to hold the LUNs.

```
New-NcQtree -Volume sc_sql_db -Qtree SCSMDB
New-NcQtree -Volume sc_sql_db -Qtree SCSMDW
New-NcQtree -Volume sc_sql_db -Qtree SCSMAS
New-NcQtree -Volume sc_sql_db -Qtree SCDB
New-NcQtree -Volume sc_sql_db -Qtree SCVMMDB
New-NcQtree -Volume sc_sql_db -Qtree SCOMDB
New-NcQtree -Volume sc_sql_db -Qtree SCOMDW
New-NcQtree -Volume quorum -Qtree scslq-cluster01
New-NcQtree -Volume scvmm_lib -Qtree scvmm_lib01
```

4. Create the SQL Server database LUNs.

```
New-NcLun /vol/sc_sql_db/SCSMDB/SCSMDB_DB.lun -Size 145gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCSMDB/SCSMDB_Logs.lun -Size 70gb -OsType windows_2008 -
Unreserved
```

```
New-NcLun /vol/sc_sql_db/SCSMDW/SCSMDW_DB.lun -Size 1TB -OsType windows_2008 -Unreserved
New-NcLun /vol/sc_sql_db/SCSMDW/SCSMDW_Logs.lun -Size 500gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCSMAS/SCSMAS_DB.lun -Size 8GB -OsType windows_2008 -Unreserved
New-NcLun /vol/sc_sql_db/SCSMAS/SCSMAS_Logs.lun -Size 4gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCMDB/SCMDB_DB.lun -Size 10GB -OsType windows_2008 -Unreserved
New-NcLun /vol/sc_sql_db/SCMDB/SCMDB_Logs.lun -Size 5gb -OsType windows_2008 -Unreserved
New-NcLun /vol/sc_sql_db/SCVMMDB/SCVMMDB_DB.lun -Size 6GB -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCVMMDB/SCVMMDB_Logs.lun -Size 3gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCOMDB/SCOMDB_DB.lun -Size 130GB -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCOMDB/SCOMDB_Logs.lun -Size 65gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/sc_sql_db/SCOMDW/SCOMDW_DB.lun -Size 1TB -OsType windows_2008 -Unreserved
New-NcLun /vol/sc_sql_db/SCOMDW/SCOMDW_Logs.lun -Size 500gb -OsType windows_2008 -
Unreserved
New-NcLun /vol/quorum/scslq_cluster01/scslq-cluster01-quorum.lun -Size 1gb -OsType
windows_2008 -Unreserved
New-NcLun /vol/scvmm_lib/scvmm_lib01/scvmm_lib01.lun -Size 100gb -OsType windows_2008 -
Unreserved
```

5. Create the NetApp igroup for the SQL Server Cluster LUNs.

```
New-NcIgroup -Name scsql-cluster01 -Protocol fcp -Type windows
```

8. Add the WWPN of the Hyper-V virtual fibre channel HBAs to the SQL Server cluster igroup.

```
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL01-A-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL01-A-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL01-B-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL01-B-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL02-A-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL02-A-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL02-B-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scslq-cluster01 -Initiator < vFC-SCSQL02-B-SetB_WWPN>
```

6. Map the SQL Server database LUNs to the new iGroup, initialize the new LUNs, assign a drive letter and format the volume.

```
Add-NcLunMap -Path /vol/sc_sql_db/SCSMDB/SCSMDB_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCSMDB_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCSMDB/SCSMDB_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCSMDB_Logs"

Add-NcLunMap -Path /vol/sc_sql_db/SCSMDW/SCSMDW_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCSMDW_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCSMDW/SCSMDW_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCSMDW_Logs"

Add-NcLunMap -Path /vol/sc_sql_db/SCSMAS/SCSMAS_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
```

```

"SCSMAS_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCSMAS/SCSMAS_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCSMAS_Logs"

Add-NcLunMap -Path /vol/sc_sql_db/SCDB/SCDB_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCDB_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCDB/SCDB_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCDB_Logs"

Add-NcLunMap -Path /vol/sc_sql_db/SCVMMDB/SCVMMDB_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCVMMDB_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCVMMDB/SCVMMDB_Logs.lun -InitiatorGroup scsql-
cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCVMMDB_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCOMDB/SCOMDB_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCOMDB_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCOMDB/SCOMDB_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCOMDB_Logs"

Add-NcLunMap -Path /vol/sc_sql_db/SCOMDW/SCOMDW_DB.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCOMDW_DB"

Add-NcLunMap -Path /vol/sc_sql_db/SCOMDW/SCOMDW_Logs.lun -InitiatorGroup scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel
"SCOMDW_Logs"

Add-NcLunMap -Path /vol/quorum/scsql_cluster01/scsql-cluster01-quorum.lun -InitiatorGroup
scsql-cluster01

get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-
Partition -UseMaximumSize | Format-Volume -NewFileSystemLabel "Cluster_Quroum"

Add-NcLunMap -Path /vol/scvmm_lib/scvmm_lib01/scvmm_lib01.lun -InitiatorGroup scsql-
cluster01

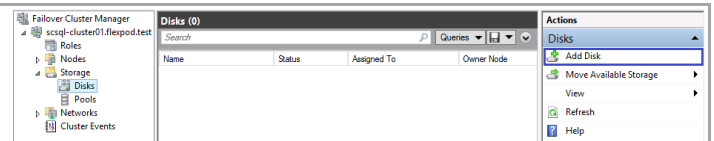
get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-

```

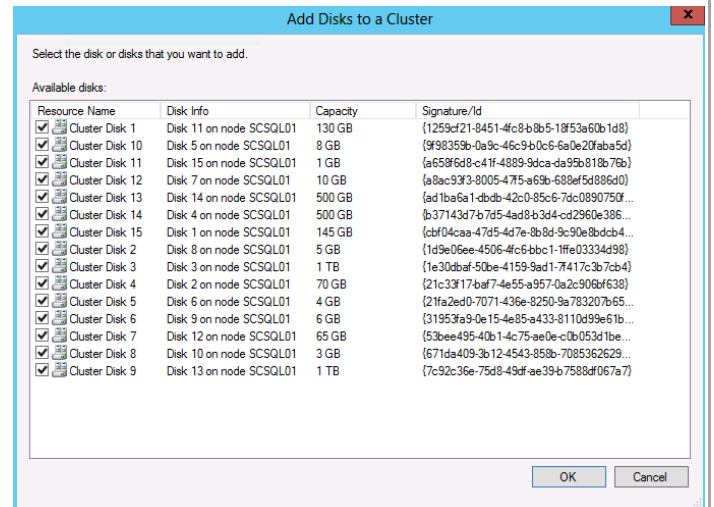
Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -NewFileSystemLabel "SCVMMLib01"

Assign SQL Cluster Disk Names

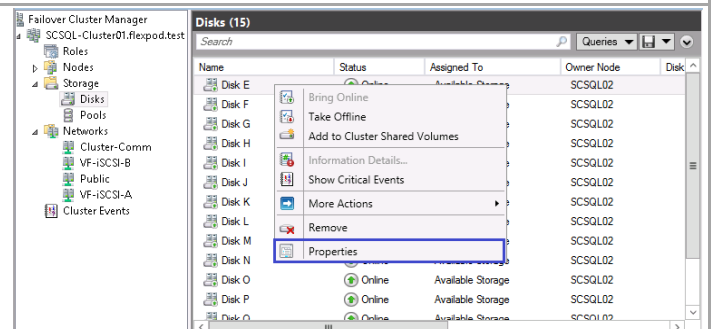
Select the **SQL Server cluster** in the left tree view. Expand the **Storage** object and select **Disks**. Right click each disk in the middle pane. Click **Add Disk** in the Action pane.



Verify that all 15 disks are checked and click **OK**.

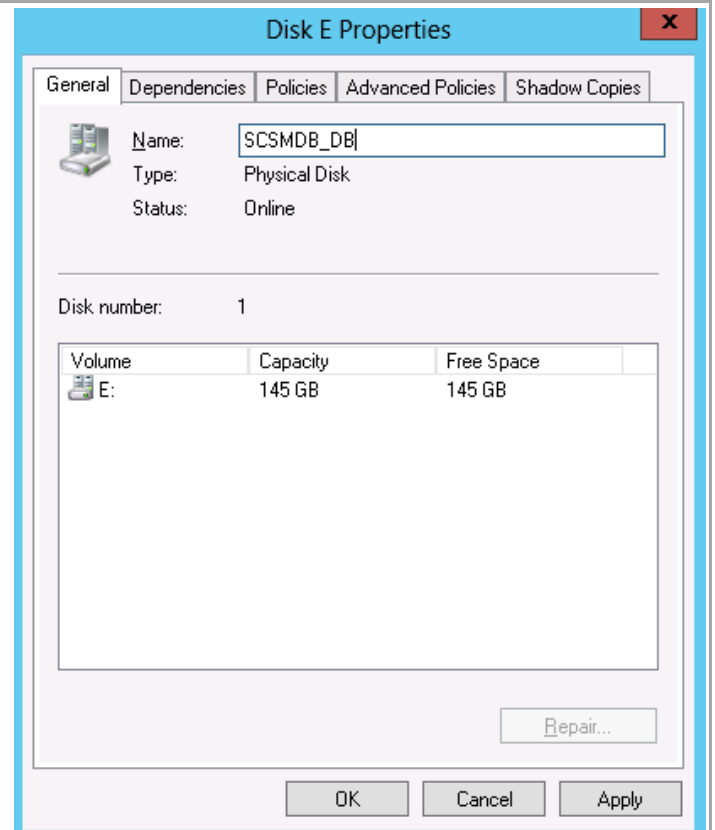


Select the SQL Server cluster in the left tree view. Expand the Storage object and select Disks. Right click each disk in the middle pane and select properties.



In the Name field, enter a name that reflects the LUN names used in section 13.3.

Repeat this procedure for all cluster disks.

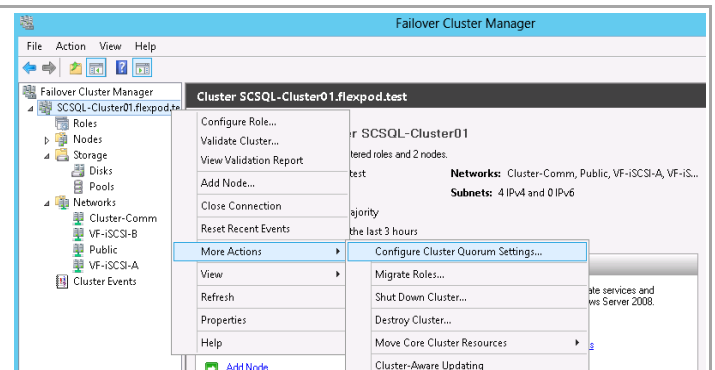


Change the SQL Server Cluster to Use a Quorum Disk

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**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Select Quorum Configuration Option'. On the left, a navigation pane lists steps: 'Before You Begin', 'Select Quorum Configuration Option' (highlighted), 'Select Quorum Witness', 'Confirmation', 'Configure Cluster Quorum Settings', and 'Summary'. The main area contains the text: 'Select a quorum configuration for your cluster.' followed by three radio button options: 'Use typical settings (recommended)' (with subtext 'The cluster determines quorum management options and, if necessary, selects the quorum witness.'), 'Add or change the quorum witness' (selected, with subtext 'You can select the quorum witness. The cluster determines quorum management options.'), and 'Advanced quorum configuration and witness selection' (with subtext 'You determine the quorum management options and the quorum witness.'). A link 'Failover Cluster Quorum and Witness Configuration Options' is at the bottom. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Select **Configure a disk witness** and click **Next**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Select Quorum Witness'. The left navigation pane is the same as the previous screen, with 'Select Quorum Witness' highlighted. The main area displays cluster information: 'Nodes that are configured to be members of the cluster: 2', 'Nodes that are assigned votes to participate in quorum calculations: 2', and 'Cluster dynamically manages vote assignment: Enabled'. Below this, it says 'Select to add or change the quorum witness for your cluster configuration. The recommendations are based on providing the highest availability for your cluster.' There are three radio button options: 'Configure a disk witness (recommended for your current configuration)' (selected, with subtext 'Adds a quorum vote of the disk witness'), 'Configure a file share witness (recommended for special configurations)' (with subtext 'Adds a quorum vote of the file share witness'), and 'Do not configure a quorum witness (not recommended for your current configuration)'. The same link and navigation buttons are present at the bottom.

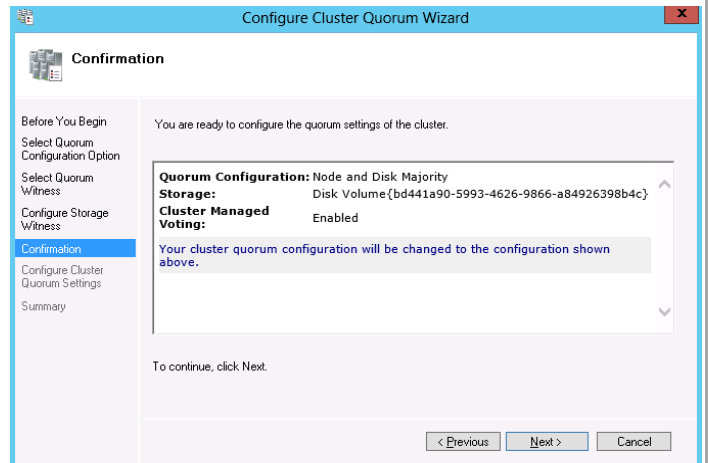
Select the **LUN** without a drive letter that was previously created to be the quorum LUN. Click **Next**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Configure Storage Witness'. The left navigation pane is the same, with 'Configure Storage Witness' highlighted. The main area says 'Select the storage volume that you want to assign as the disk witness.' Below this is a table with two columns: 'Name' and 'Status'.

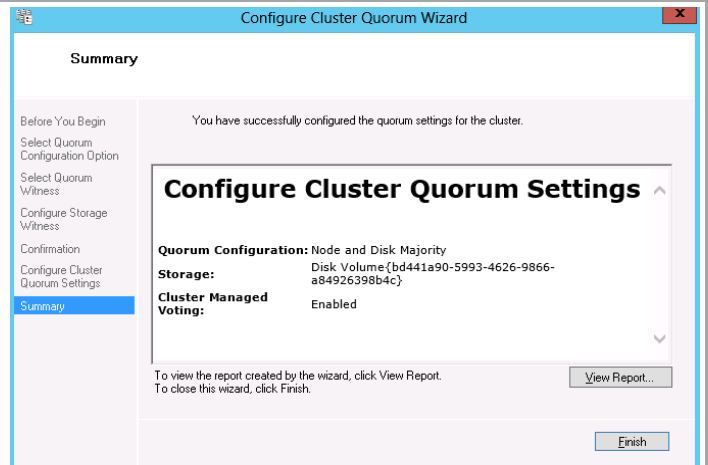
Name	Status
<input type="checkbox"/> Disk N	Online
<input type="checkbox"/> Disk O	Online
<input type="checkbox"/> Disk P	Online
<input type="checkbox"/> Disk Q	Online
<input type="checkbox"/> Disk R	Online
<input checked="" type="checkbox"/> Disk Volume{bd441a90-5993-4626-9866-a84926398b4c}	Online
Volume: (\\?\Volume{bd441a90-5993-4626-9866-a84926398b4c}...) File System: NTFS	

Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Confirm the settings and click **Next**.

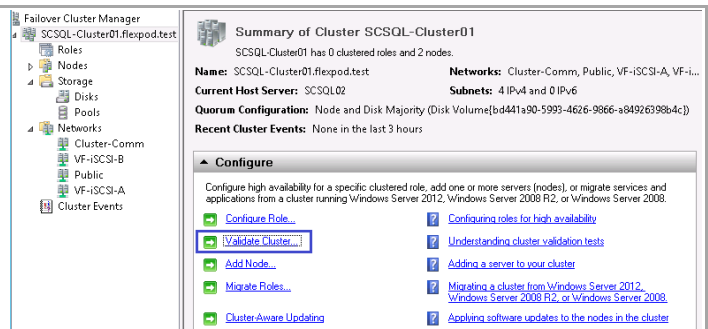


Review the results and click **Finish** to close the wizard screen.



Validated 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.

The screenshot shows the 'Testing Options' step of the 'Validate a Configuration Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Testing Options' (selected), 'Review Storage Status', 'Confirmation', 'Validating', and 'Summary'. The main area has a heading 'Testing Options' with a green checkmark icon. Below it, text explains that the tests examine Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration. It also states that Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests. Two radio buttons are present: 'Run all tests (recommended)' (selected) and 'Run only tests I select'. A link 'More about cluster validation tests' is at the bottom. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Select all the disks on the cluster and Click Next.

The screenshot shows the 'Review Storage Status' step of the 'Validate a Configuration Wizard'. The left sidebar shows 'Review Storage Status' selected. The main area has a heading 'Review Storage Status' with a green checkmark icon. Text indicates that additional storage can be selected for validation. A table lists storage components and their assigned roles:

Name	Assigned To
Quorum	Disk Witness in Quorum
SCCMDW_DB	Available Storage
SCCMDW_Logs	Available Storage
SCDB_DB	Available Storage
SCDB_Logs	Available Storage
SCDM_DB	Available Storage
SCDM_Logs	Available Storage
SCCMDW_DB	Available Storage
SCCMDW_Logs	Available Storage
SCSMAS_DB	Available Storage
SCSMAS_Logs	Available Storage
SCSMAS_DB	Available Storage

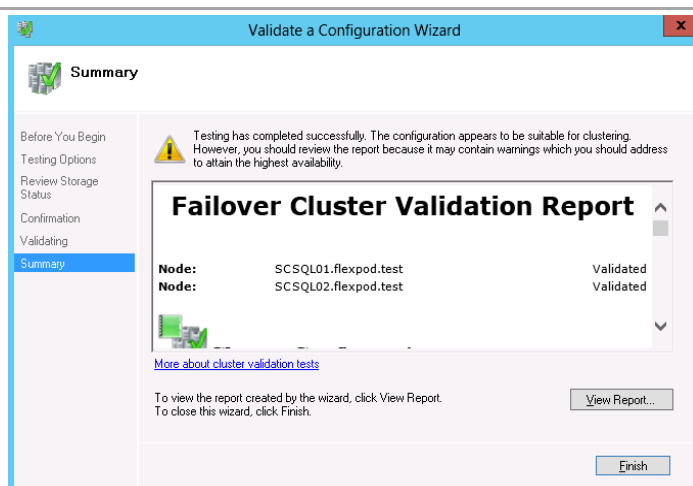
A warning icon and text state: 'To avoid role failures, it is recommended that all roles using this Cluster Shared Volume be stopped before the storage is validated.' Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Confirm the selected options and click **Next**.

The screenshot shows the 'Confirmation' step of the 'Validate a Configuration Wizard'. The left sidebar shows 'Confirmation' selected. The main area has a heading 'Confirmation' with a green checkmark icon. Text states: 'You are ready to start validation. Please confirm that the following settings are correct:'. Two lists are shown: 'Servers to Test' (SCSQL01.flexpod.test, SCSQL02.flexpod.test) and 'Tests Selected by the User' (List Cluster Core Groups, List Cluster Network Information, List Cluster Resources, List Cluster Volumes, List Clustered Roles). The 'Category' for all tests is 'Cluster Configuration'. A link 'More about cluster validation tests' is at the bottom. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

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

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



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

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

Note: n and y are variable numbers

13.3 Install SQL Server 2012 SP1

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

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

Component	Service Manager management server	Service Manager Data Warehouse server	Service Manager analysis server	App Controller, Orchestrator, Microsoft SharePoint® services Farm and WSUS	Virtual Machine Manager	Operations Manager	Operations Manager Data Warehouse
SQL Server Instance Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance Failover Cluster Network Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance DATA Cluster Disk Resource	Cluster Disk 2	Cluster Disk 4	Cluster Disk 6	Cluster Disk 8	Cluster Disk 10	Cluster Disk 12	Cluster Disk 14
SQL Server Instance LOG Cluster Disk Resource	Cluster Disk 3	Cluster Disk 5	Cluster Disk 7	Cluster Disk 9	Cluster Disk 11	Cluster Disk 13	Cluster Disk 15
SQL Server Instance Install Drive	E:	G:	I:	K:	M:	O:	Q:
SQL Server Instance	E:	G:	I:	K:	M:	O:	Q:

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
DATA Drive							
SQL Server Instance LOG Drive	F:	H:	J:	L:	N:	P:	R:
SQL Server Instance TEMPDB Drive	F:	H:	J:	L:	N:	P:	R:
Cluster Service Name	SQL Server (SCSMDB)	SQL Server (SCSMDW)	SQL Server (SCSMAS)	SQL Server (SCDB)	SQL Server (SCVMMDB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)
Clustered SQL Server Instance IP Address	10.1.1.22	10.1.1.23	10.1.1.24	10.1.1.25	10.1.1.26	10.1.1.27	10.1.1.28
Host Cluster Public Network Interface Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Host Cluster Public Network Interface Name	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2	Cluster Network 2
SQL Server Instance Listening TCP/IP Port	10437	10438	10439	1433 ⁴	10434	10435	10436
SQL Server Instance Preferred Owners	Node2, Node4	Node2, Node4	Node2, Node4	Node1, Node4	Node1, Node4	Node3, Node4	Node3, Node4

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

The template provided in an appendix of this document should assist with capturing this information for the installation process. Once gathered, the following steps are provided to perform installation. Note that at this point during the installation, the first node of the SQL Server cluster must have ownership of the LUNs.

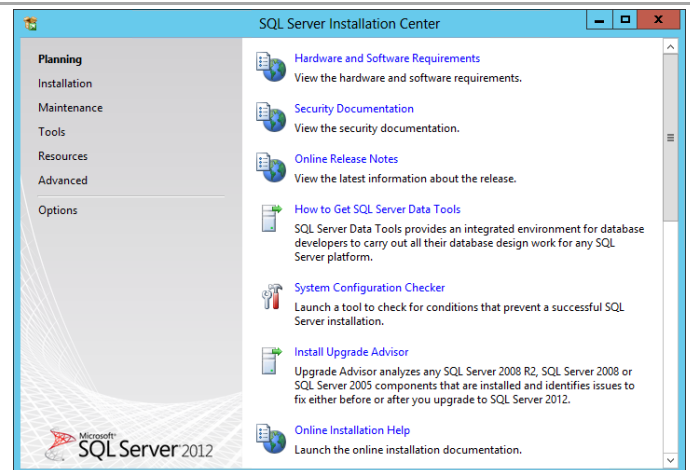
- Perform the following steps on the **first fabric management SQL Server node** virtual machine with an account that has both local Administrator rights and permissions in AD DS to create the SQL Server CNOs.

As outlined before, Fast Track requires separate instances for each System Center product. The instances associated with these products are:

1. SCSMDB (Service Manager database instance).
2. SCSMDW (Service Manager Data Warehouse instance).
3. SCSMAS (Service Manager SQL Analysis Services instance).
4. SCDB (Shared App Controller, Orchestrator, Service Manager self-service portal Microsoft SharePoint® Foundation 2010 services and WSUS database instance).
5. SCVMMDB (Virtual Machine Manager database instance and optional WSUS database instance).
6. SCOMDB (Operations Manager database instance).
7. SCOMDW (Operations Manager Data Warehouse instance).

For multi-instance failover clusters, installation of SQL Server 2012 must be performed once for each instance. As such, these steps must be performed for each instance sequentially.

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



From the **SQL Server Installation Center**, click the **New SQL Server failover cluster installation** link.

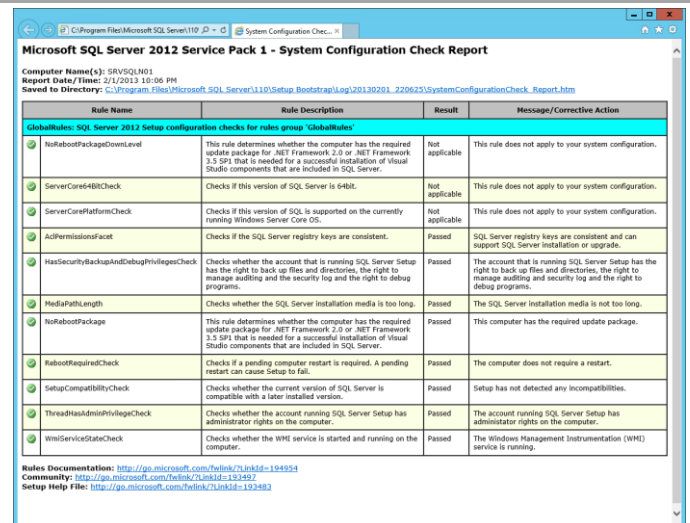
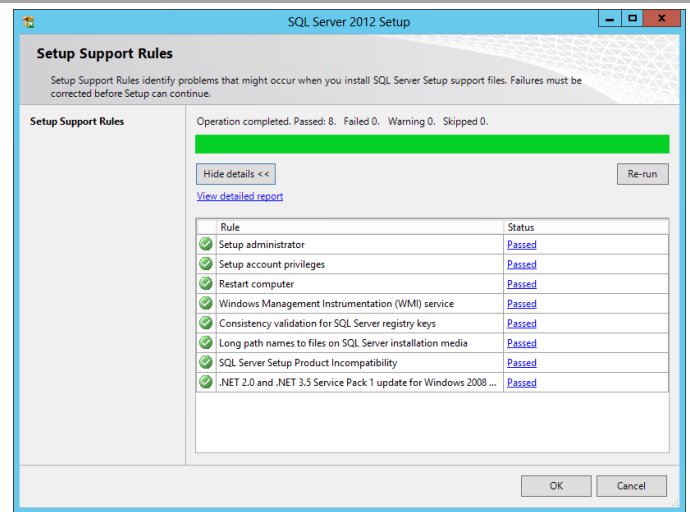
The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

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



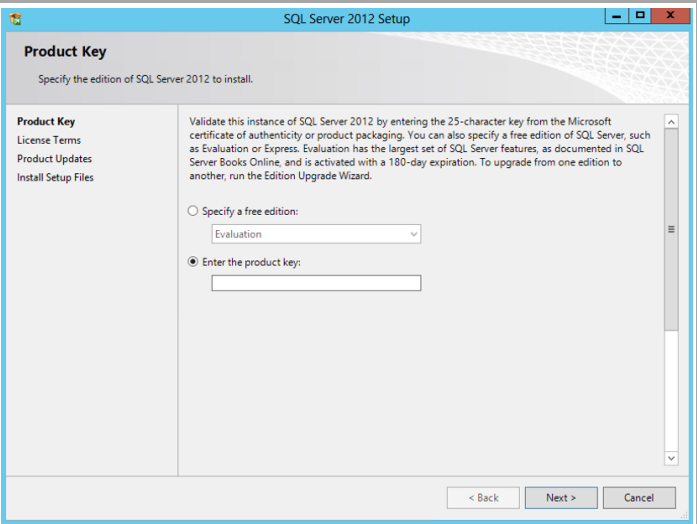
New SQL Server failover cluster installation

Launch a wizard to install a single-node SQL Server 2012 failover cluster.

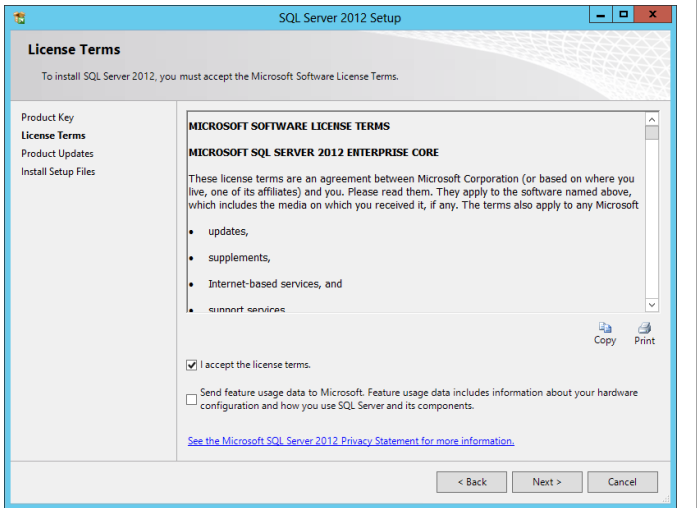


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

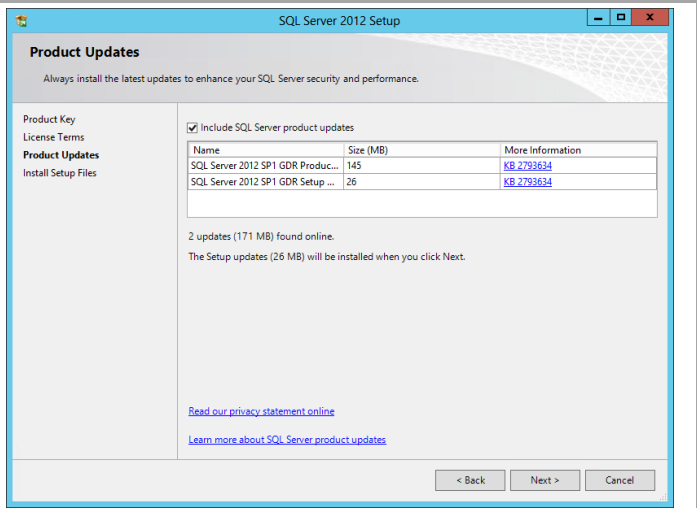
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



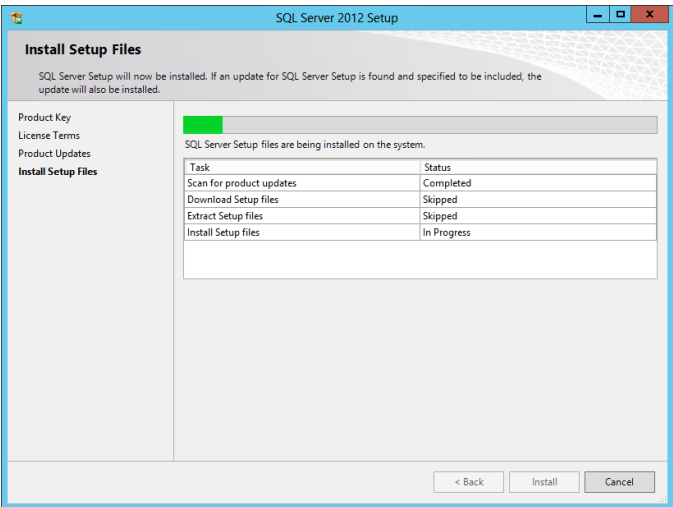
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization’s policies and click **Next** to continue.



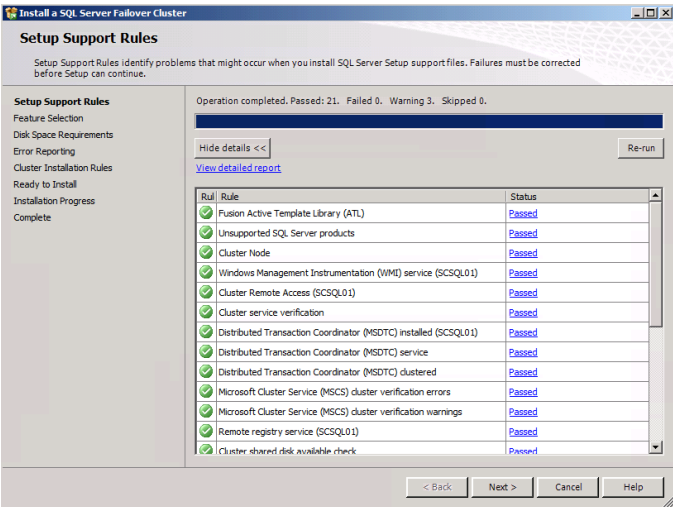
In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.



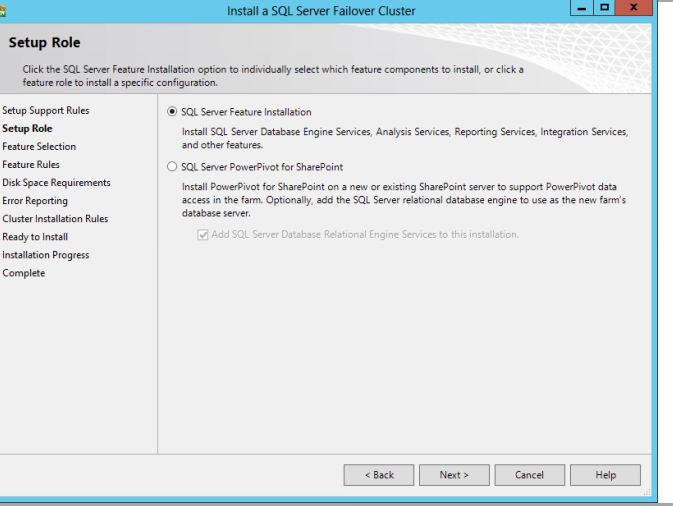
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.



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



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

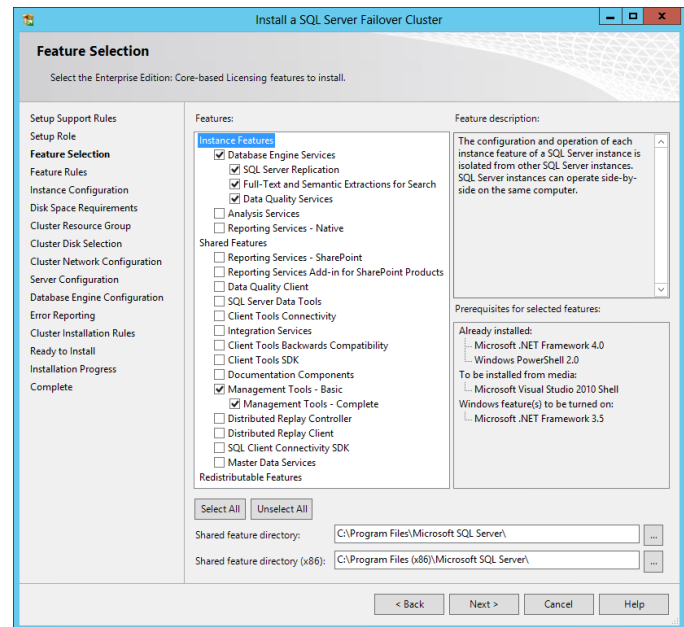


In the **Feature Selection** dialog, features for the various instances will be selected. Note that not all features are supported for failover cluster installations, so the features for Fast Track are limited to the features as listed below. SQL Server with failover clusters requires the selection of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

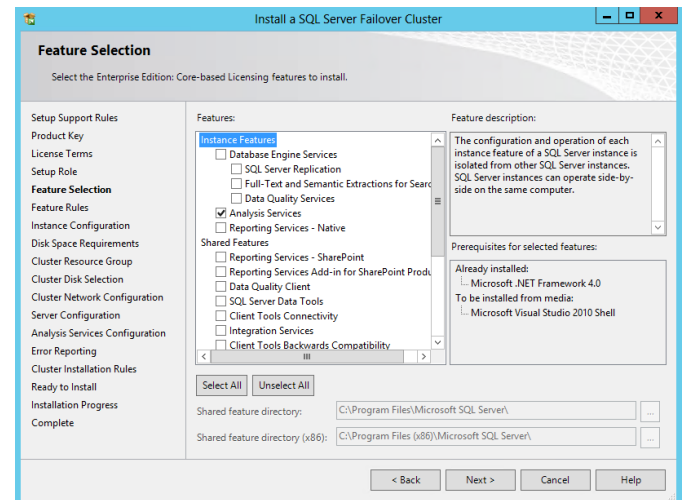
- SCDB
 - Database Engine Services
- SCOMDB
 - Database Engine Services
- SCOMDW
 - Database Engine Services
- SCSMAS
 - Analysis Services
- SCSMDB
 - Database Engine Services
- SCSMDW
 - Database Engine Services
- SCVMMDB
 - Database Engine Services

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

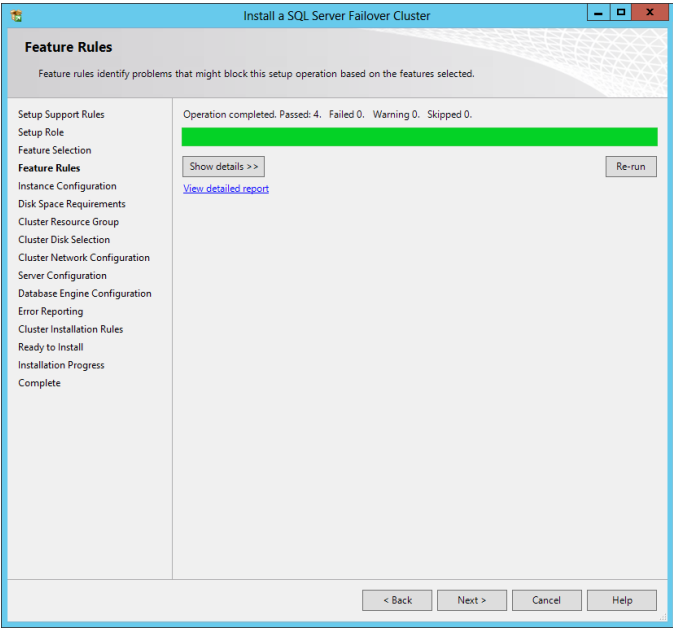
Database Engine Services (all instances except SCSMAS):



Analysis Services (SCSMAS instance only):



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



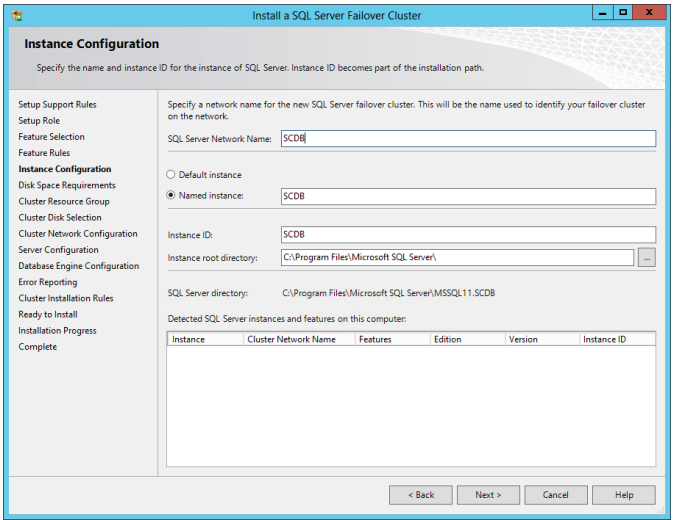
In the **Instance Configuration** dialog, make the following selections (refer to the worksheet created earlier):

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

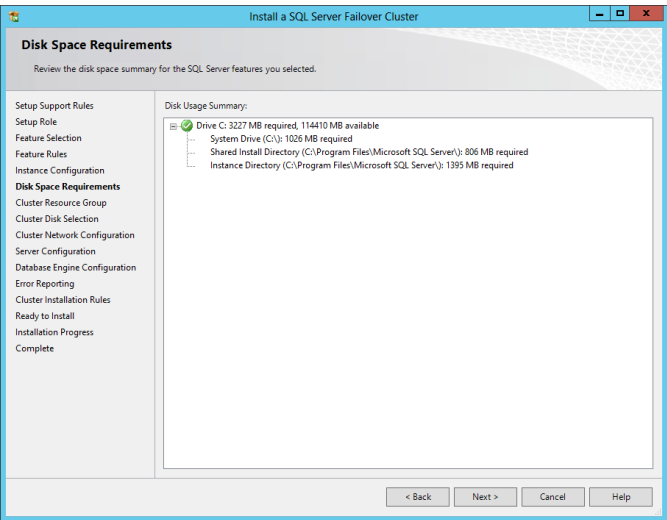
Select the **Named instance** option. In the provided text box, specify the instance name being installed.

- **Instance ID** – *specify the instance name being installed. Verify that it matches the **Named instance** value.*
- **Instance root directory** – *accept the default location of %ProgramFiles%Microsoft SQL Server.*

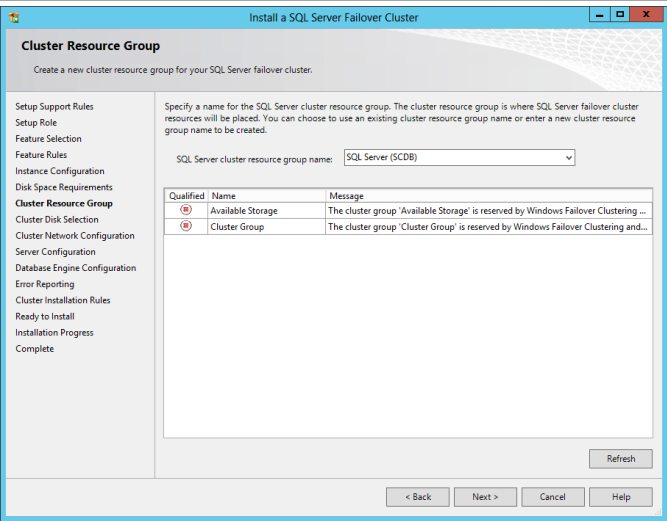
Click **Next** to continue.



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

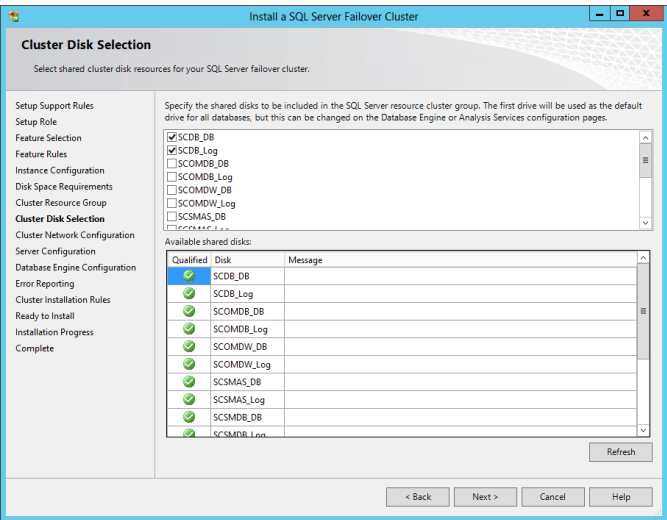


In the **Cluster Resource Group** dialog, in the **SQL Server clusterresourcegroup name** drop-down menu, accept the default value of **SQL Server (<InstanceName>)**. Click **Next** to continue.



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

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



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

Cluster Network Configuration

Select network resources for your SQL Server failover cluster.

Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Instance Configuration
Disk Space Requirements
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Analysis Services Configuration
Error Reporting
Cluster Installation Rules
Ready to Install
Installation Progress
Complete

Specify the network settings for this failover cluster:

IP Type	DHCP	Address	Subnet Mask	Subnet(s)	Network
<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.2.51	255.255.255.0	192.168.2.0/24	Database

Refresh

< Back Next > Cancel Help

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.

Server Configuration

Specify the service accounts and collation configuration.

Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Disk Space Requirements
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Error Reporting
Cluster Installation Rules
Ready to Install
Installation Progress
Complete

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	FLEXPOD\FT-SQL-SVC	*****	Manual
SQL Server Database Engine	FLEXPOD\FT-SQL-SVC	*****	Manual
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

< Back Next > Cancel Help

Server Configuration

Specify the service accounts and collation configuration.

Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Disk Space Requirements
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Analysis Services Configuration
Error Reporting
Cluster Installation Rules
Ready to Install
Installation Progress
Complete

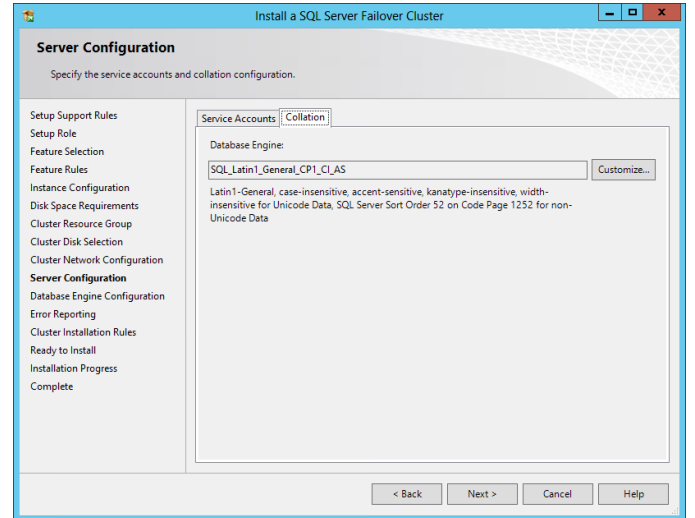
Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

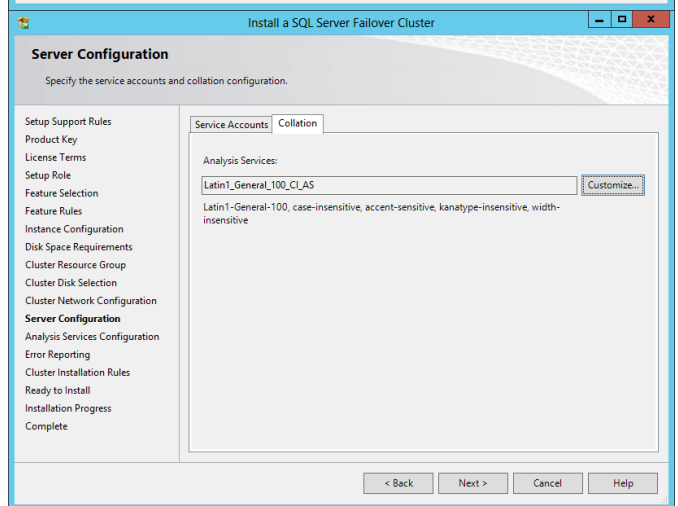
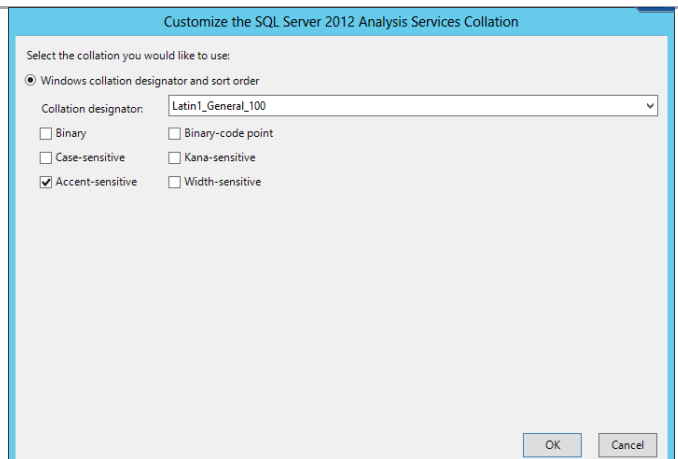
Service	Account Name	Password	Startup Type
SQL Server Analysis Services	FLEXPOD\FT-SQL-SVC	*****	Manual
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

< Back Next > Cancel Help

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 Manager⁵) and click **Next** to continue.

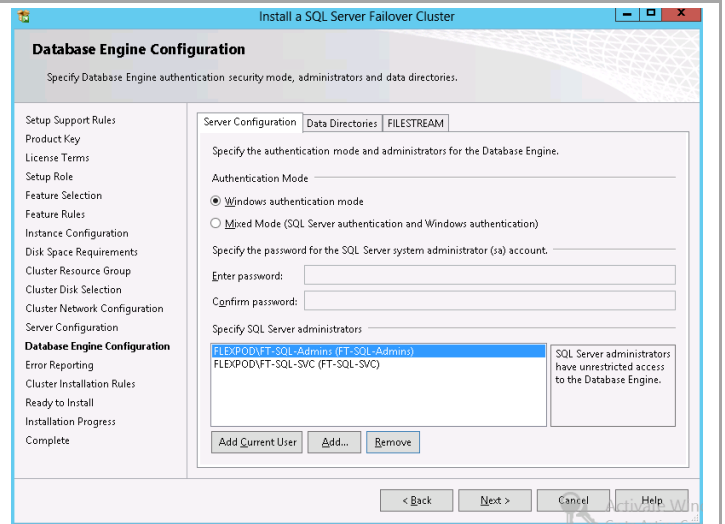


Note, in the case of Service Manager instances, the collation must be specified differently. This is done through the **Customize...** button. In these cases you can select accent and case sensitivity along with other collation designators. The following example is provided.



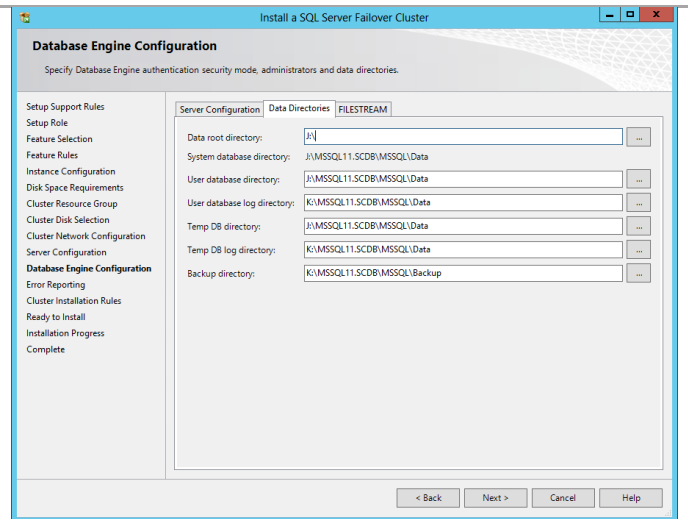
⁵ <http://social.technet.microsoft.com/wiki/contents/articles/7784.collation-in-system-center-2012-service-manager.aspx>.

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

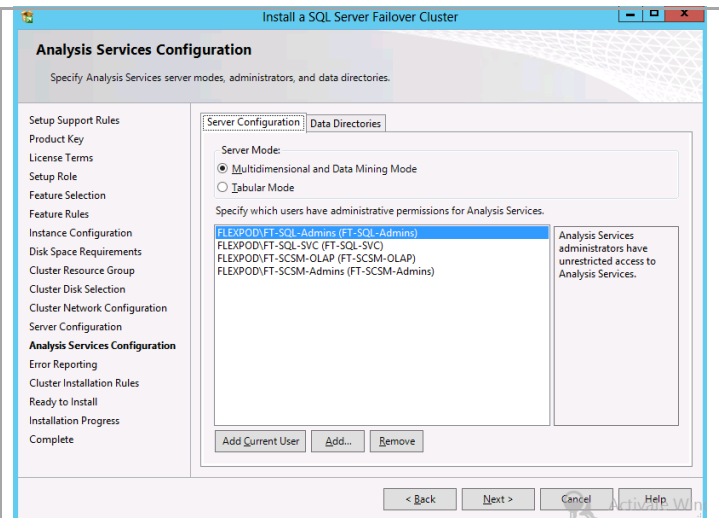
Note: It may be necessary to relocate the Temp DB files to a dedicated LUN if performance is not adequate using the two primary SQL LUNs.



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

Service Manager instance:

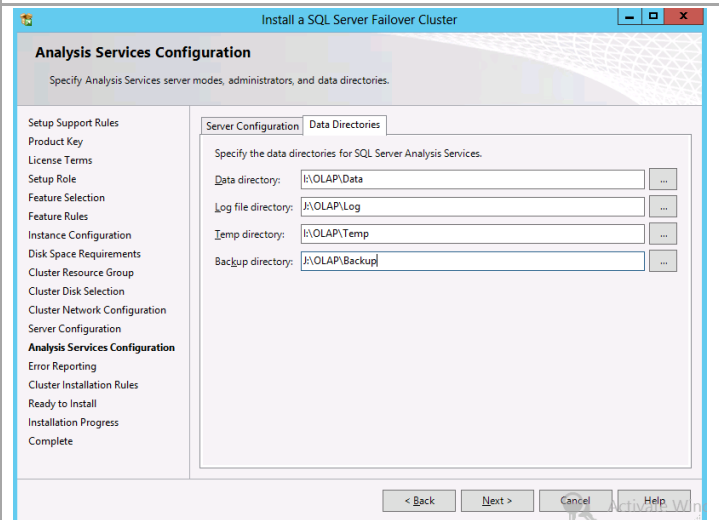
- Fast Track SQL Server Admins group
- Fast Track SQL Server Service account
- Fast Track SM Admins group
- Fast Track SM OLAP account



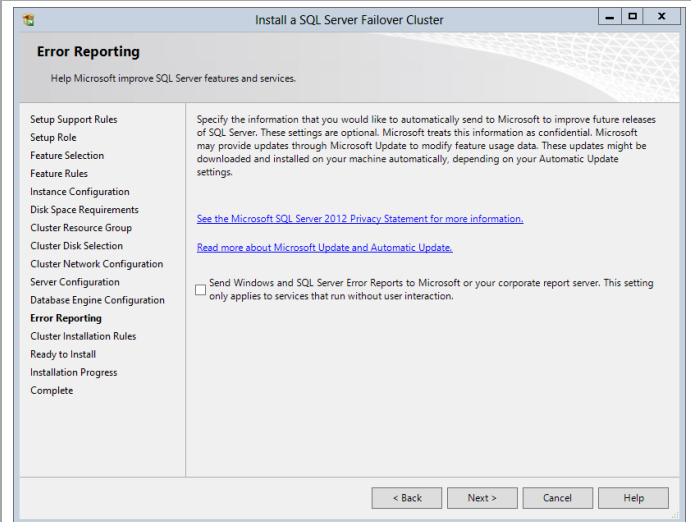
For instances with Analysis Services, use the following configuration:

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.

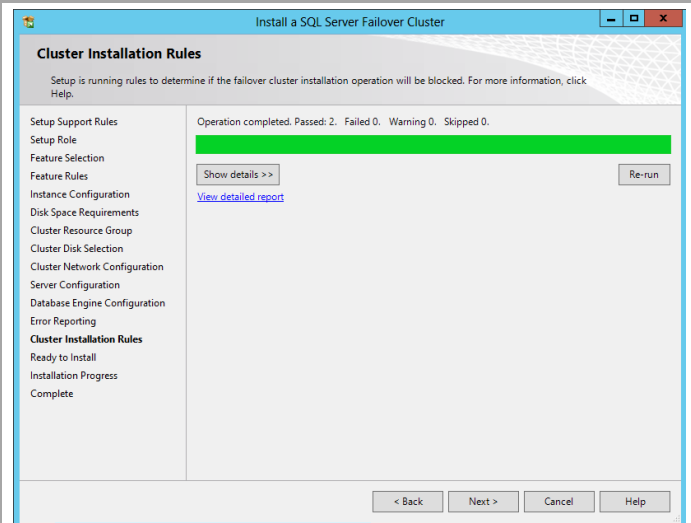
When complete, click **Next** to continue.



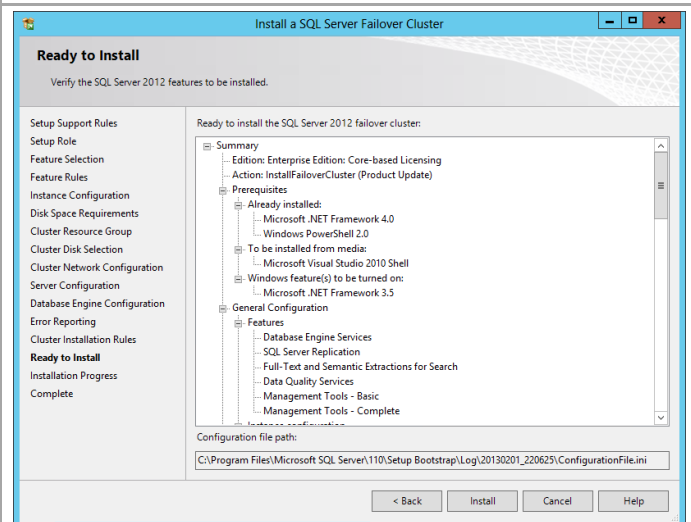
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



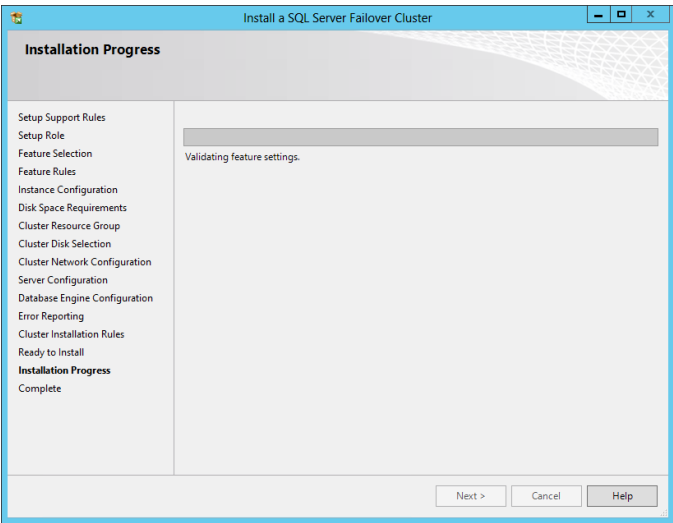
In the **Cluster Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



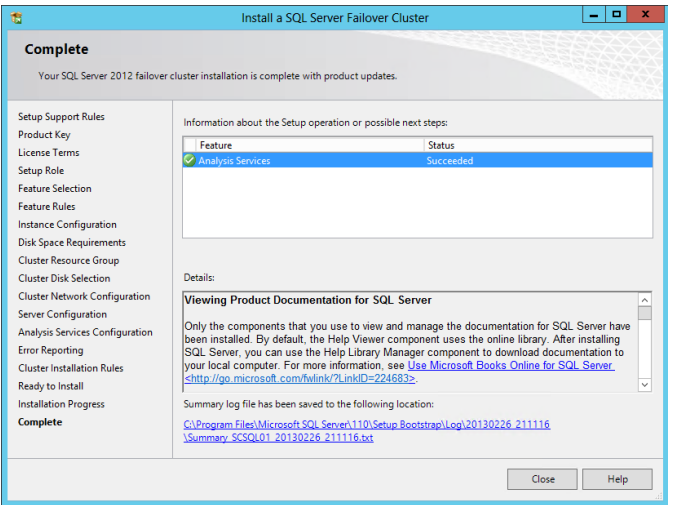
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



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



Once complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).

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

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Failover Cluster Manager' tree is expanded to 'Roles', showing a list of roles for 'scsql-cluster01.flexpod.test'. The main pane shows the 'Roles (7)' list, which includes seven SQL Server roles, all with a status of 'Running' and an owner node of 'SCSQL01'. Below this, the 'Object Explorer' pane is visible, showing a list of server instances under the 'Connect' button. The instances listed are: SCDB\SCDB (SQL Server 11.0.3128 - FLEXPOD\administrator), SCOMDB\SCOMDB (SQL Server 11.0.3128 - FLEXPOD\administrator), SCOMDW\SCOMDW (SQL Server 11.0.3128 - FLEXPOD\administrator), SCSMDB\SCSMDB (SQL Server 11.0.3128 - FLEXPOD\administrator), SCSMDW\SCSMDW (SQL Server 11.0.3128 - FLEXPOD\administrator), SCVMMDB\SCVMMDB (SQL Server 11.0.3128 - FLEXPOD\administrator), and SCSMAS\SCSMAS (Microsoft Analysis Server 11.0.3000.0 - FLEXPOD\administrator).

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SCSQL01
SQL Server (SCOMDB)	Running	Other	SCSQL01
SQL Server (SCOMDW)	Running	Other	SCSQL01
SQL Server (SCSMAS)	Running	Other	SCSQL01
SQL Server (SCSMDB)	Running	Other	SCSQL01
SQL Server (SCSMDW)	Running	Other	SCSQL01
SQL Server (SCVMMDB)	Running	Other	SCSQL01

Object Explorer

Connect

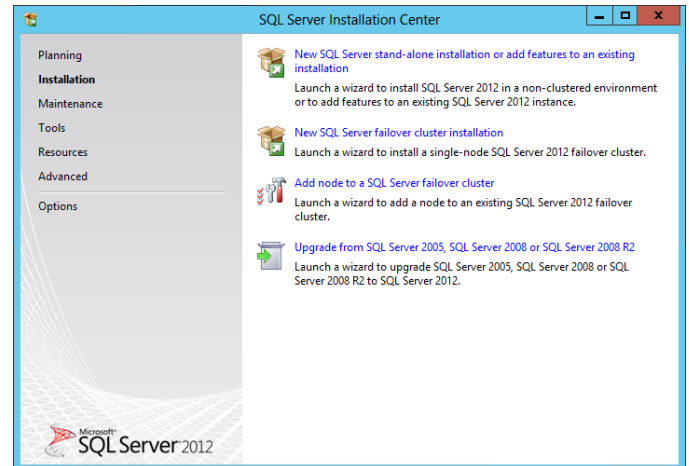
- SCDB\SCDB (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCOMDB\SCOMDB (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCOMDW\SCOMDW (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCSMDB\SCSMDB (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCSMDW\SCSMDW (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCVMMDB\SCVMMDB (SQL Server 11.0.3128 - FLEXPOD\administrator)
- SCSMAS\SCSMAS (Microsoft Analysis Server 11.0.3000.0 - FLEXPOD\administrator)

Install the SQL Server Named Instances on the Guest Cluster (Node 2)

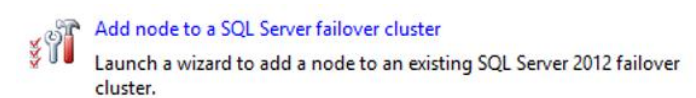
Once the creation of all required SQL Server instances on Node 1 is complete, the second node can be added to each instance of the cluster. Follow the steps below to begin the installation of additional nodes of the cluster.

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

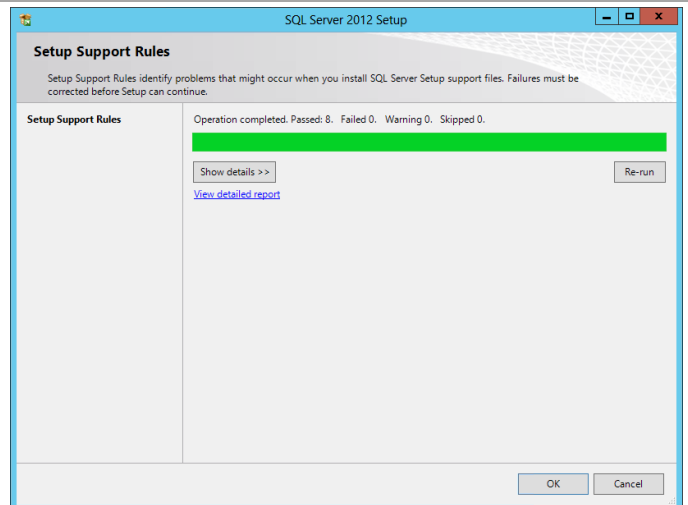
From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as administrator from the context menu to begin setup. The **SQL Server Installation Center** will appear.



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

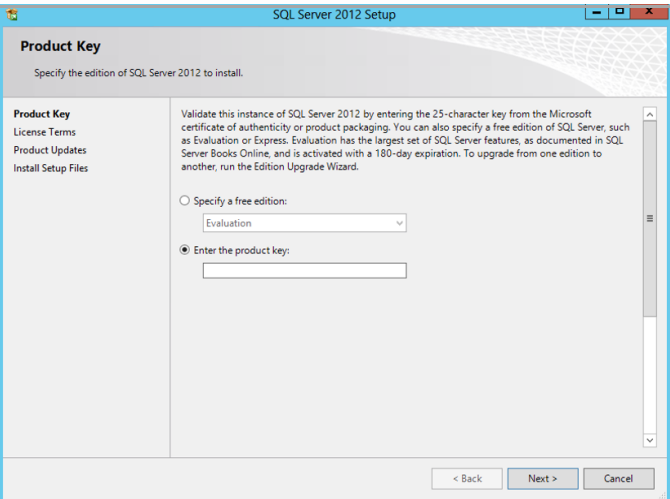


The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

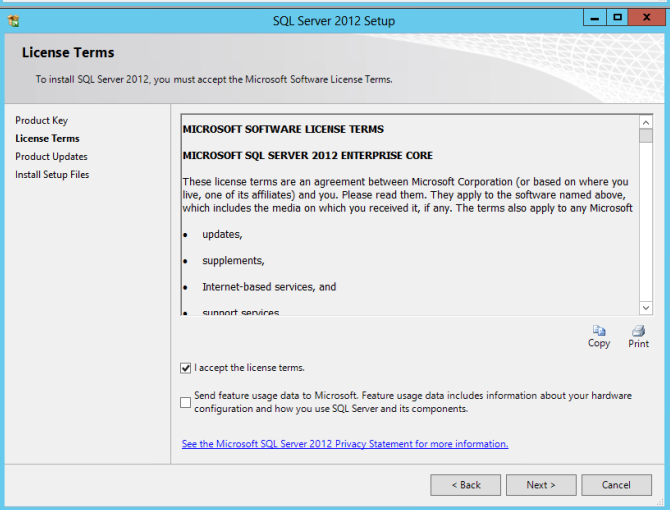


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

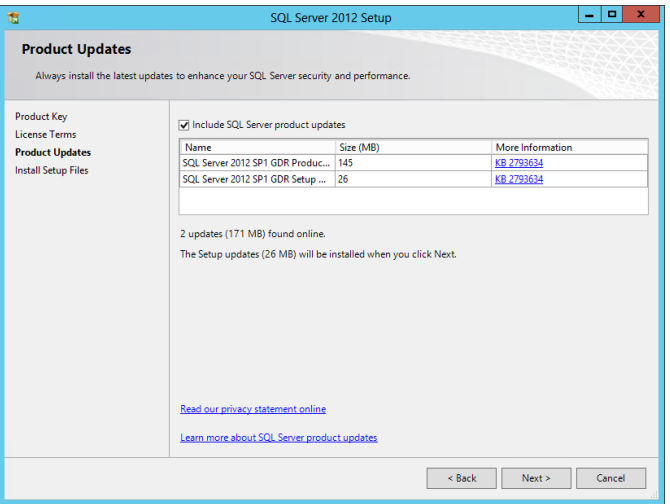
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



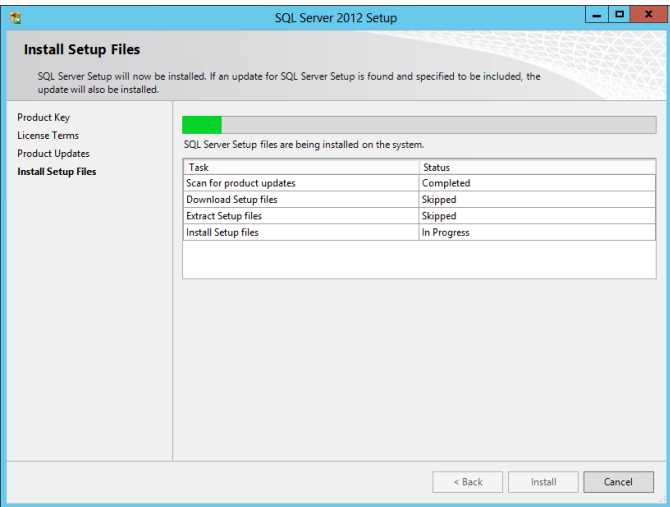
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.



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

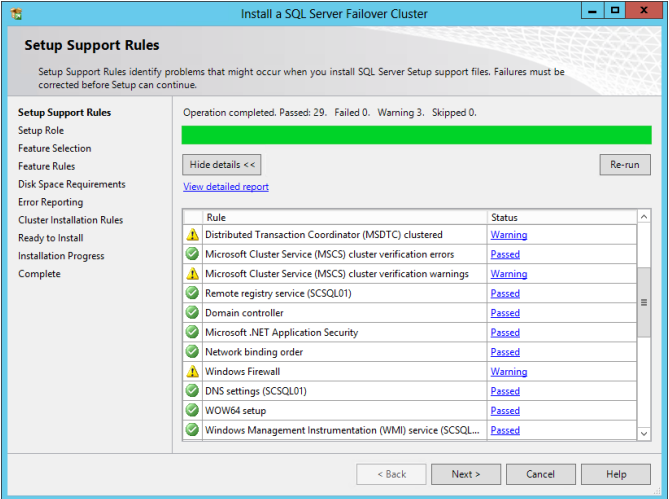


In the **Install Setup Files** dialog, click **Install** and allow the support files to install.

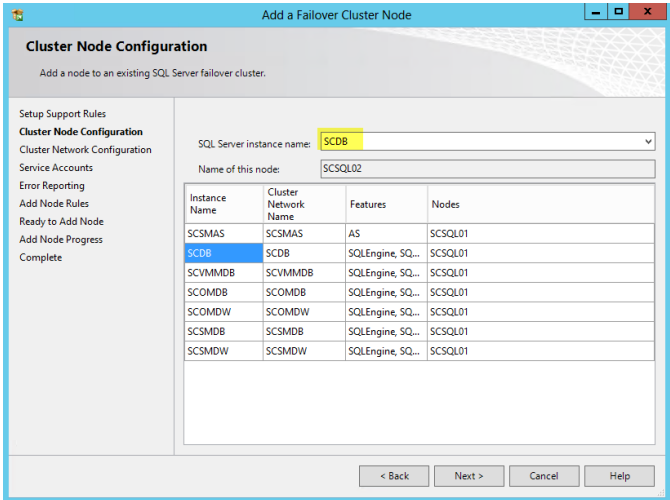


In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Click **Next** to continue.

Note that 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.

The screenshot shows the 'Add a Failover Cluster Node' dialog box, specifically the 'Cluster Network Configuration' step. The left sidebar lists the setup steps: Setup Support Rules, Cluster Node Configuration, Cluster Network Configuration (selected), Service Accounts, Error Reporting, Add Node Rules, Ready to Add Node, Add Node Progress, and Complete. The main area has a title bar 'Add a Failover Cluster Node' and a subtitle 'Cluster Network Configuration'. Below the subtitle is a note: 'The current node that is being added does not require any additional or new IP addresses. The IP addresses and subnets shown are the previously configured settings for the SQL Server cluster, and cannot be modified. Review and click Next t...'. The main content area is titled 'Specify the network settings for this failover cluster:' and contains a table with columns: IP Type, DHCP, Address, Subnet Mask, Subnet(s), and Network. The table has one row with the following values: IP Type is checked, DHCP is unchecked, Address is 192.168.2.54, Subnet Mask is 255.255.255.0, Subnet(s) is 192.168.2.0/24, and Network is Database. There is a 'Refresh' button at the bottom right of the table. At the bottom of the dialog are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

IP Type	DHCP	Address	Subnet Mask	Subnet(s)	Network
<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.2.54	255.255.255.0	192.168.2.0/24	Database

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

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

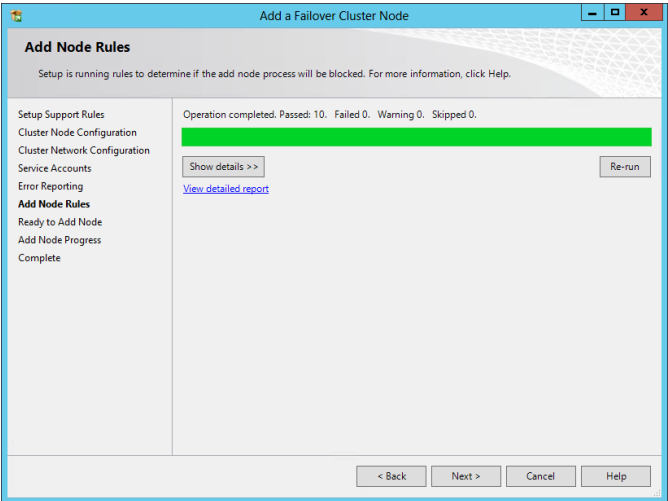
The screenshot shows the 'Add a Failover Cluster Node' dialog box, specifically the 'Service Accounts' step. The left sidebar lists the setup steps: Setup Support Rules, Product Key, License Terms, Cluster Node Configuration, Cluster Network Configuration, Service Accounts (selected), Error Reporting, Add Node Rules, Ready to Add Node, Add Node Progress, and Complete. The main area has a title bar 'Add a Failover Cluster Node' and a subtitle 'Service Accounts'. Below the subtitle is a note: 'Specify the service accounts and collation configuration. Microsoft recommends that you use a separate account for each SQL Server service.' The main content area contains a table with columns: Service, Account Name, Password, and Startup Type. The table has four rows: SQL Full-text Filter Daemon Launcher (NT Service\MSSQLFDLaun..., Manual), SQL Server Database Engine (FLEXPOD\FT-SQL-SVC, Manual), SQL Server Browser (NT AUTHORITY\LOCALSE..., Automatic), and SQL Server Agent (FLEXPOD\FT-SQL-SVC, Manual). At the bottom of the dialog are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Service	Account Name	Password	Startup Type
SQL Full-text Filter Daemon Launcher	NT Service\MSSQLFDLaun...		Manual
SQL Server Database Engine	FLEXPOD\FT-SQL-SVC	*****	Manual
SQL Server Browser	NT AUTHORITY\LOCALSE...		Automatic
SQL Server Agent	FLEXPOD\FT-SQL-SVC	*****	Manual

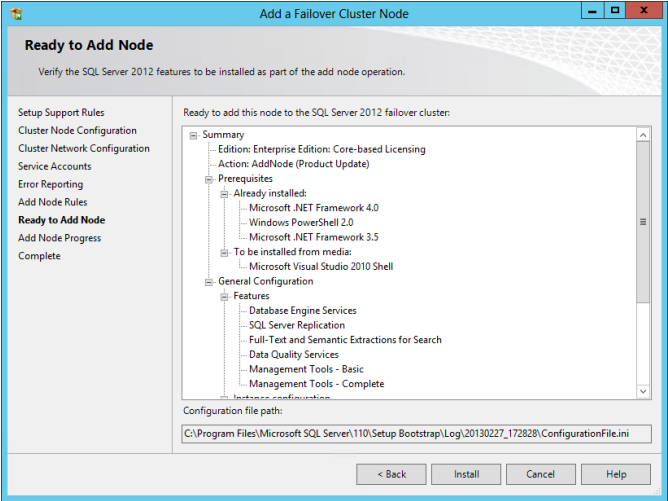
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.

The screenshot shows the 'Add a Failover Cluster Node' dialog box, specifically the 'Error Reporting' step. The left sidebar lists the setup steps: Setup Support Rules, Cluster Node Configuration, Cluster Network Configuration, Service Accounts, Error Reporting (selected), Add Node Rules, Ready to Add Node, Add Node Progress, and Complete. The main area has a title bar 'Add a Failover Cluster Node' and a subtitle 'Error Reporting'. Below the subtitle is a note: 'Help Microsoft improve SQL Server features and services.' The main content area is titled 'Specify the information that you would like to automatically send to Microsoft to improve future releases of SQL Server. These settings are optional. Microsoft treats this information as confidential. Microsoft may provide updates through Microsoft Update to modify feature usage data. These updates might be downloaded and installed on your machine automatically, depending on your Automatic Update settings.' There are two links: 'See the Microsoft SQL Server 2012 Privacy Statement for more information.' and 'Read more about Microsoft Update and Automatic Update.' At the bottom, there is a checkbox labeled 'Send Windows and SQL Server Error Reports to Microsoft or your corporate report server. This setting only applies to services that run without user interaction.' At the bottom of the dialog are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

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.

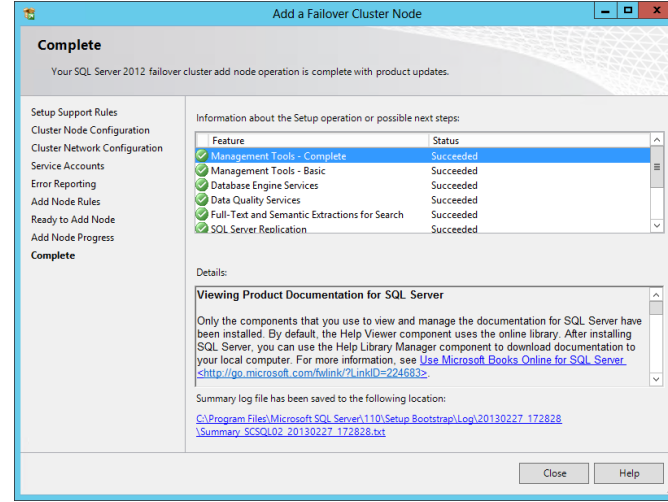


In the **Ready to Add Node** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the second SQL Server node for the selected instance.



Once complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.

Repeat these steps for each associated SQL Server instance required for Fast Track installation (seven instances total).



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

The screenshot displays two windows from SQL Server 2012 Management Studio. The top window is the Failover Cluster Manager, showing a cluster named 'SCSQL-Cluster01.flexpod.te' with two nodes: 'SCSQL01' and 'SCSQL02'. The 'Roles' tab is selected, showing a list of 7 roles, all of which are 'Running' and owned by 'SCSQL02'. The bottom window is the Object Explorer, showing the 'Connect' dropdown menu with a list of server instances. The first instance, 'SCDB\SCDB (SQL Server 11.0.3128 - FLEXP0D\administrator)', is selected and highlighted in blue.

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SCSQL02
SQL Server (SCOMDB)	Running	Other	SCSQL02
SQL Server (SCOMDW)	Running	Other	SCSQL02
SQL Server (SCSMAS)	Running	Other	SCSQL02
SQL Server (SCSMDB)	Running	Other	SCSQL02
SQL Server (SCSMDW)	Running	Other	SCSQL02
SQL Server (SCVMMDB)	Running	Other	SCSQL02

Server Name	Version	Administrator
SCDB\SCDB	SQL Server 11.0.3128	FLEXP0D\administrator
SCOMDW\SCOMDW	SQL Server 11.0.3128	FLEXP0D\administrator
SCOMDB\SCOMDB	SQL Server 11.0.3128	FLEXP0D\administrator
SCSMAS\SCSMAS	Microsoft Analysis Server 11.0.3000.0	FLEXP0D\administrator
SCVMMDB\SCVMMDB	SQL Server 11.0.3128	FLEXP0D\administrator
SCSMDB\SCSMDB	SQL Server 11.0.3128	FLEXP0D\administrator
SCSMDW\SCSMDW	SQL Server 11.0.3128	FLEXP0D\administrator

13.4 Post-Installation Tasks

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

Configure Windows Firewall Settings for SQL Named Instances

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

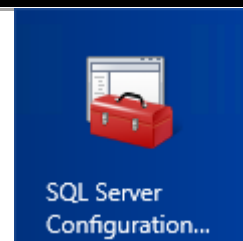
This process is described in TechNet⁶ and instructions are provided in this document.

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

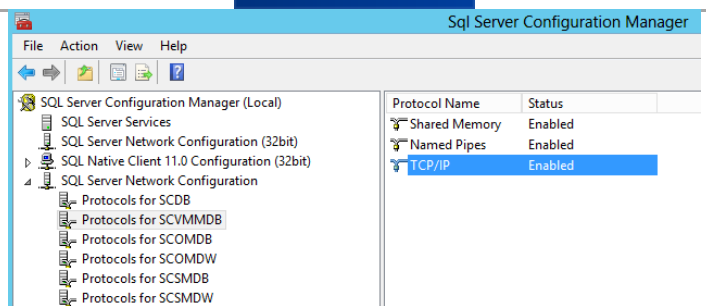
Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt execute the following command:
netstat -b
Notice the existing dynamic ports used by the SQLSERVER.EXE sessions.

TCP	192.168.1.35:54021	SCS QL01:49366	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.35:54021	SCS QL01:49396	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.35:54021	SCS QL01:49398	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.36:53818	SCS QL01:49370	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.36:53818	SCS QL01:49402	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.36:53818	SCS QL01:49403	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.37:50617	SCS QL01:49342	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.37:50617	SCS QL01:49400	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.37:50617	SCS QL01:49401	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.38:49199	SCS QL01:49357	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.38:49199	SCS QL01:49391	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.38:49199	SCS QL01:49393	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.39:49813	SCS QL01:49818	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.39:49813	SCS QL01:49846	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.39:49813	SCS QL01:49848	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.40:62291	SCS QL01:62301	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.40:62291	SCS QL01:62311	ESTABLISHED
[sqlservr.exe]			
TCP	192.168.1.40:62291	SCS QL01:62312	ESTABLISHED
[sqlservr.exe]			

On the first SQL Server node open **SQL Configuration Manager**.



In the **SQL Server Configuration Manager** console pane, expand the **SQL Server Network Configuration** node and then expand the **Protocols for the <instance name>** node. Once selected, double-click **TCP/IP** from the available protocol names to observe its properties.



⁶ 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.

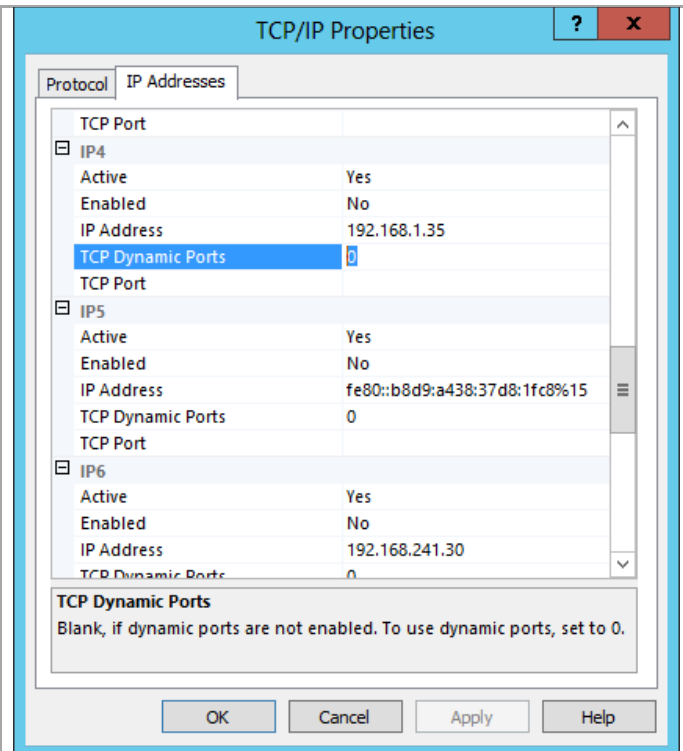
Enabled - If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to No, this property indicates whether SQL Server is listening on the IP address. If the Listen All property on the TCP/IP Properties (Protocol Tab) is set to Yes, the property is disregarded. Not available for IPAll.

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 used.

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

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



Within the dialog, browse to each IP address section for the instance and delete the numerical value (0) from the **TCP Dynamic Ports** field.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'IP Addresses' tab selected. It lists three IP addresses: IP4 (192.168.1.35), IP5 (fe80::b8d9:a438:37d8:1fc8%15), and IP6 (192.168.241.30). For each IP address, the 'TCP Dynamic Ports' field is highlighted in yellow. Below the list, there is a section for 'TCP Dynamic Ports' with a note: 'Blank, if dynamic ports are not enabled. To use dynamic ports, set to 0.' The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Protocol	IP Address	Active	Enabled	TCP Dynamic Ports
IP4	192.168.1.35	Yes	No	
IP5	fe80::b8d9:a438:37d8:1fc8%15	Yes	No	
IP6	192.168.241.30	Yes	No	

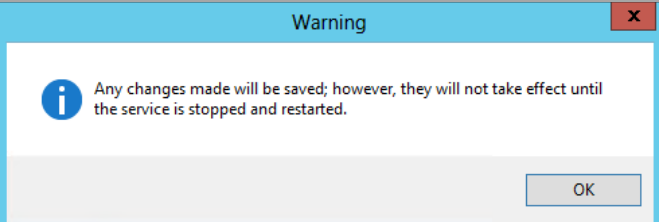
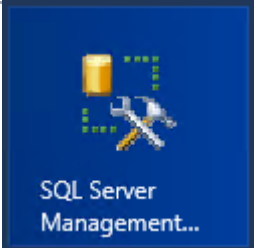
TCP Dynamic Ports
Blank, if dynamic ports are not enabled. To use dynamic ports, set to 0.

Scroll down to the **IPALL** section and delete the existing dynamic port value from **TCP Dynamic Ports** property. Assign static port value under **TCP Port** to one that is appropriate for the instance. For this example, port 10437 was specified. Click **Apply** to save the changes.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'IP Addresses' tab selected. It lists three IP addresses: IP8 (192.168.1.39), IP9 (fe80::b8d9:a438:37d8:1fc8%15), and IPALL. For IP8 and IP9, the 'TCP Dynamic Ports' field is highlighted in yellow. For IPALL, the 'TCP Port' field is highlighted in blue and contains the value '10437'. Below the list, there is a section for 'TCP Port' with a note: 'Blank, if dynamic ports are not enabled. To use dynamic ports, set to 0.' The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

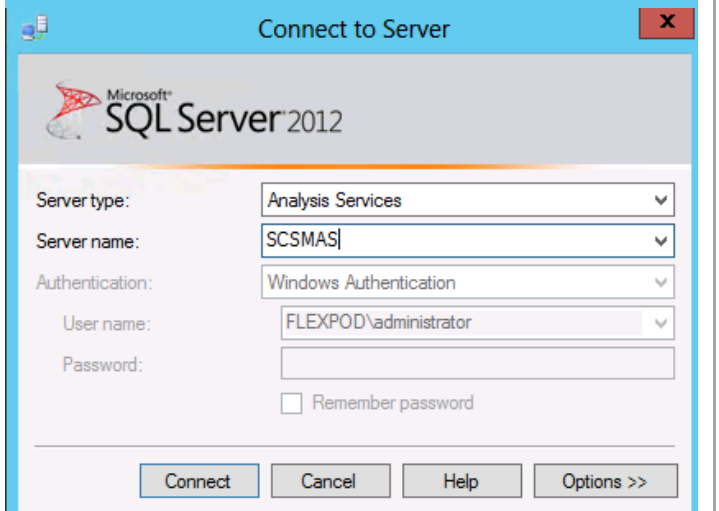
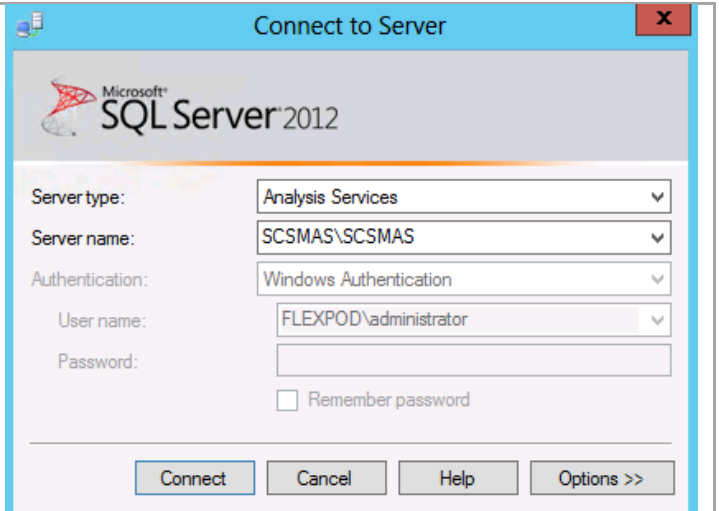
Protocol	IP Address	Active	Enabled	TCP Dynamic Ports	TCP Port
IP8	192.168.1.39	Yes	No		
IP9	fe80::b8d9:a438:37d8:1fc8%15	Yes	No		
IPALL					10437

TCP Port
Blank, if dynamic ports are not enabled. To use dynamic ports, set to 0.

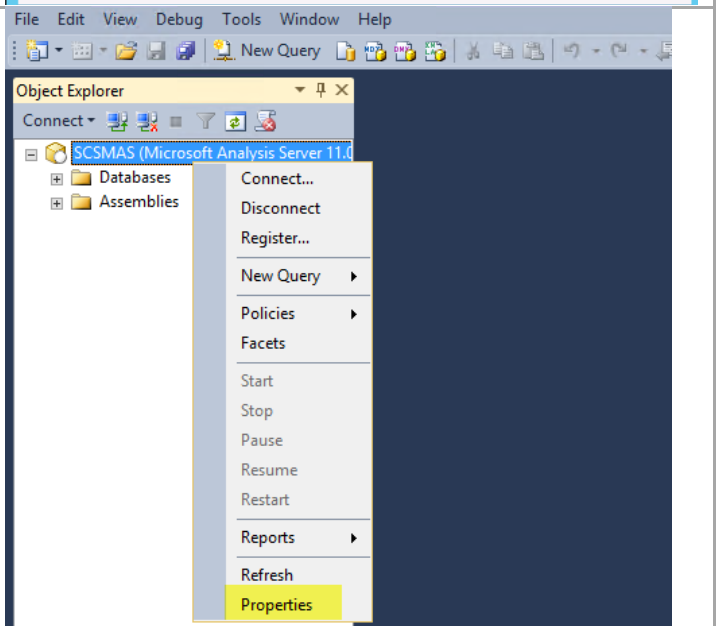
<p>Note that a warning dialog will appear stating that the settings will not take effect until the SQL Server service has been restarted for that instance.</p>	 <p>A warning dialog box with a blue header bar containing the word "Warning" and a red close button. The main area has a light blue background with an information icon (i) and the text: "Any changes made will be saved; however, they will not take effect until the service is stopped and restarted." At the bottom right is an "OK" button.</p>																
<p>Repeat these steps to set a static port for each database service instance. Reference the SQL settings table at the beginning of this section for the default values used in this guide. Once all of the database instances are configured close SQL Server Configuration Manager and continue on to the next steps to change the SSAS instance listening port.</p>	<table border="1" data-bbox="984 422 1398 787"> <thead> <tr> <th>SQL Instance</th><th>Listening Port</th></tr> </thead> <tbody> <tr> <td>SCDB</td><td>1433</td></tr> <tr> <td>SCVMMDB</td><td>10434</td></tr> <tr> <td>SCOMDB</td><td>10435</td></tr> <tr> <td>SCOMDW</td><td>10436</td></tr> <tr> <td>SCSMDB</td><td>10437</td></tr> <tr> <td>SCSMDW</td><td>10438</td></tr> <tr> <td>SCSMAS</td><td>10439</td></tr> </tbody> </table> <p><i><u>Note:</u> The SCDB instance must use port 1433 if the Cloud Services Process Pack (CSPP) is used in the environment.</i></p>	SQL Instance	Listening Port	SCDB	1433	SCVMMDB	10434	SCOMDB	10435	SCOMDW	10436	SCSMDB	10437	SCSMDW	10438	SCSMAS	10439
SQL Instance	Listening Port																
SCDB	1433																
SCVMMDB	10434																
SCOMDB	10435																
SCOMDW	10436																
SCSMDB	10437																
SCSMDW	10438																
SCSMAS	10439																
<p>Open SQL Server Management Studio.</p>	 <p>The icon for SQL Server Management Studio, featuring a blue square background with a yellow cylinder, a hammer, and a wrench. Below the icon, the text "SQL Server Management..." is visible.</p>																

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

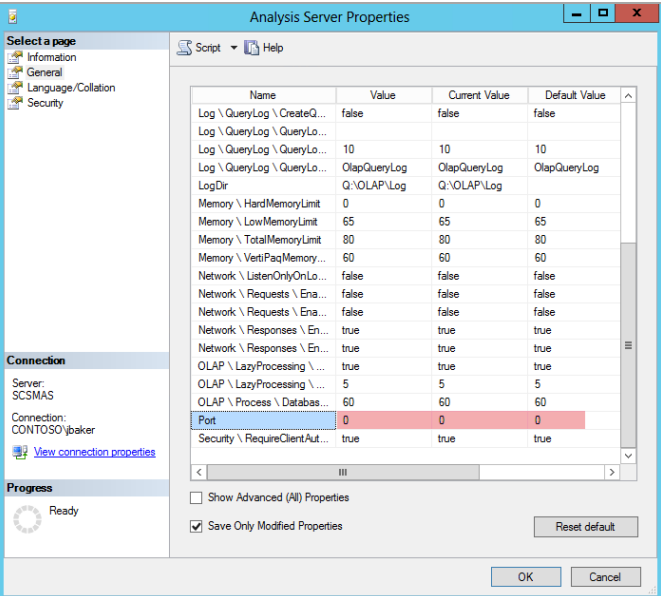
Note: Be sure the account you are logged on with is a member of the FT-SQL-Admins domain group or has otherwise been defined as a SQL sysadmin for the instance.



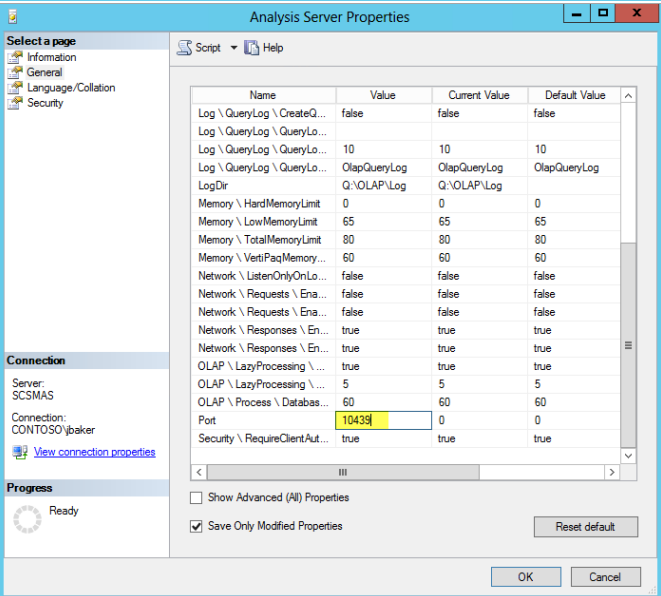
Once connected to the instance in **SQL Management Studio**, right-click the SSAS instance and select **Properties**.



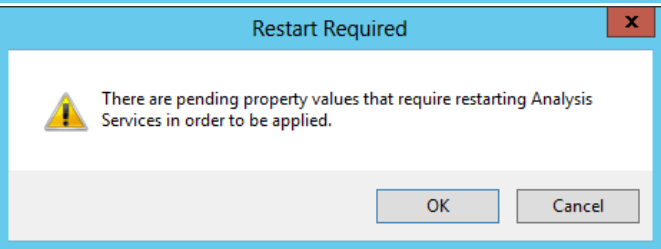
In the Analysis Server Properties dialog, select the **General** tab and then select **Port** (SQL listening port) from the **Name** column. By default the value will be set to “0” (zero) to specify a dynamic port.



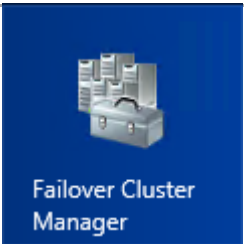
In the same dialog, specify an appropriate static port value then click **OK** to save the changes.



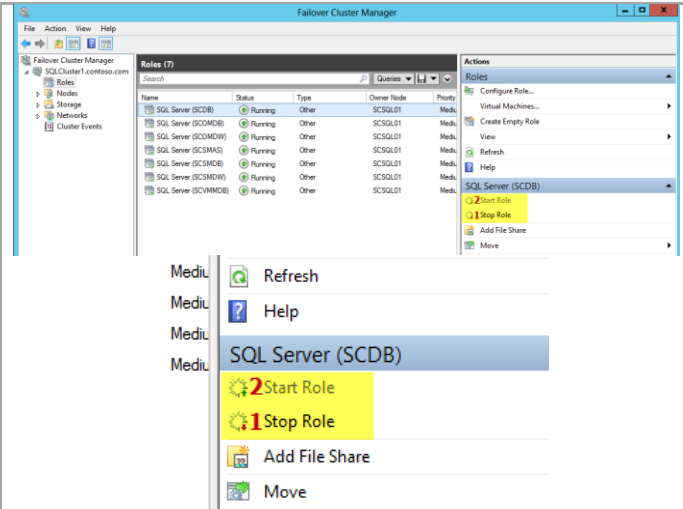
A dialog will appear outlining that a restart is required. Click **OK** and close SQL Management Studio.



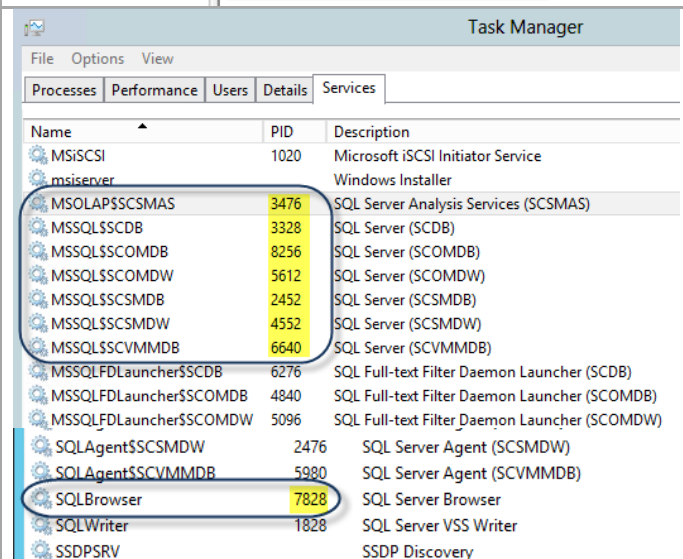
Open **Failover Cluster Manager** and expand the **Roles** node.



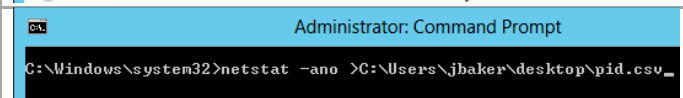
To apply the new port settings, in **Failover Cluster Manager** select each SQL Server instance. In the action pane, select **Stop Role** to stop the service for each instance. Restart each instance by selecting **Start Role** from the action Pane. Close the **Failover Cluster Manager** console.



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 -an** to export the output to a CSV file.



Import the CSV file into Excel and then format the data into a table.

Filter on the PID column, selecting only the PIDs you documented from the task manager step previously and then filter on the state column selecting only the listening and blank values.

The resulting table should confirm that all of the SQL instances are listening on only the static port assigned previously.

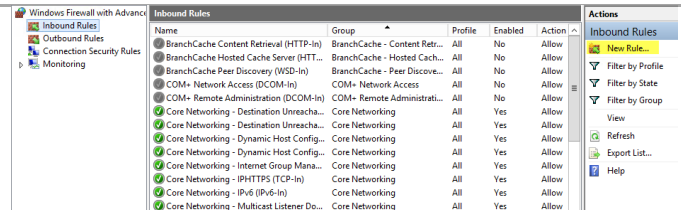
In addition to the static ports for each instance the 2382 TCP/UDP and 1434 TCP/UDP ports for SQL Browser will also be listed and will need to be opened in the firewall settings to support the Analysis and Database Engine instances.

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

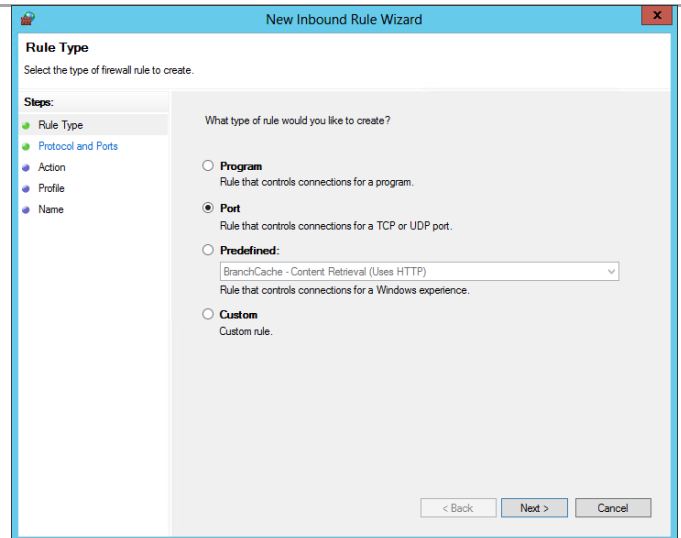
Once completed, configure the Windows Firewall Rule for the SQL Browser Service. To perform this action, on each node in the Windows Failover Cluster that will host SQL instances, open the **Windows Firewall with Advanced Security** MMC console.



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.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a blue title bar and a sidebar on the left with steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains the following options:

- Does this rule apply to TCP or UDP?
 - ☐ TCP
 - ☒ UDP
- Does this rule apply to all local ports or specific local ports?
 - ☐ All local ports
 - ☒ Specific local ports:
Example: 80, 443, 5000-5010

At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.

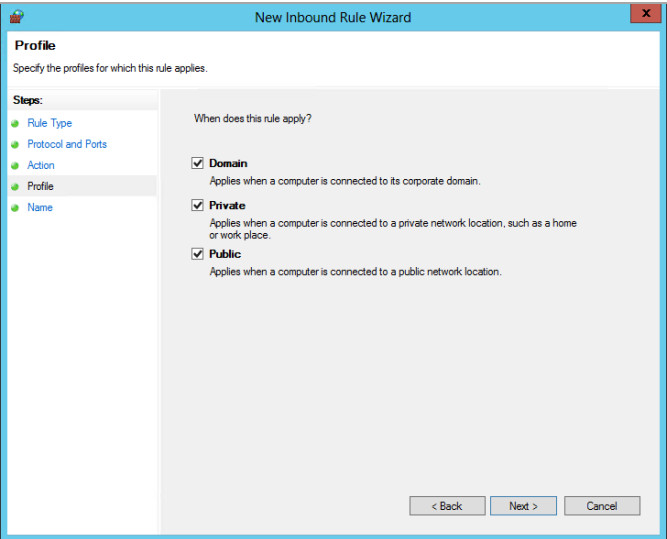
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The window has a blue title bar and a sidebar on the left with steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the following options:

- What action should be taken when a connection matches the specified conditions?
 - ☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
 - ☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
 - ☐ **Block the connection**

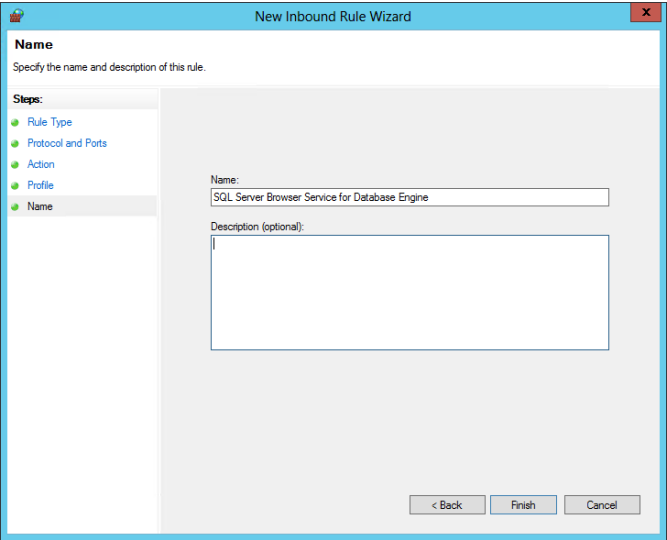
At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.

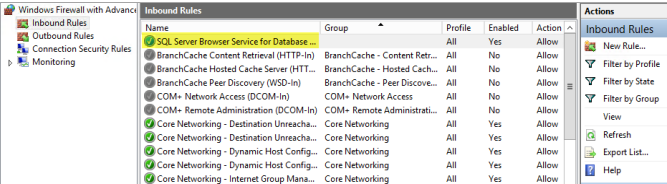
Allowing the Private and Public network types will enable this rule to support other scenarios such as SQL Always On multi-site Failover Cluster Instances with Database Availability Groups where replication may take place on a network other than the domain network.



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.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The 'Steps' pane on the left shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'Specify the protocols and ports to which this rule applies.' It has two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). A text box next to 'Specific local ports' contains the value '2382'. Below it is an example: 'Example: 80, 443, 5000-5010'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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.

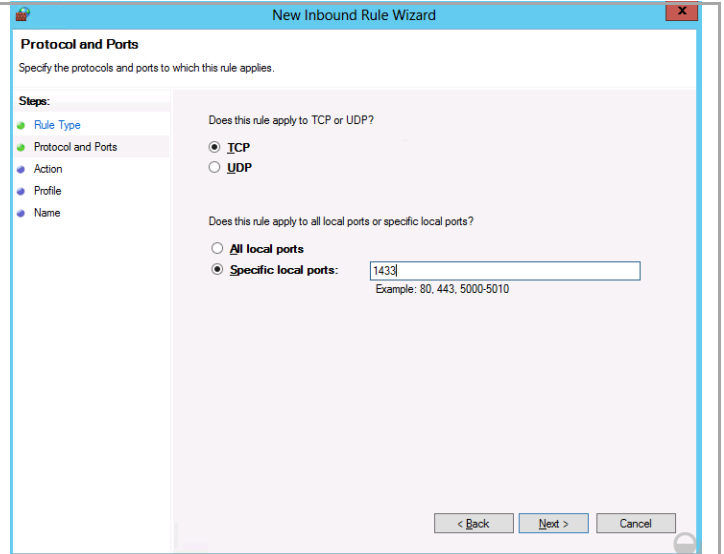
The screenshot shows the 'Windows Firewall with Advanced Security' console, specifically the 'Inbound Rules' pane. A table lists various inbound rules. The rule 'SQL Server Browser Service for Analysis Se...' is highlighted. The 'Actions' pane on the right shows 'New Rule...' as the first option.

Name	Group	Profile	Enabled	Action
SQL Server Browser Service for Analysis Se...		All	Yes	Allow
BranchCache - Content Retrieval (HTTP-In)	BranchCache - Content Retrieval	All	No	Allow
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery	All	No	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administration	All	No	Allow
Core Networking - Destination Unreachable	Core Networking	All	Yes	Allow
Core Networking - Destination Unreachable	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Configuration	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Configuration	Core Networking	All	Yes	Allow

In the **New Inbound Rule Wizard** dialog, on the **Rule Type** page, select the **Port** radio button and click **Next** to continue.

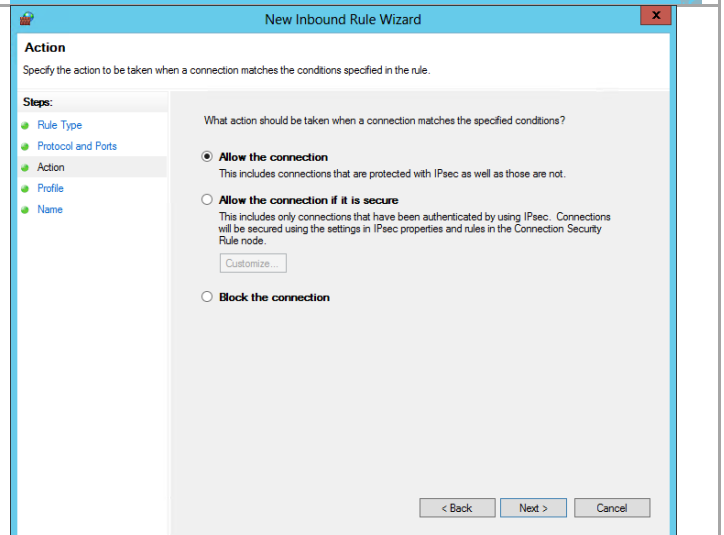
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Rule Type' step. The 'Steps' pane on the left shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' It has three radio buttons: 'Program' (Rule that controls connections for a program.), 'Port' (selected, Rule that controls connections for a TCP or UDP port.), and 'Predefined:' (Rule that controls connections for a Windows experience.). Below 'Predefined:' is a dropdown menu showing 'BranchCache - Content Retrieval (Uses HTTP)'. Below 'Custom' is the text 'Custom rule.'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

On the **Protocol and Ports** page select the **UDP** radio button. Select the **Specific local ports** radio button and input the specific local TCP/IP port to enable access to the first named SQL instance. In this example to enable access to the SQL instance SCDB the port specified is 1433. Click **Next** to continue.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The 'Steps' list on the left includes Rule Type, Protocol and Ports (highlighted), Action, Profile, and Name. The main area contains two sections: 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text box next to 'Specific local ports' contains the value '1433', with an example '80, 443, 5000-5010' shown below it. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

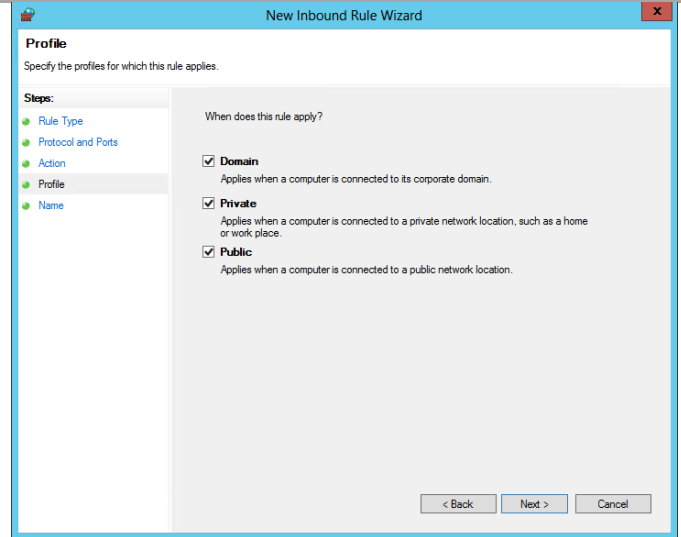
On the **Action** page, select the **Allow the connection** radio button and click **Next** to continue.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The 'Steps' list on the left includes Rule Type, Protocol and Ports, Action (highlighted), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

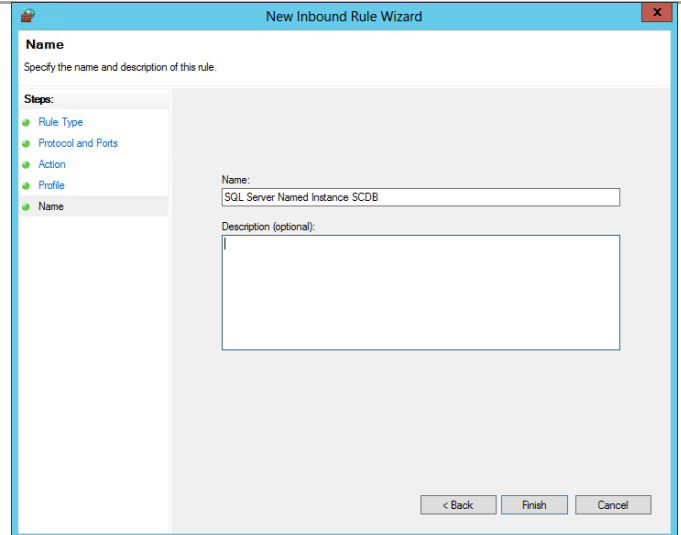
On the **Profile** page, leave the **Domain**, **Private** and **Public** checkboxes selected and click **Next** to continue.

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.



The screenshot shows the 'Profile' step of the 'New Inbound Rule Wizard'. The 'Steps' pane on the left has 'Profile' selected. The main area is titled 'When does this rule apply?' and contains three checked checkboxes: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). Navigation buttons at the bottom are '< Back', 'Next >', and 'Cancel'.

Specify a name for the new rule such as “*SQL Server Named Instance SCDB*” and click **Finish**.



The screenshot shows the 'Name' step of the 'New Inbound Rule Wizard'. The 'Steps' pane on the left has 'Name' selected. The main area is titled 'Specify the name and description of this rule.' and contains a 'Name:' text box with the value 'SQL Server Named Instance SCDB' and a 'Description (optional):' text box. Navigation buttons at the bottom are '< Back', 'Finish', and 'Cancel'.

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.

Inbound Rules			
Name	Group	Local Port	Protocol
✓ SQL Server Named Instance SCSMAS		10439	TCP
✓ SQL Server Named Instance SCSMDW		10438	TCP
✓ SQL Server Named Instance SCSMDB		10437	TCP
✓ SQL Server Named Instance SCOMDW		10436	TCP
✓ SQL Server Named Instance SCOMDB		10435	TCP
✓ SQL Server Named Instance SCVMMDB		10434	TCP
✓ SQL Server Named Instance SCDB		1433	TCP
✓ SQL Server Browser Service for Alalysis Se...		2382	TCP
✓ SQL Server Browser Service for Database ...		1434	UDP
● BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	80	TCP

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.

```
$RemoteSession = New-CimSession -ComputerName  
SCSQL02  
  
New-NetFirewallRule -DisplayName "SQL Server  
Browser Service for Database Engine" -LocalPort  
1434 -Protocol UDP -Action Allow
```

To create the rules on the remote nodes through PowerShell, the following commands are provided as an example.

Note that the SCDB instance must be set to 1433 if the Cloud Services Process Pack will be used.

This procedure assumes that commands are executed on SQL Server node SCSQL01.

```
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
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Browser Service for Analysis Server" -LocalPort  
2382 -Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCDB" -LocalPort 1433 -Protocol  
TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCDB" -LocalPort 1433 -Protocol  
TCP -Action Allow -CimSession $RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCVMMDB" -LocalPort 10434 -  
Protocol TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCVMMDB" -LocalPort 10434 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDB" -LocalPort 10435 -  
Protocol TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDB" -LocalPort 10435 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDW" -LocalPort 10436 -  
Protocol TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDW" -LocalPort 10436 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDB" -LocalPort 10437 -  
Protocol TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDB" -LocalPort 10437 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDW" -LocalPort 10438 -  
Protocol TCP -Action Allow
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDW" -LocalPort 10438 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMAS" -LocalPort 10439 -  
Protocol TCP -Action Allow
```

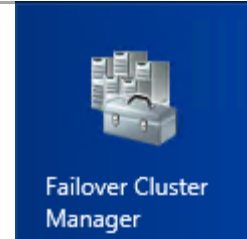
```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMAS" -LocalPort 10439 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```


Assign Preferred Owners for SQL Instances in Failover Cluster Manager

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

3. 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**.

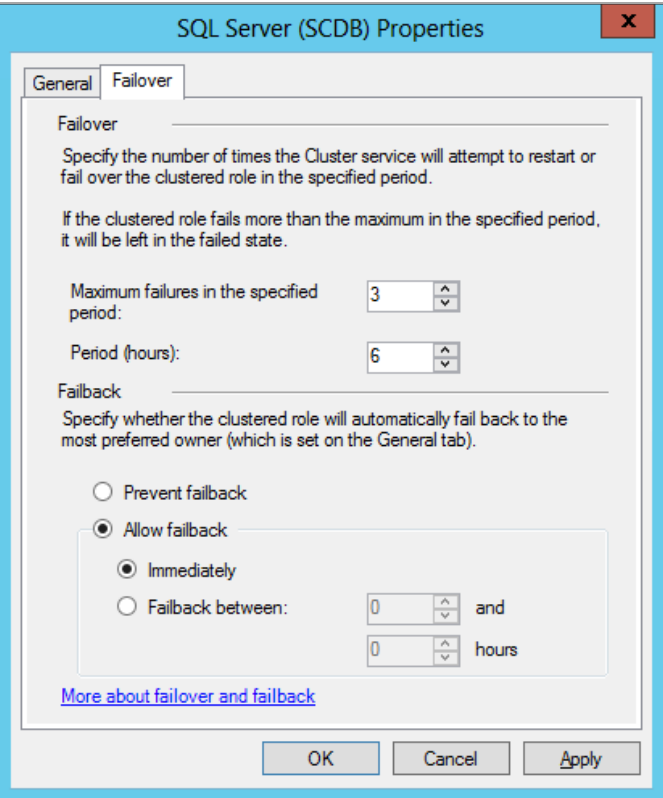
Name	Status	Type	Owner Node	Priority	Information
SQL Server (SCDB)	Running	Other	SCSQL01	Medium	
SQL Server (SCOMDB)	Running	Other	SCSQL01	Medium	
SQL Server (SCOMDW)	Running	Other	SCSQL01	Medium	
SQL Server (SCSMAS)	Running	Other	SCSQL01	Medium	
SQL Server (SCSMDB)	Running	Other	SCSQL01	Medium	
SQL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

SQL Server (SCDB) Preferred Owners: [Any node](#)

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

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.



SQL Server (SCDB) Properties

Failover

Specify the number of times the Cluster service will attempt to restart or fail over the clustered role in the specified period.

If the clustered role fails more than the maximum in the specified period, it will be left in the failed state.

Maximum failures in the specified period: 3

Period (hours): 6

Failback

Specify whether the clustered role will automatically fail back to the most preferred owner (which is set on the General tab).

☐ Prevent failback

☒ Allow failback

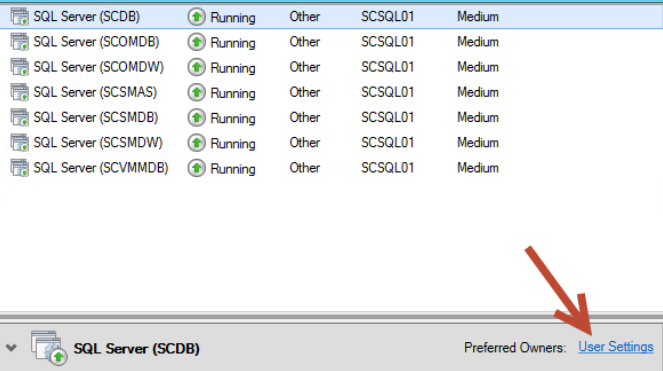
☒ Immediately

☐ Failback between: 0 and 0 hours

[More about failover and failback](#)

OK Cancel Apply

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

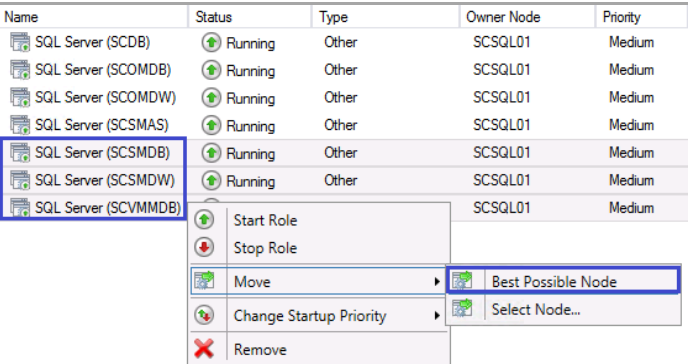


SQL Server (SCDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCSMAS)	Running	Other	SCSQL01	Medium
SQL Server (SCSMDB)	Running	Other	SCSQL01	Medium
SQL Server (SCSMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCVMMDB)	Running	Other	SCSQL01	Medium

SQL Server (SCDB) Preferred Owners: [User Settings](#)

Once all instances have been configured correctly for Preferred Owners you must initiate a planned failover to balance the SQL Server instances across nodes.

In **Failover Cluster Manager**, select the roles for each of the five SQL Instances that should not run on Node1 (SCSMDB, SCSMDW, SCVMMDB). 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	Priority
SQL Server (SCDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCSMAS)	Running	Other	SCSQL01	Medium
SQL Server (SCSMDB)	Running	Other	SCSQL01	Medium
SQL Server (SCSMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCVMMDB)	Running	Other	SCSQL01	Medium

Start Role

Stop Role

Move

Change Startup Priority















Remove

Best Possible Node

Select Node...

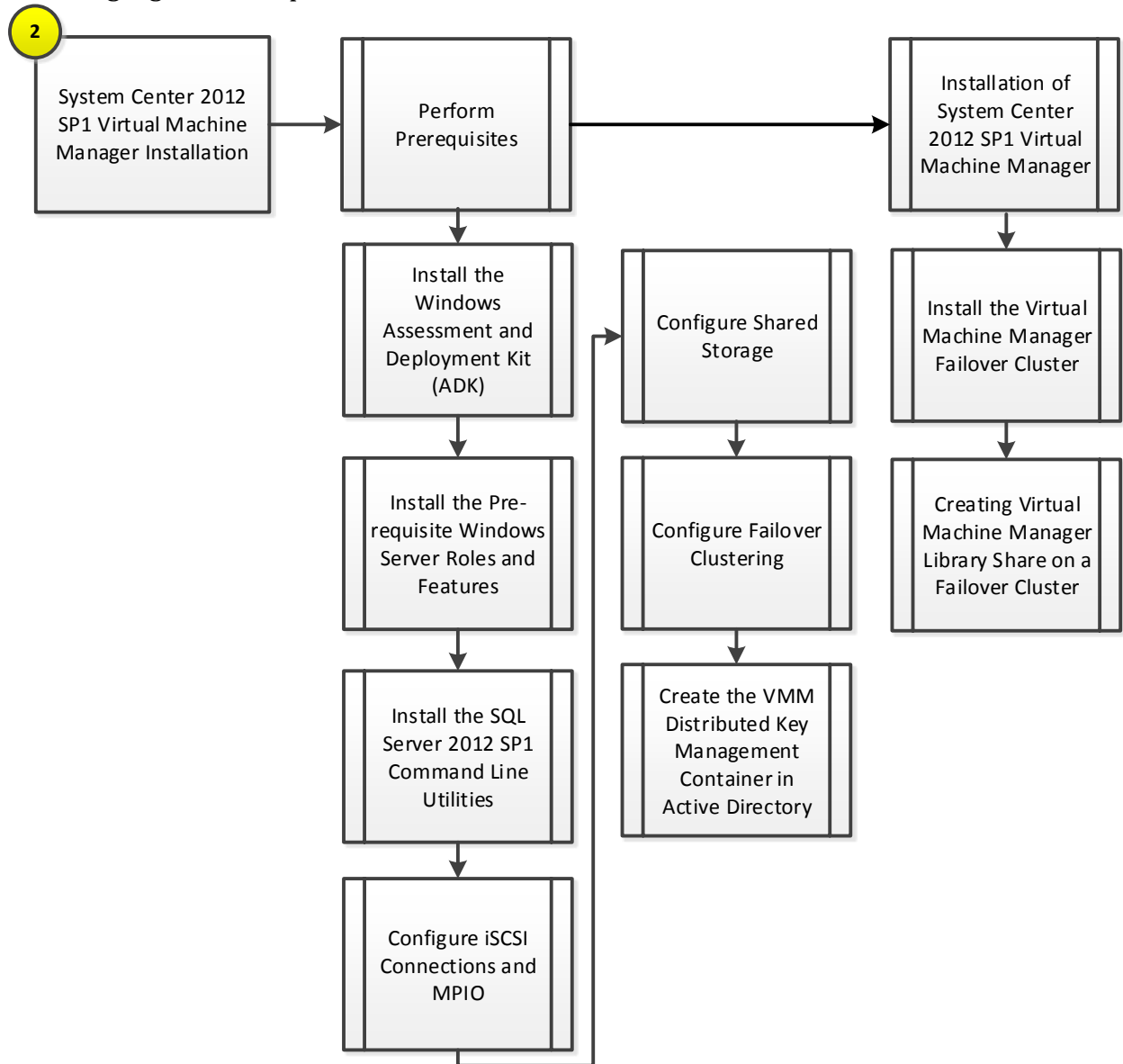
When the moves are completed, all Instances should be distributed across Node1 and Node2.

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

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

14 Virtual Machine Manager

The System Center 2012 Virtual Machine Manager installation process includes the following high-level steps:



14.1 Overview

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

- Two base virtual machines running Windows Server 2012 have been provisioned and configured as a Windows Failover Cluster.

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

14.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

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

Groups

Verify that the following security groups have been created:

Security group name	Group scope	Members
---------------------	-------------	---------

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 TechNet⁷.

Install the Windows Assessment and Deployment Kit

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

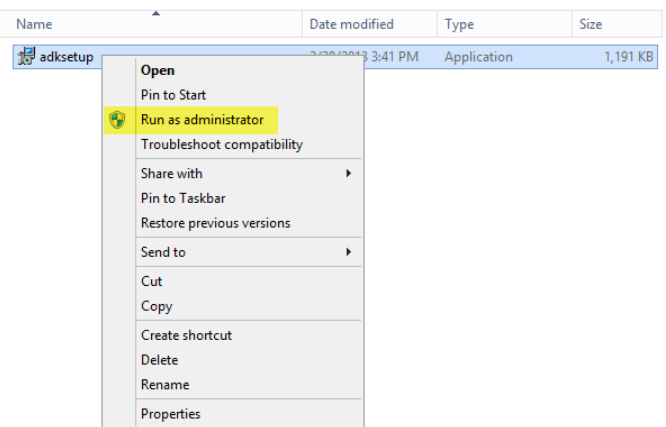
During installation, only the Deployment Tools and the Windows Preinstallation Environment features will be selected. This installation also assumes the VMM servers have internet access. If that is not the case an offline installation can be performed and information for this installation option along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

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

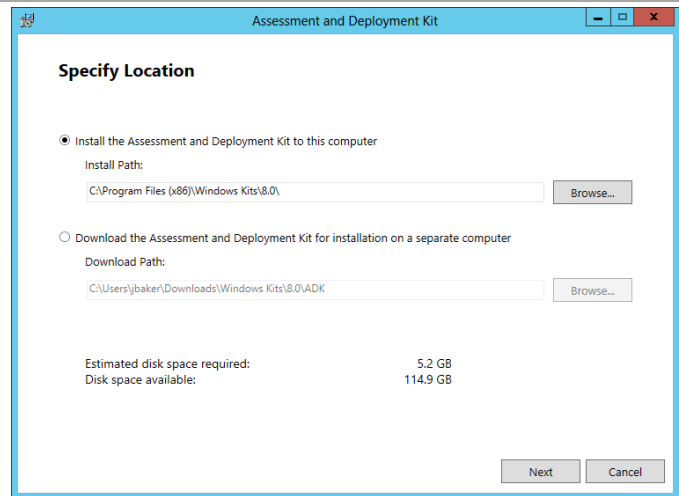
► Perform the following steps on both **Virtual Machine Manager** virtual machines.

⁷ Creating User Roles in VMM - <http://technet.microsoft.com/en-us/library/gg696971.aspx>.

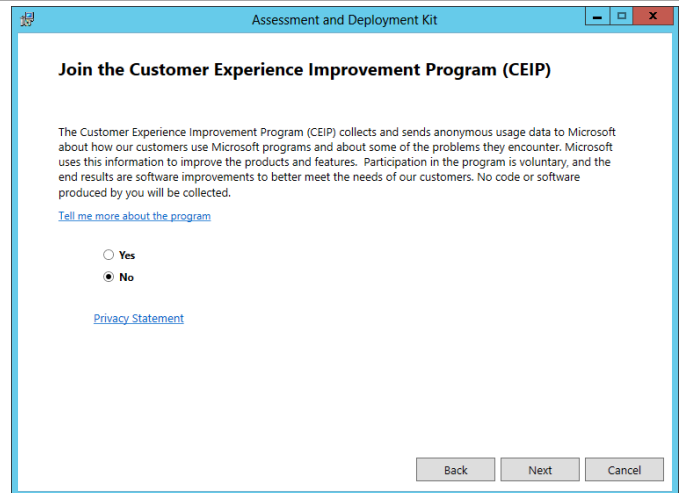
From the Windows ADK installation media source, right-click **adksetup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



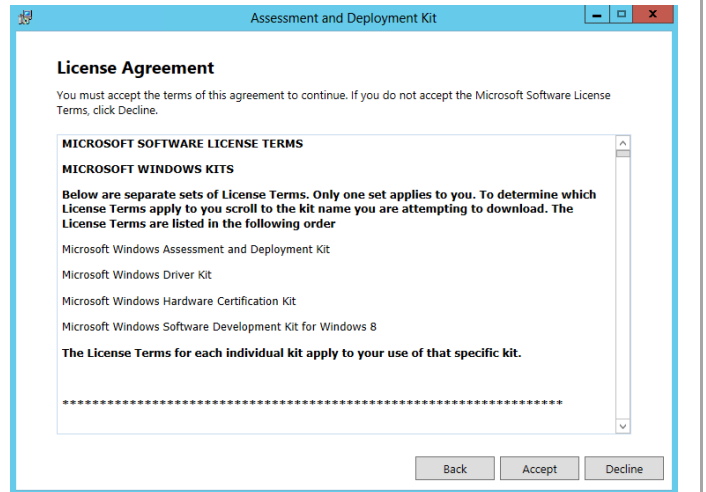
A splash screen will appear. In the **Specify Location** dialog, accept the default folder location of `%ProgramFiles%\Windows Kits\8.0` and click **Next** to continue.



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.



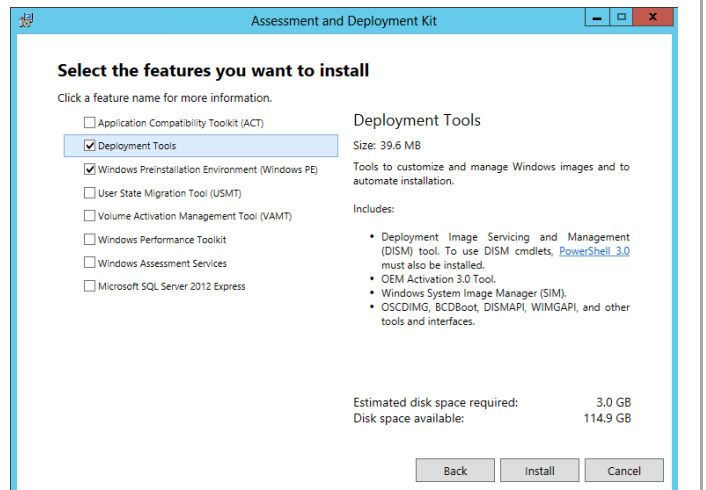
In the **License Agreement** dialog, click **Accept** to continue.



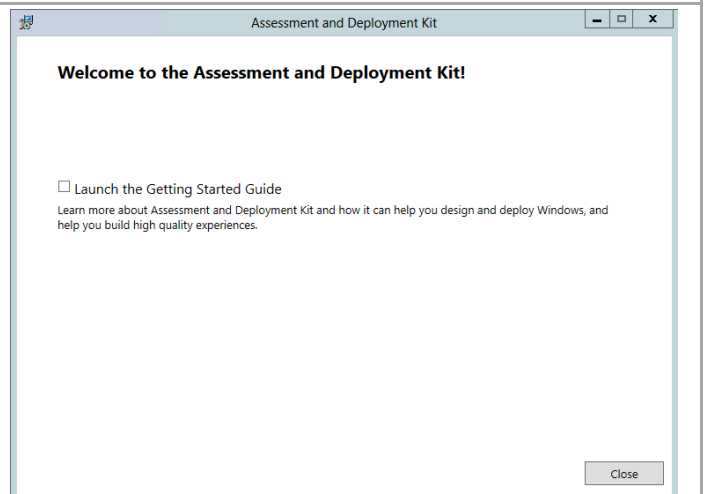
In the **Select the features you want to install** dialog, select the following option checkboxes:

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

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



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

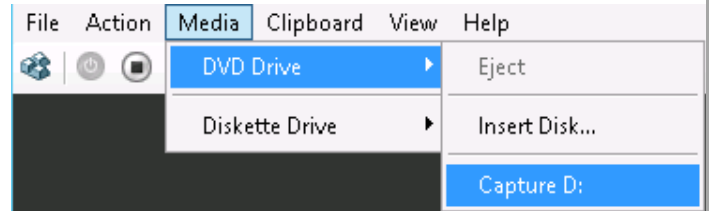


14.3 Install the Pre-requisite Windows Server Roles and Features

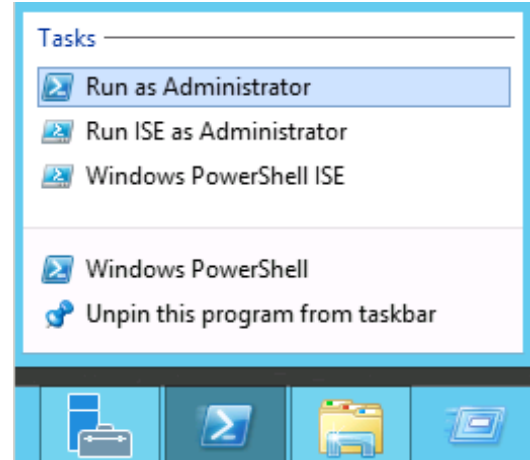
The Virtual Machine Manager installation requires the WSUS Administration Tools to be installed on the Virtual Machine Manager management servers. In addition, the MPIO and Failover Clustering Features must be installed. Follow the steps below to install the pre-requisite roles and features on the Virtual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

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

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**.

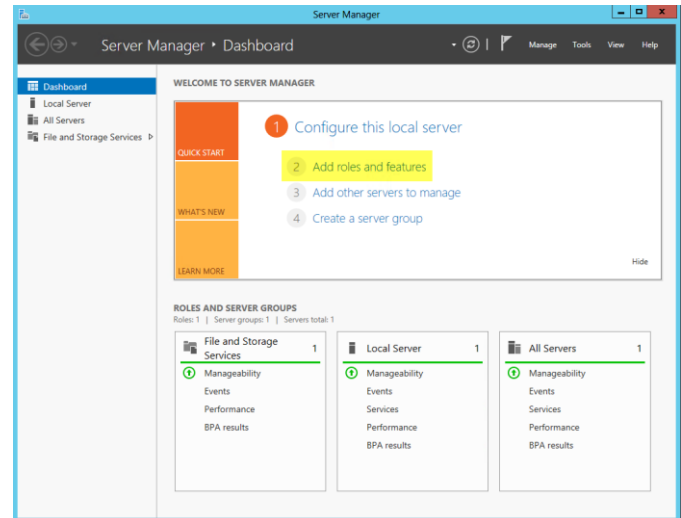


Add the .Net 3.5 feature by entering the following command:

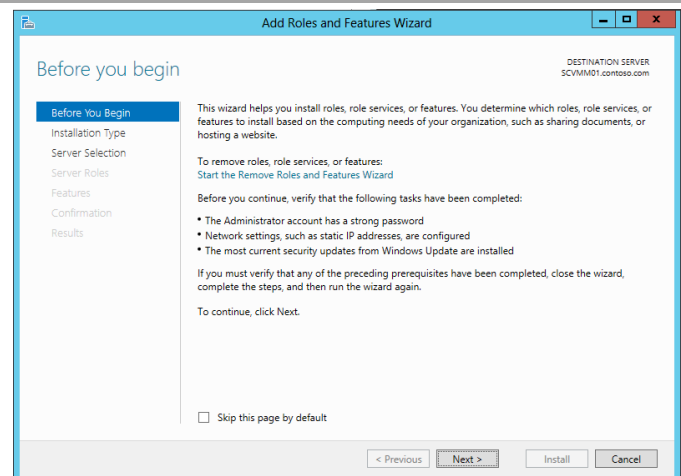
```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```

```
PS C:\Users\administrator.FLEXP00> Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
Success Restart Needed Exit Code      Feature Result
-----
True    No          Success      (.NET Framework 3.5 (includes .NET 2.0 and...
```


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.



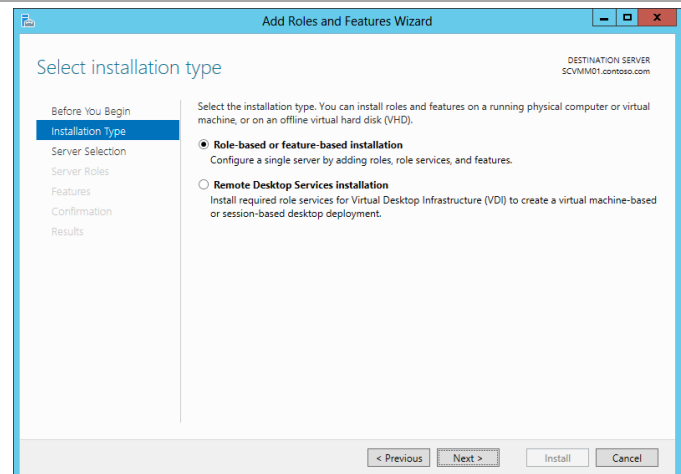
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, click **Next** to continue.



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.



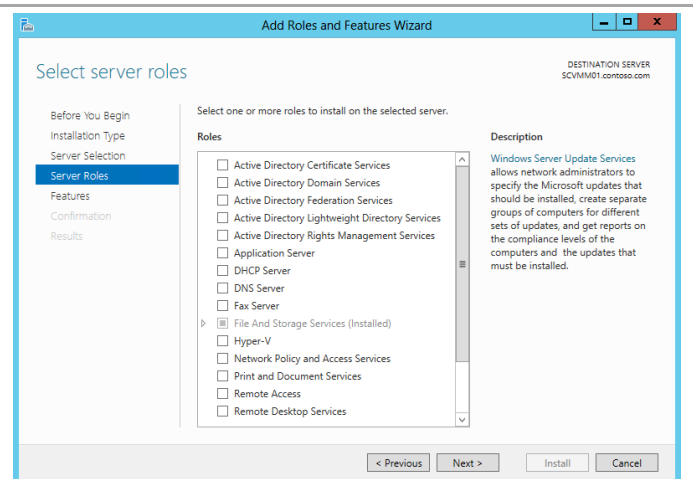
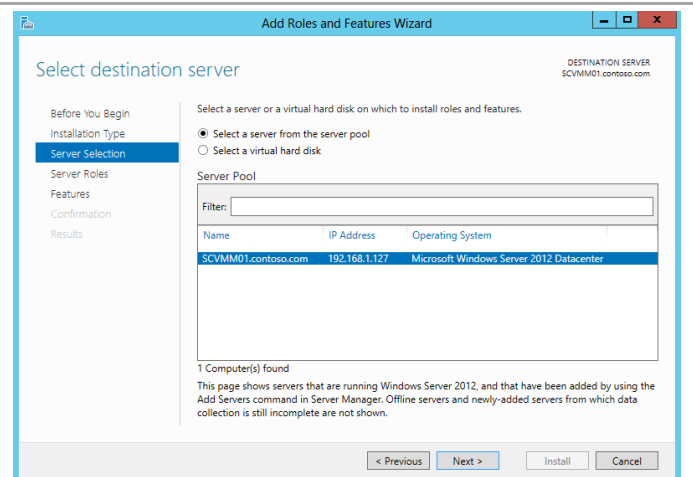
In the **Select destination server** dialog, you are presented with two options:

- *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.

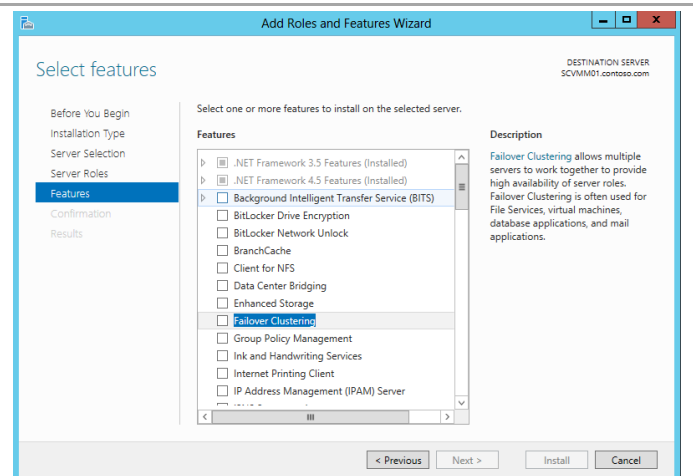
For this installation, select the **Select a server from the server pool** radio button, select the local server and click **Next** to continue.

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.

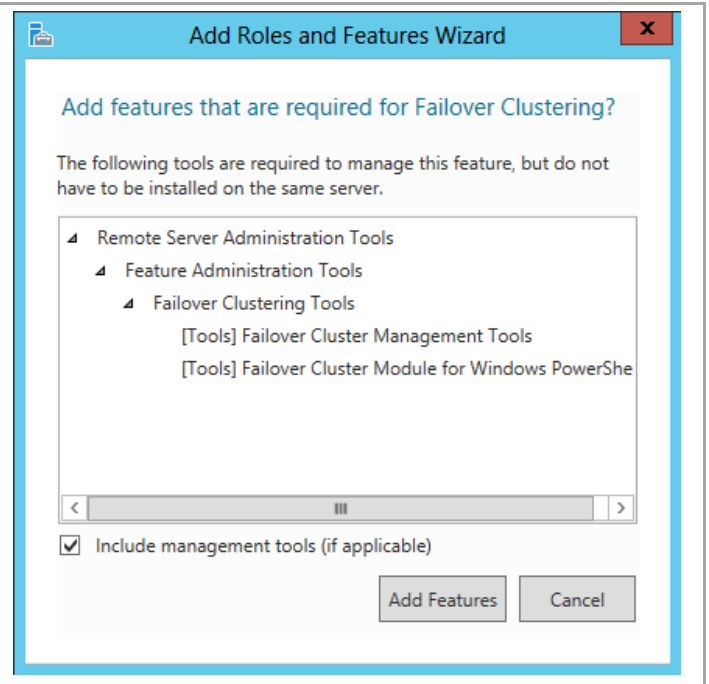
In the **Select Server Roles** dialog, do not make any additional selections and click **Next** to continue.



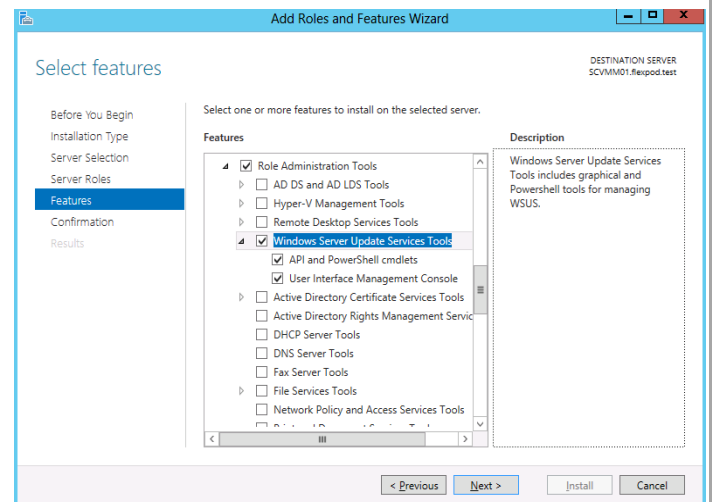
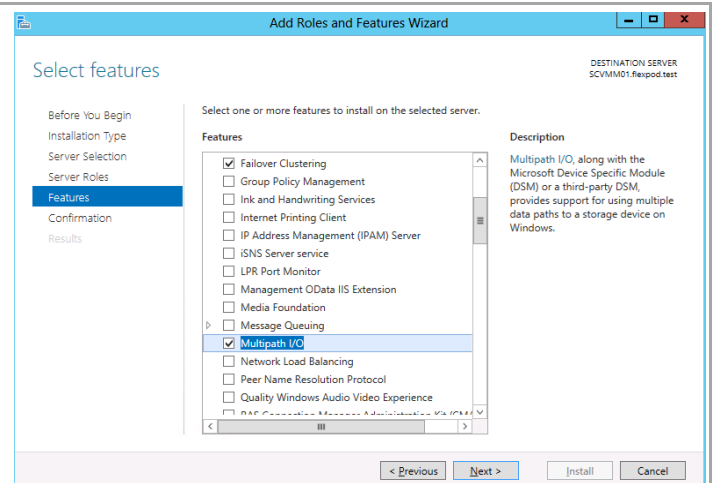
In the **Features** dialog, select **Failover Clustering**.



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.

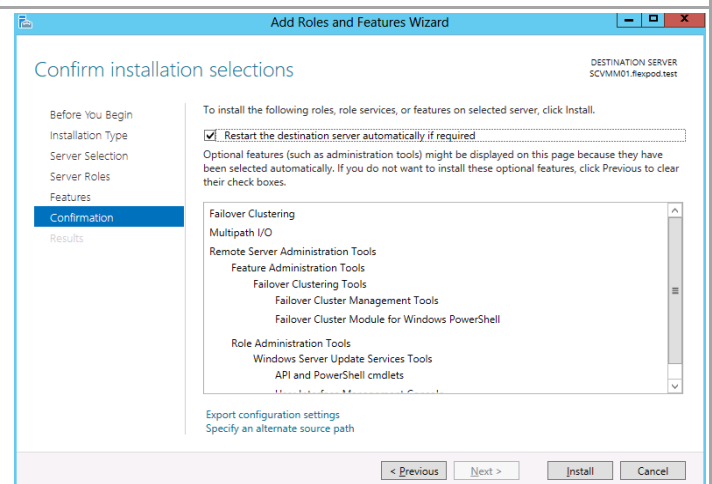


Next select the **Multipath I/O** and the **Windows Server Update Services Tools** top level features. Click Next to continue.

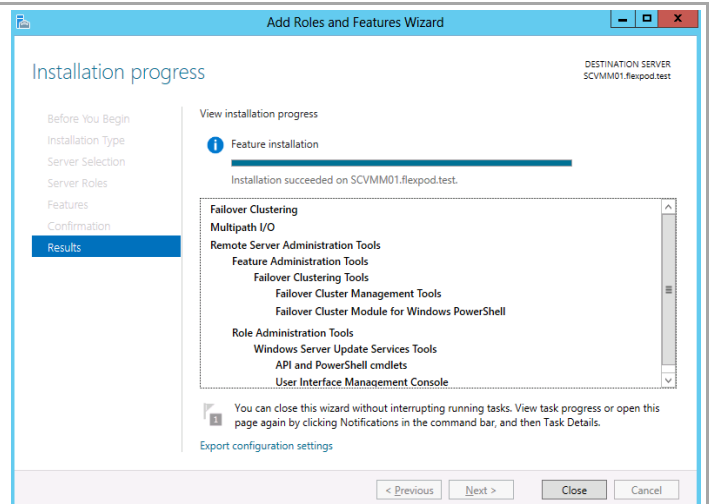


In the **Confirm installation selections** dialog, verify that the Multipath I/O and Failover Clustering features are selected. Ensure that the **Restart each destination server automatically if required** is selected. This is especially important for remote role/feature installation. Click **Install** to begin installation.

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

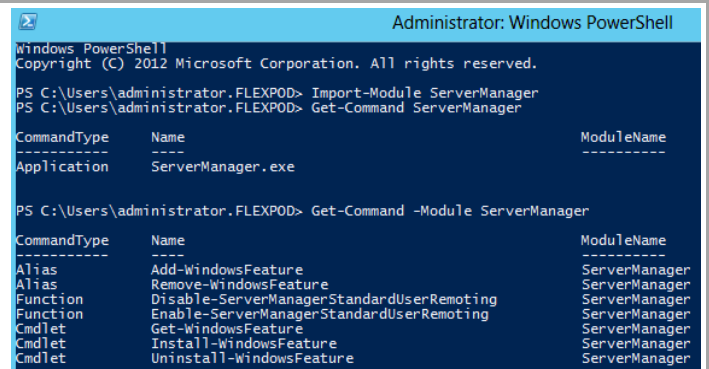


The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.



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

```
Add-WindowsFeature -Name Failover-Clustering,
Multipath-IO, UpdateServices-RSAT -
IncludeManagementTools -Restart
```



Install the SQL Server 2012 SP1 Command Line Utilities

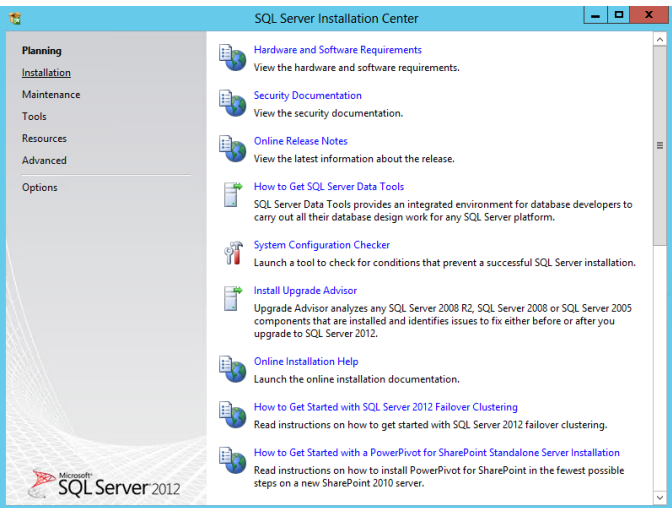
The Virtual Machine Manager installation requires that the SQL Server 2012 Command Line Utilities and Management Tools be installed on the Virtual Machine Manager management server. Follow the steps below to install the Command Line Utilities and Management Tools on the Virtual Machine Manager management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

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

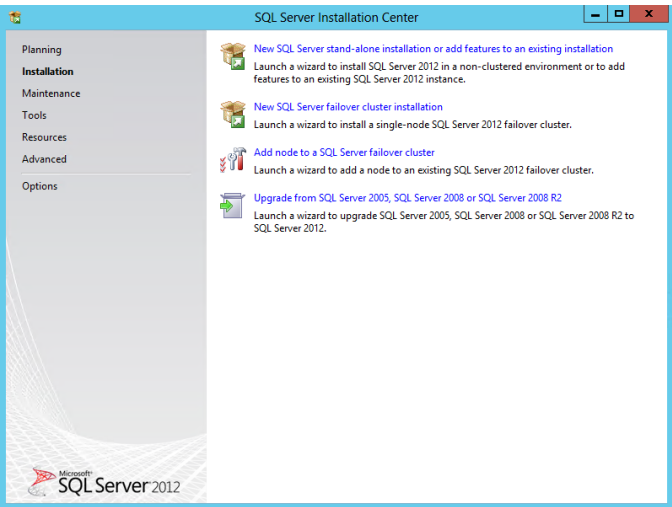
From the SQL Server 2012 with SP1 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

Name	Date modified	Type	Size
1033_ENU_LP	11/13/2012 4:45 PM	File folder	
boxstub_sql	11/13/2012 4:48 PM	File folder	
PCUSOURCE	11/13/2012 4:48 PM	File folder	
redist	11/13/2012 4:49 PM	File folder	
resources	11/13/2012 4:50 PM	File folder	
StreamInsight	11/13/2012 4:50 PM	File folder	
Tools	11/13/2012 4:50 PM	File folder	
x64	11/13/2012 4:53 PM	File folder	
autorun	2/10/2012 8:29 PM	Setup Information	1 KB
MedialInfo	10/20/2012 4:44 PM	XML Document	1 KB
setup	2012 3:21 AM	Application	197 KB
setup.e	2012 7:29 PM	CONFIG File	1 KB
sqmapi	2012 3:16 AM	Application extens...	147 KB

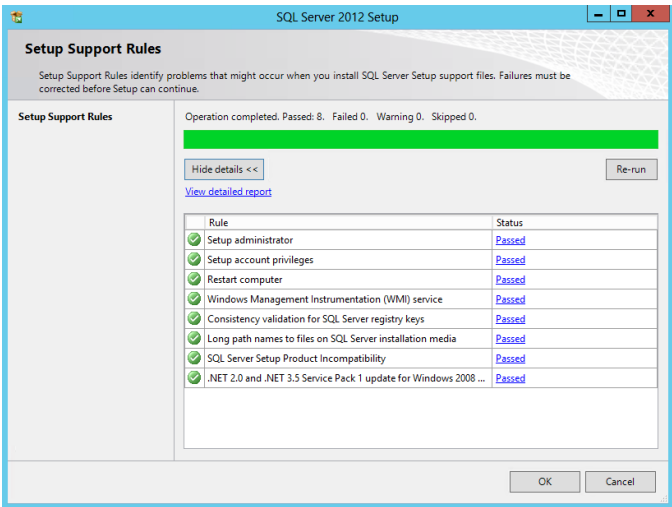
The **SQL Server Installation Center** will appear. Select **Installation**.



From the **SQL Server Installation Center**, click the **New installation or add features to an existing installation** link.

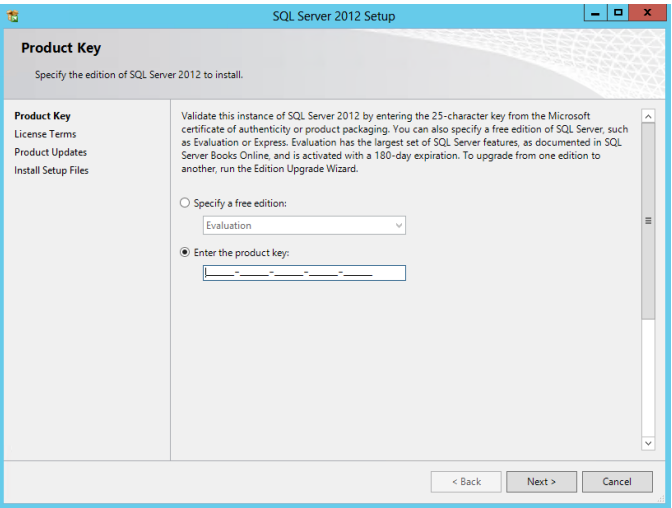


The **SQL Server 2012 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.

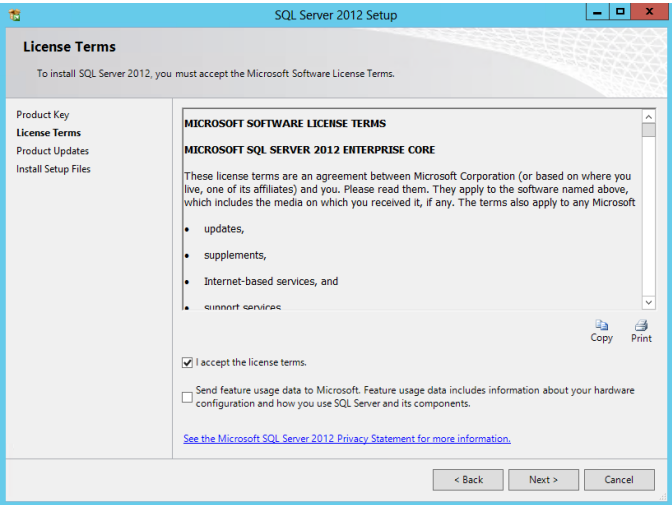


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

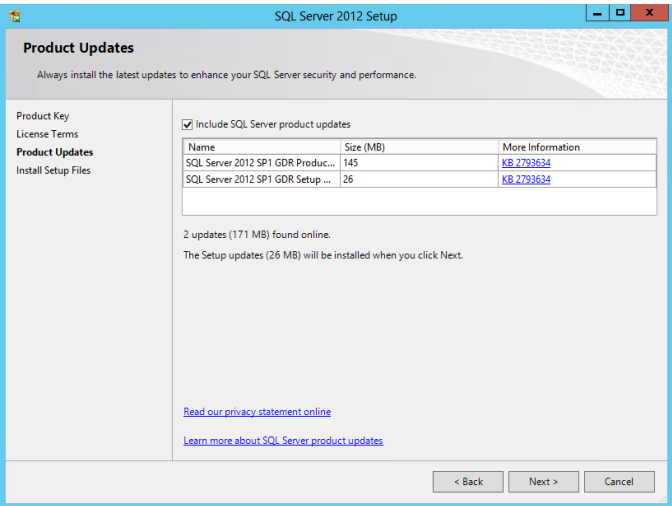
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



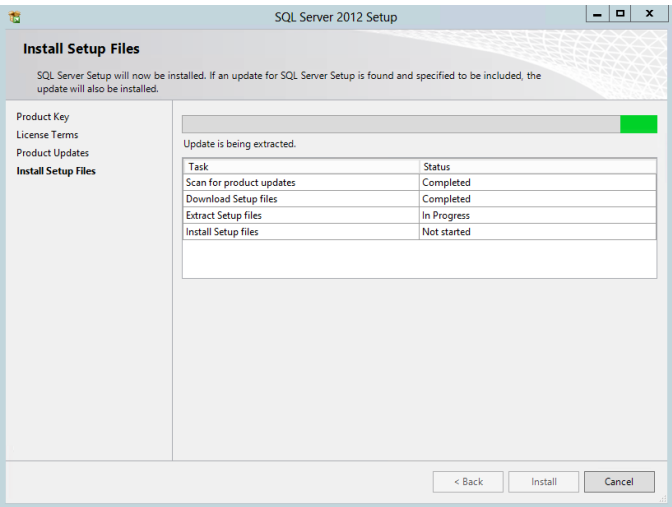
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** based on your organization's policies and click **Next** to continue.



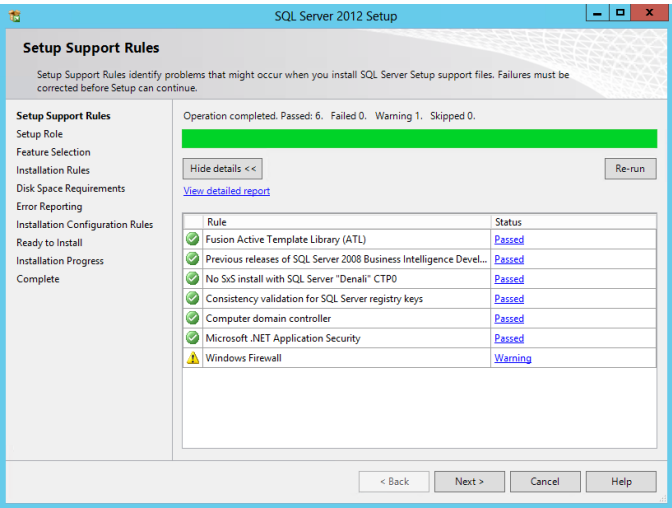
In the Product Updates dialog, leave the **Include SQL Server product updates**, selection checked and click **Next**.



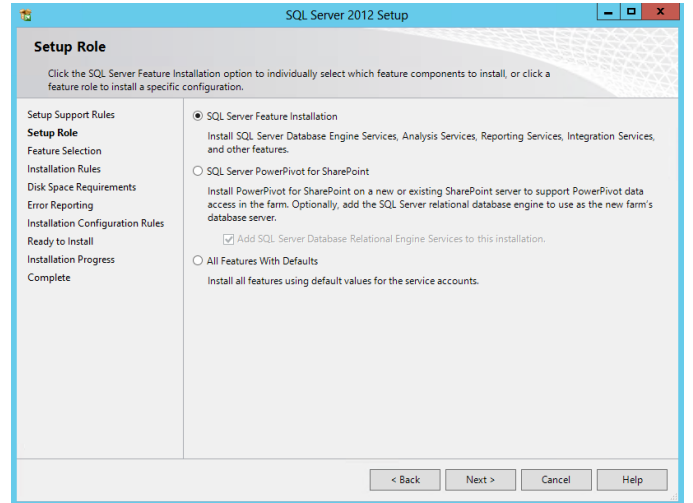
On the **Install Setup Files** dialog the update and install process will be displayed.



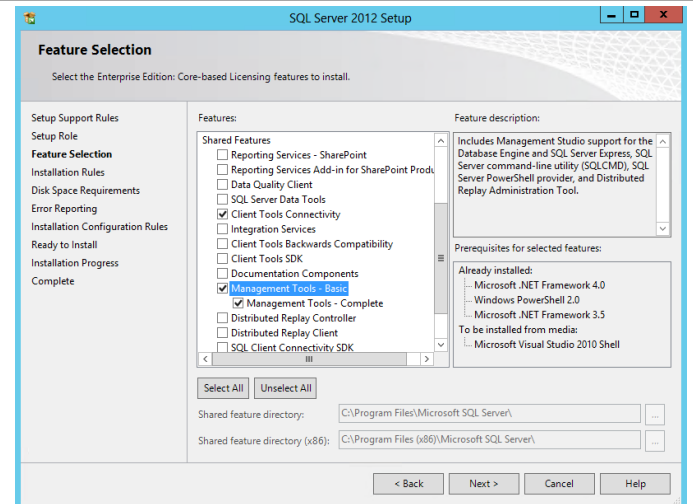
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



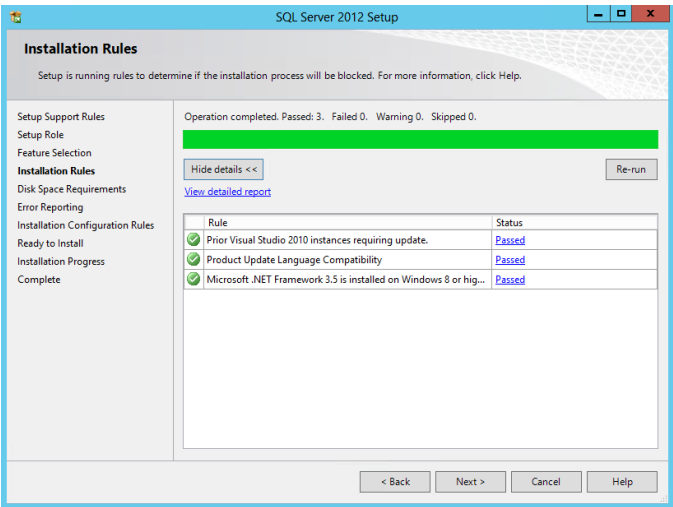
In the **Setup Role** dialog, select the **SQL Server Feature Installation** option and click **Next** to continue.



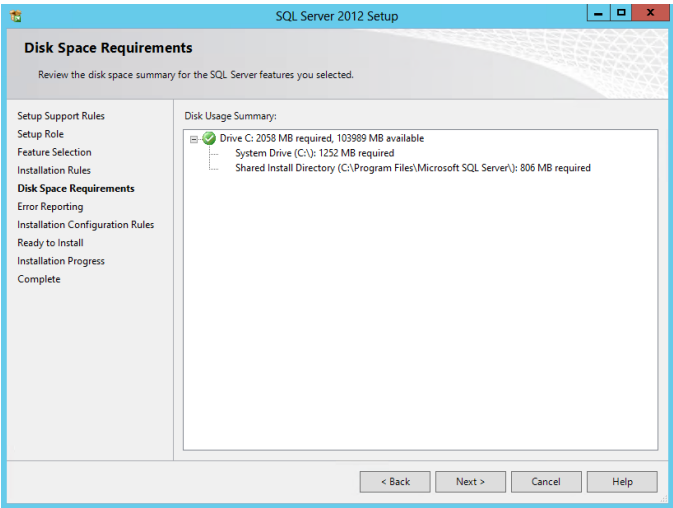
In the **Feature Selection** dialog, select the **Client Tools Connectivity, Management Tools – Basic** and **Management Tools – Complete** checkboxes. When all selections are made, click **Next** to continue.



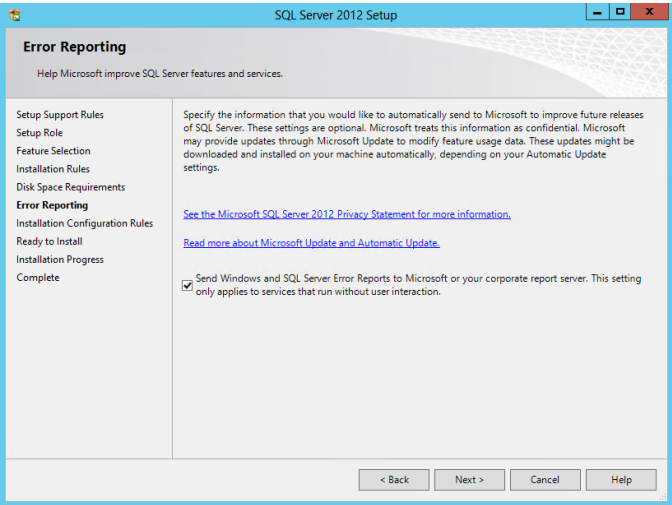
In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



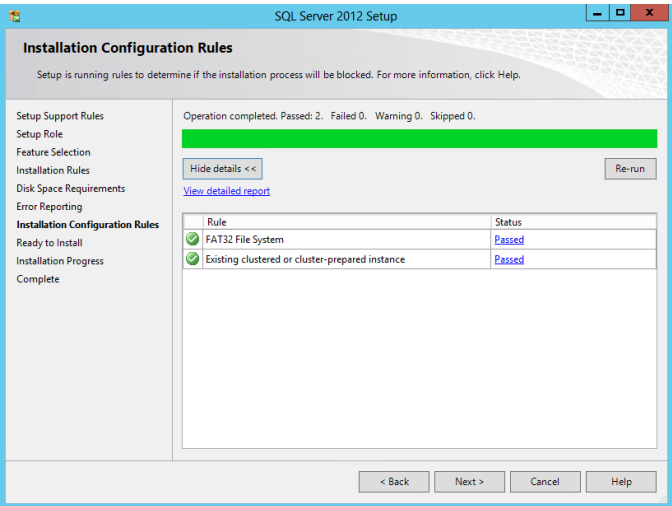
In the **Disk Space Requirements** dialog, verify that the installation has enough space on the target drive and click **Next** to continue.



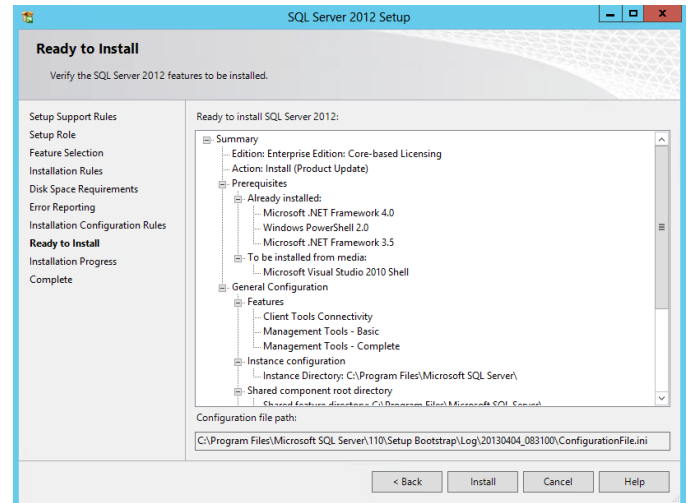
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization’s policies and click **Next** to continue.



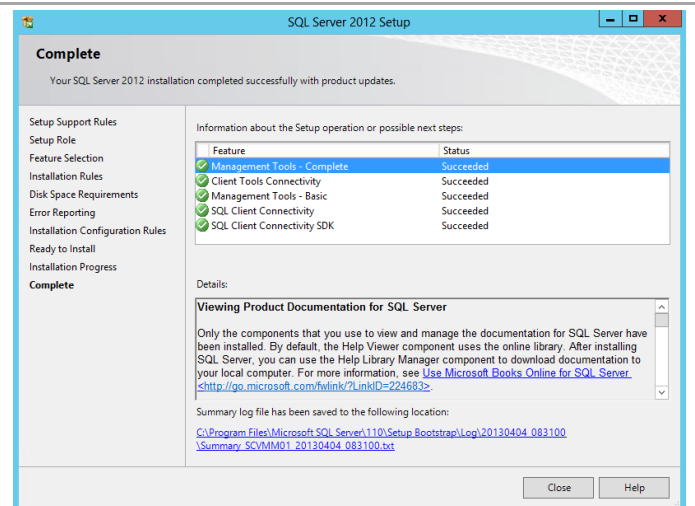
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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



Once complete, the **Complete** dialog will appear. Click **Close** to complete the installation of SQL Server tools.



Configure Windows MPIO

The following section describes how to configure Windows MPIO to claim NetApp Luns.

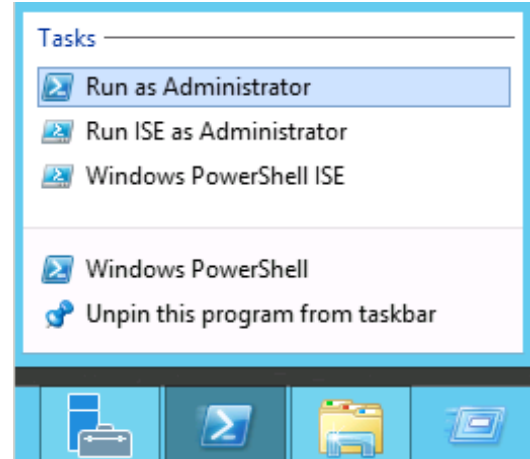
1. Configure Windows Server 2012 MSDSM to claim any NetApp LUNs.

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId LUN
New-MSDSMSupportedHW -VendorId NETAPP -ProductId "LUN C-Mode"
Update-MPIOClaimedHW
Restart-Computer
```

Create the Cluster

Create a the Windows Failover Cluster in the two Virtual Machine Manager virtual machines provisioned 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>, <Node2> -NoStorage -
StaticAddress <cluster_ip_address>
```

```
PS C:\Users\administrator.FLEXP00> New-Cluster -Name SCVMM-Cluster01 -Node SCVMM01, SCVMM02 -NoStorage -StaticAddress 19
2.168.1.70
Report File location: C:\Windows\cluster\Reports\Create Cluster Wizard SCVMM-Cluster01 on 2013.04.28 At 13.01.18.mht
Name
----
SCVMM-Cluster01
```

Rename the cluster networks to match there function.

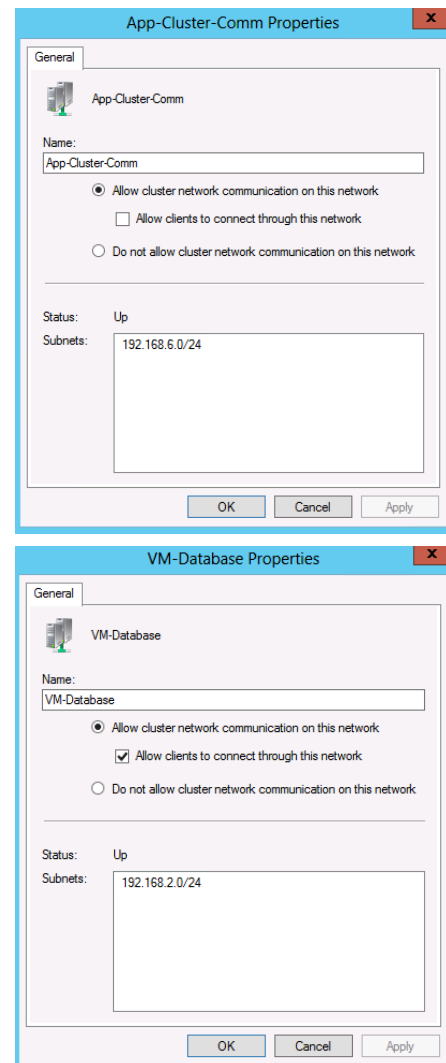
```
Get-ClusterNetworkInterface | ? Name -
like *VM-Database* | Group Network | %{
(Get-ClusterNetwork $_.Name).Name = 'VM-
Database'}

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

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 App-Cluster-Comm network.

Check Allow clients to connect through this network for the VM-Database network.



Create and Map the LUNs using SnapDrive

Create Virtual Machine Manager Cluster quorum LUN. Perform this action from the one node in the Virtual Machine Manager Cluster.

These steps provide details for creating Virtual Machine Manager Cluster quorum LUN.

1. Start a Windows PowerShell session on the SQL Server node and import the Data ONTAP PowerShell Toolkit module.

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

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

```
New-NcQtree -Volume quorum -Qtree scvmm_cluster01
```

4. Create the SQL Server database LUNs.

```
New-NcLun /vol/quorum/scvmm_cluster01/scvmm-cluster01-quorum.lun -Size 1gb -OsType windows_2008 -Unreserved
```

5. Create the NetApp igroup for the SQL Server Cluster LUNs.

```
New-NcIgroup -Name scvmm_cluster01 -Protocol fcp -Type windows
```

9. Add the WWPN of the Hyper-V virtual fibre channel HBAs to the SQL Server cluster igroup.

```
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM01-A-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM01-A-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM01-B-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM01-B-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM02-A-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM02-A-SetB_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM02-B-SetA_WWPN>
Add-NcIgroupInitiator -Igroup scvmm-cluster01 -Initiator < vFC-SCVMM02-B-SetB_WWPN>
```

6. Map the SQL Server database LUNs to the new iGroup, initialize the new LUNs, assign a drive letter and format the volume.

```
Add-NcLunMap -Path /vol/quorum/scvmm_cluster01/scvmm-cluster01-quorum.lun -InitiatorGroup scvmm-cluster01
```

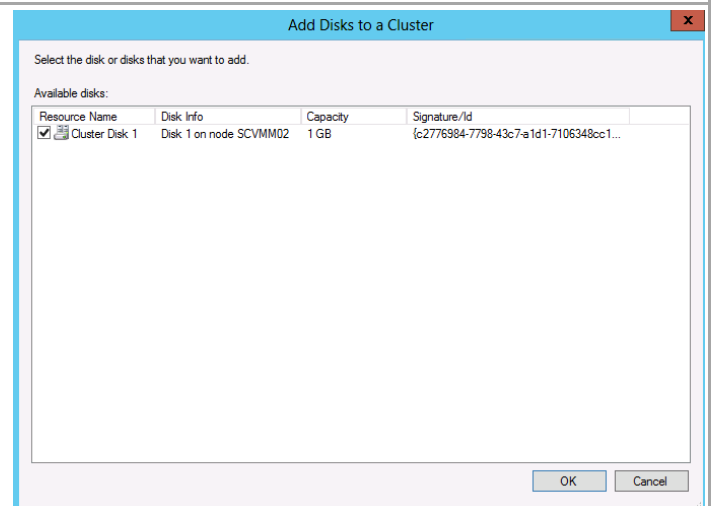
```
get-disk | Where-Object PartitionStyle -EQ RAW | Initialize-Disk -PassThru | New-Partition -UseMaximumSize | Format-Volume -NewFileSystemLabel "Cluster_Quroum"
```

Assign SQL Cluster Disk Names

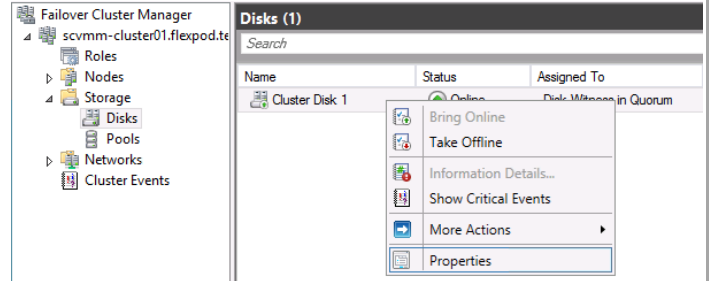
Select the **VMM Server cluster** in the left tree view. Expand the **Storage** object and select **Disks**. Right click each disk in the middle pane. Click **Add Disk** in the Action pane.



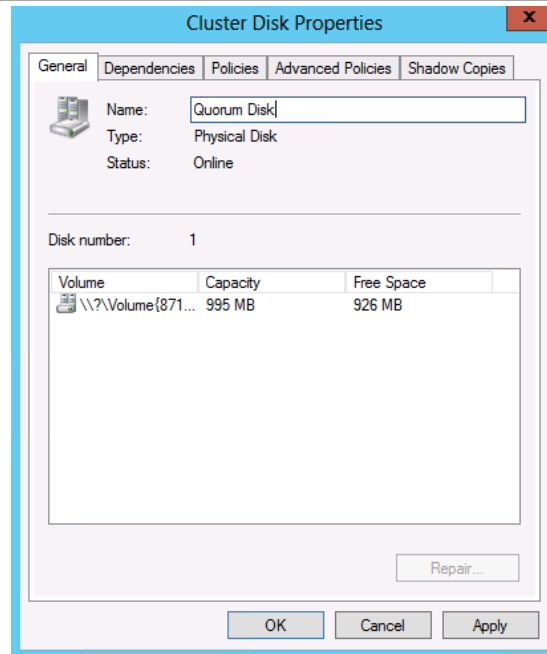
Verify that the disks is checked and click **OK**.



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



In the Name field, enter the name Quorum Disk and click OK.

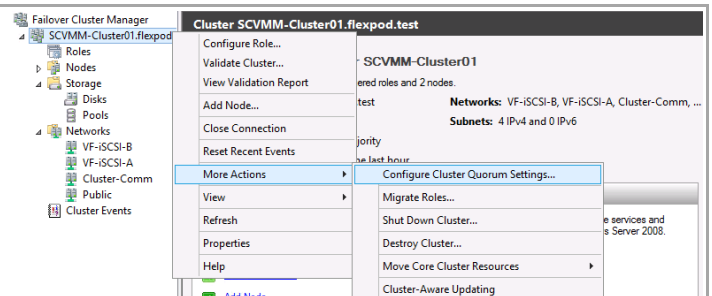


Change the VMM Server Cluster to Use a Quorum Disk

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**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Select Quorum Configuration Option'. On the left, a navigation pane lists steps: 'Before You Begin', 'Select Quorum Configuration Option' (highlighted), 'Select Quorum Witness', 'Confirmation', 'Configure Cluster Quorum Settings', and 'Summary'. The main area contains the text: 'Select a quorum configuration for your cluster.' followed by three radio button options: 'Use typical settings (recommended)' (with subtext 'The cluster determines quorum management options and, if necessary, selects the quorum witness.'), 'Add or change the quorum witness' (selected, with subtext 'You can select the quorum witness. The cluster determines quorum management options.'), and 'Advanced quorum configuration and witness selection' (with subtext 'You determine the quorum management options and the quorum witness.'). A link 'Failover Cluster Quorum and Witness Configuration Options' is at the bottom. Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom right.

Select **Configure a disk witness** and click **Next**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Select Quorum Witness'. The left navigation pane is the same as the previous screen, with 'Select Quorum Witness' highlighted. The main area contains information: 'Nodes that are configured to be members of the cluster: 2', 'Nodes that are assigned votes to participate in quorum calculations: 2', and 'Cluster dynamically manages vote assignment: Enabled'. Below this, it says 'Select to add or change the quorum witness for your cluster configuration. The recommendations are based on providing the highest availability for your cluster.' There are three radio button options: 'Configure a disk witness (recommended for your current configuration)' (selected, with subtext 'Adds a quorum vote of the disk witness'), 'Configure a file share witness (recommended for special configurations)' (with subtext 'Adds a quorum vote of the file share witness'), and 'Do not configure a quorum witness (not recommended for your current configuration)'. The same link and navigation buttons are present at the bottom.

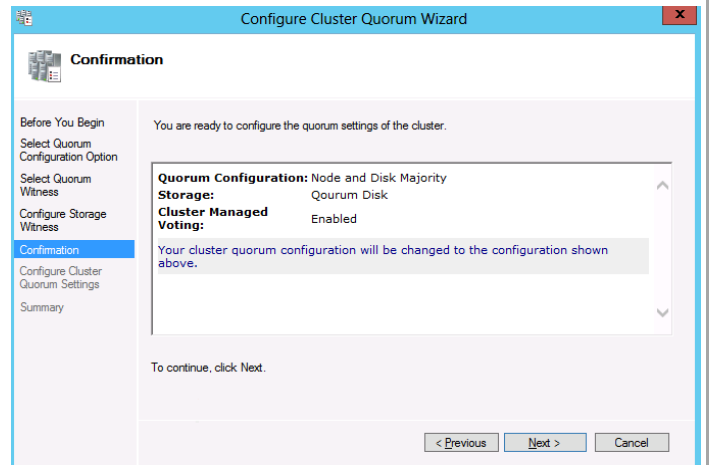
Select the **LUN** without a drive letter that was previously created to be the quorum LUN. Click **Next**.

The screenshot shows the 'Configure Cluster Quorum Wizard' window. The title bar reads 'Configure Cluster Quorum Wizard'. The main heading is 'Configure Storage Witness'. The left navigation pane is the same, with 'Configure Storage Witness' highlighted. The main area contains the text: 'Select the storage volume that you want to assign as the disk witness.' Below this is a table with columns: 'Name', 'Status', 'Node', and 'Location'.

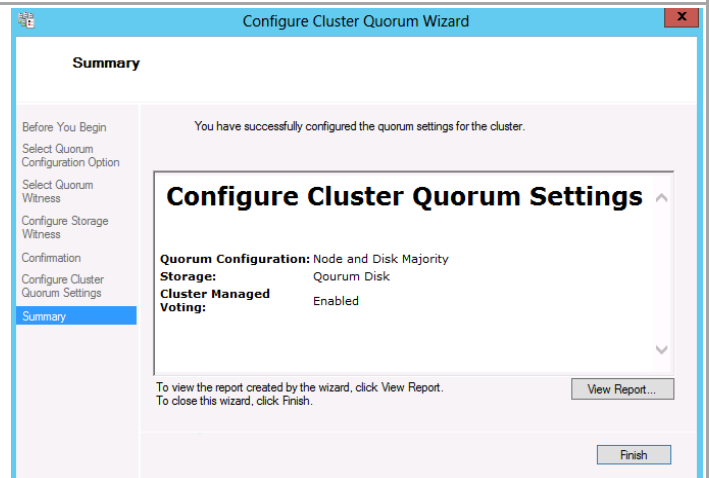
Name	Status	Node	Location
<input checked="" type="checkbox"/> Goum Disk Volume: (\?\?...) File System: NTFS	Online	SCVMM01	Available Storage

The table shows one entry with a checked checkbox. At the bottom right are the navigation buttons '< Previous', 'Next >', and 'Cancel'.

Confirm the settings and click **Next**.

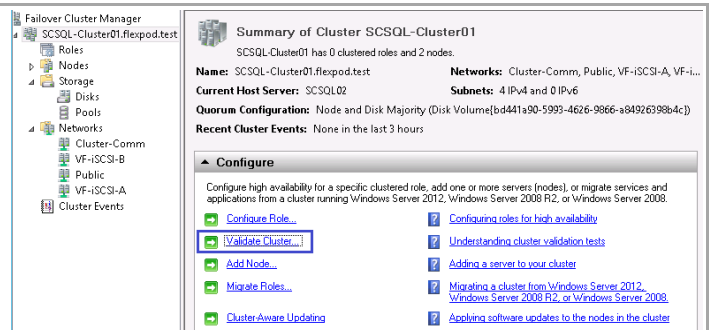


Review the results and click **Finish** to close the wizard screen.



Validated the VMM Server Cluster

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



Select **Run all tests** and click Next.

The screenshot shows the 'Testing Options' step of the 'Validate a Configuration Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Testing Options' (highlighted), 'Review Storage Status', 'Confirmation', 'Validating', and 'Summary'. The main area has the following text:

Choose between running all tests or running selected tests.

The tests examine the Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration.

Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in this wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2012."

There are two radio buttons:

- ☒ Run all tests (recommended)
- ☐ Run only tests I select

Below the radio buttons is a link: [More about cluster validation tests](#).

At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

Select all the disks on the cluster and Click Next.

The screenshot shows the 'Review Storage Status' step of the 'Validate a Configuration Wizard'. The left sidebar is the same as the previous screen, with 'Review Storage Status' highlighted. The main area has the following text:

You can select additional storage to validate from the list below.

Name	Assigned To
<input checked="" type="checkbox"/> Qorum Disk	Disk Witness in Quorum

Below the table is a warning icon and text: "To avoid role failures, it is recommended that all roles using this Cluster Shared Volume be stopped before the storage is validated."

At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

Confirm the selected options and click **Next**.

The screenshot shows the 'Confirmation' step of the 'Validate a Configuration Wizard'. The left sidebar is the same as the previous screens, with 'Confirmation' highlighted. The main area has the following text:

You are ready to start validation. Please confirm that the following settings are correct:

Servers to Test

- SCVMM01.flexpod.test
- SCVMM02.flexpod.test

Tests Selected by the User

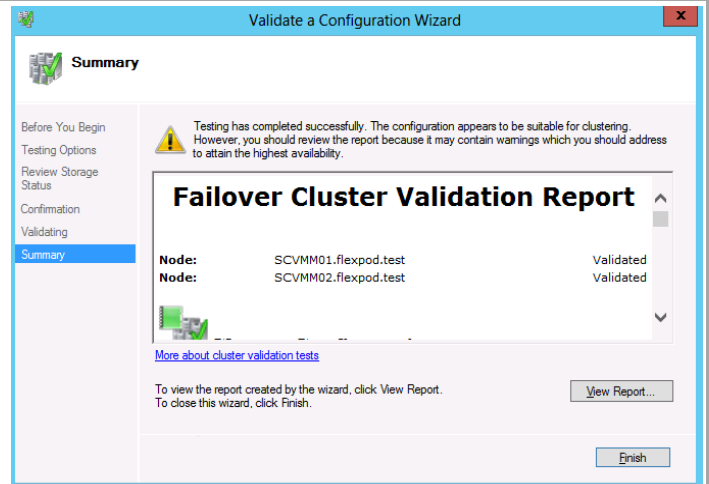
Tests Selected by the User	Category
List Cluster Core Groups	Cluster Configuration
List Cluster Network Information	Cluster Configuration
List Cluster Resources	Cluster Configuration
List Cluster Volumes	Cluster Configuration
List Clustered Roles	Cluster Configuration

Below the lists is the text: "To continue, click Next." and a link: [More about cluster validation tests](#).

At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

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

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



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

Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node SCVMM01.flexpod.test.

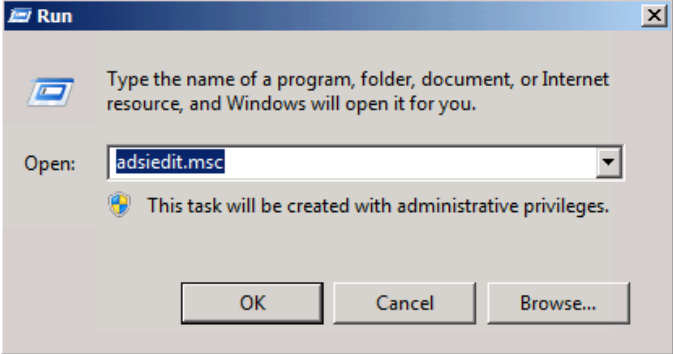
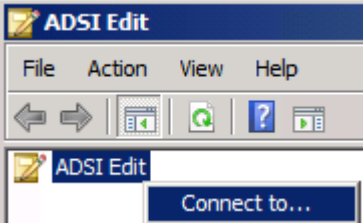
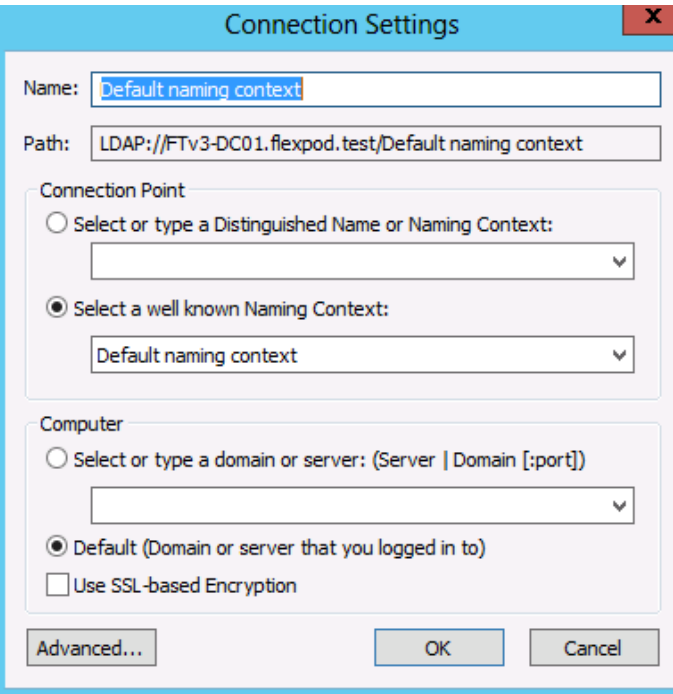
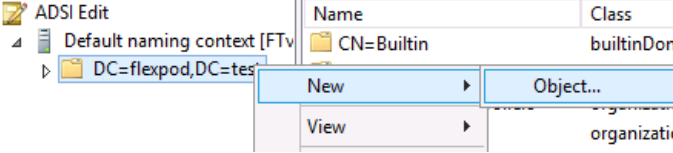
Test Disk 0 does not support SCSI-3 Persistent Reservations commands needed to support clustered Storage Pools. Some storage devices require specific firmware versions or settings to function properly with failover clusters. Please contact your storage administrator or storage vendor to check the configuration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

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

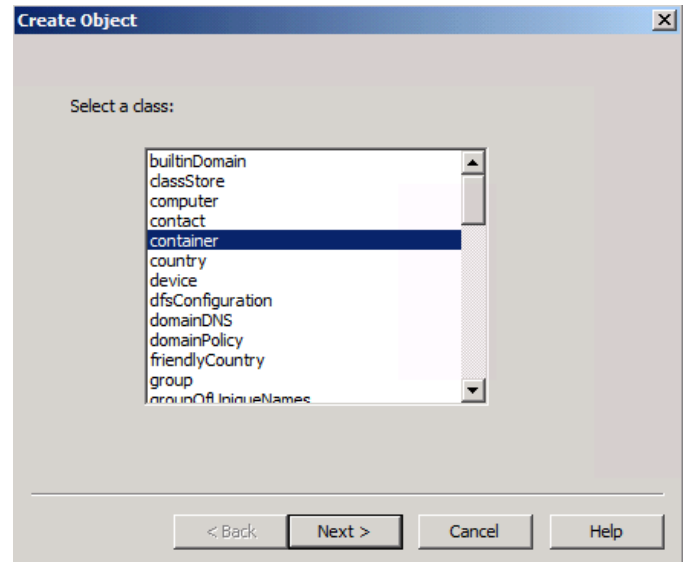
The Virtual Machine Manager installation requires that an Active Directory container be created to house the distributed key information for Virtual Machine Manager.⁸ **Note:** *if Virtual Machine Manager will be deployed using an account with rights to create containers in AD DS this step can be skipped.* Perform the following steps to create an AD DS container to house the distributed key information. These instructions assume a Windows Server 2008 R2 domain controller is in use, similar steps would be followed for other versions of Active Directory including Windows Server 2008 and Windows Server 2012.

- ▶ Perform the following steps on a **Domain Controller** in the domain where Virtual Machine Manager is to be installed.

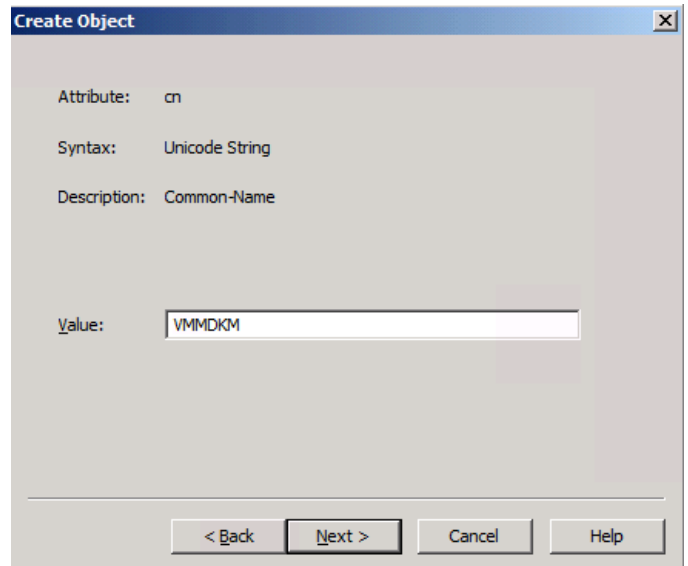
⁸ Configuring Distributed Key Management in VMM - <http://technet.microsoft.com/library/gg697604.aspx>.

<p>Log on to a Domain Controller with a user that has Domain Admin privileges and run adsiedit.msc.</p>	 <p>The Run dialog box is open, showing 'adsiedit.msc' in the 'Open:' field. Below the field, it says 'This task will be created with administrative privileges.' The 'OK' button is highlighted.</p>
<p>Right-click the ADSI Edit node and select Connect to... from the context menu.</p>	 <p>The ADSI Edit application window is shown. The 'Connect to...' option is highlighted in the context menu.</p>
<p>In the Connections Settings dialog in the Connection Point section, select the Select a well known Naming Context option. Select Default naming context from the drop-down menu and click OK.</p>	 <p>The Connections Settings dialog box is open. In the 'Connection Point' section, the radio button for 'Select a well known Naming Context' is selected. The drop-down menu below it shows 'Default naming context'. The 'OK' button is highlighted.</p>
<p>Expand <i>Domain Default naming context</i> [<i><computer fully qualified domain name></i>], expand <i><distinguished name of domain></i>, right-click the root node and select New – Object... from the context menu.</p>	 <p>The ADSI Edit tree view is shown. The 'DC=flexpod,DC=test' node is selected. The context menu is open, and 'New - Object...' is highlighted.</p>

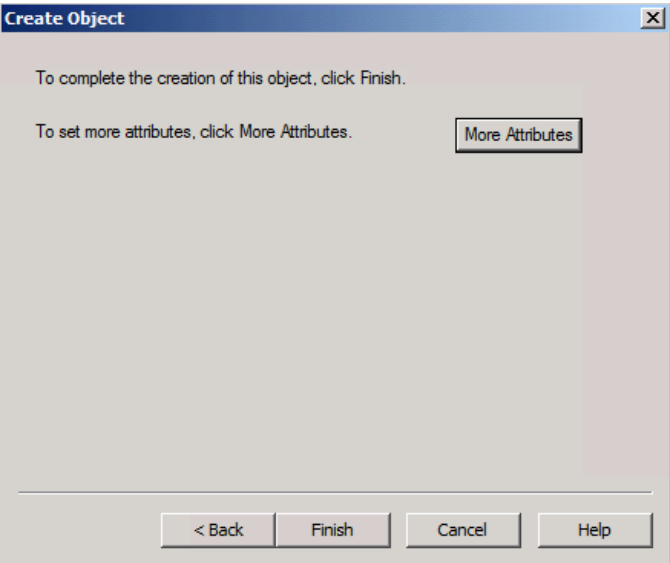
In the **Create Object** dialog box, select **Container** and then click **Next**.



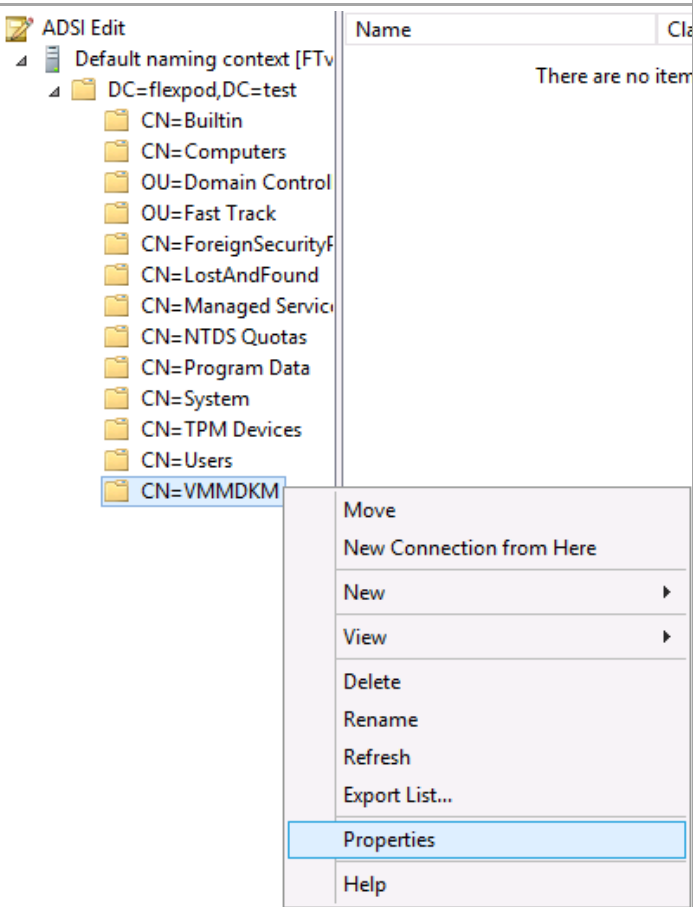
In the **Value** text box, type *VMMDKM* and then click **Next**.



Click **Finish** to create the container object.

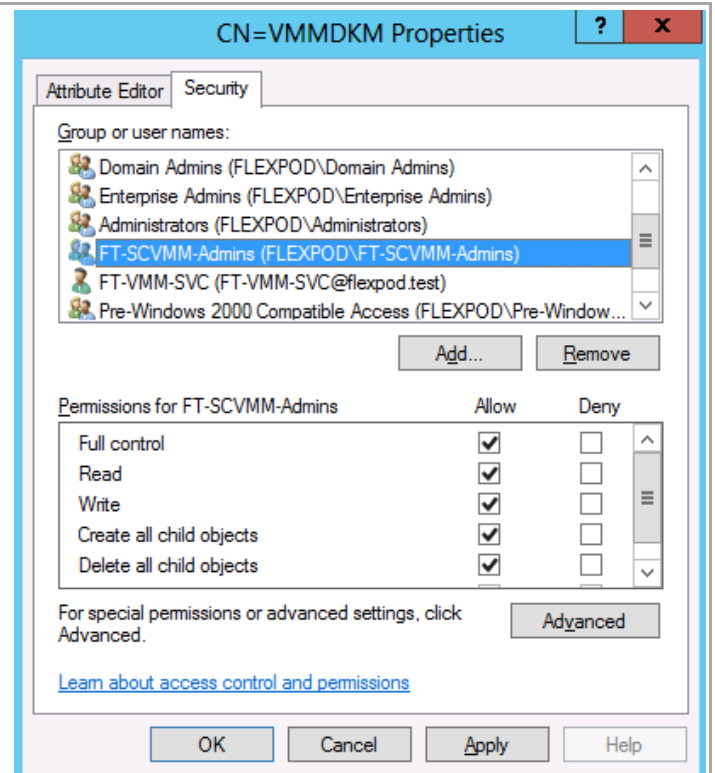


Within ADSI Edit, right-click the new **VMMDKM** object and then click **Properties**.



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

Click **OK** three times and close ADSI Edit.



14.4 Installation

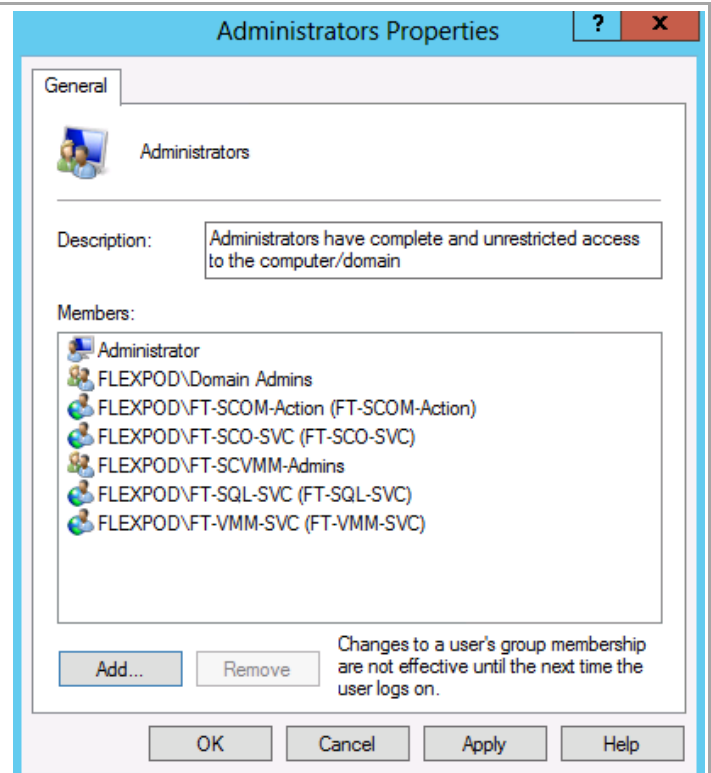
Install the Virtual Machine Manager Failover Cluster

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

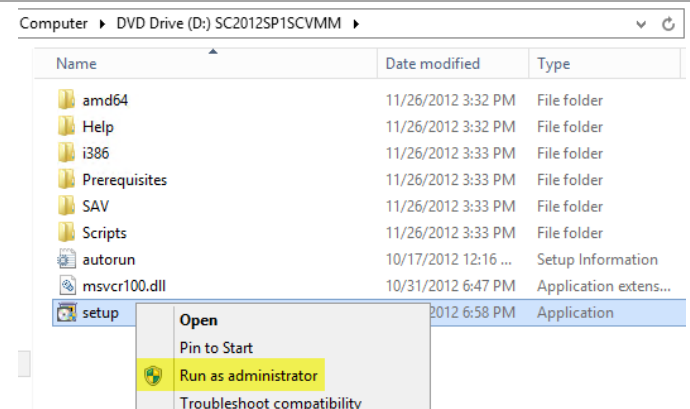
Log on to the Virtual Machine Manager virtual machine with a user with local admin rights.

Verify the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager virtual machine:

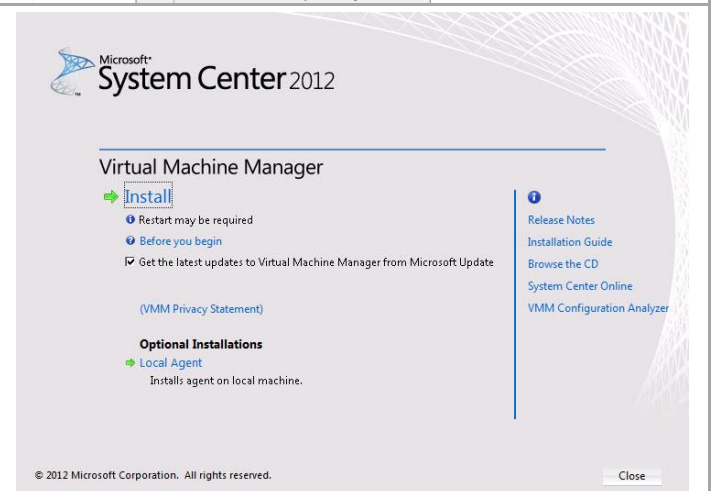
- Orchestrator service account.
- Operations Manager action account.
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.
- SQL Server service account.



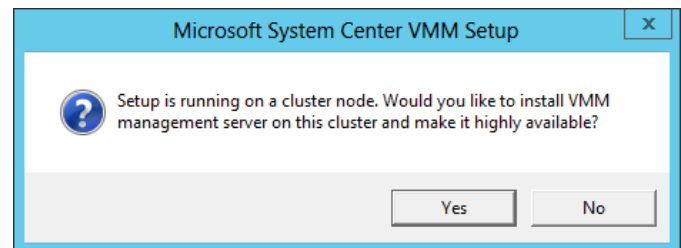
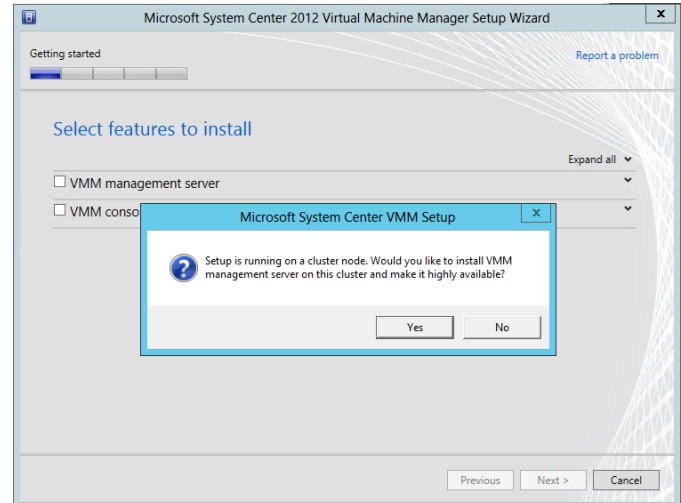
From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup. If prompted by user account control, select **Yes** to allow the installation to make changes to the computer.



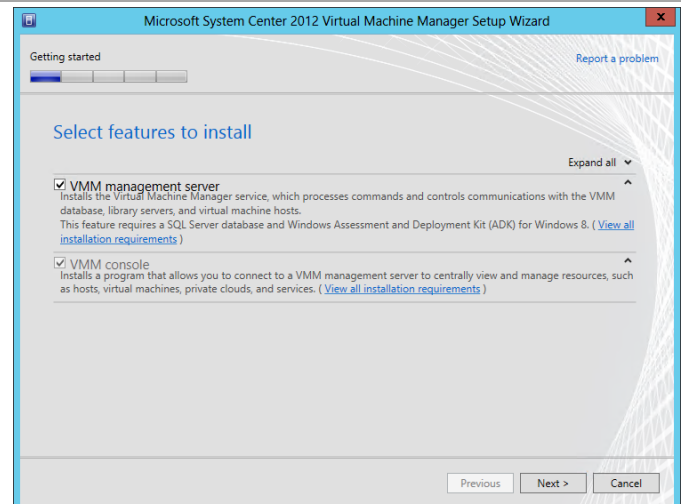
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



Attempting to select any feature will cause the cluster management server notice to appear.
Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard.



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



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

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

Click **Next** to continue.

The screenshot shows the 'Product registration information' dialog box. It has a title bar 'Microsoft System Center 2012 Virtual Machine Manager Setup Wizard' and a progress bar at the top. The main area contains three text input fields: 'Name' (with 'Fast Track' entered), 'Organization' (with 'FlexPod' entered), and 'Product key' (empty). Below the fields is a blue information icon and a note: 'If you don't provide a product key during setup, VMM will be installed as an evaluation edition. You can provide a product key after setup is complete by using the VMM console.' At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

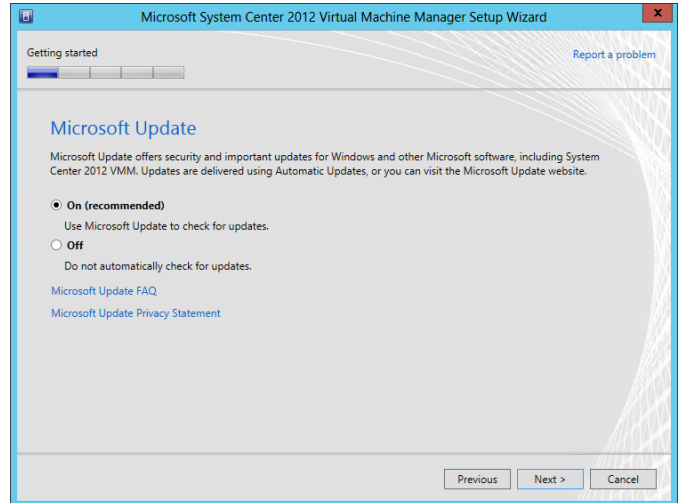
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option checkbox is selected and click **Next** to continue.

The screenshot shows the 'Please read this license agreement' dialog box. It has a title bar 'Microsoft System Center 2012 Virtual Machine Manager Setup Wizard' and a progress bar. The main area displays the 'MICROSOFT EVALUATION SOFTWARE LICENSE TERMS' and 'MICROSOFT SYSTEM CENTER 2012 STANDARD SERVICE PACK 1'. Below the terms is a list of bullet points: 'updates', 'supplements', 'Internet-based services, and', 'support services'. At the bottom, there is a checkbox labeled 'I have read, understood, and agree with the terms of the license agreement' which is checked. To the right of the checkbox is a 'Print' button. At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

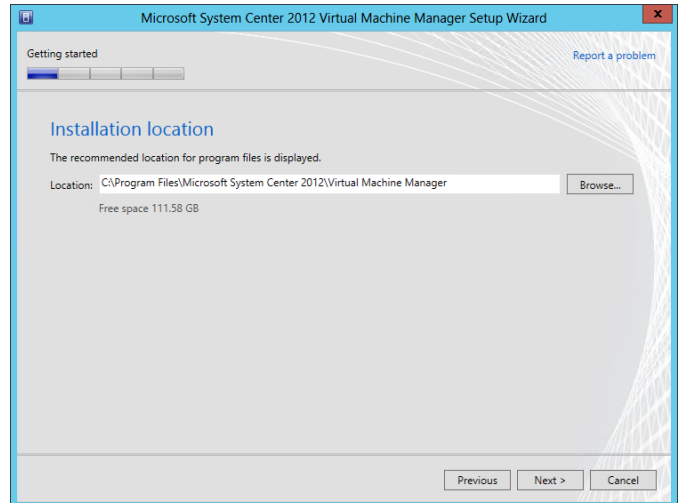
In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.

The screenshot shows the 'Customer Experience Improvement Program (CEIP)' dialog box. It has a title bar 'Microsoft System Center 2012 Virtual Machine Manager Setup Wizard' and a progress bar. The main area contains text about the CEIP, including 'If you choose to participate:', 'Microsoft will', and 'Microsoft will not'. Below this is a list of radio buttons: 'Yes, I am willing to participate in the Customer Experience Improvement Program' (selected) and 'No, I am not willing to participate'. At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.



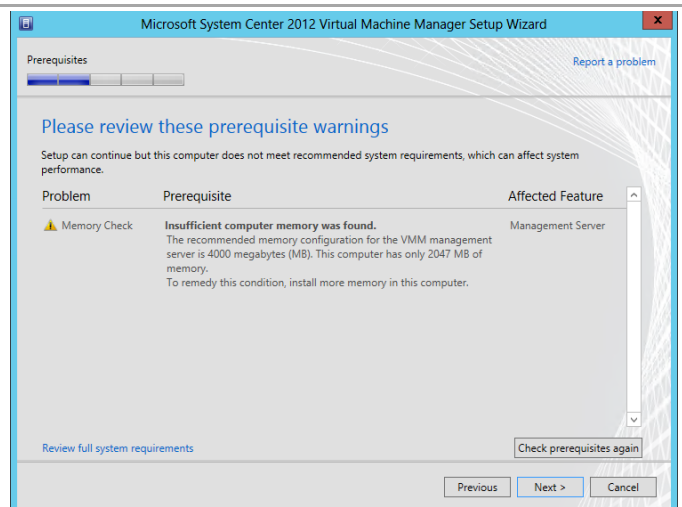
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.



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

The following is just an example of that UI.

If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



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

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

The screenshot shows the 'Database configuration' step of the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard. The dialog has a title bar with the text 'Microsoft System Center 2012 Virtual Machine Manager Setup Wizard' and a 'Report a problem' link. Below the title bar is a progress bar and a 'Configuration' section. The main area is titled 'Database configuration' and contains the following fields and options:

- Server name:** SCVMMDB (with a 'Browse' button)
- Port:** (empty text box)
- ☐ **Use the following credentials**
- User name and domain:** (empty text box, with a 'Format: Domain\UserName' hint)
- Password:** (empty text box)
- Instance name:** SCVMMDB (dropdown menu)
- Select an existing database or create a new database:**
 - ☒ **New database:** VirtualManagerDB
 - ☐ **Existing database:** (empty dropdown menu)

At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

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.

The screenshot shows the 'Cluster configuration' step of the Microsoft System Center 2012 Virtual Machine Manager Setup Wizard. The dialog has a title bar with the text 'Microsoft System Center 2012 Virtual Machine Manager Setup Wizard' and a 'Report a problem' link. Below the title bar is a progress bar and a 'Configuration' section. The main area is titled 'Cluster configuration' and contains the following fields and options:

- Type the name that clients will use when accessing this service or application:**
 - Name:** SCVMMHA01
- One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.**
- | Networks | Address |
|----------------------------------------------------|--------------|
| <input checked="" type="checkbox"/> 192.168.2.0/24 | 192.168.2.72 |

At the bottom are 'Previous', 'Next >', and 'Cancel' buttons.

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.

The screenshot shows the 'Configure service account and distributed key management' dialog box. Under 'Virtual Machine Manager Service Account', the 'Domain account' radio button is selected. The 'User name and domain' field contains 'FLEXPOD\FT-VMM-SVC' and the 'Password' field is masked with dots. A 'Select...' button is next to the password field. In the 'Distributed Key Management' section, the 'Store my keys in Active Directory' checkbox is checked. Below it, a text box contains 'CN=VMMDKM,DC=FLEXPOD,DC=TEST'. A link 'How do I configure distributed key management?' is at the bottom. Navigation buttons 'Previous', 'Next >', and 'Cancel' are at the bottom right.

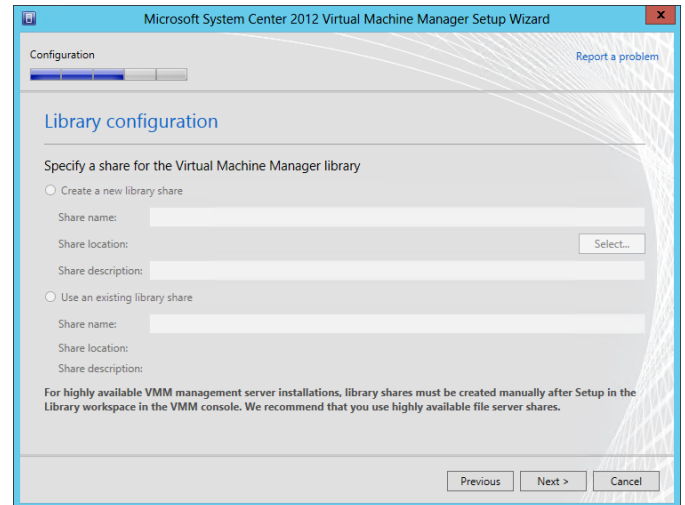
In the **Port configuration** dialog, accept the default values in the provided text boxes:

- **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.

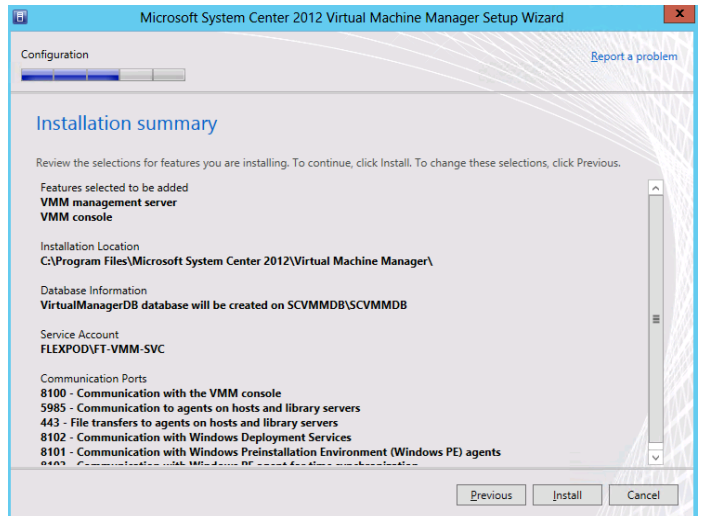
Click **Next** to continue.

The screenshot shows the 'Port configuration' dialog box. It lists several ports for VMM features. All ports are set to their default values: 8100 for 'Communication with the VMM console', 5985 for 'Communication to agents on hosts and library servers', 443 for 'File transfers to agents on hosts and library servers', 8102 for 'Communication with Windows Deployment Services', 8101 for 'Communication with Windows Preinstallation Environment (Windows PE) agents', and 8103 for 'Communication with Windows PE agent for time synchronization'. Navigation buttons 'Previous', 'Next >', and 'Cancel' are at the bottom right.

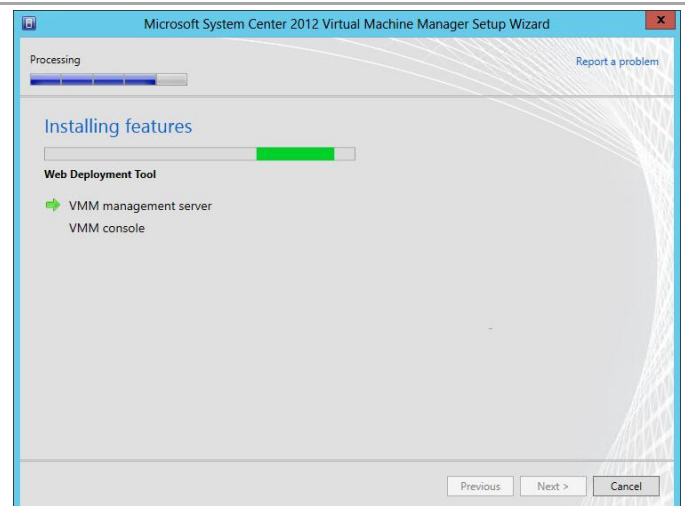
In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.



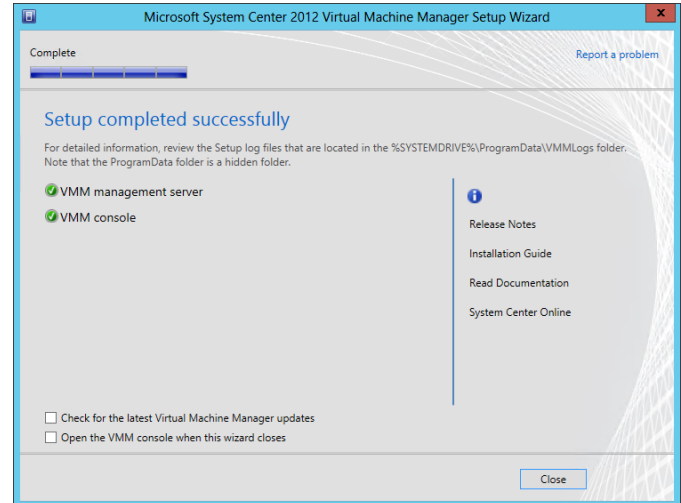
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



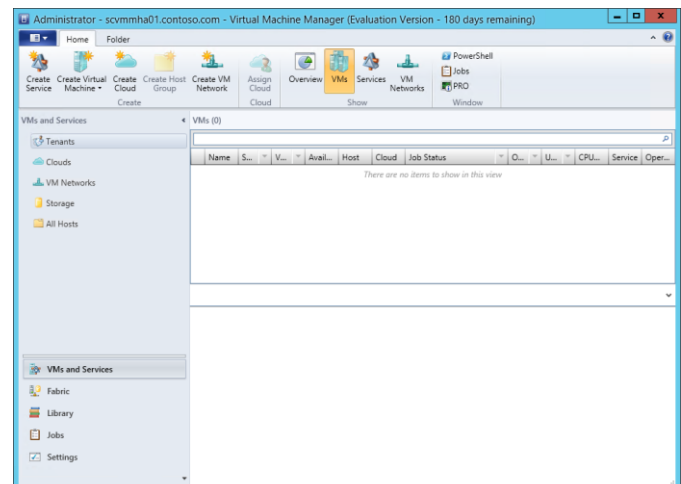
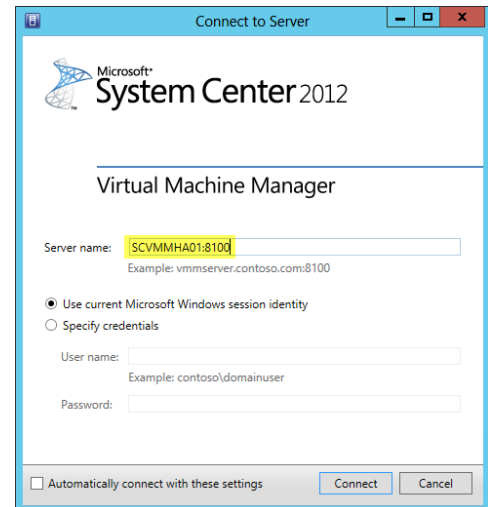
The wizard will display the progress while installing features.



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



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

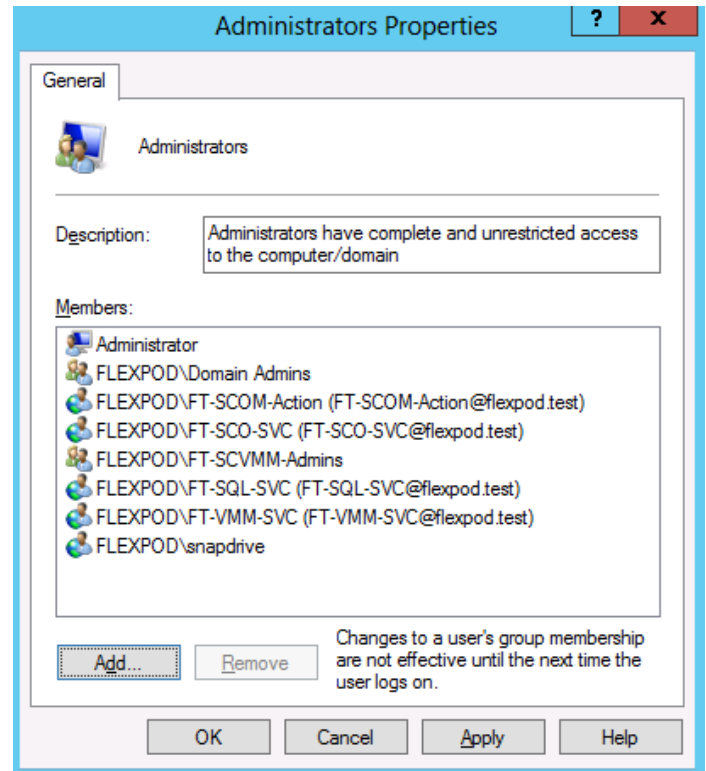


► Perform the following steps on the second Virtual Machine Manager virtual machine.

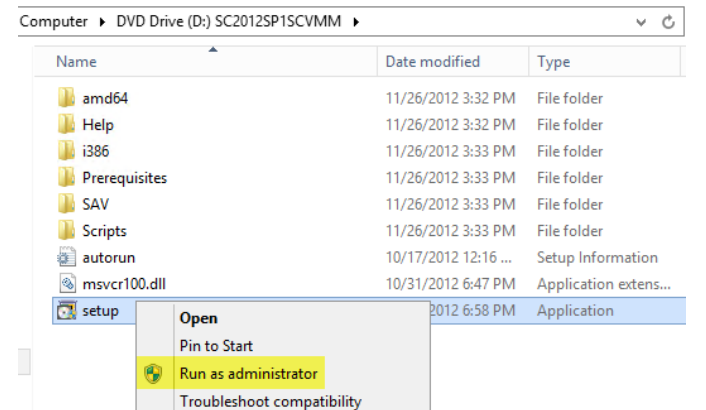
Log on to the **second** Virtual Machine Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager Virtual Machine:

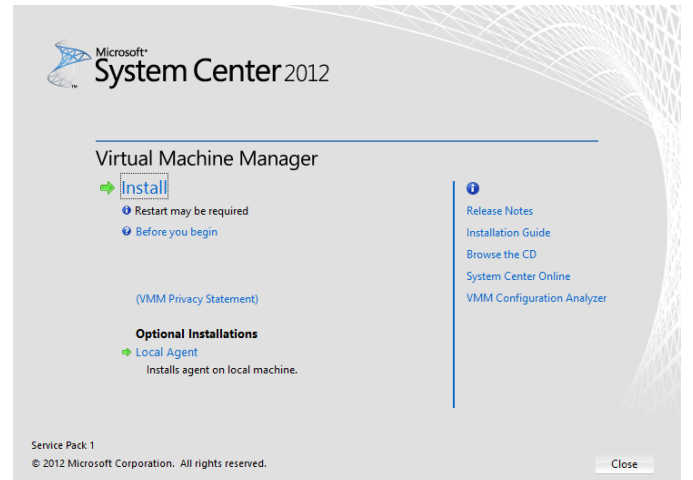
- Orchestrator service account.
- Operations Manager action account.
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.
- SQL Server service account.



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



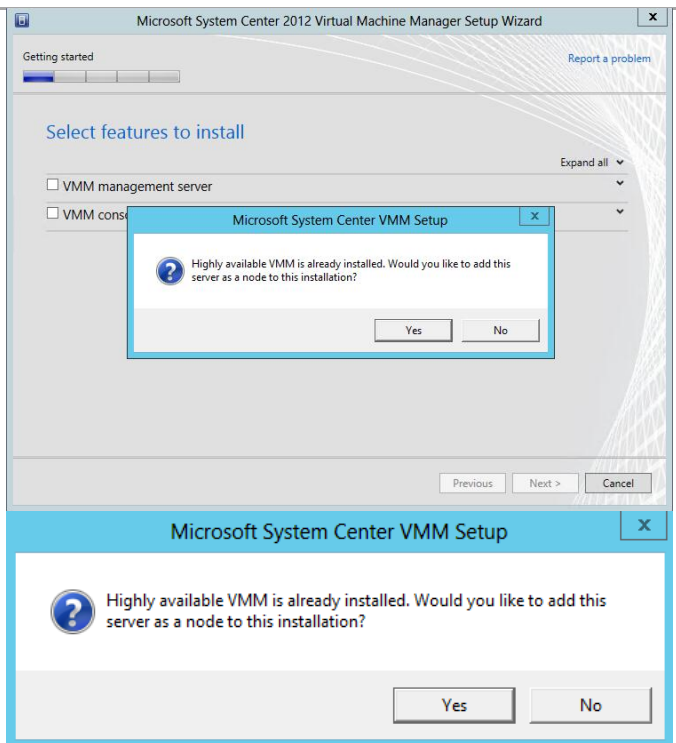
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



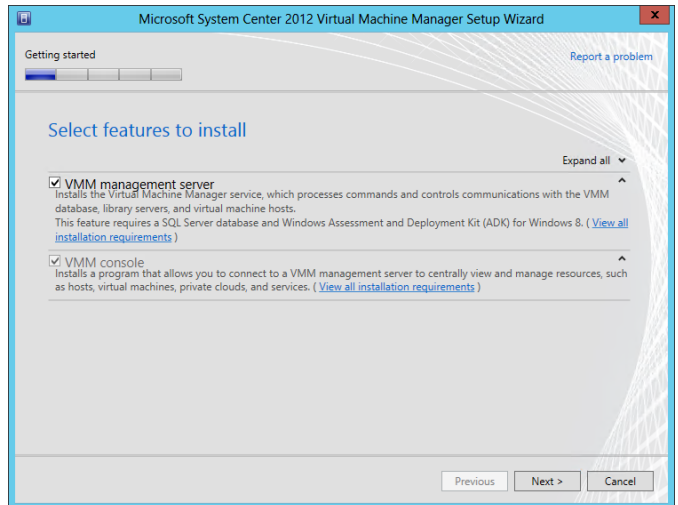
Attempting to select any feature will cause the cluster management server notice to appear.

Click **Yes** to switch to the highly available Virtual Machine Manager setup wizard and add the second node.

Note: Virtual Machine Manager can be deployed on up to 16 cluster nodes but only a single node can be active at any time.



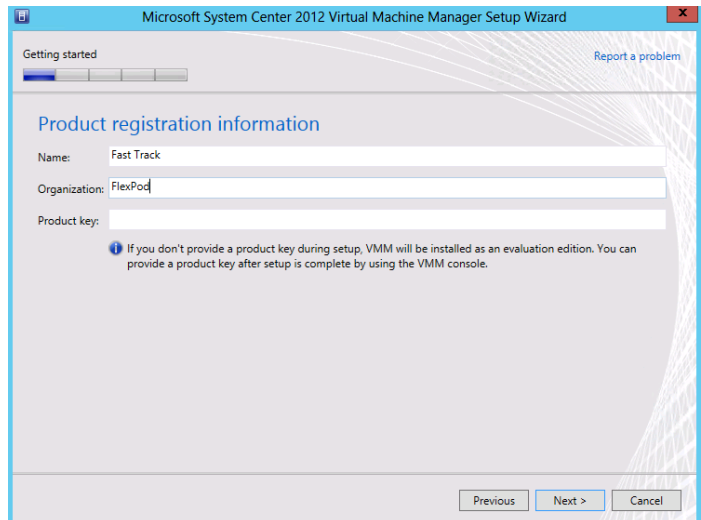
In the **Select features to install** dialog, verify that the **VMM management server** installation option check box is selected. After selecting it, the **Virtual Machine Manager console** installation option check box will be selected by default. Click **Next** to continue.



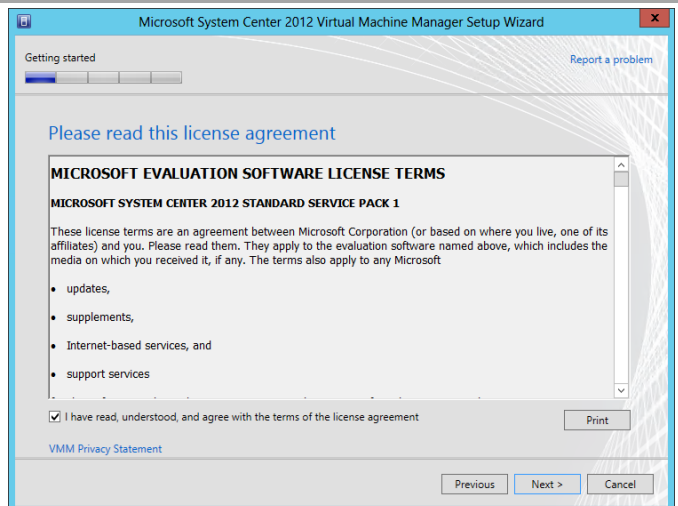
In the **Product registration information** dialog, enter the following information in the provided text boxes:

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

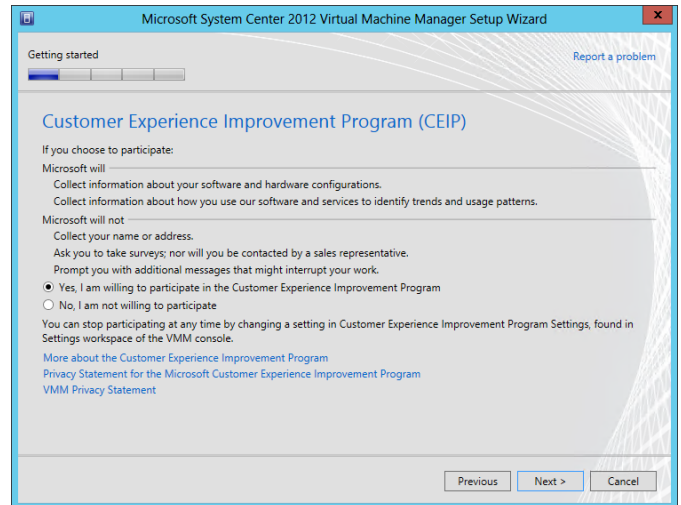
Click **Next** to continue.



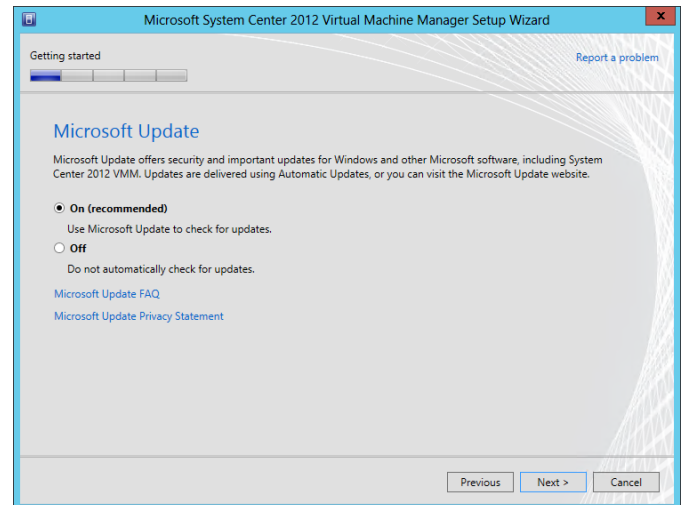
In the **Please read this license agreement** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



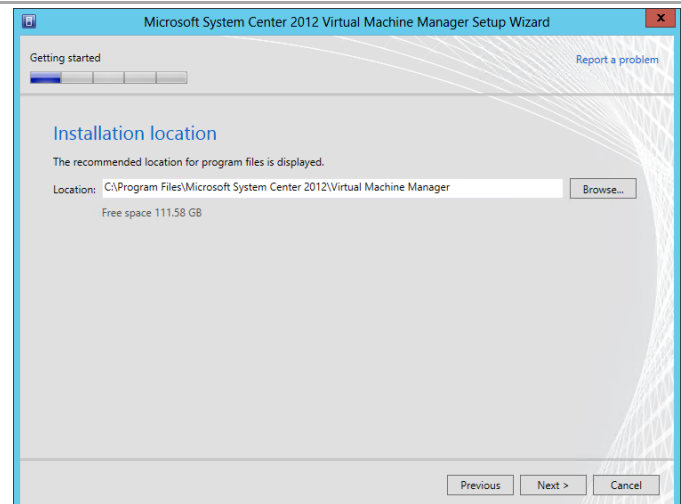
In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.



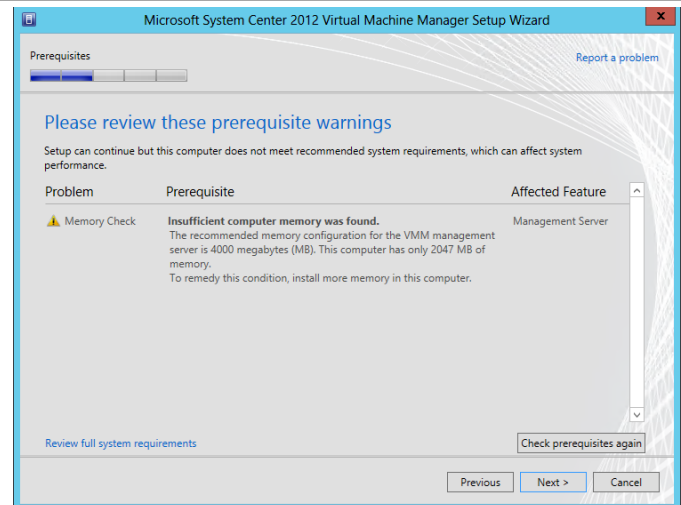
In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager* for the installation. Click **Next** to continue.



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

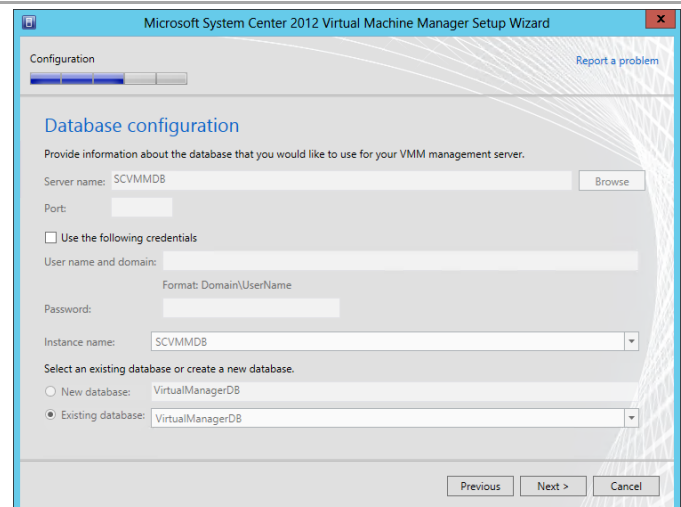
The following is just an example of that UI.

If the system passes the prerequisite check, no screen will be displayed and the setup wizard will proceed to the Database configuration screen.



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

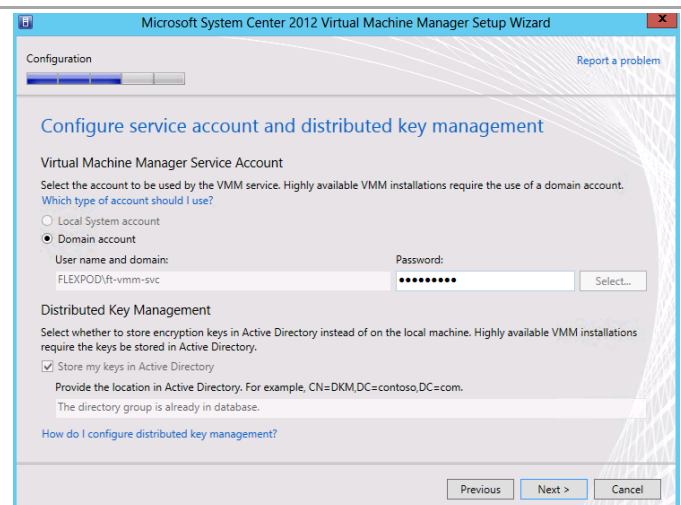
Click **Next** to continue.



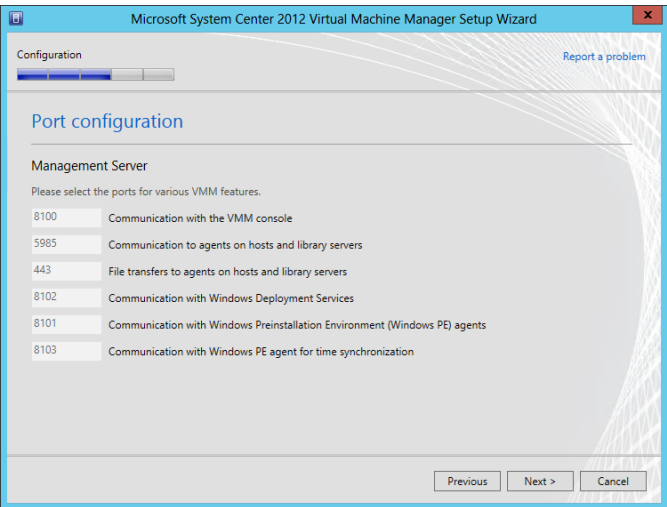
In the **Configure service account and distributed key management** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields other than **Password** are greyed out.

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

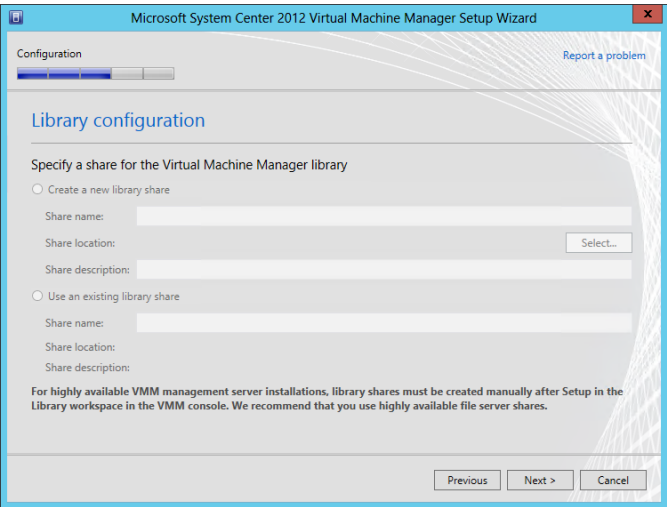
Click **Next** to continue.



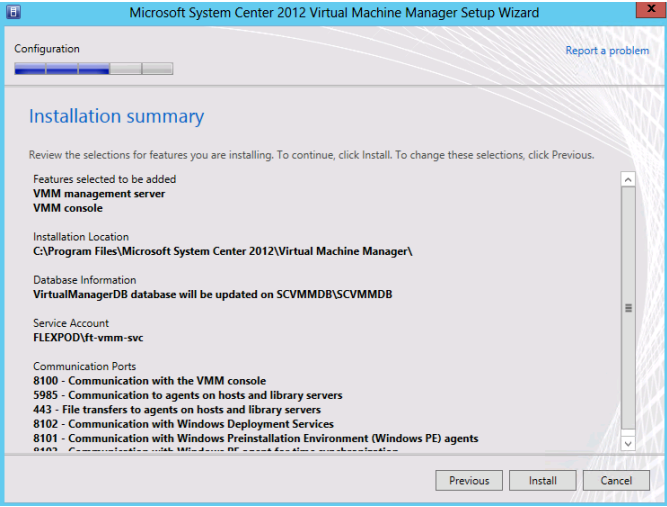
In the **Port configuration** dialog, when deploying additional nodes to a Virtual Machine Manager cluster, all fields are greyed out. Click **Next** to continue.



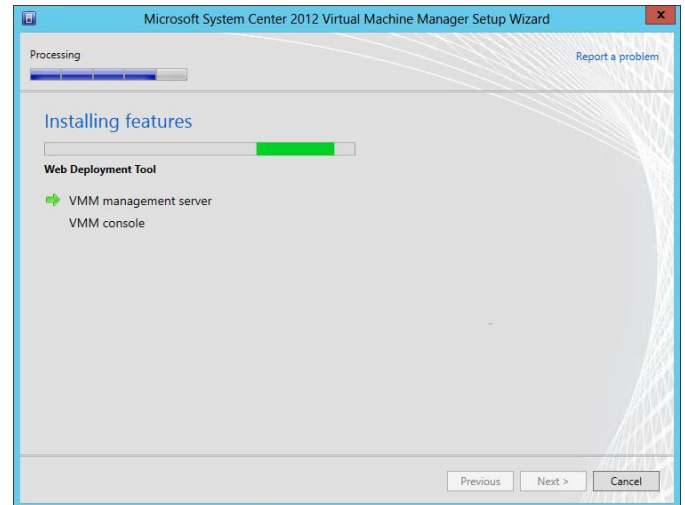
In the **Library configuration** dialog, no options are available for a highly available installation. The Library must be configured separately and should point to a highly available file share. The process will be covered separately in this guide. Click **Next** to continue.



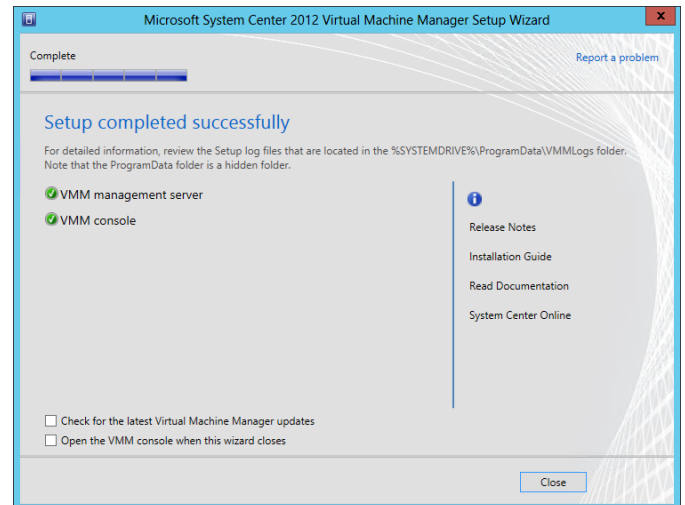
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



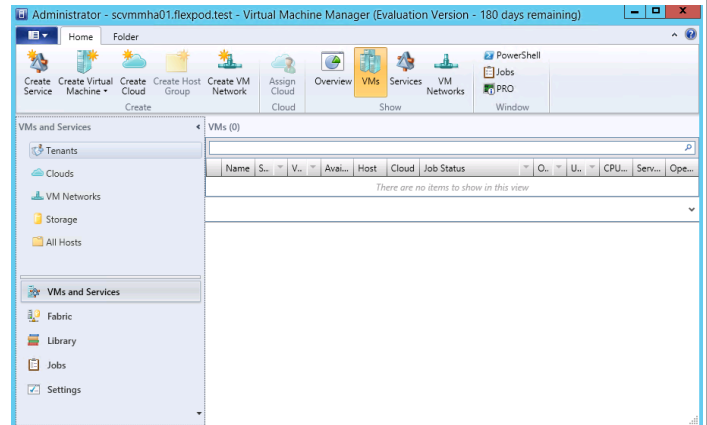
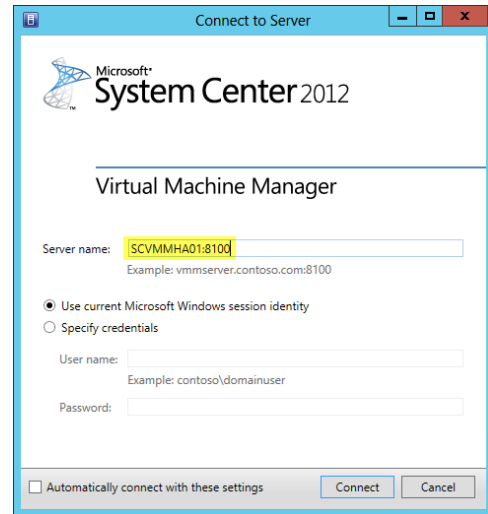
The wizard will display the progress while installing features.



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

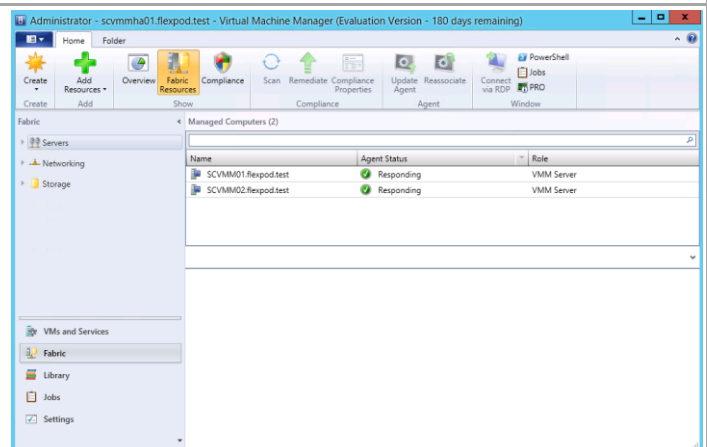


Once complete, launch the Virtual Machine Manager console to verify the installation occurred properly. Set the **Server Name** value to match the name that was provided for the **Cluster Resource** name during setup (for example, HAVMM:8100). Verify that the console launches and connects to the Virtual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



In the **Virtual Machine Manager Console**, expand **Servers** and select **VMM Server**.

Verify that both cluster nodes are listed as **VMM Servers** under **Role** and that both nodes are listed as **Responding** under **Agent Status**.

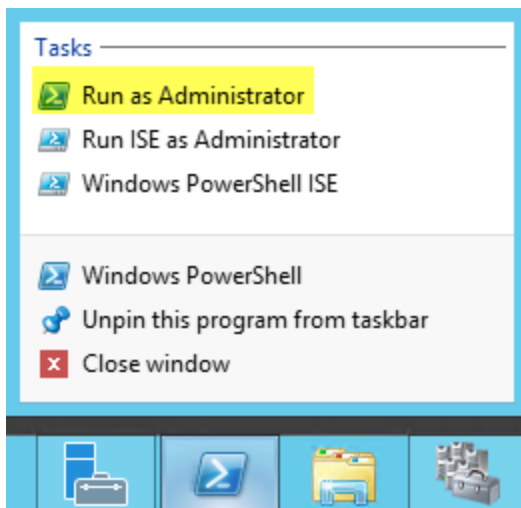


14.5 Creating Virtual Machine Manager Library Share on a Failover Cluster

In a highly available installation of Virtual Machine Manager, the Virtual Machine Manager Library must reside on a server outside of the Virtual Machine Manager Cluster infrastructure; it is not a supported configuration to reside upon the Virtual Machine Manager cluster or its nodes. In addition, making the Virtual Machine Manager Library highly available is a recommended practice given that the Virtual Machine Manager servers themselves are highly available. While any file server cluster will suffice, this document will detail the steps required to host the Virtual Machine Manager Library upon the SQL Server Cluster created in earlier portions of this document.

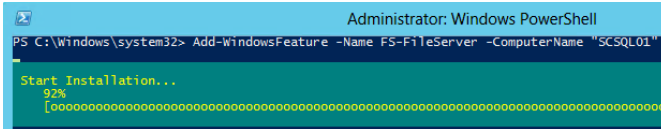
Perform the following steps on each SQL Server virtual machine.

1. Open a PowerShell session as an administrator.

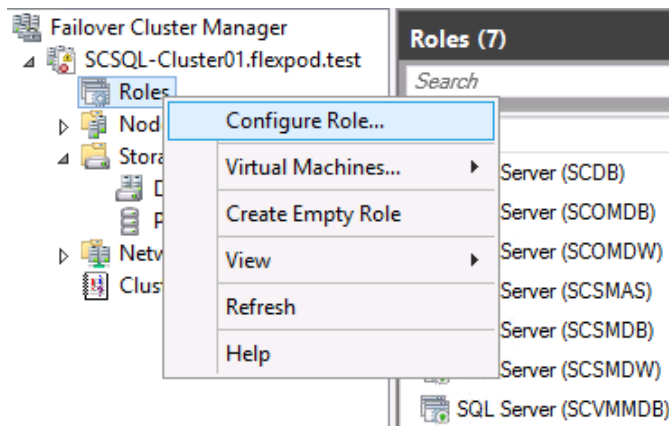


2. From the administrator PowerShell session run the following command once for each SQL cluster node changing the ComputerName value each time to that of a different SQL cluster node.

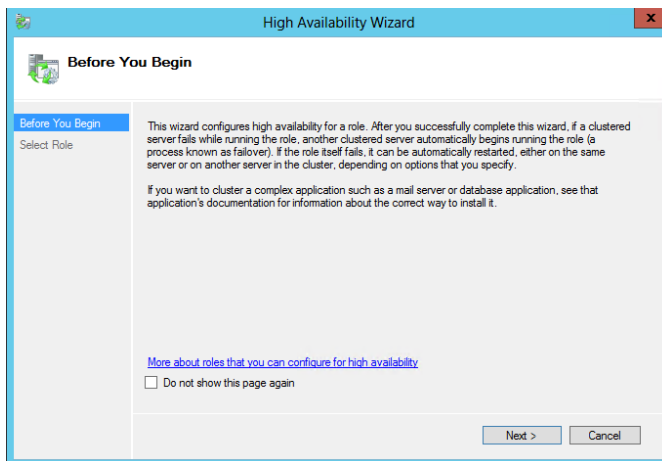
3. Add-WindowsFeature-NameFS-FileServer-ComputerName“SCSQL01”



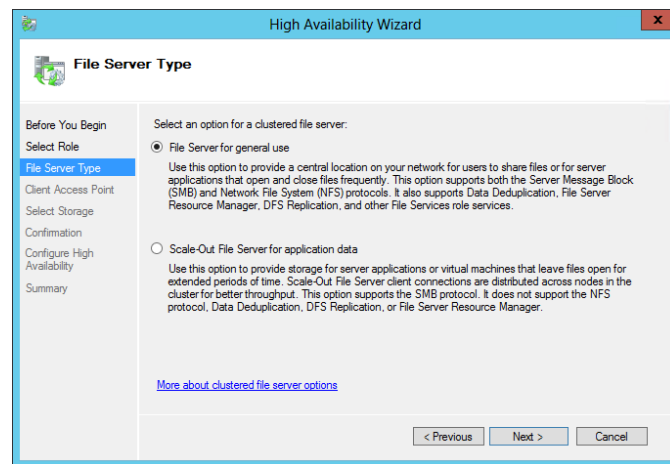
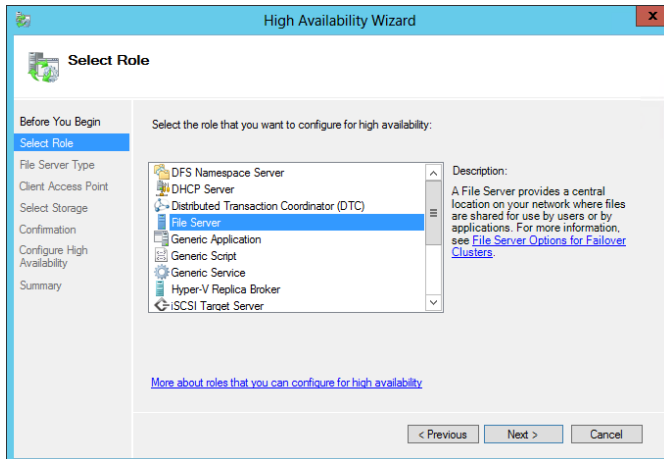
4. Add an additional iSCSI or Fibre Channel LUN and prepare it as described in previous steps. This should appear as available storage in the Failover Cluster Manager Storage node. **Perform the following steps on the first SQL Server cluster node. Within Failover Cluster Manager, right-click on Services and applications and select Configure Role... from the context menu.**



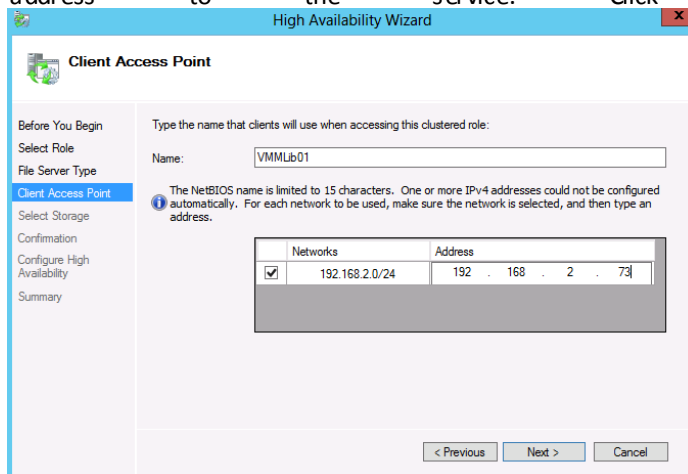
5. The **High Availability Wizard** will appear. In the **Before You Begin** dialog click **Next** to begin the wizard.



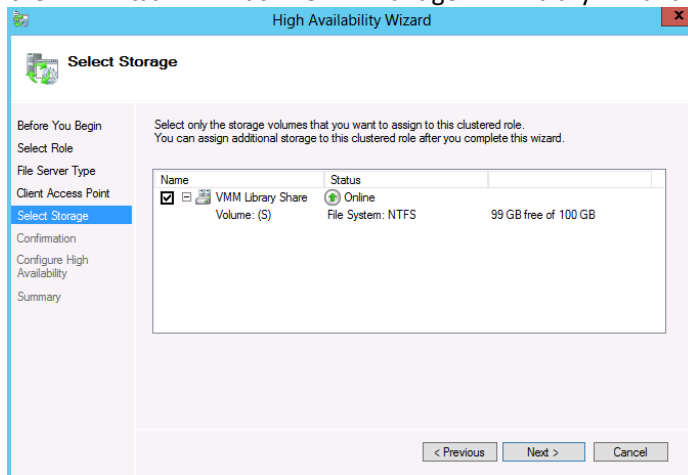
6. In the **Select Role** dialog, from the available services and applications, select **File Server** and click **Next** to continue. In the **File Server Type** dialog, select the **File Server for general use** radio button and click **Next** to continue.



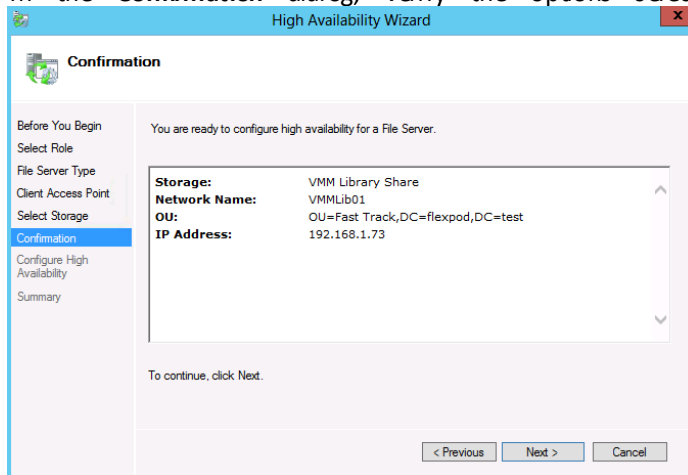
7. In the **Client Access Point** dialog, specify a unique name for the clustered file server in the **Name** text box. Additionally, for static IP configurations, select the appropriate network and assign a unique IP address to the service. Click **Next** to continue.



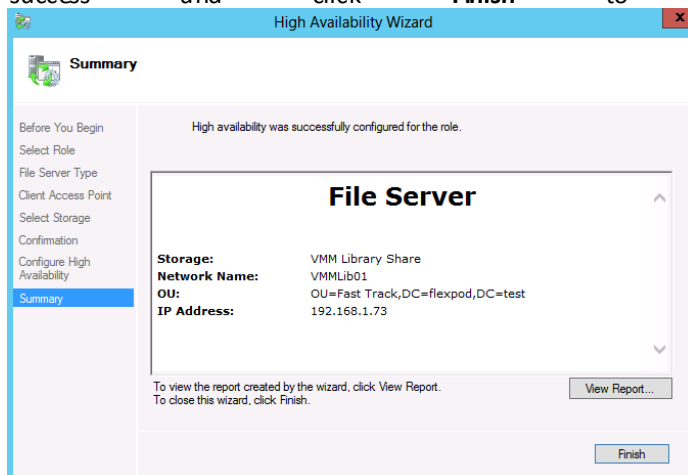
8. In the **Select Storage** dialog, from the available storage, select the Cluster Disk that will be used for the Virtual Machine Manager Library and click **Next** to continue.



9. In the **Confirmation** dialog, verify the options selected and click **Next** to continue.



10. When complete, the **Summary** dialog will show a report of the actions taken by the wizard. Verify success and click **Finish** to complete the wizard.



11. Note that the new highly available file server is available as a new service in Failover Cluster Manager.

Name	Status	Type	Owner Node	Priority
SQL Server (SCDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDB)	Running	Other	SCSQL02	Medium
SQL Server (SCOMDW)	Running	Other	SCSQL02	Medium
SQL Server (SCSMAS)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDB)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDW)	Running	Other	SCSQL01	Medium
SQL Server (SCVMMDB)	Running	Other	SCSQL02	Medium
VMMlib01	Running	File Server	SCSQL01	Medium

12. Within **Failover Cluster Manager**, right-click the newly created file server service and select **Add File Share** from the context menu.

Name	Status	Type	Owner Node	Priority
VMMlib01	Running	File Server	SCSQL01	Medium
SQL Server (SCDB)	Running	Other	SCSQL02	Medium
SQL Server (SCOMDB)	Running	Other	SCSQL01	Medium
SQL Server (SCOMDW)	Running	Other	SCSQL02	Medium
SQL Server (SCSMAS)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDB)	Running	Other	SCSQL02	Medium
SQL Server (SCSMDW)	Running	Other	SCSQL02	Medium
SQL Server (SCVMMDB)	Running	Other	SCSQL01	Medium

13. The **New Share Wizard** will appear. In the **Select Profile** dialog, select **SMB Share – Quick** and click **Next** to continue.

14. In the **Shared Folder Location** dialog, in the **Server** pane select the File Server cluster role object name created earlier. In the **Share location** pane, choose the **Select by volume** radio button option and click **Next** to continue.

New Share Wizard

Select the server and path for this share

Select Profile

Share Location

Other Settings

Permissions

Confirmation

Results

Server:

Server Name	Status	Cluster Role	Owner Node
SCSMAS	Online	Unknown	
SCSMDB	Online	Unknown	
SCSMDW	Online	Unknown	
SCVMMDB	Online	Unknown	
VmmLib01	Online	File Server	

Share location:

☒ Select by volume:

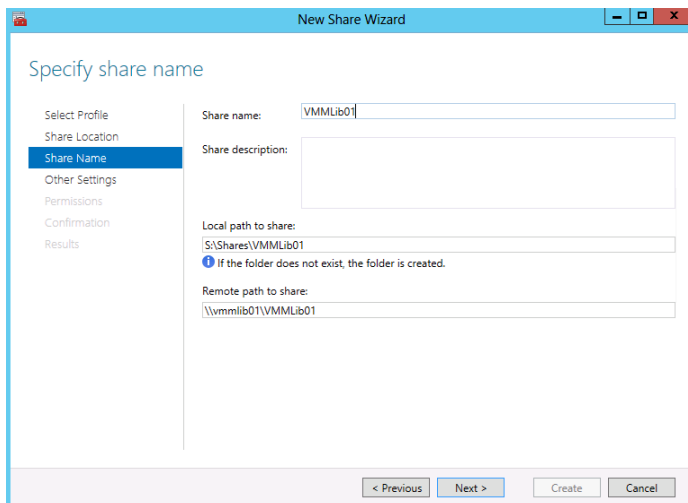
Volume	Free Space	Capacity	File System
S:	99.3 GB	99.9 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

☐ Type a custom path:

< Previous Next > Create Cancel

15. In the **Share Name** dialog, type the value of “VMMLibrary” in the **Share name** field and then click **Next** to continue.



Specify share name

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Share name: VMMLib01

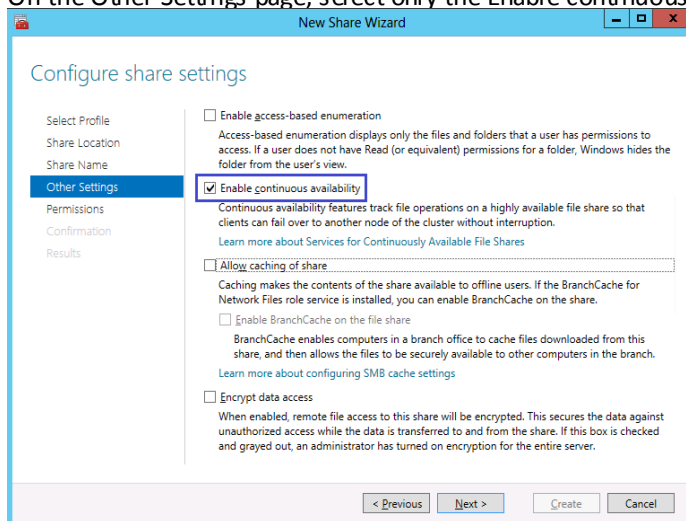
Share description:

Local path to share: S:\Shares\VMMLib01
If the folder does not exist, the folder is created.

Remote path to share: \\vmmlib01\VMMLib01

< Previous Next > Create Cancel

16. On the **Other Settings** page, select only the **Enable continuous availability** option and then click **Next**.



Configure share settings

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

☐ Enable access-based enumeration
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ **Enable continuous availability**
Continuous availability features track file operations on a highly available file share so that clients can fail over to another node of the cluster without interruption.
[Learn more about Services for Continuously Available File Shares](#)

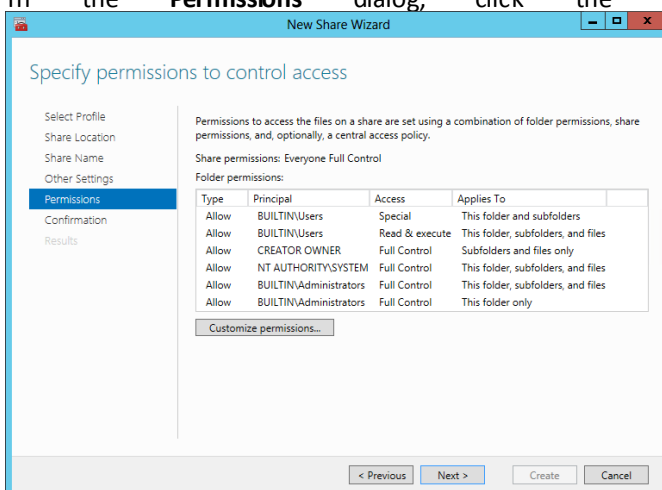
☐ Allow caching of share
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ Enable BranchCache on the file share
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.
[Learn more about configuring SMB cache settings](#)

☐ Encrypt data access
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

< Previous Next > Create Cancel

17. In the **Permissions** dialog, click the **Customize Permissions...** button.



Specify permissions to control access

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

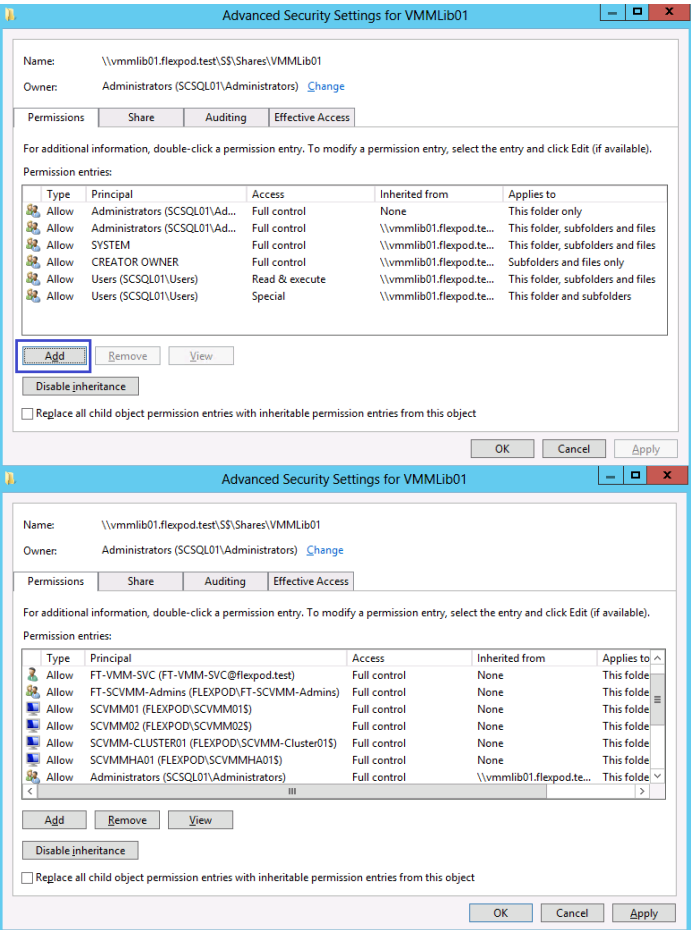
Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

Customize permissions...

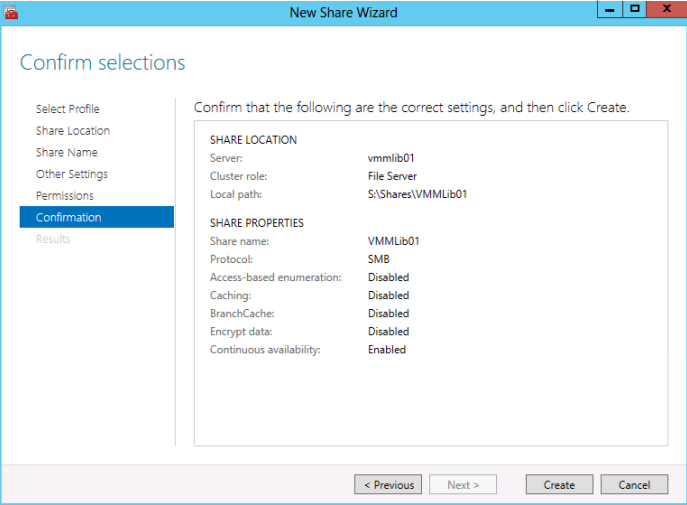
< Previous Next > Create Cancel

18. In the **Permissions for VMMLibrary** dialog, add the following accounts with NTFS Full Control permissions over the folder: The VMM service account. The VMM Admins group. Both VMM computer

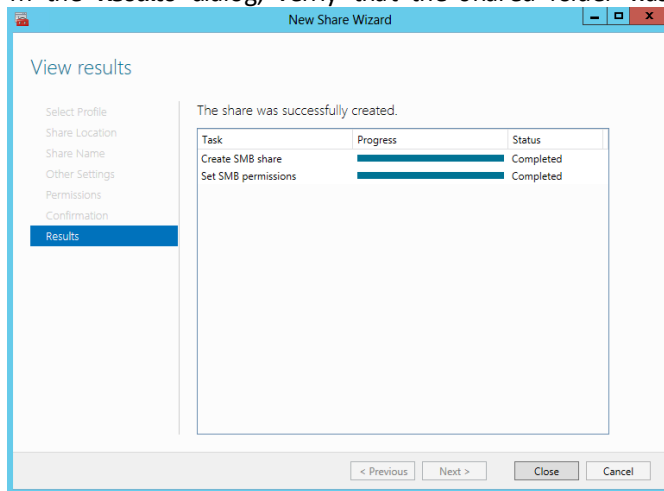
accounts. The VMM CNO computer account. The VMM VCO computer account. Click **OK** to save the changes.



19. Click **Next** to continue in the wizard. Review the settings on the **Confirmation** dialog and click **Create**.

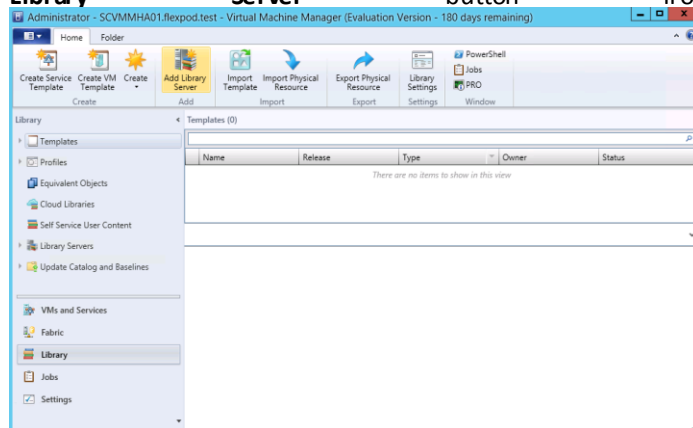


20. In the **Results** dialog, verify that the shared folder was provisioned properly and click **Close**.



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

1. In the **Virtual Machine Manager** console, select the **Library** node. In the **Home** tab, click the **Add Library Server** button from the ribbon.



2. The **Add Library Server** wizard will appear. In the **Enter Credentials** dialog, select the **Enter a user name and password** option. In the **User name** and **Password** text boxes, enter credentials that have administrative rights over each of the target servers where the new HA Virtual Machine Manager

Library share will reside. Click **Next** to continue.

The screenshot shows the 'Add Library Server' dialog box with the 'Enter Credentials' tab selected. The left sidebar contains 'Enter Credentials', 'Select Library Servers', 'Add Library Shares', and 'Summary'. The main area has two radio buttons: 'Use an existing Run As account:' (unselected) and 'Enter a user name and password:' (selected). Below the second option are text boxes for 'User name:' (containing 'flexpodfit-vmm-library' with an example 'contoso\domainuser' below it) and 'Password:' (masked with dots). A 'Browse...' button is next to the first radio button. At the bottom are 'Next' and 'Cancel' buttons.

3. In the **Select Library Servers** dialog, specify the FQDN of the target domain in the **Domain** text box. In the **Computer name** text box, type the name of the newly created HA File Server CNO and click **Add**.

The screenshot shows the 'Add Library Server' dialog box with the 'Select Library Servers' tab selected. The left sidebar is the same. The main area has text boxes for 'Domain:' (containing 'flexpod.test') and 'Computer name:' (containing 'VMMULb01'). Below these is a checkbox for 'Skip Active Directory name verification' with a note: 'If you use this option, ensure that your computer name entry is a registered host Service Principal Name (SPN) in Active Directory.' There are 'Search...' and 'Add' buttons. Below is a table titled 'Selected servers:' with columns 'Computer Name' and 'Operating System'. At the bottom right is a 'Remove' button. At the very bottom are 'Previous', 'Next', and 'Cancel' buttons. A small information icon and note are at the bottom left of the main area.

4. In the **Specified Servers** pane, the cluster object will appear in the dialog. Click **Next** to continue.

The screenshot shows the 'Add Library Server' dialog box with the 'Select Library Servers' pane active. The left sidebar contains 'Enter Credentials', 'Select Library Servers' (selected), 'Add Library Shares', and 'Summary'. The main area has input fields for 'Domain' (flexpod.test) and 'Computer name'. Below these is a checkbox for 'Skip Active Directory name verification' with a note: 'If you use this option, ensure that your computer name entry is a registered host Service Principal Name (SPN) in Active Directory.' There are 'Search...' and 'Add' buttons. A table titled 'Selected servers:' lists one server: VMMLib01 (SCSQL01, SCSQL02) with Operating System 'Windows Server 2012 Datacenter'. A 'Remove' button is at the bottom right of the table. A note at the bottom states: 'If you select multiple computers to add as library servers, the credentials you provide must be for a domain account that has administrative rights on all the selected computers.' Navigation buttons 'Previous', 'Next', and 'Cancel' are at the bottom.

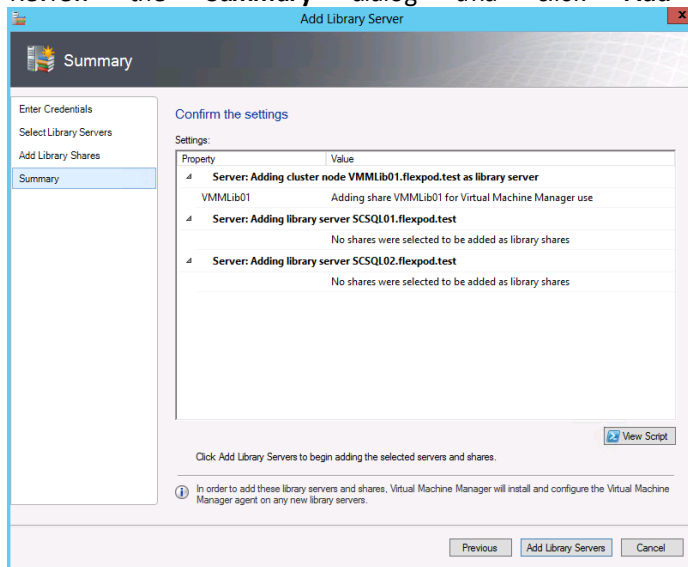
Computer Name	Operating System
VMMLib01 (SCSQL01, SCSQL02)	Windows Server 2012 Datacenter

5. In the **Add Library Shares** dialog, select the check box associated with the VMMLibrary share created earlier. Verify that the **Add Default Resources** check box is selected and click **Next** to continue.

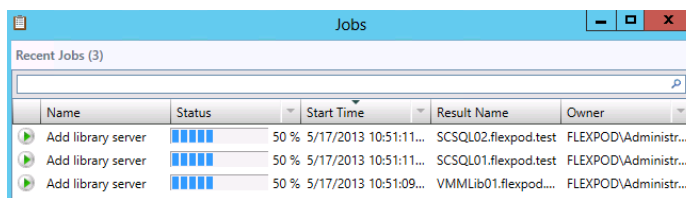
The screenshot shows the 'Add Library Shares' dialog box with the 'Add Library Shares' pane active. The left sidebar contains 'Enter Credentials', 'Select Library Servers', 'Add Library Shares' (selected), and 'Summary'. The main area has a table titled 'Select library shares to add' with columns: 'Share Name', 'Shared Path', 'Comment', and 'Add Default Resources'. The table lists two shares: 'Server: VMMLib01.flexpod.test' and 'VMMLib01'. The 'VMMLib01' row has a checked checkbox in the 'Add Default Resources' column. Below the table is a checkbox for 'Show hidden shares'. Navigation buttons 'Previous', 'Next', and 'Cancel' are at the bottom.

Share Name	Shared Path	Comment	Add Default Resources
Server: VMMLib01.flexpod.test			
VMMLib01	S:\Shares\VMMLib01		<input checked="" type="checkbox"/>

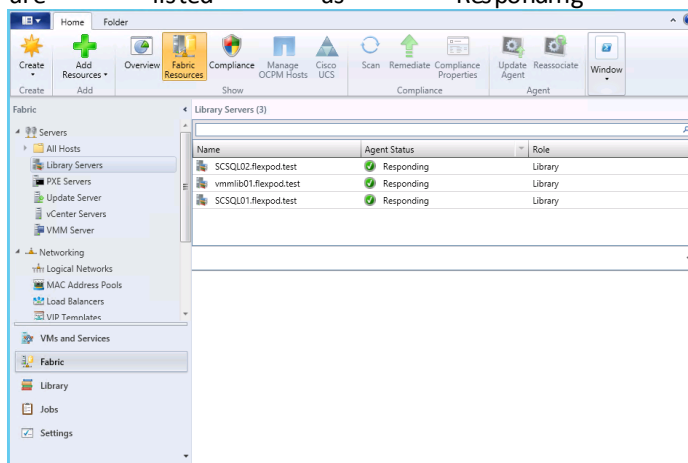
6. Review the **Summary** dialog and click **Add Library Servers** to continue.



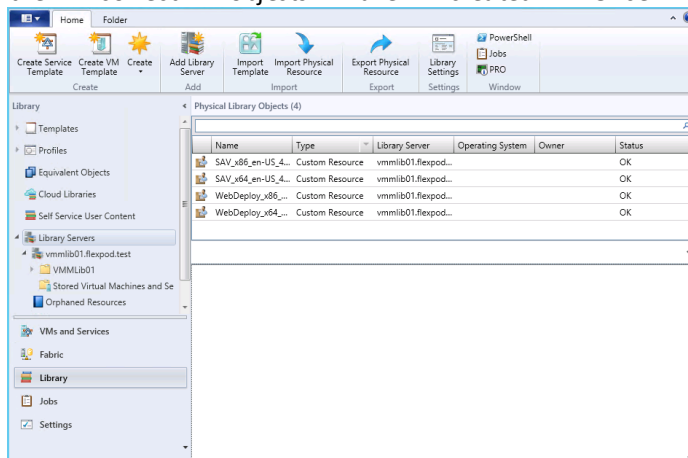
7. The **Jobs** dialog will appear showing the progress of the Add Library Server action. In the **Jobs** dialog, verify that all steps have completed.



8. In the **Virtual Machine Manager** console, expand, select **Fabric**, and navigate to the **Library Servers** node. Verify that all cluster nodes are listed along with the cluster object name and that all servers are listed as **Responding** under **Agent Status**.



9. In the **Virtual Machine Manager** console, navigate to the **Library Servers** node and verify that all of the correct objects are created. Once verified, exit the console.

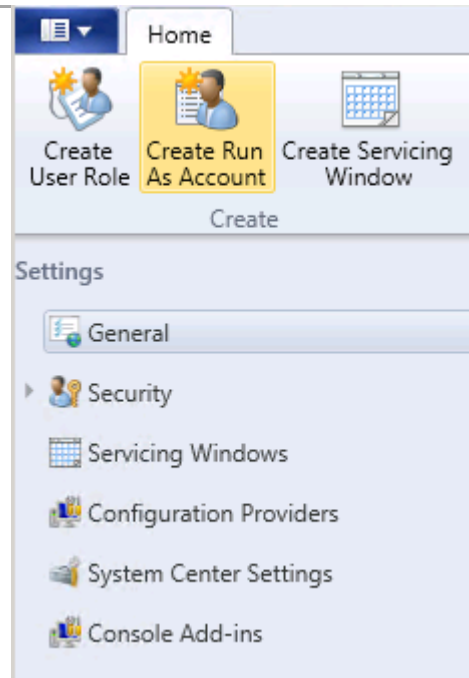


10. Add a Run-As-Account

Complete the following steps to add a Run-Ass-Account to VMM.

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

Click **Settings** in the left tree view and click **Create Run As Account**.



Name the account. Provide and active directory account name and pass word with administrator rights. Click OK to create the Run-Ass Account

Create Run As Account

Provide the details for this Run As account

Name: System Center Administrator

Description:

User name: flexpod/administrator
Example: contoso/domainuser or localuser

Password:

Confirm password:

☒ Validate domain credentials

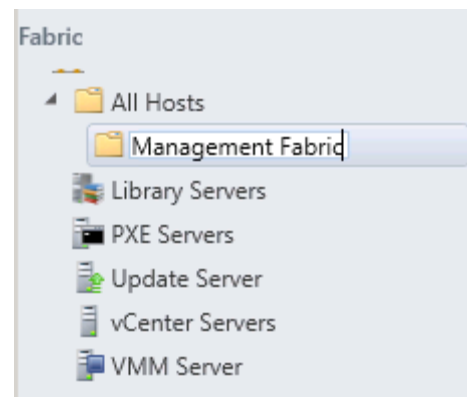
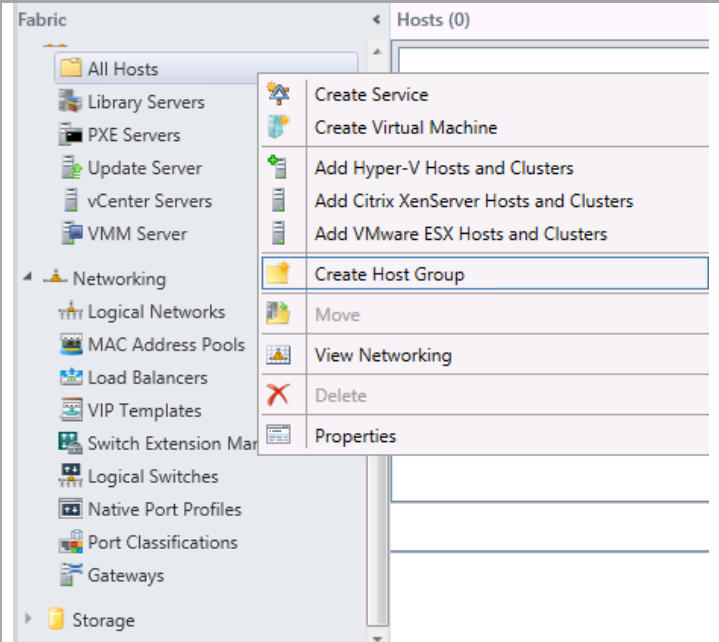
View Script OK Cancel

14.6 Add Fabric Management Resources Virtual Machine Manager

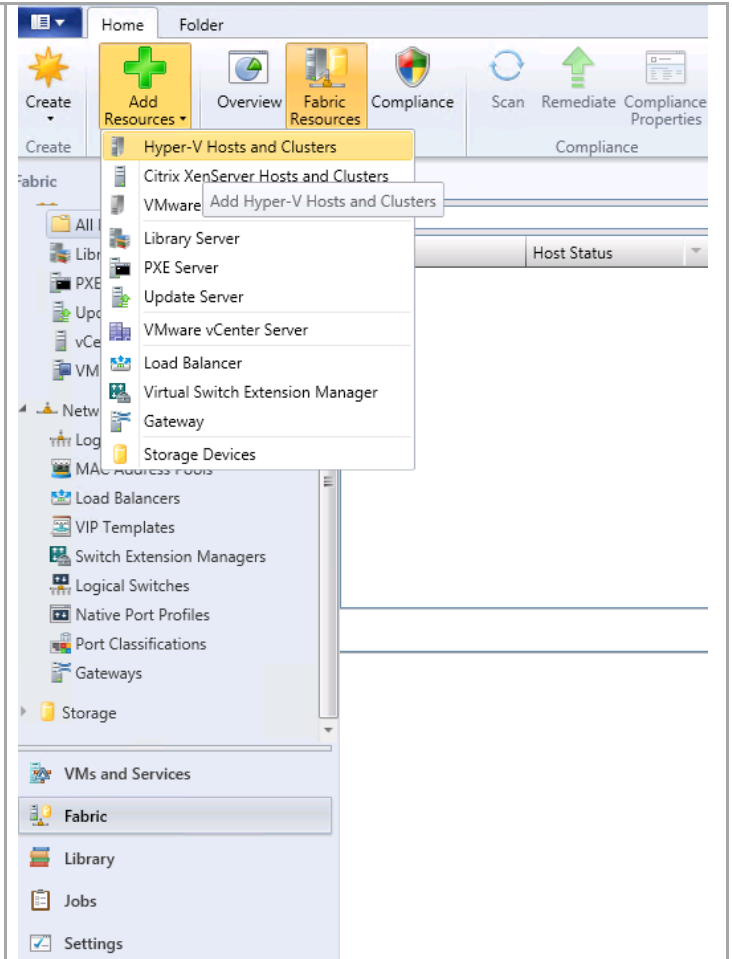
Complete the following steps to Add the Fabric Management Hyper-V hosts to VMM.

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

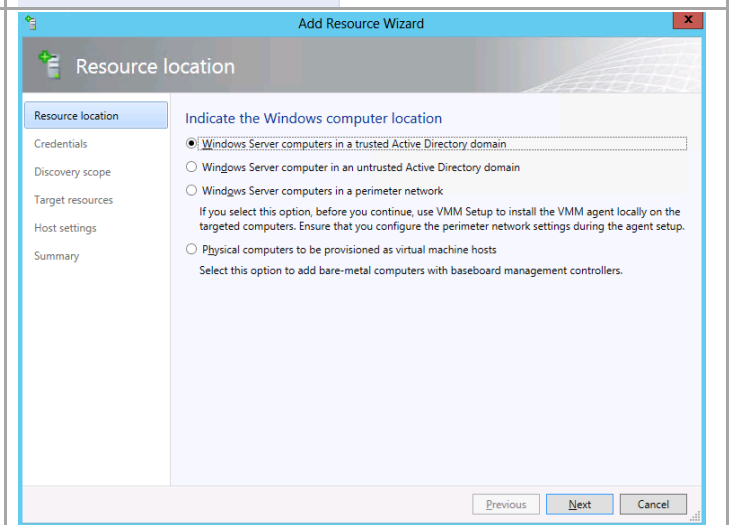
Click **Fabric** in the left tree view and right click **All Hosts**. Select **Create Host Group**. Name the new Host Group.



Select Fabric and All Hosts. Click Add Resources.



In the Indicate the Windows computer location window, select **Windows Server computers in a trusted Active Directory domain**.



Select Use and Existing Run As account and click browse.

Add Resource Wizard

Credentials

Resource location
Discovery scope
Target resources
Host settings
Summary

Specify the credentials to use for discovery

The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary.

☒ Use an existing Run As account

Run As account:

☐ Manually enter the credentials

User name:

Example: contoso\domainuser

Password:

ⓘ The above provided credentials or Run As account should be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If credentials are entered manually, then they will only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it.

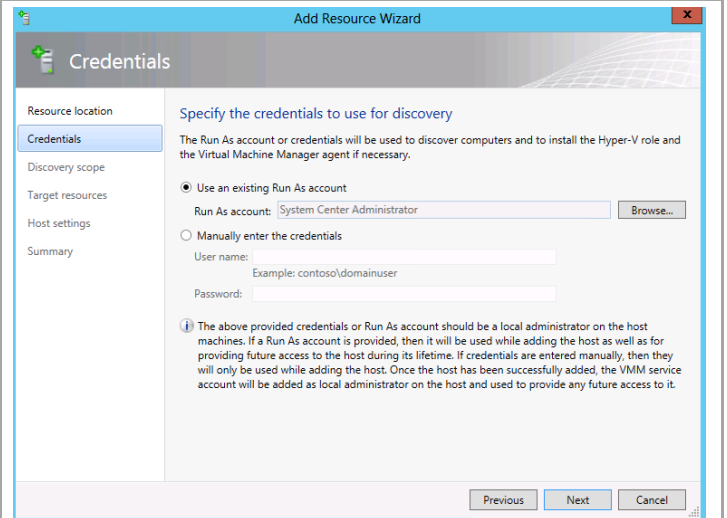
Select the previously created account and click OK.

Select a Run As Account

Select a Run As account

Name	Description	User Role
NT AUTHORITY\System		
NT AUTHORITY\LocalS...		
NT AUTHORITY\Netwo...		
System Center Adminis...		Administrator

Click Next to proceed to the next screen.



The screenshot shows the 'Add Resource Wizard' window, specifically the 'Credentials' step. The left sidebar has 'Credentials' selected. The main area is titled 'Specify the credentials to use for discovery'. It contains a note about the Run As account or credentials being used for discovery. There are two radio buttons: 'Use an existing Run As account' (selected) and 'Manually enter the credentials'. The 'Run As account' field is set to 'System Center Administrator'. Below it, there are fields for 'User name' (with an example 'contoso/domainuser') and 'Password'. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

Resource location

Credentials

Discovery scope

Target resources

Host settings

Summary

Specify the credentials to use for discovery

The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary.

☒ Use an existing Run As account

Run As account: System Center Administrator Browse...

☐ Manually enter the credentials

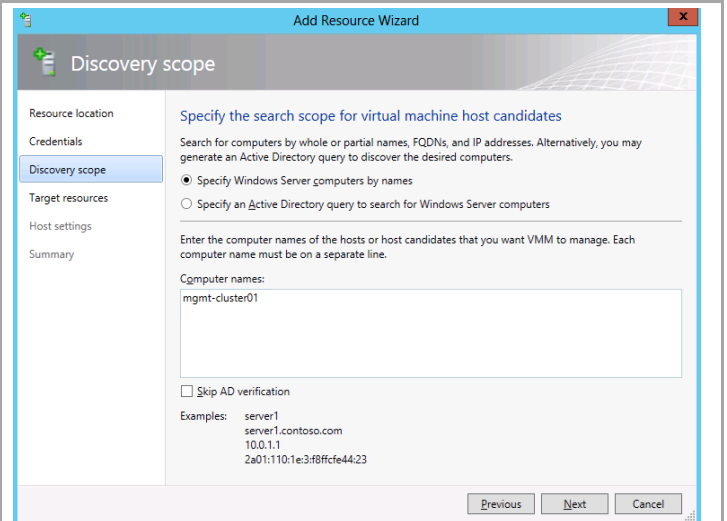
User name: Example: contoso/domainuser

Password:

The above provided credentials or Run As account should be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If credentials are entered manually, then they will only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it.

Previous Next Cancel

Enter the cluster name and click Next.



The screenshot shows the 'Add Resource Wizard' window, specifically the 'Discovery scope' step. The left sidebar has 'Discovery scope' selected. The main area is titled 'Specify the search scope for virtual machine host candidates'. It contains a note about searching for computers by whole or partial names, FQDNs, and IP addresses. There are two radio buttons: 'Specify Windows Server computers by names' (selected) and 'Specify an Active Directory query to search for Windows Server computers'. Below it, there is a text box for 'Computer names' with the example 'mgmt-cluster01'. There is a checkbox for 'Skip AD verification'. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

Resource location

Credentials

Discovery scope

Target resources

Host settings

Summary

Specify the search scope for virtual machine host candidates

Search for computers by whole or partial names, FQDNs, and IP addresses. Alternatively, you may generate an Active Directory query to discover the desired computers.

☒ Specify Windows Server computers by names

☐ Specify an Active Directory query to search for Windows Server computers

Enter the computer names of the hosts or host candidates that you want VMM to manage. Each computer name must be on a separate line.

Computer names:

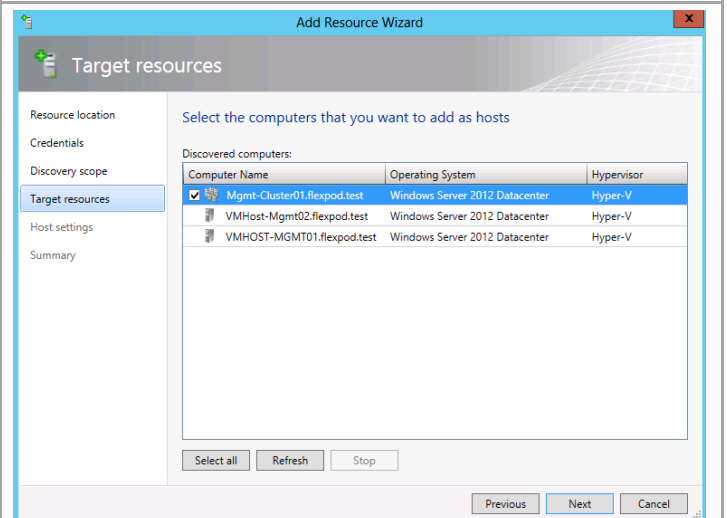
mgmt-cluster01

☐ Skip AD verification

Examples: server1
server1.contoso.com
10.0.1.1
2a01:110:1e:3:f8ffcf44:23

Previous Next Cancel

Click Select All and click Next.



The screenshot shows the 'Add Resource Wizard' window, specifically the 'Target resources' step. The left sidebar has 'Target resources' selected. The main area is titled 'Select the computers that you want to add as hosts'. It contains a table of 'Discovered computers' with columns 'Computer Name', 'Operating System', and 'Hypervisor'. The first row is selected. Below the table, there are 'Select all', 'Refresh', and 'Stop' buttons. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

Resource location

Credentials

Discovery scope

Target resources

Host settings

Summary

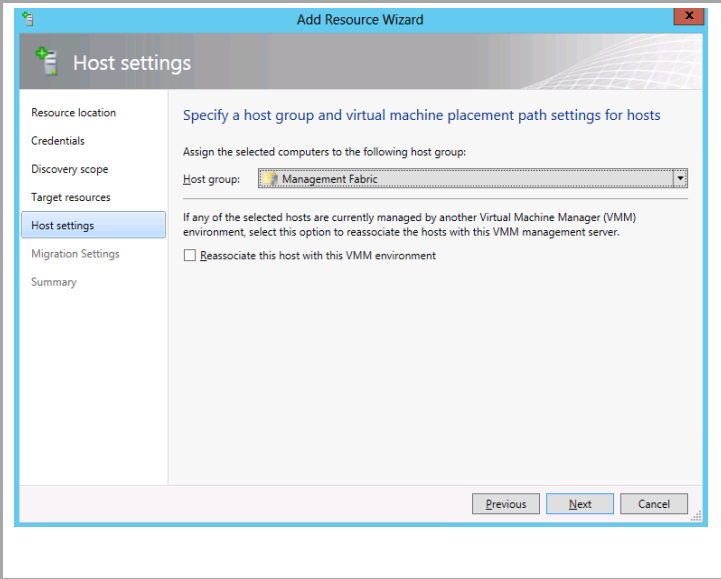
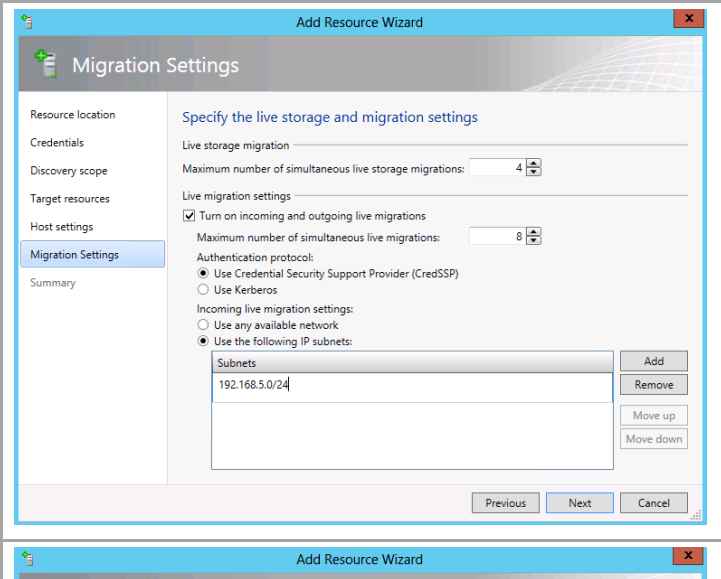
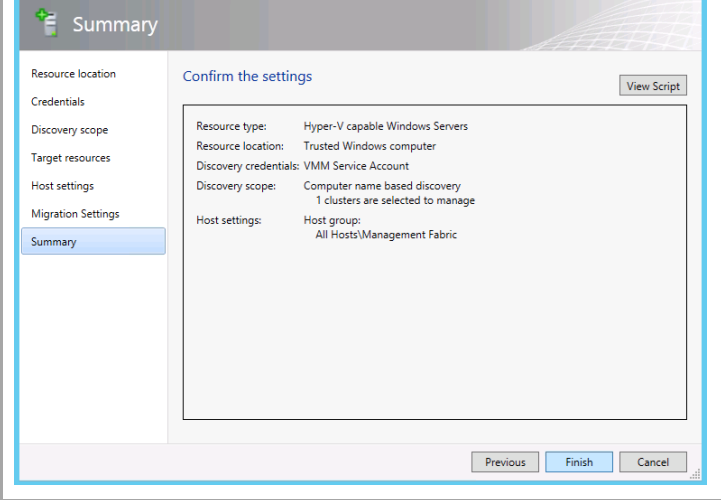
Select the computers that you want to add as hosts

Discovered computers:

Computer Name	Operating System	Hypervisor
Mgmt-Cluster01.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHost-Mgmt02.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-MGMT01.flexpod.test	Windows Server 2012 Datacenter	Hyper-V

Select all Refresh Stop

Previous Next Cancel

	
Set live migration settings. Default is 2 for each. Check the box Turn on incoming and out going live migrations . Set the IP subnet for live migration network.	
Click Finish	

Verify job completion.

Name	Status	Start Time	Result Name
Refresh host cluster		0 % 10/8/2013 3:08:08 PM	Mgmt-Cluster01.flexpod.test
Add virtual machine host		50 % 10/8/2013 3:08:07 PM	VMHOST-MGMT01.flexpod.test
Add virtual machine host		50 % 10/8/2013 3:08:07 PM	VMHost-Mgmt02.flexpod.test
Create new host cluster	Completed	10/8/2013 3:08:06 PM	Mgmt-Cluster01.flexpod.test

Verify that the hosts are added.

Fabric

- Servers
 - All Hosts
 - Management Fabric
 - Mgmt-Cluster01
 - VMHOST-MGMT01
 - VMHost-Mgmt02

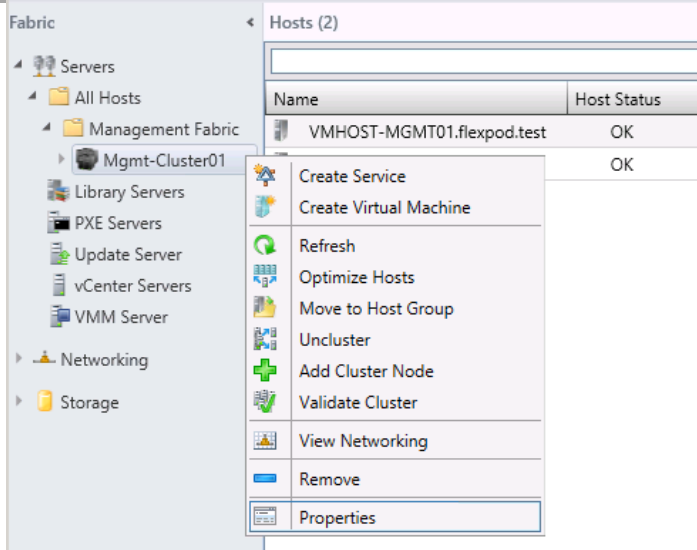
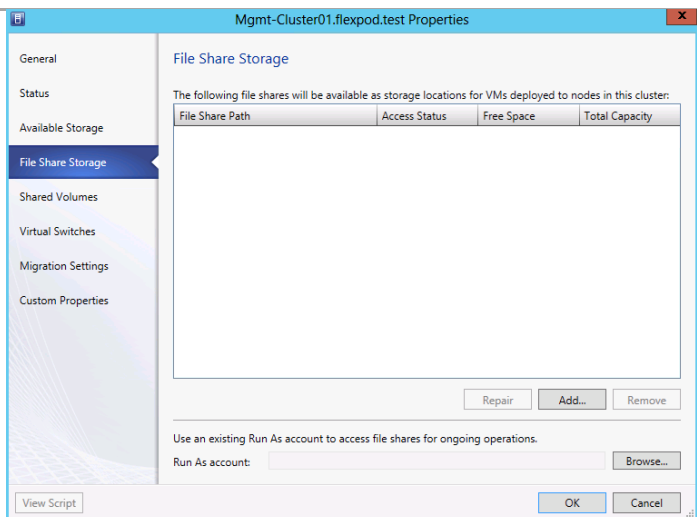
Hosts (2)

Name	Host Status	Role
VMHOST-MGMT01.flexpod.test	OK	Host
VMHost-Mgmt02.flexpod.test	OK	Host

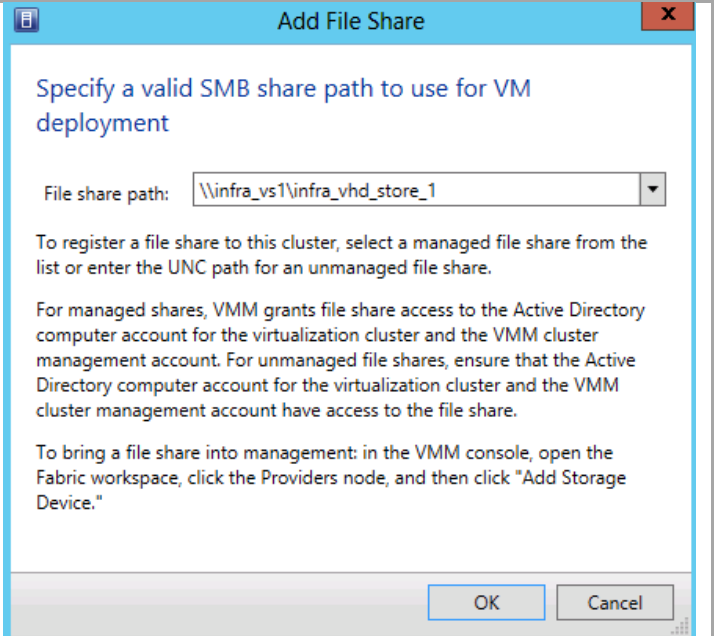
14.7 Register the File Share to the Management Cluster

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 Serves , 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.



Add File Share

Specify a valid SMB share path to use for VM deployment

File share path:

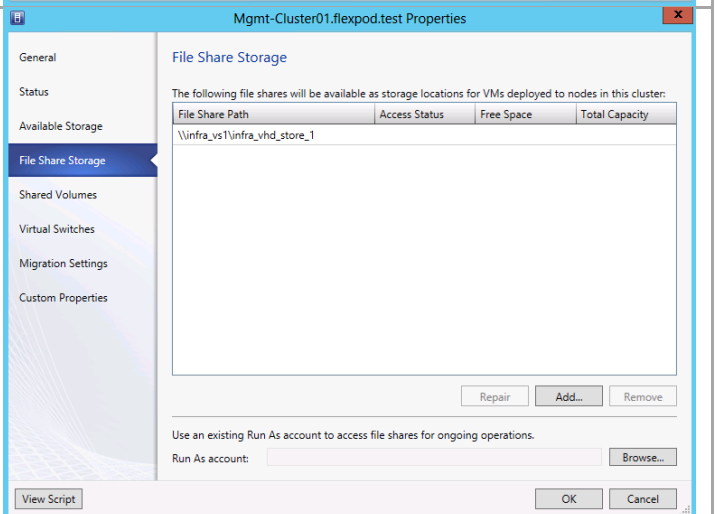
To register a file share to this cluster, select a managed file share from the list or enter the UNC path for an unmanaged file share.

For managed shares, VMM grants file share access to the Active Directory computer account for the virtualization cluster and the VMM cluster management account. For unmanaged file shares, ensure that the Active Directory computer account for the virtualization cluster and the VMM cluster management account have access to the file share.

To bring a file share into management: in the VMM console, open the Fabric workspace, click the Providers node, and then click "Add Storage Device."

OK Cancel

Click **Browse** to add a **Run As** account.



Mgmt-Cluster01.flexpod.test Properties

General
Status
Available Storage
File Share Storage
Shared Volumes
Virtual Switches
Migration Settings
Custom Properties

File Share Storage

The following file shares will be available as storage locations for VMs deployed to nodes in this cluster:

File Share Path	Access Status	Free Space	Total Capacity
\\infra_vs1\infra_vhd_store_1			

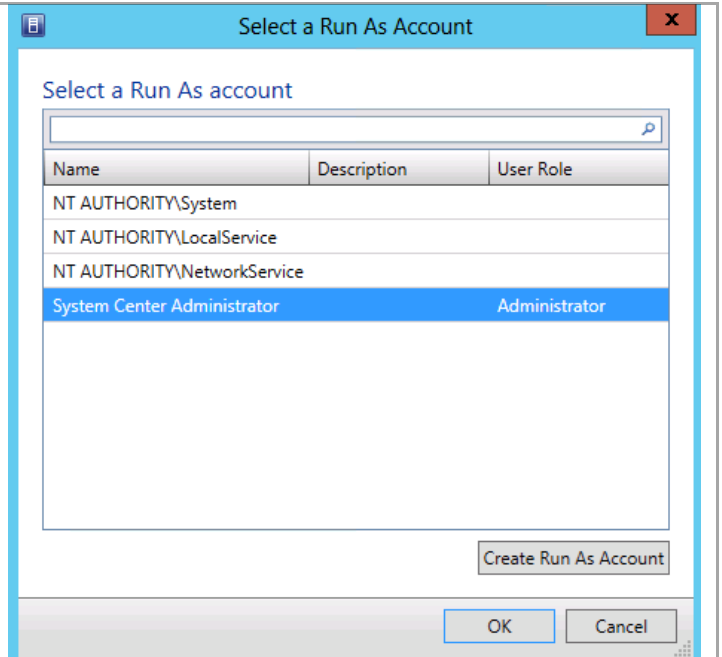
Repair Add... Remove

Use an existing Run As account to access file shares for ongoing operations.

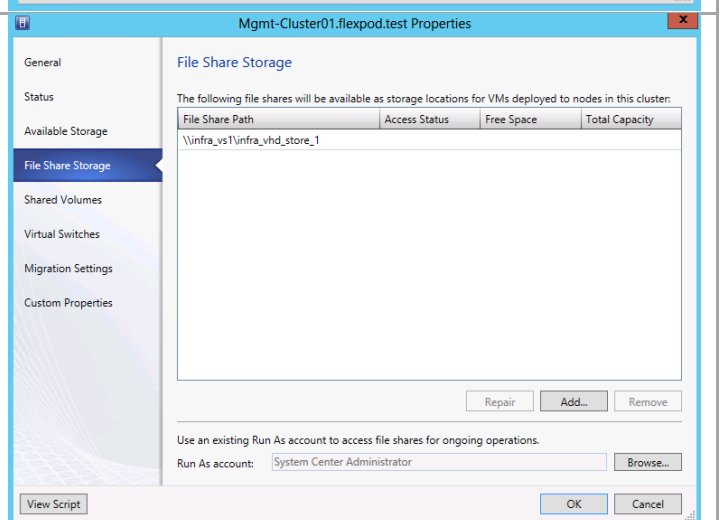
Run As account: Browse...

View Script OK Cancel

Select the Run As account and click **OK**.



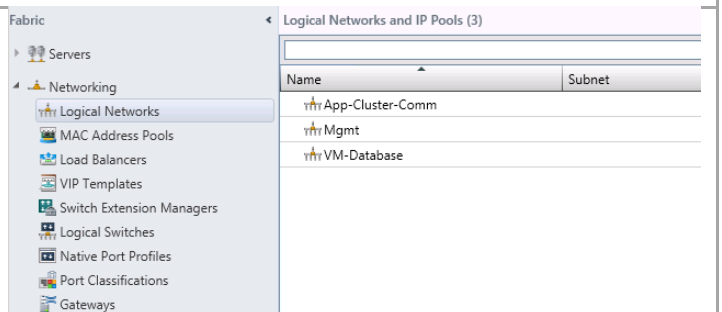
Click **OK** to register the file share.



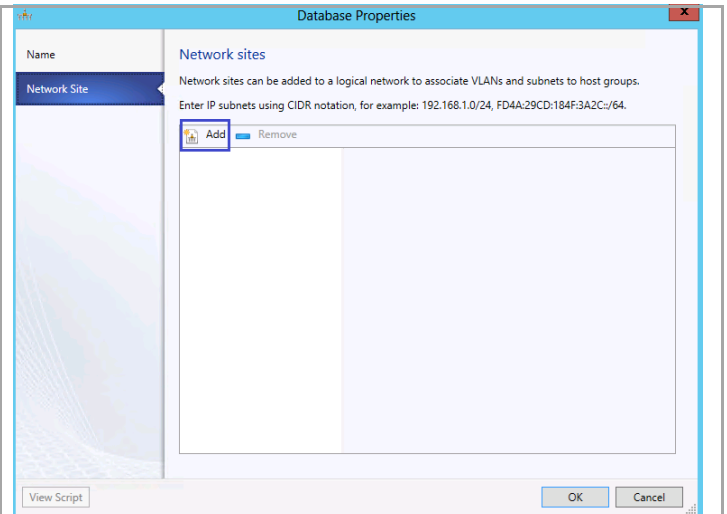
14.8 Configure Logical Networks

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

Select Fabric and Networking. Select each 1 Logical Networks and click Properties.



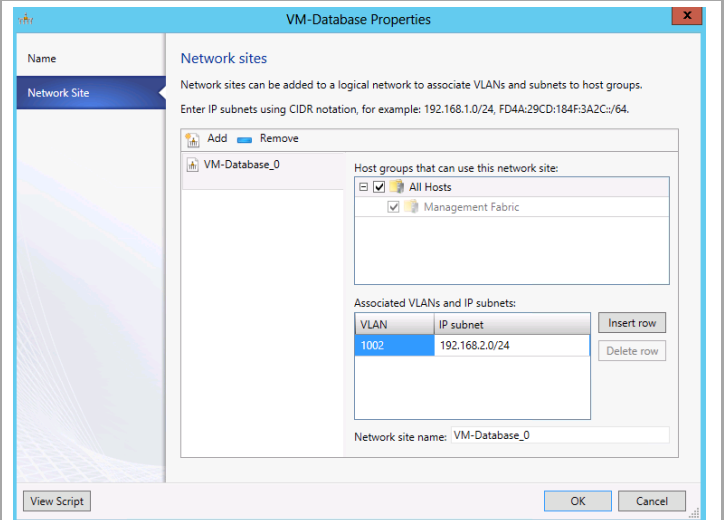
Select Network Site and click add.



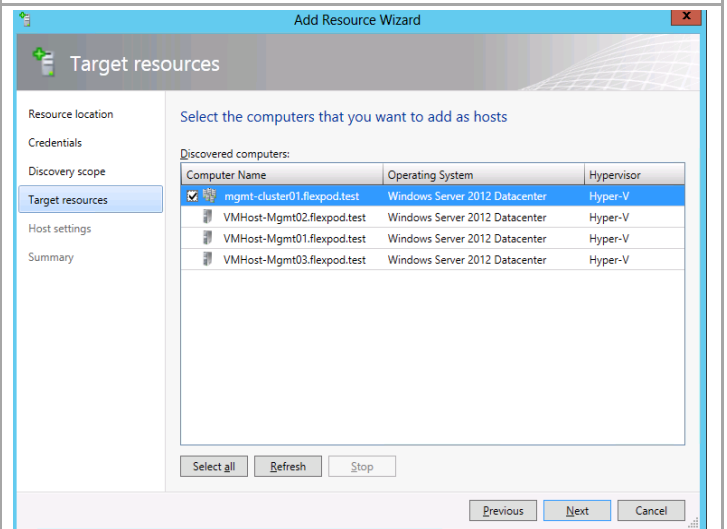
Check All Hosts. Click Insert row. Enter the VLAN ID and IP subnet the network site. Click OK.

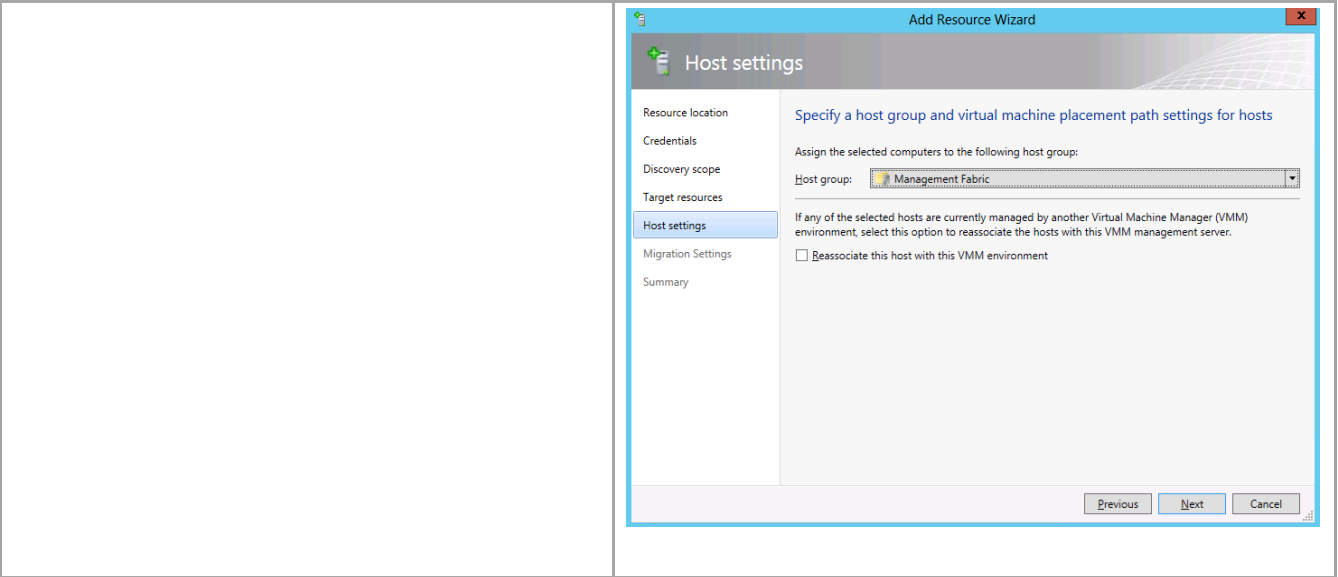
Repeat this procedure for each Logical Network.

Note: Enter 0 for the VLAN ID for the native VLAN.



Click Select All and click Next.





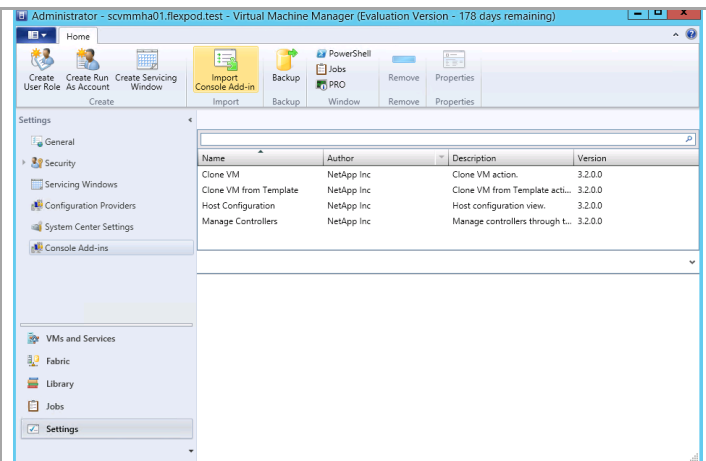
14.9 Install Cisco UCS User Interface Extensions for Virtual Machine Manager

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=1.0.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

► Perform the following steps on both **Virtual Machine Manager** virtual machine.

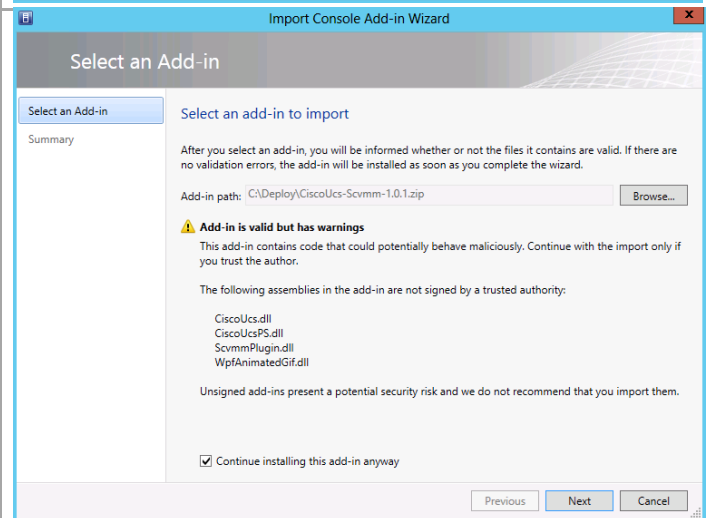
In the **Virtual Machine Manager** console, navigate to the **Settings** pane and select the **Import Console Add-in**



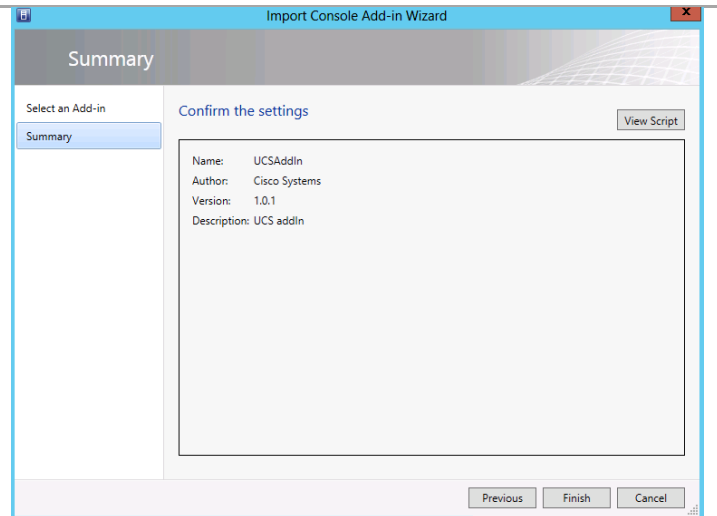
On the Import Console Add-in Wizard, click **Browse** on the Add-in Path. Select the **Cisco UCS UI Extensions for Virtual Machine Manager** package and click **Open**.

Note: The warning about signed binaries can safely be ignored in this case.

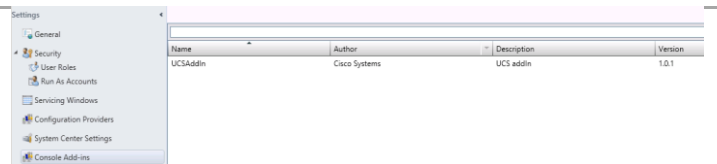
Click the check box **“Continue installing this add-in anyway”** and click **Next** to continue.



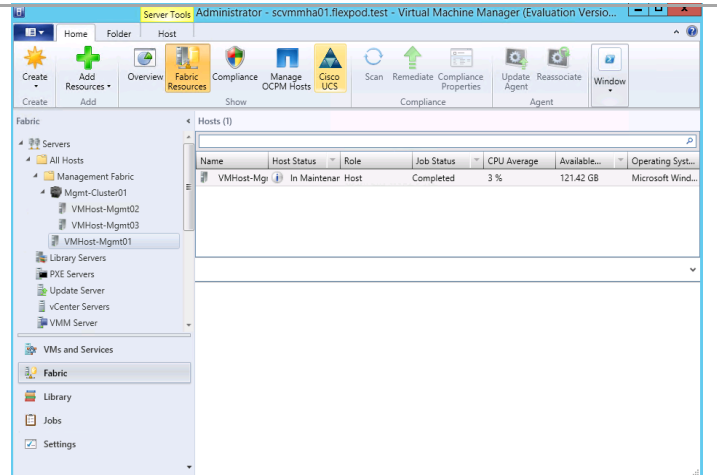
Review the summary information and click **Finish**.



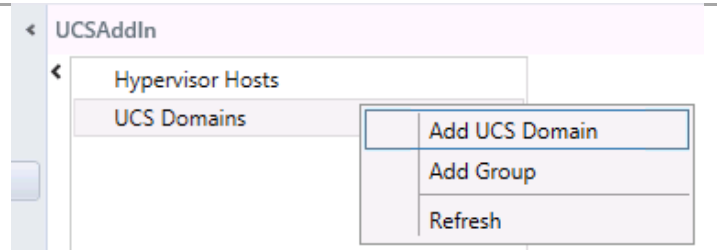
Click Console Add-ins to view the installed UCS User Interface Extensions.



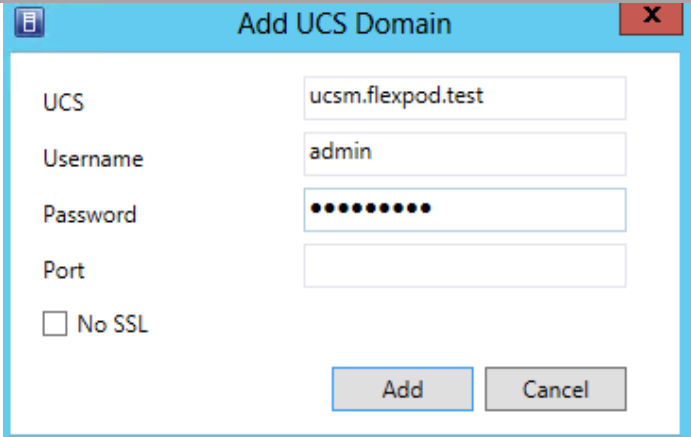
Select **Fabric** in the left pane and click the **Cisco UCS** icon.



Right click **UCS Domain** and select **Add UCS Domain**.

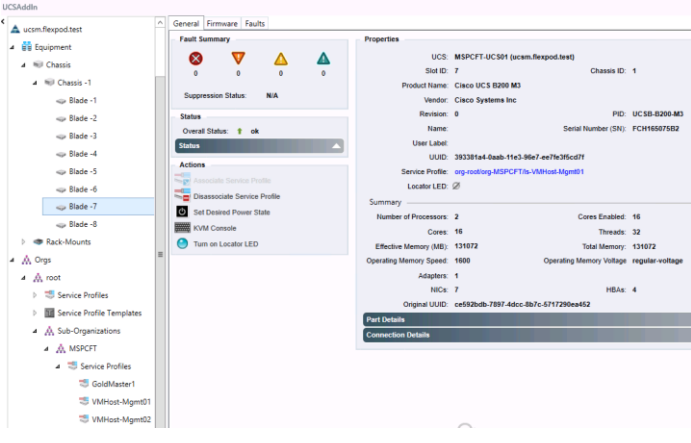


Enter the **UCS Manager host name**, **admin account**, and **password**. Click **Add**.



The 'Add UCS Domain' dialog box is shown. It has a title bar with a close button. The fields are: UCS (ucsm.flexpod.test), Username (admin), Password (masked with dots), and Port (empty). There is a 'No SSL' checkbox which is unchecked. At the bottom right are 'Add' and 'Cancel' buttons.

The UCS Manager objects are displayed in the review view pane.



The review view for the UCS Manager domain 'ucsm.flexpod.test' is displayed. The left pane shows a tree view with 'Equipment' expanded, showing 'Chassis' and 'Blade' objects. The main pane shows the 'Properties' tab for the selected object, displaying details like 'Product Name: Cisco UCS B200 M3', 'Vendor: Cisco Systems Inc', 'Revision: 0', 'Name: UC5B-B200-M3', 'Serial Number (SN): FCH15507582', 'User Label: 393381ad-6a0b-11e3-90e7-ee763ffcd7f1', 'Service Profile: mg-mgmt-MSPCFT13a-Virtual-Mgmt01', 'Locator LED: 0', 'Number of Processors: 2', 'Cores Enabled: 16', 'Cores: 16', 'Threads: 32', 'Effective Memory (MB): 131072', 'Total Memory: 131072', 'Operating Memory Speed: 1600', 'Operating Memory Voltage: regular voltage', 'Adapters: 1', 'NICs: 7', 'HBAs: 4', 'Original UUID: ce582b0b-788f-4dce-8b7c-5717290ae452'.

15 Install and Configure Nexus 1000V for Hyper-V

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

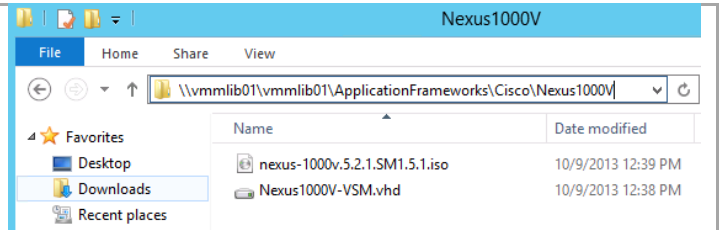
- Virtual Supervisor Module (VSM) ISO (Nexus-1000V-5.2.1.SM1.5. 1.iso)
- Virtual Ethernet Module (VEM) MSI package (Nexus1000V-VEM-5.2.1.SM1.5.1.0.msi)
- Cisco VSEM Provider MSI package (Nexus1000V-VSEMPProvider-5.2.1SM1.5.1.0.msi)
- Nexus 1000V Virtual Machine Template(Nexus1000V-VSM-Template.xml)
- Nexus 1000V VSM Virtual Hard Drive (Nexus1000V-VSM.vhd)

Nexus 1000V for Hyper-V can be downloaded at the following link:

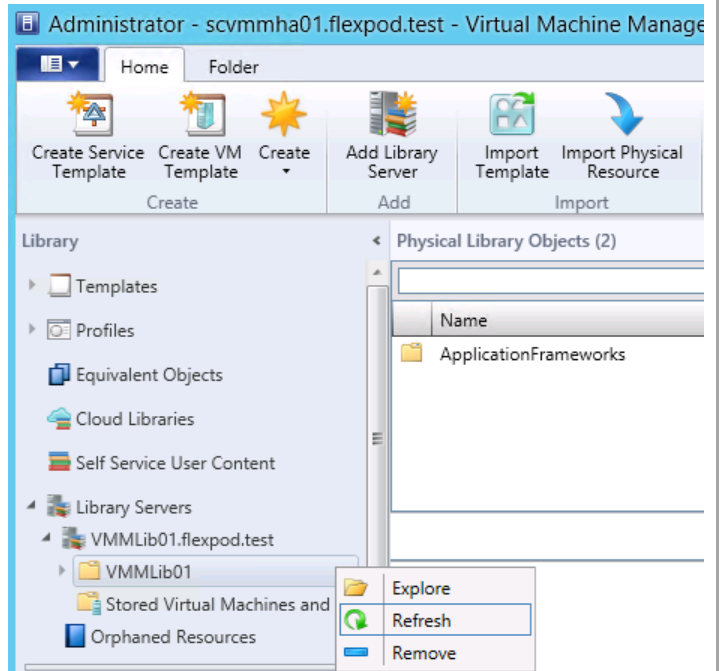
[http://software.cisco.com/download/release.html?mdfid=284786025&flowid=42792&softwareid=282088129&release=5.2\(1\)SM1\(5.1\)&relind=AVAILABLE&rellifecycle=&reltype=latest](http://software.cisco.com/download/release.html?mdfid=284786025&flowid=42792&softwareid=282088129&release=5.2(1)SM1(5.1)&relind=AVAILABLE&rellifecycle=&reltype=latest)

15.1 Intall the Virtual Supervisor Modules Virtual Machine Template

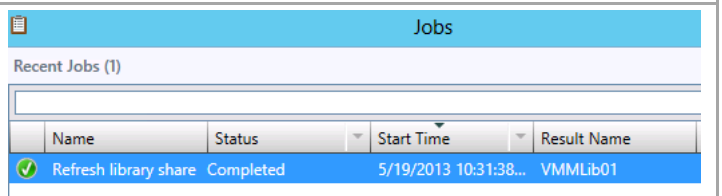
Copy the Nexus 1000V ISO image and VHD to the VMM Library share created earlier.



In Virtual Machine Manager, click Library and select the library share. Right click the share and select Refresh.

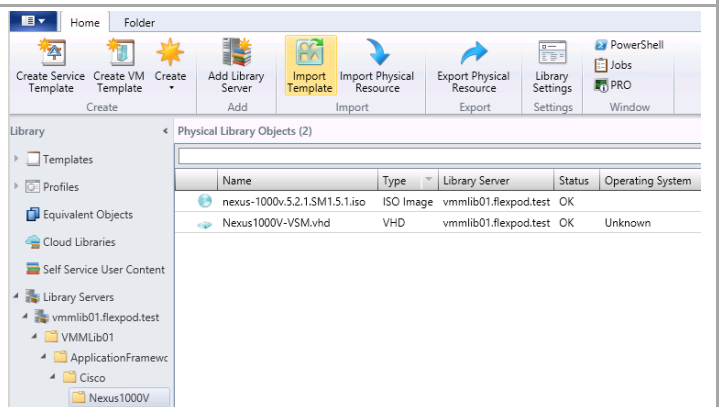


Verify that the refresh operation completed successfully.

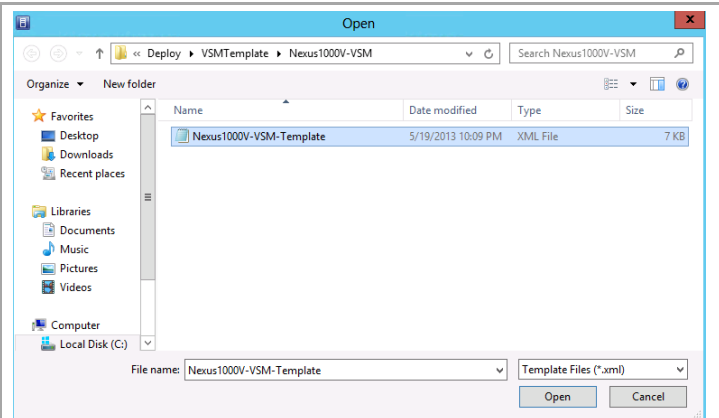


Navigate the library share structure and verify the location of the Nexus 1000V VSM ISO image.

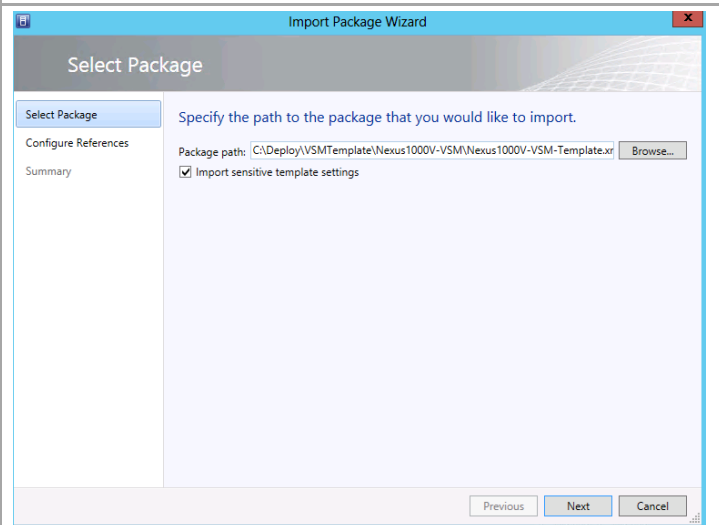
Click Import Library.



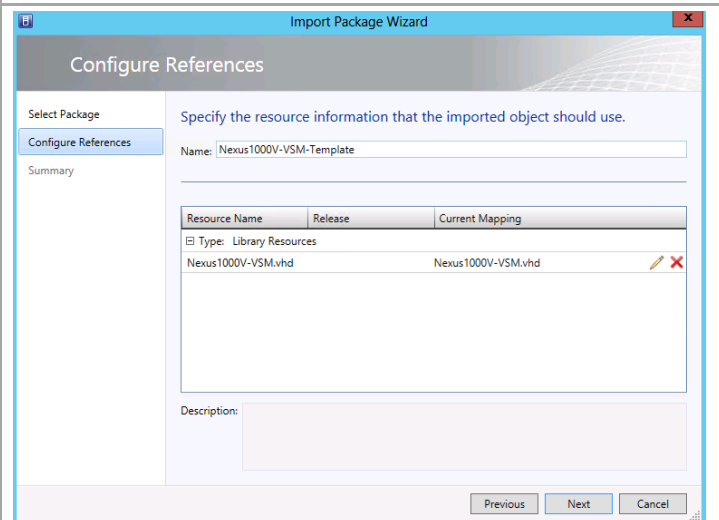
Browes to the location of the Nexus 1000V VSM virtual machine template and click Open.



Click Next to proceede.



Review the configuraiotn refrences and click Next to proceed.



Review the summary and click Import.

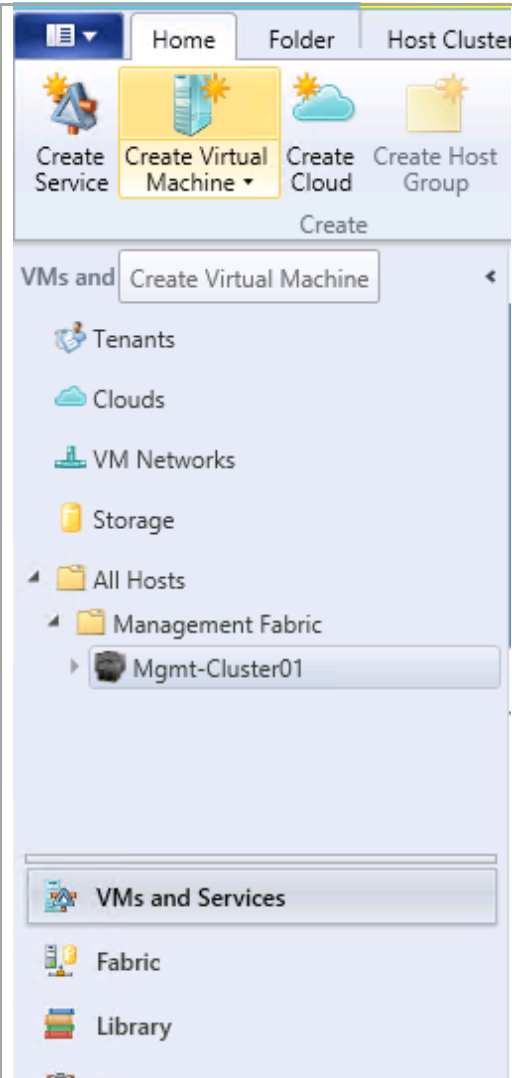
The screenshot shows the 'Import Package Wizard' window with the 'Summary' tab selected. The window has a blue title bar and a sidebar on the left with three buttons: 'Select Package', 'Configure References', and 'Summary' (which is highlighted). The main area is titled 'Confirm the settings' and contains a 'View Script...' button. Below this, there is a large text box displaying the following information:

Package Location: C:\Deploy\VSMTTemplate\Nexus1000V-VSM\Nexus1000V-VSM-Template.xml
Name: Nexus1000V-VSM-Template
Release:

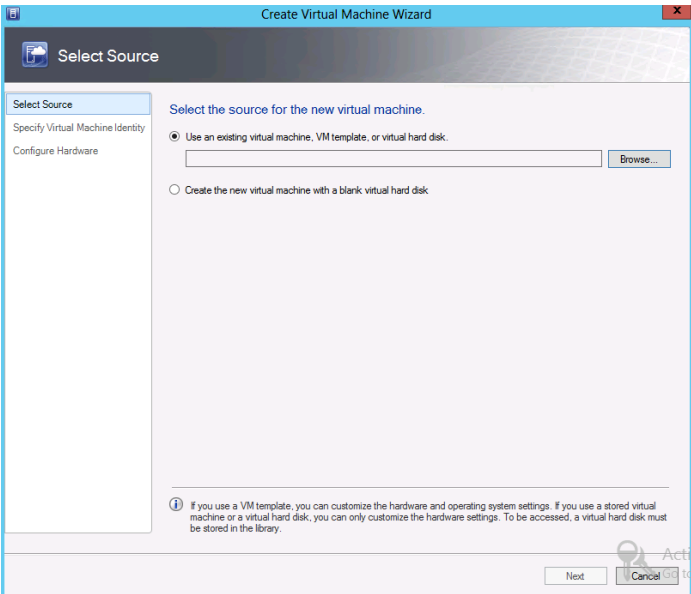
At the bottom of the window, there are three buttons: 'Previous', 'Import', and 'Cancel'.

15.2 Create the Virtual Supervisor Modules in the VMS Virtual Machines

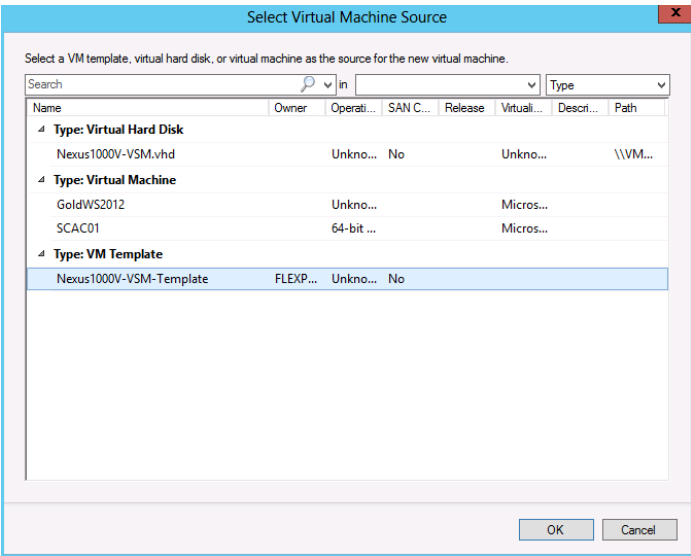
Select VMs and Services and click Create Virtual Machine



Select the default option Use and existing virtual machine, VM template, or virtual hard disk. Click **Browse.**



Select the **Nexus 1000V-VSM-Template** and click **OK.**



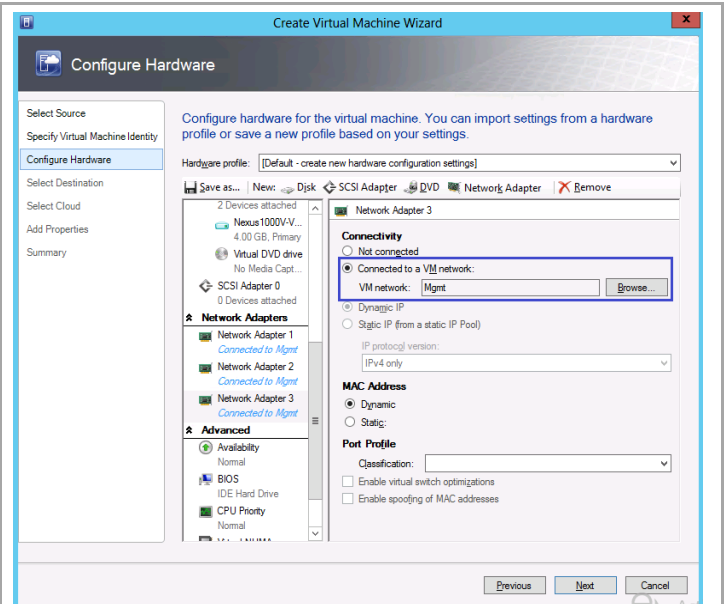
Click **Next** to proceed.

The screenshot shows the 'Create Virtual Machine Wizard' window, specifically the 'Select Source' step. The left sidebar contains a list of steps: 'Select Source' (highlighted), 'Specify Virtual Machine Identity', 'Configure Hardware', 'Select Destination', 'Select Cloud', 'Add Properties', and 'Summary'. The main area is titled 'Select the source for the new virtual machine.' and contains two radio button options. The first option, 'Use an existing virtual machine, VM template, or virtual hard disk.', is selected. Below it, a text box contains 'Nexus1000V-VSM-Template' and a 'Browse...' button. The second option is 'Create the new virtual machine with a blank virtual hard disk'. At the bottom right, there are 'Next' and 'Cancel' buttons. A small information icon and text at the bottom state: 'If you use a VM template, you can customize the hardware and operating system settings. If you use a stored virtual machine or a virtual hard disk, you can only customize the hardware settings. To be accessed, a virtual hard disk must be stored in the library.'

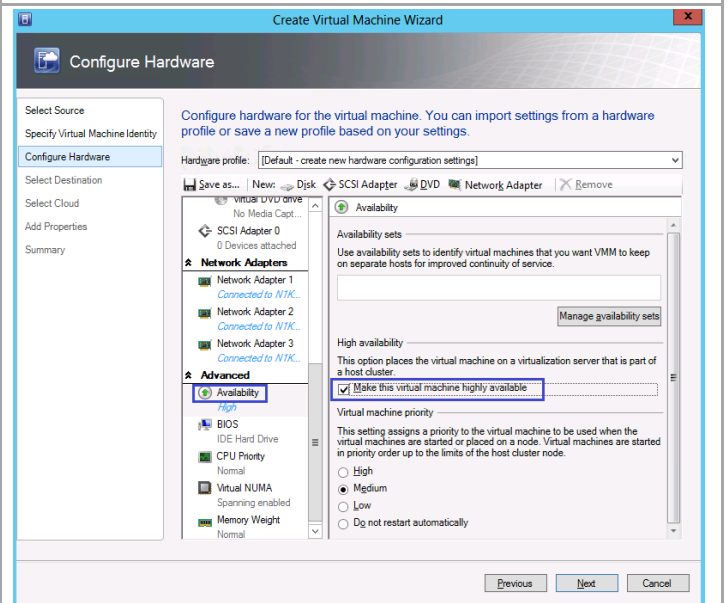
Enter the virtual machine name and click Next.

The screenshot shows the 'Create Virtual Machine Wizard' window, specifically the 'Specify Virtual Machine Identity' step. The left sidebar contains a list of steps: 'Select Source', 'Specify Virtual Machine Identity' (highlighted), 'Configure Hardware', 'Select Destination', 'Select Cloud', 'Add Properties', and 'Summary'. The main area is titled 'Specify Virtual Machine Identity' and contains two text input fields. The first is 'Virtual machine name:' with the value 'N1KV-VSM01'. The second is 'Description:' with an empty text box. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons. A small information icon and text at the bottom state: 'The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, using the same name ensures consistent displays in System Center Operations Manager.'

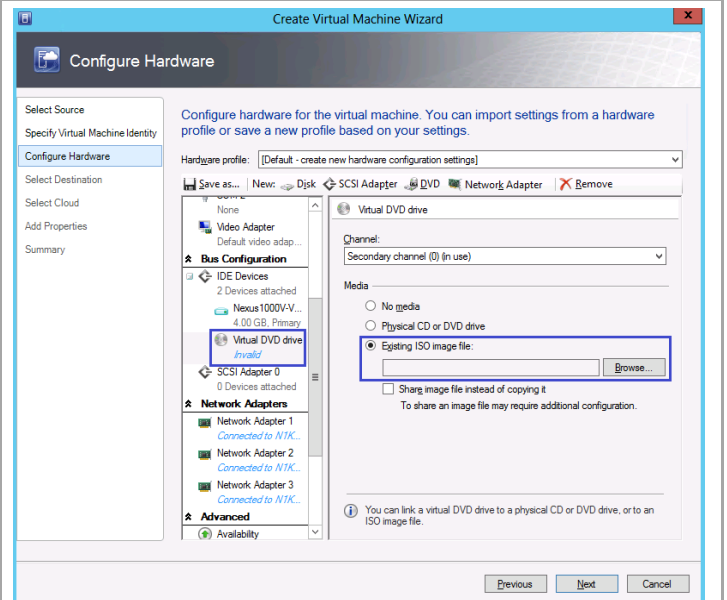
Navigate the the three network adapters in the center pane. Configure all three adaptaters to connect to the Mgmt VM Network.



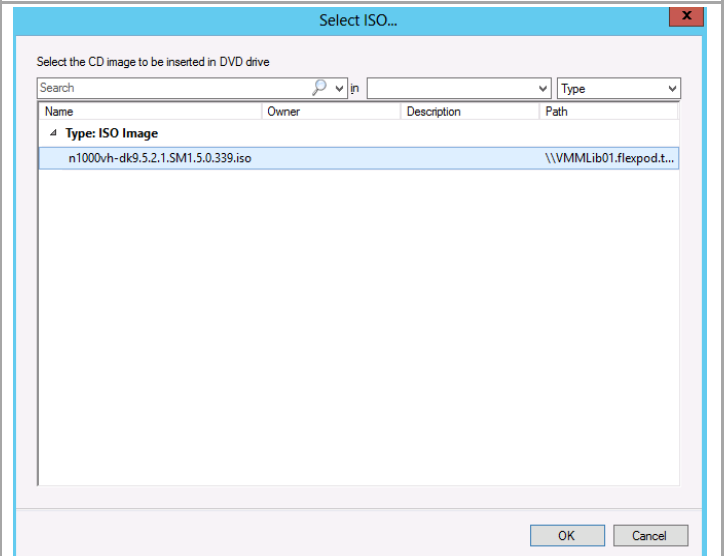
Scroll down to the Advance objects in the middle pane and select Availability. Check the box Make this virtual machine highly available.



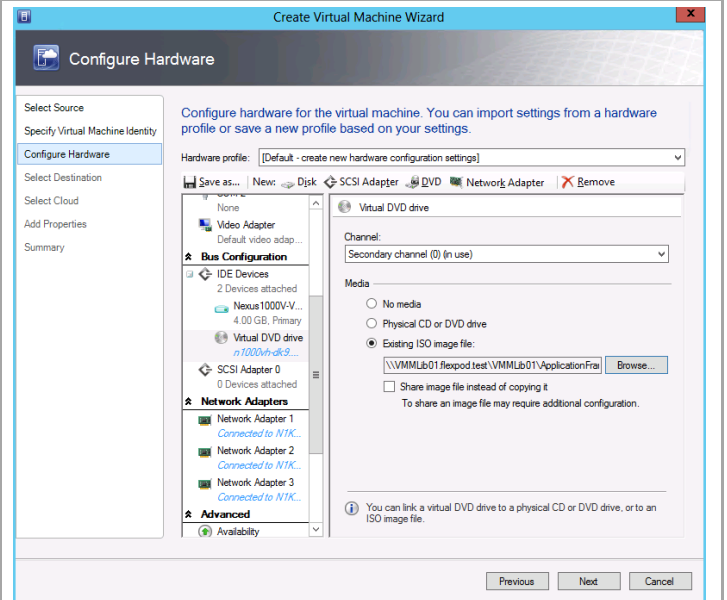
Scroll up to the Bus Configuration objects in the middle pane and select Virtual DVD drive. In the right pane select Existing DVD and click Browse...



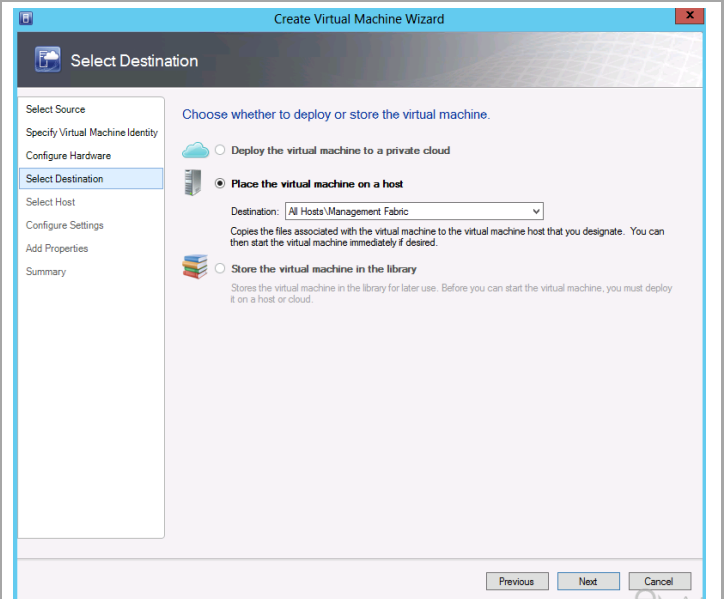
Select the Nexus 1000V VMS ISO and click OK.



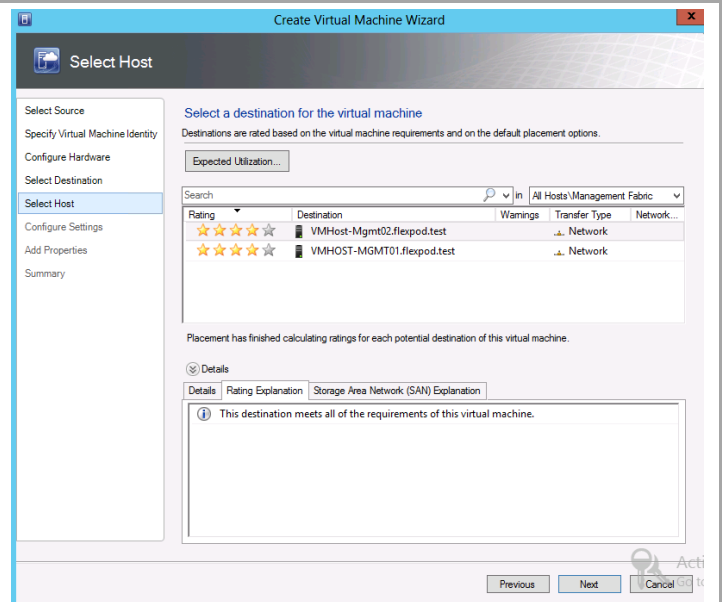
Click Next to proceed.



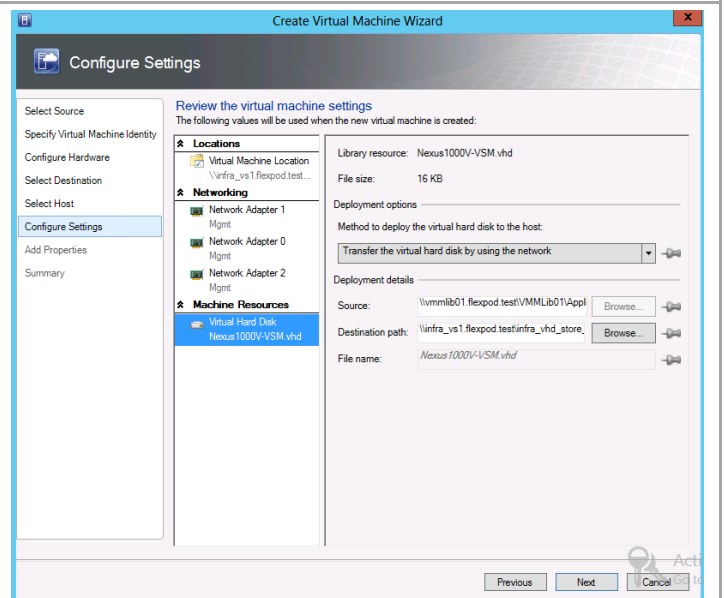
Select the default placement option to place the virtual machine on all hosts and click Next.



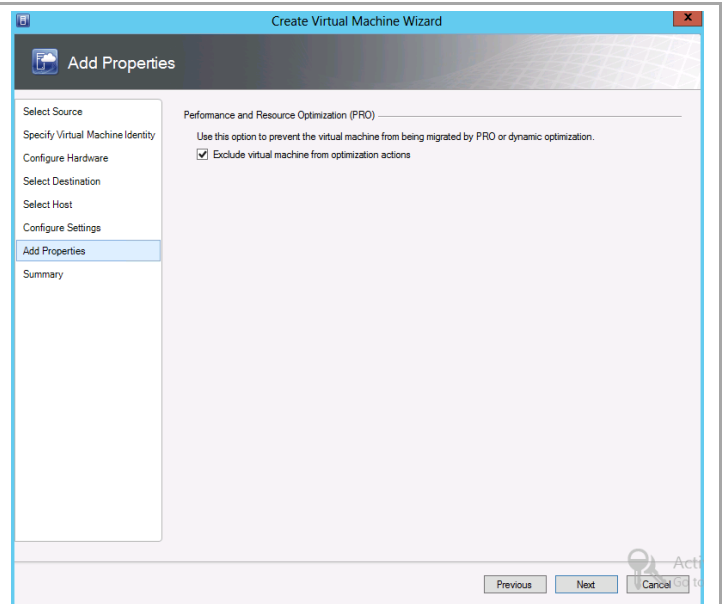
In the Select Host window, click Next.



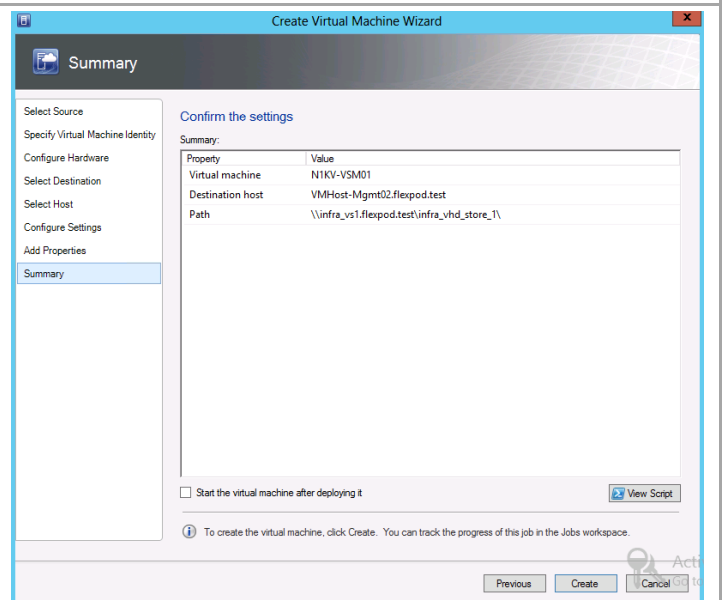
Review the path to store the virtual machine configuration and VHD. Click Next to proceed.



In the add properties window select “**Exclude virtual machine from optimization actions**”. Click **Next** to proceed.



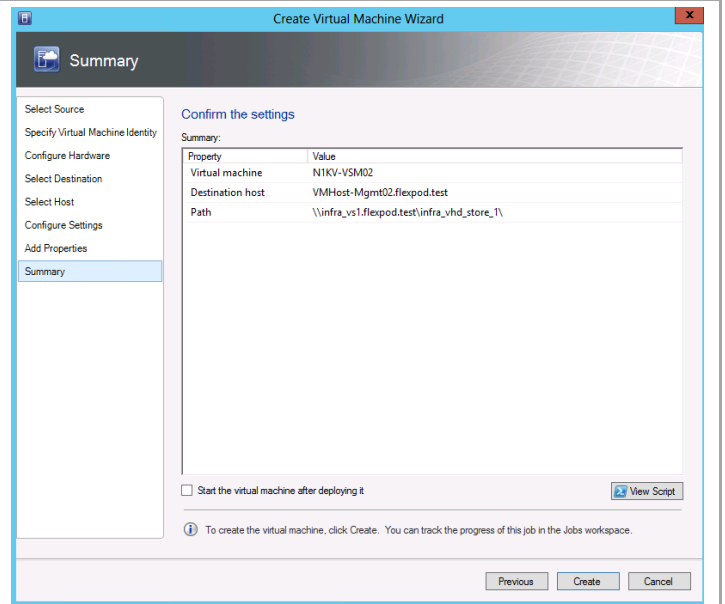
Review the summary and click **Create**.



Verify that virtual machine is created successfully.

	Name	Status	Start Time	Result Name
✓	Create virtual machine	Completed	10/9/2013 3:17:39 PM	N1KV-VSM01
✓	Update the placement settings...	Completed	10/9/2013 3:11:11 PM	N1KV-VSM01
✓	Modify existing VM deployme...	Completed	10/9/2013 3:11:11 PM	N1KV-VSM01
✓	Create new VM deployment co...	Completed	10/9/2013 3:08:41 PM	N1KV-VSM01
✓	Create virtual machine			
Step	Name	Status		
✓ 1	Create virtual machine	Completed		
✓ 1.1	Create virtual machine	Completed		
✓ 1.2	Deploy file (using LAN)	Completed		
✓ 1.3	Change properties of virtual machine	Completed		
✓ 1.4	Fix up differencing disks	Completed		

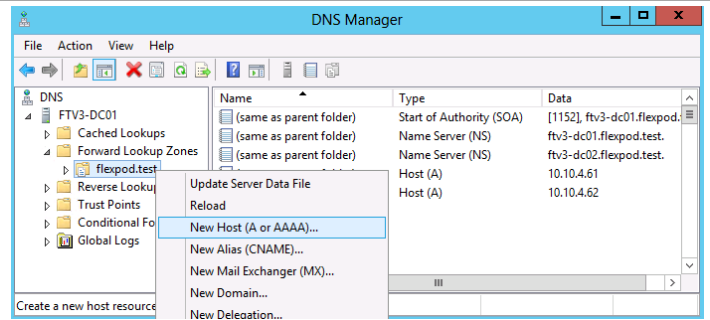
Repeat this procedure to create the second VSM virtual machine. Place the second VSM.



15.3 Add a Domain Name Service Record for the Virtual Supervisor Module

Perform the following configuration operation on the server running Domain Name Service.

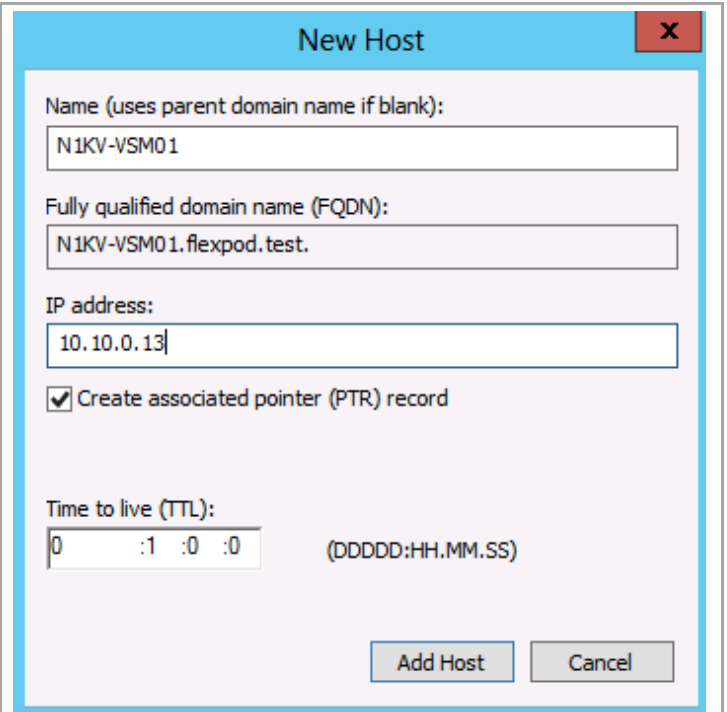
Open DNS Manager and navigate the forward lookup zone for the domain. Right click the forward lookup zone and select New Host (A or AAAA) ...



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.



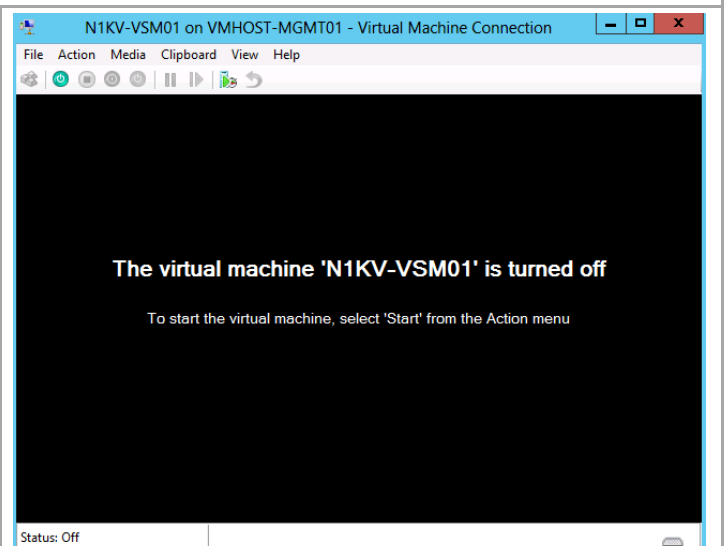
The 'New Host' dialog box is shown with a blue title bar and a red close button. It contains the following fields and options:

- Name (uses parent domain name if blank):** N1KV-VSM01
- Fully qualified domain name (FQDN):** N1KV-VSM01.flexpod.test.
- IP address:** 10.10.0.13
- ☒ **Create associated pointer (PTR) record**
- Time to live (TTL):** 0 : 1 : 0 : 0 (DDDD:HH.MM.SS)
- Buttons:** Add Host, Cancel

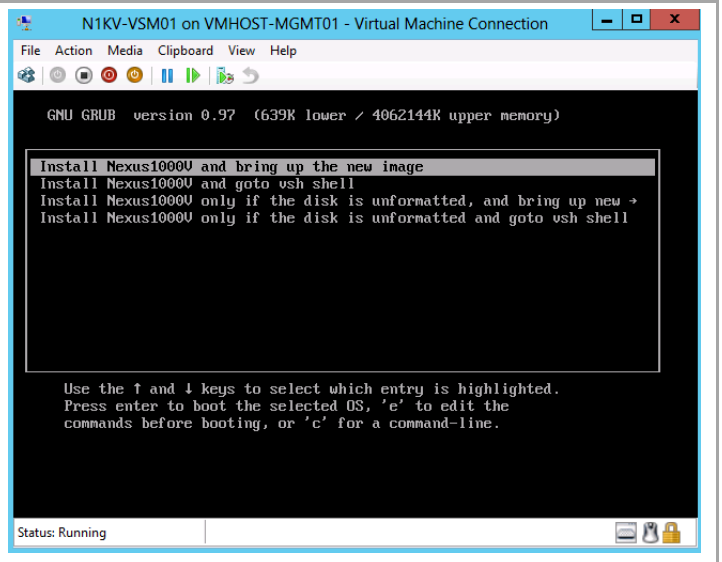
15.4 Configure Virtual Supervisor Modules in the VMS Virtual Machines

Perform the following configuration operation on the first VSM virtual machine.

In VMM, connect to the first VSM01 VM and power it on.



Select Install Nexus 1000V and bring up the new image. Hit Return.

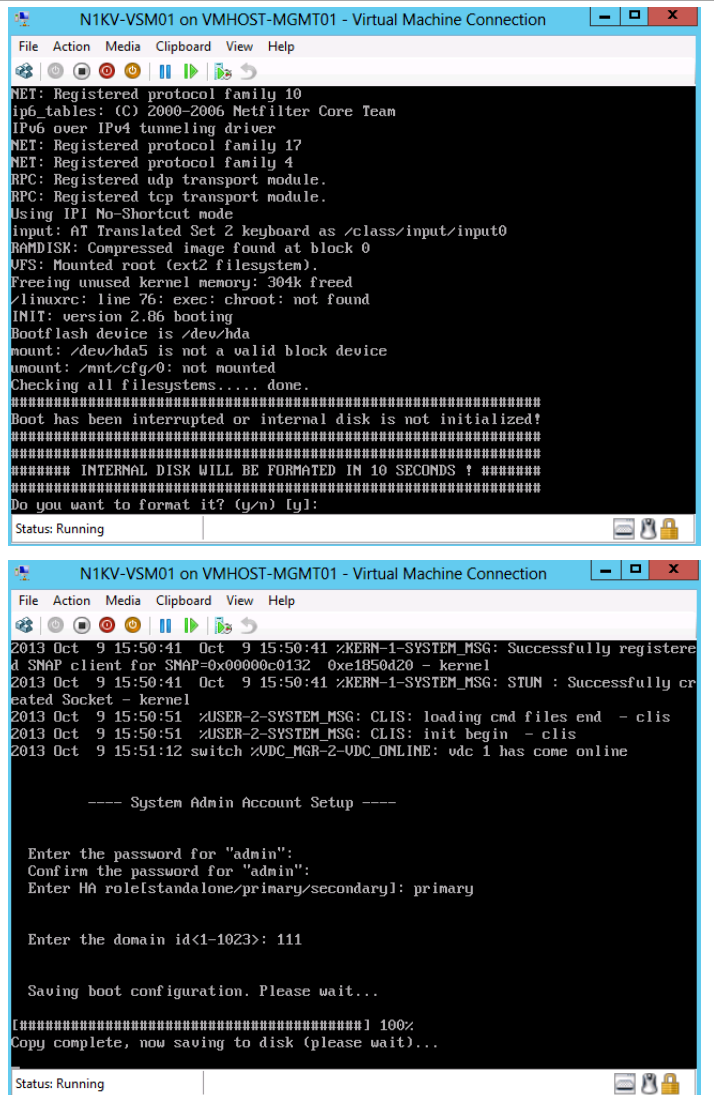


The Virtual Machine Viewer window opens up. While it processes, it stops at the command prompt with the following message: Do you want to format it? (y/n). **Enter Y for yes at the prompt.**

At the next command prompt, the following message is displayed: Perform r/w tests (takes very long time) on target disks? (y/n). **Enter Y for yes at the prompt.**

You are prompted to enter the System Administrator Account Setup. At the Enter the password for "admin": prompt, enter the password. At the Confirm the password for "admin": prompt, re-enter the password.

Enter the high availability (HA) role at the next prompt enter **Primary**.



```
N1KV-VSM01 on VMHOST-MGMT01 - Virtual Machine Connection
File Action Media Clipboard View Help

NET: Registered protocol family 10
ip6_tables: (C) 2000-2006 Netfilter Core Team
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 17
NET: Registered protocol family 4
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
Using IPI No-Shortcut mode
input: AT Translated Set 2 keyboard as /class/input/input0
RAMDISK: Compressed image found at block 0
VFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 304k freed
/linuxrc: line 76: exec: chroot: not found
INIT: version 2.86 booting
Bootflash device is /dev/hda
mount: /dev/hda5 is not a valid block device
umount: /mnt/cfg/0: not mounted
Checking all filesystems..... done.
=====
Boot has been interrupted or internal disk is not initialized!
=====
##### INTERNAL DISK WILL BE FORMATED IN 10 SECONDS ! #####
Do you want to format it? (y/n) [y]:

Status: Running

N1KV-VSM01 on VMHOST-MGMT01 - Virtual Machine Connection
File Action Media Clipboard View Help

2013 Oct 9 15:50:41 Oct 9 15:50:41 %KERN-1-SYSTEM_MSG: Successfully registered SNAP client for SNAP=0x00000c0132 0xe1850d20 - kernel
2013 Oct 9 15:50:41 Oct 9 15:50:41 %KERN-1-SYSTEM_MSG: STUN : Successfully created Socket - kernel
2013 Oct 9 15:50:51 %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2013 Oct 9 15:50:51 %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2013 Oct 9 15:51:12 switch %UDC_MGR-2-UDC_ONLINE: vdc 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

Saving boot configuration. Please wait...
[=====] 100%
Copy complete, now saving to disk (please wait)...

Status: Running
```

Enter **Y** to enter the basic configuration.

Enter **N** to creating and another login account.

Enter the switch name : N1KV-VSM01

Enter **Y** to configure Out-of-Band management interface.

Enter the Mgmt0 IPv4 address: 10.10.0.13

Enter the IPv4 netmask: 255.255.255.0

Enter **Y** to configure the default gateway.

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 **N** not to enable telnet service.

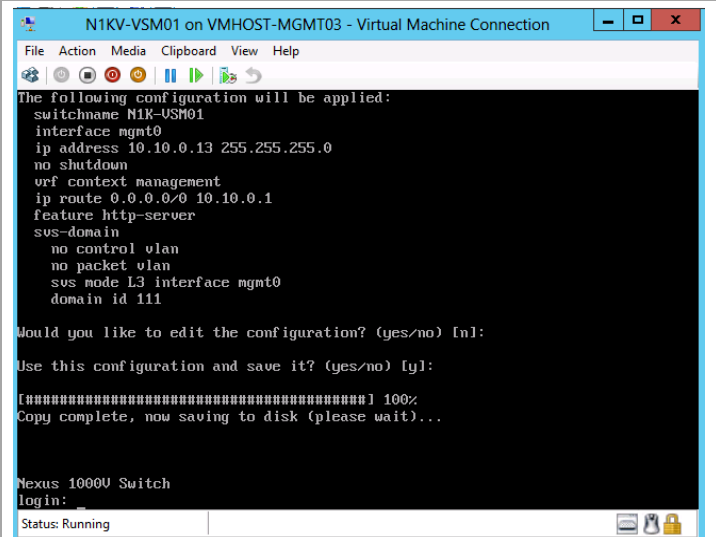
Enter **Y** to enable ssh service.

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.

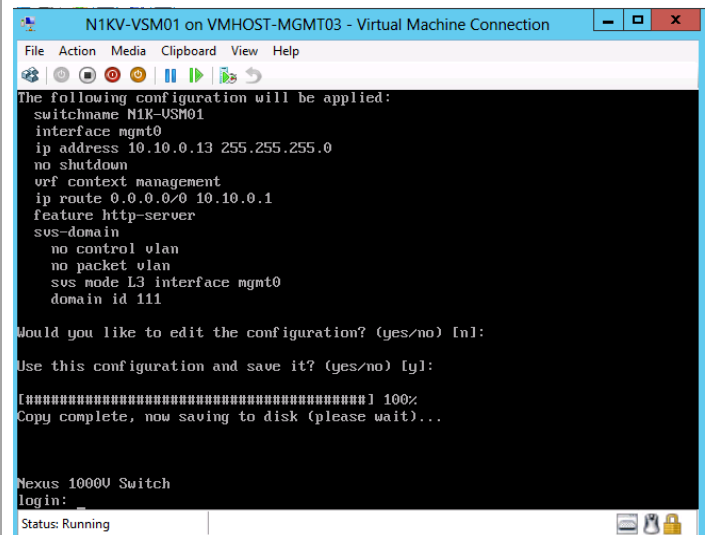


```
N1KV-VSM01 on VMHOST-MGMT03 - Virtual Machine Connection
File Action Media Clipboard View Help

The following configuration will be applied:
switchname N1K-USM01
interface mgmt0
ip address 10.10.0.13 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.10.0.1
feature http-server
svs-domain
no control vlan
no packet vlan
svs mode L3 interface mgmt0
domain id 111

Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[#####] 100%
Copy complete, now saving to disk (please wait)...

Nexus 1000V Switch
login:
Status: Running
```

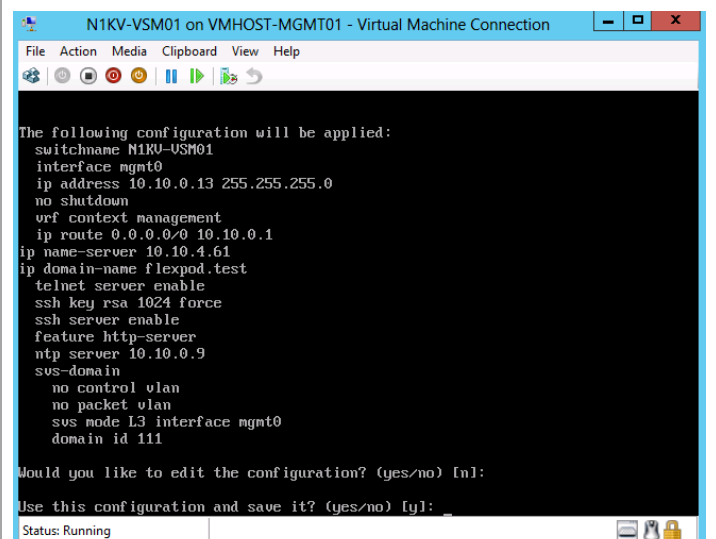


```
N1KV-VSM01 on VMHOST-MGMT03 - Virtual Machine Connection
File Action Media Clipboard View Help

The following configuration will be applied:
switchname N1K-USM01
interface mgmt0
ip address 10.10.0.13 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.10.0.1
feature http-server
svs-domain
no control vlan
no packet vlan
svs mode L3 interface mgmt0
domain id 111

Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[#####] 100%
Copy complete, now saving to disk (please wait)...

Nexus 1000V Switch
login:
Status: Running
```



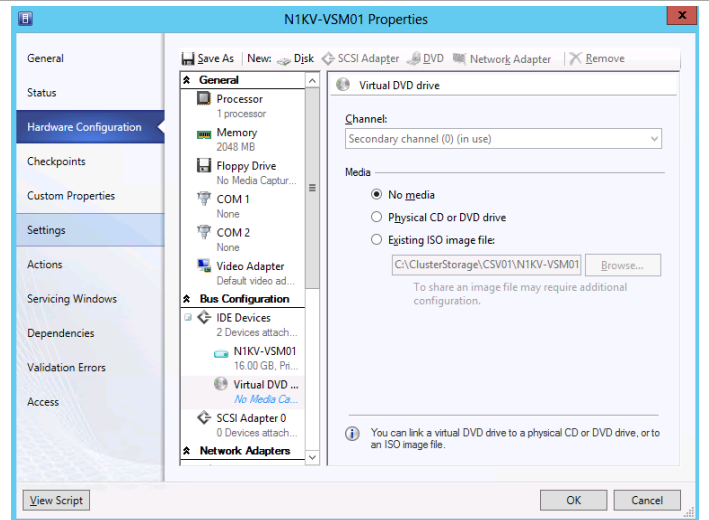
```
N1KV-VSM01 on VMHOST-MGMT01 - Virtual Machine Connection
File Action Media Clipboard View Help

The following configuration will be applied:
switchname N1K-USM01
interface mgmt0
ip address 10.10.0.13 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.10.0.1
ip name-server 10.10.4.61
ip domain-name flexpod.test
telnet server enable
ssh key rsa 1024 force
ssh server enable
feature http-server
ntp server 10.10.0.9
svs-domain
no control vlan
no packet vlan
svs mode L3 interface mgmt0
domain id 111

Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[#####] 100%
Copy complete, now saving to disk (please wait)...

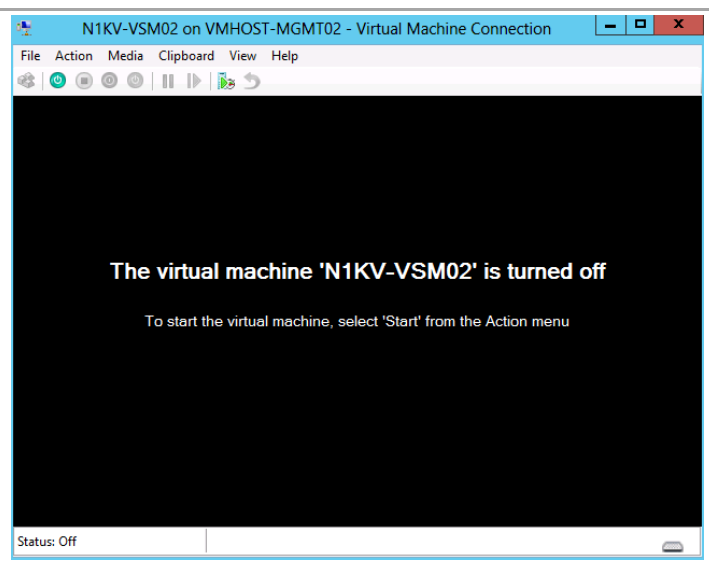
Nexus 1000V Switch
login:
Status: Running
```

Remove ISO from the first VSM Virtual Machine if there is an ISO image connected to the virtual machine.



Perform the following configuration operation on the SecondVSM virtual machine.

In VMM, connect to the first VSM02 VM and power it on.



Select Install Nexus 1000V and bring up the new image. Hit Return.

```
File Action Media Clipboard View Help
GNU GRUB version 0.97 (639K lower / 2096064K upper memory)

Install Nexus1000V and bring up the new image
Install Nexus1000V and goto vsh shell
Install Nexus1000V only if the disk is unformatted, and bring up new →
Install Nexus1000V only if the disk is unformatted and goto vsh shell

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

The Virtual Machine Viewer window opens up. While it processes, it stops at the command prompt with the following message: Do you want to format it? (y/n). Enter Y for yes at the prompt.

```
File Action Media Clipboard View Help
NET: Registered protocol family 10
ip6_tables: (C) 2000-2006 Netfilter Core Team
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 17
NET: Registered protocol family 4
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
Using IPI No-Shortcut mode
input: AT Translated Set 2 keyboard as /class/input/input0
RAMDISK: Compressed image found at block 0
JFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 304k freed
linuxrc: line 76: exec: chroot: not found
INIT: version 2.86 booting
Bootflash device is /dev/hda
mount: /dev/hda5 is not a valid block device
mount: /mnt/cfg/0: not mounted
Checking all filesystems..... done.
*****
***** Boot has been interrupted or internal disk is not initialized!
*****
***** INTERNAL DISK WILL BE FORMATED IN 10 SECONDS ! *****
Do you want to format it? (y/n) [y]:
```

At the next command prompt, the following message is displayed: Perform r/w tests (takes very long time) on target disks? (y/n). Enter Y for yes at the prompt.

You are prompted to enter the System Administrator Account Setup. At the Enter the password for "admin": prompt, enter the password. At the Confirm the password for "admin": prompt, re-enter the password.

```
File Action Media Clipboard View Help
Confirm the password for "admin":
Enter HA role(standalone/primary/secondary): secondary

Setting HA role to secondary will cause a system reboot. Are you sure (yes/no)?: yes

Enter the domain id(1-4095): 111

Saving boot configuration. Please wait...
[*****] 100%
Copy complete, now saving to disk (please wait)...

HA mode set to secondary. Rebooting now...
```

Enter the high availability (HA) role at the next prompt enter **secondary**.

Enter the domain ID: 111

Acknowledge that the system will reboot.

Login to the VMS and verify the redundancy status:

Show redundancy status

```
File Action Media Clipboard View Help
Redundancy mode
-----
administrative: HA
operational: HA

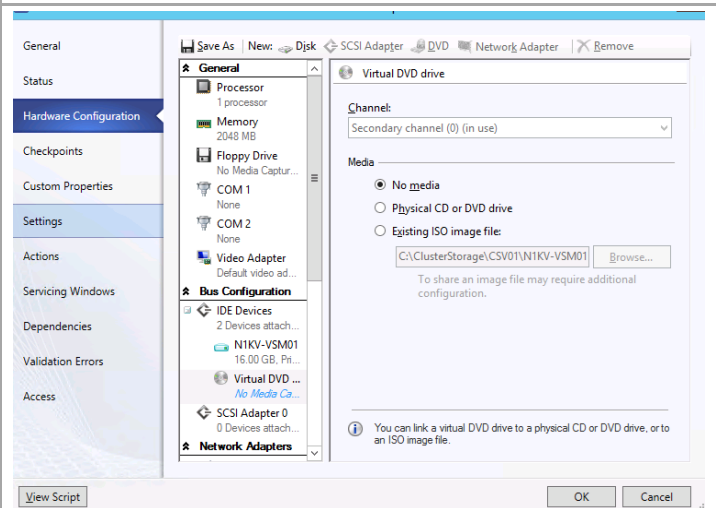
This supervisor (sup-2)
-----
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby

Other supervisor (sup-1)
-----
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby

System start time: Sun May 12 19:00:12 2013

System uptime: 3 days, 22 hours, 20 minutes, 9 seconds
Kernel uptime: 0 days, 0 hours, 3 minutes, 7 seconds
This supervisor is not up and running
N1KV-USM01(standby)#
```

Remove ISO from the first VSM02 Virtual Machine if there is an ISO image connected to the virtual machine.



15.5 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-FM-Public-IP-Pool
ip address 192.168.1.90 192.168.1.99
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-FM-Public-IP-Pool
publish network segment
exit

port-profile type vethernet AllAccess1
no shutdown
state enabled
publish port-profile
exit

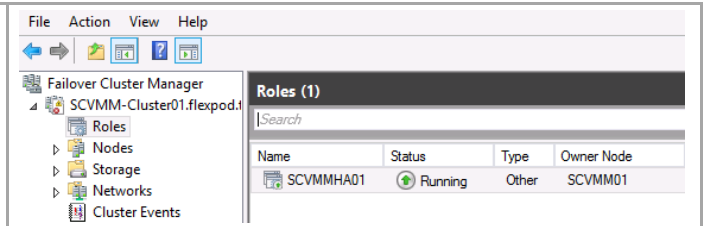
port-profile type ethernet N1KV_Uplink_Policy_FastTrack
channel-group auto mode on mac-pinning
no shutdown
state enabled
exit

nsm network uplink N1KV-MF-Uplink
import port-profile N1KV_Uplink_Policy_FastTrack
allow network segment pool Mgmt-Fabric
system network uplink
publish network uplink
exit

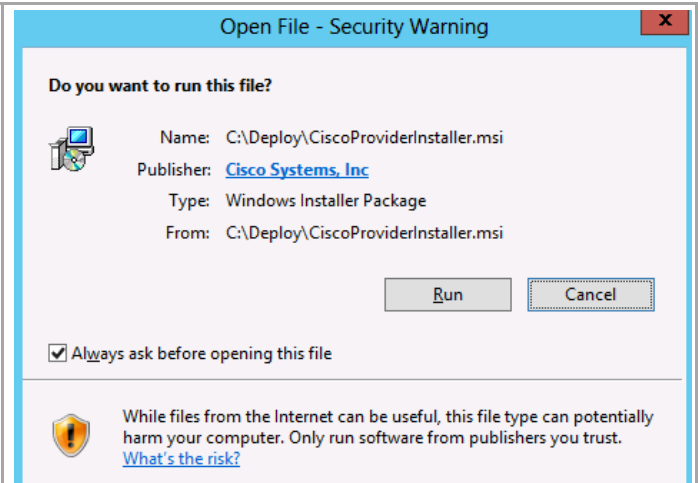
copy running-config startup-config
```

15.6 Configure Virtual Switch Extension Manager in Virtual Machine Manager

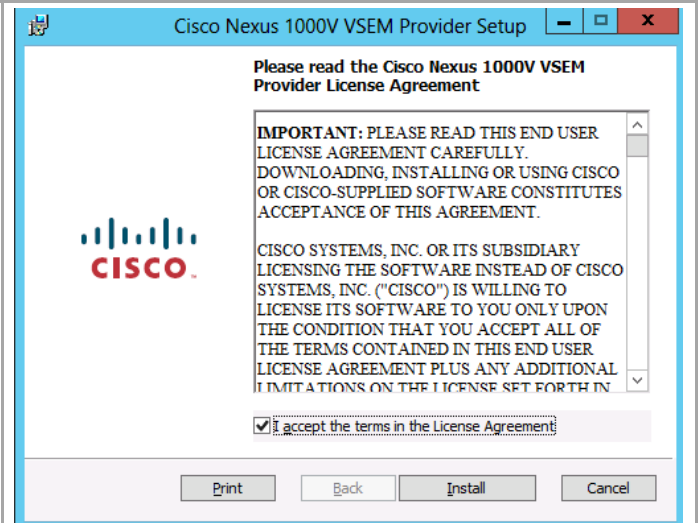
On the Virtual Machine Manager virtual machine, verify that it owns the highly available Virtual Machine Manager instance. Move the instance to this node if it is currently owned by the other Virtual Machine Manager node.



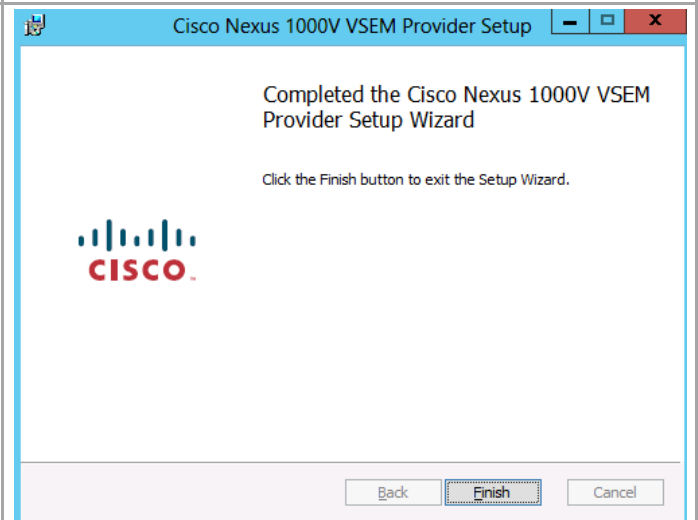
Install the Cisco Nexus 1000V switch extensions by running Nexus1000V-VSEMPProvider-5.2.1.SM1.5.1.0.msi. In the security warning window, click Run.



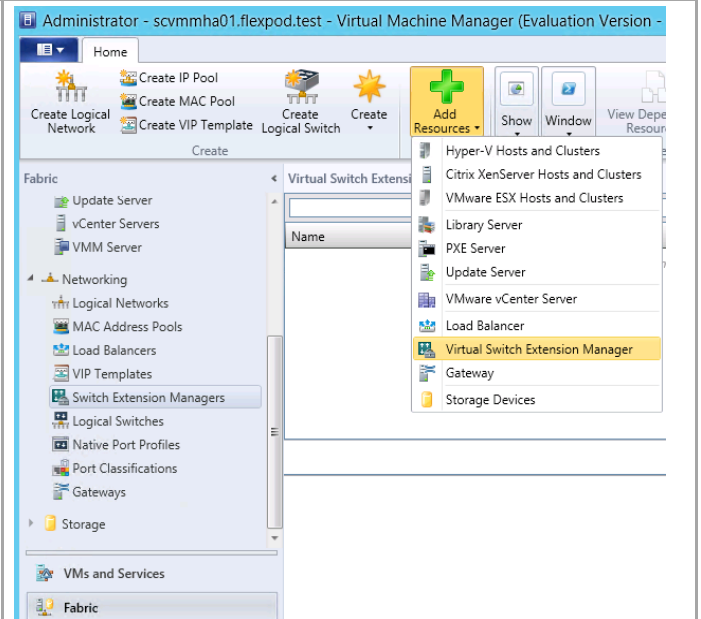
Review the license agreement. Check the box I **accept the terms in the License Agreement** and click **Install**.



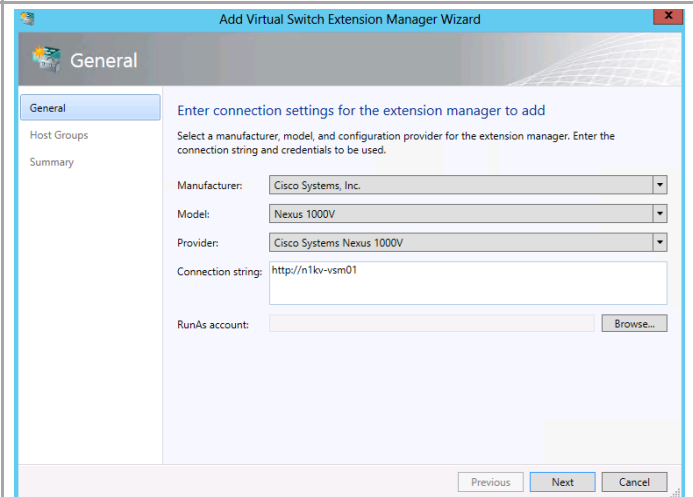
Click **Finish** to close the installation wizard.



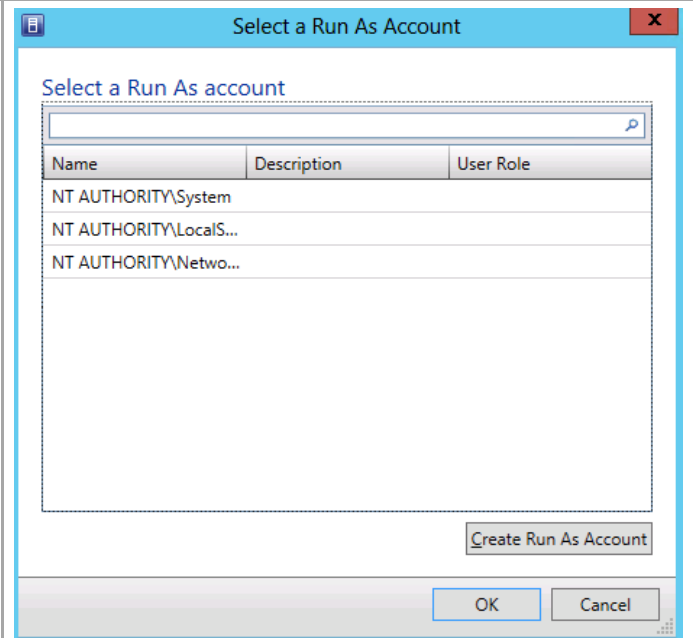
In the left pane of Virtual Machine Manager select **Fabric**. Expand **Networking** and select **Switch Extension Manager**. Click Add Resources and select **Virtual Switch Extension Manager**.



Enter connection string URL for the Nexus 1000V VSM. Click Browse.



Click **Create Run As Account**.

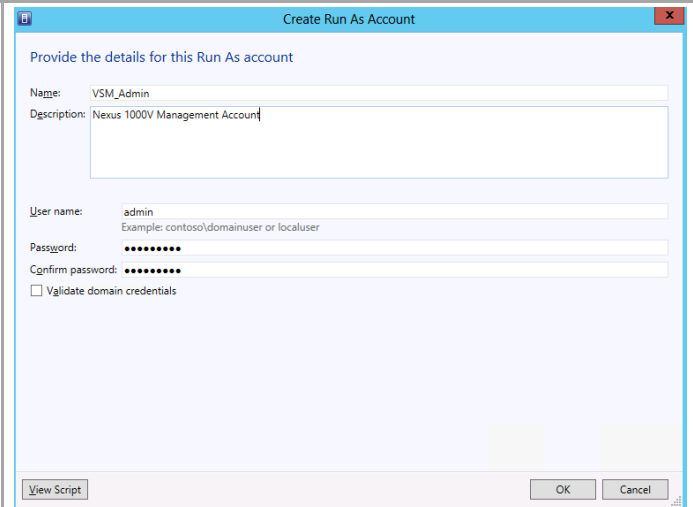


The screenshot shows a Windows-style dialog box titled "Select a Run As Account". It features a search bar at the top. Below it is a table with three columns: "Name", "Description", and "User Role". The table contains three entries: "NT AUTHORITY\System", "NT AUTHORITY\LocalS...", and "NT AUTHORITY\Netwo...". At the bottom right of the table area is a button labeled "Create Run As Account". At the very bottom of the dialog are "OK" and "Cancel" buttons.

Name	Description	User Role
NT AUTHORITY\System		
NT AUTHORITY\LocalS...		
NT AUTHORITY\Netwo...		

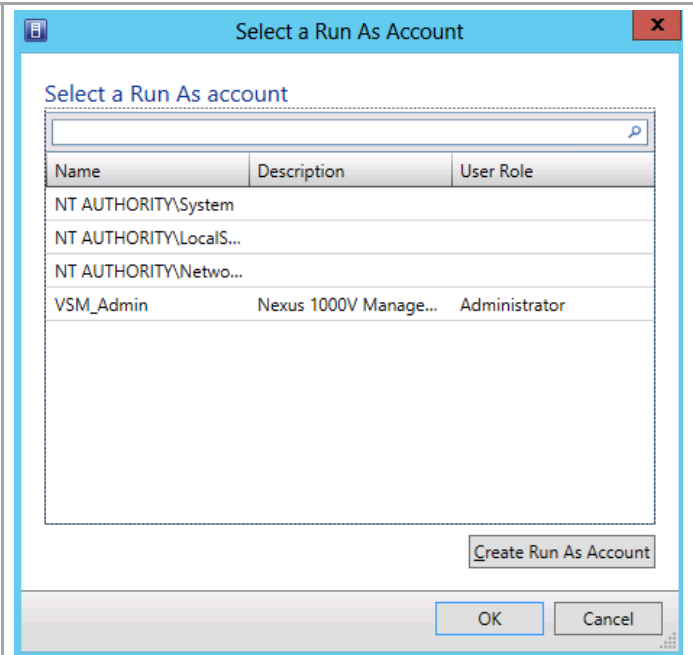
Enter the **Run As account name** and description.
Enter the **user name** with rights to manager the Nexus 1000V VMS and password. This is the account configured and password configured during Nexus 1000V VSM installation.

Clear the check box for validating the domain credentials.



The screenshot shows a Windows-style dialog box titled "Create Run As Account". It contains a section titled "Provide the details for this Run As account". This section has several input fields: "Name:" with the value "VSM_Admin", "Description:" with the value "Nexus 1000V Management Account", "User name:" with the value "admin", and "Password:" and "Confirm password:" fields both containing masked text (dots). Below these fields is a checkbox labeled "Validate domain credentials" which is currently unchecked. At the bottom left is a "View Script" button, and at the bottom right are "OK" and "Cancel" buttons.

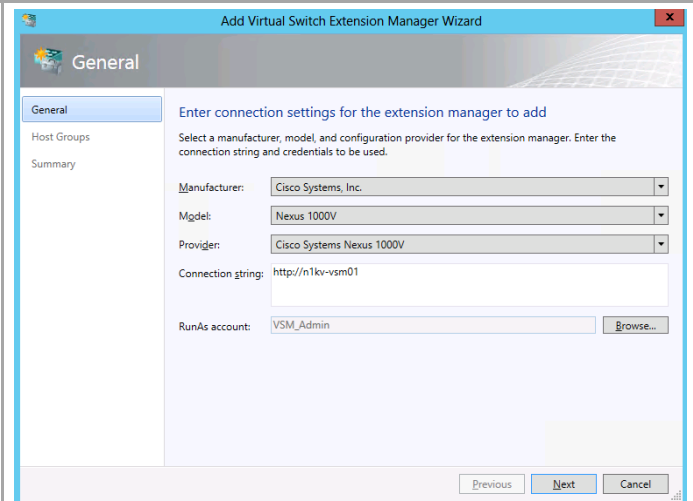
Select **VSM_Admin** account and click **OK**.



The screenshot shows a Windows-style dialog box titled "Select a Run As Account". It features a search bar at the top. Below it is a table with three columns: "Name", "Description", and "User Role". The table lists several accounts, with "VSM_Admin" highlighted. At the bottom right, there is a "Create Run As Account" button and "OK" and "Cancel" buttons.

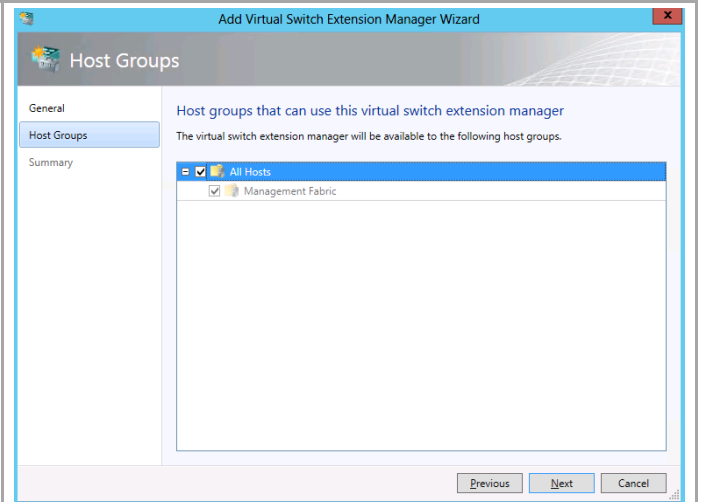
Name	Description	User Role
NT AUTHORITY\System		
NT AUTHORITY\LocalS...		
NT AUTHORITY\Netwo...		
VSM_Admin	Nexus 1000V Manage...	Administrator

Click **Next** to proceed.

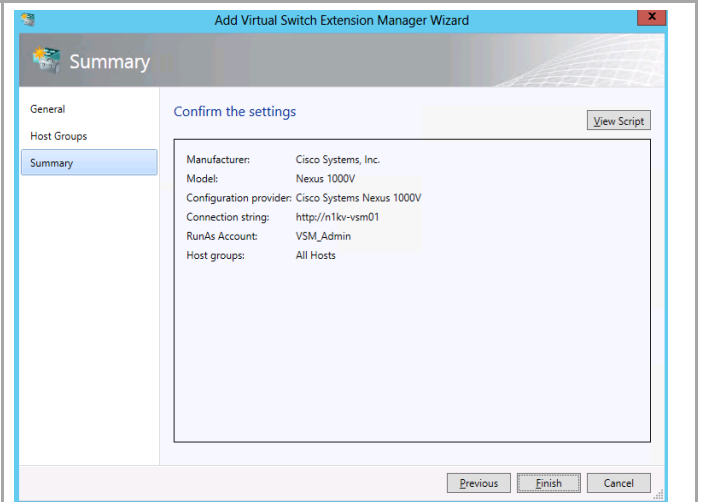


The screenshot shows a wizard titled "Add Virtual Switch Extension Manager Wizard" with the "General" tab selected. The wizard prompts the user to "Enter connection settings for the extension manager to add". It includes fields for "Manufacturer" (Cisco Systems, Inc.), "Model" (Nexus 1000V), "Provider" (Cisco Systems Nexus 1000V), "Connection string" (http://n1kv-vsm01), and "RunAs account" (VSM_Admin). A "Browse..." button is next to the RunAs account field. At the bottom, there are "Previous", "Next", and "Cancel" buttons.

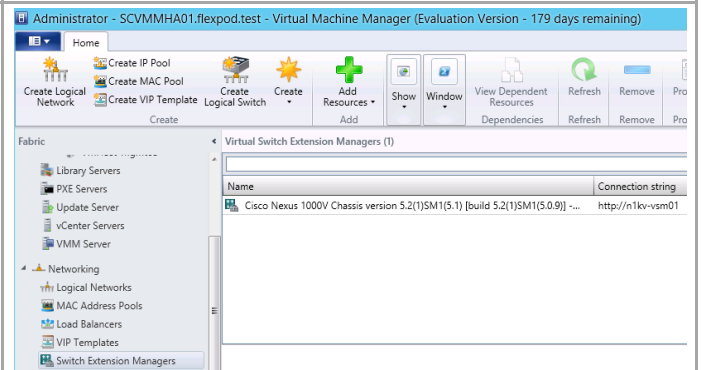
Select All Hosts group.



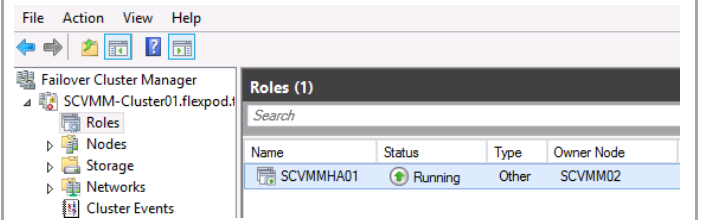
Click **Finish**.



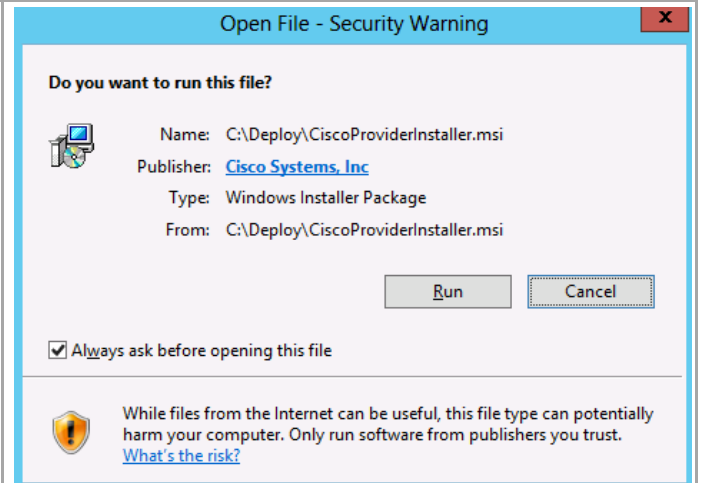
Verify that Nexus 1000V Virtual Switch Extension is installed.



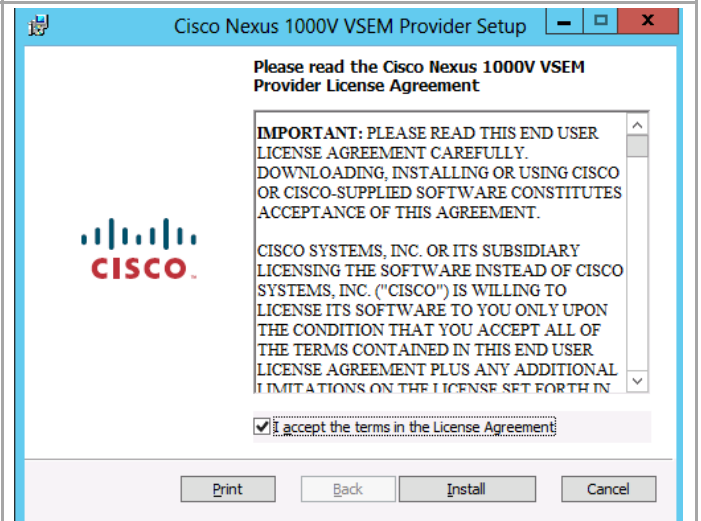
Using Cluster Failover Manager, move the highly available Virtual Machine Manager instance to the second Virtual Machine Manager node.



Connect to the second Virtual Machine Manager node. Install the Cisco Nexus 1000V switch extensions by running CiscoProviderIntaller.msi. In the security warning window, click Run.



Review the license agreement and check the box next to "I accept the terms in the License Agreement". Click Install.



Click **Finish** to close the wizard.

15.7
Copy Virtual Ethernet Module Installation Packager to the Virtual Machine Manager Virtual Machines

Perform the following procedure on each Virtual Machine Manager node.

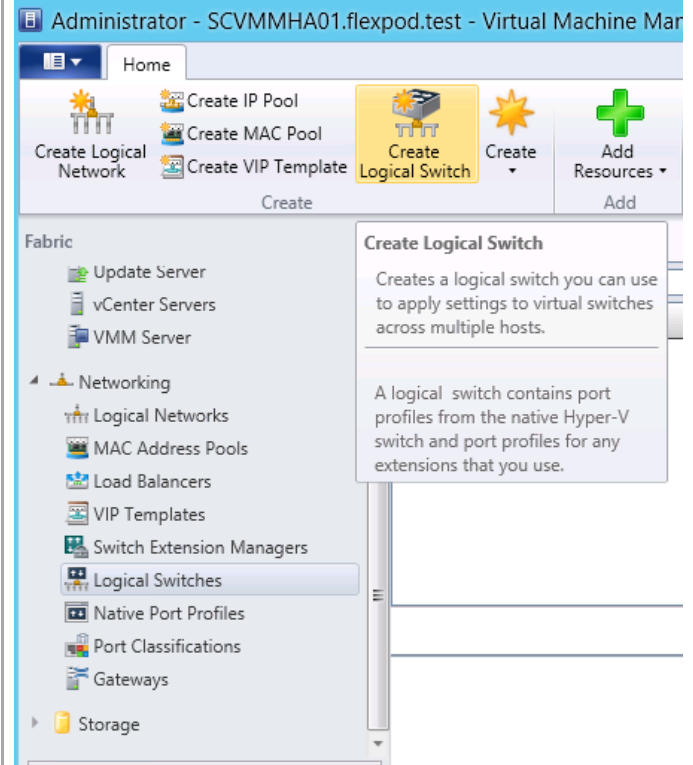
Copy Nexus1000V-VEM-5.2.1.SM1.5.1.0.msi to the following directory on each Virtual Machine Manager server:

C:\ProgramData\Switch Extensions Drivers

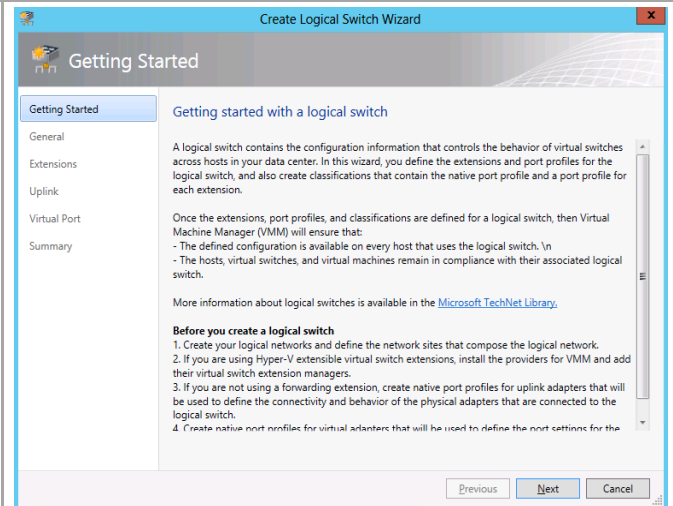
Name	Type
Nexus1000V-VEM-5.2.1.SM1.5.1.0.msi	Windows Installer ...

15.8 Configure a Logical Switch In Virtual Machine Manager

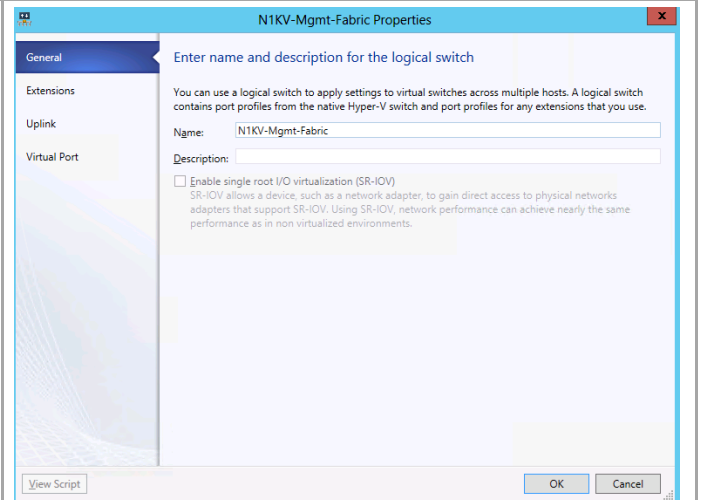
In the left pane of Virtual Machine Manager select **Fabric**. Expand **Networking** and select **Logical Switches**. Click **Create Logical Switch**.



Click **Next**.

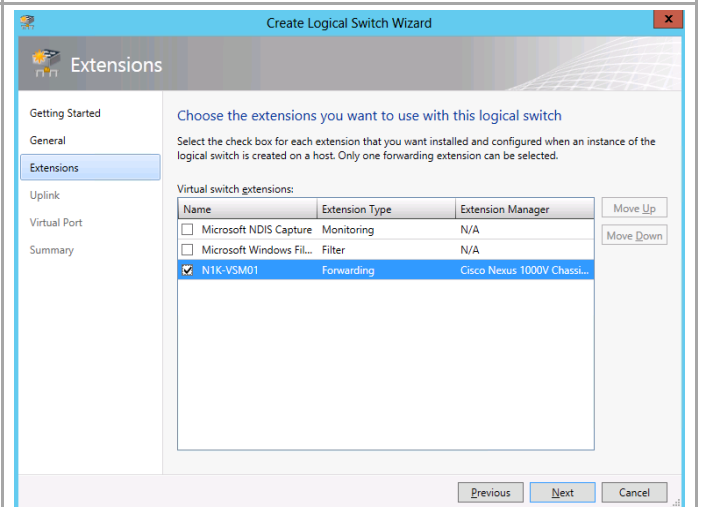


Enter a **logical switch name** for the Nexus 1000V and click **OK**.



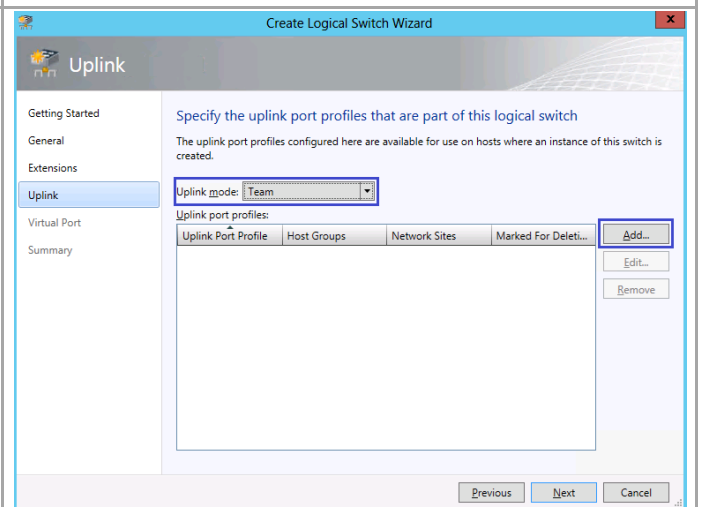
The dialog box is titled "N1KV-Mgmt-Fabric Properties". It has a sidebar on the left with tabs: "General", "Extensions", "Uplink", and "Virtual Port". The "General" tab is selected. The main area contains the text: "Enter name and description for the logical switch". Below this, it says: "You can use a logical switch to apply settings to virtual switches across multiple hosts. A logical switch contains port profiles from the native Hyper-V switch and port profiles for any extensions that you use." There are two input fields: "Name:" with the value "N1KV-Mgmt-Fabric" and "Description:". Below these is a checkbox labeled "Enable single root I/O virtualization (SR-IOV)". A note below the checkbox states: "SR-IOV allows a device, such as a network adapter, to gain direct access to physical network adapters that support SR-IOV. Using SR-IOV, network performance can achieve nearly the same performance as in non virtualized environments." At the bottom are buttons for "View Script", "OK", and "Cancel".

Uncheck **Microsoft Windows Filtering Platform**. Check **N1KV-VSM01** forwarding extension type.



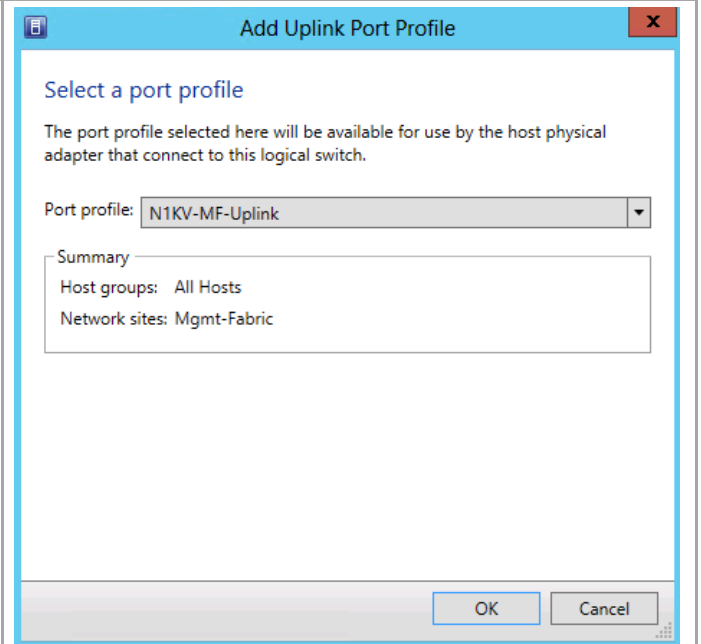
The wizard is titled "Create Logical Switch Wizard". The sidebar on the left has tabs: "Getting Started", "General", "Extensions", "Uplink", "Virtual Port", and "Summary". The "Extensions" tab is selected. The main area is titled "Choose the extensions you want to use with this logical switch". It says: "Select the check box for each extension that you want installed and configured when an instance of the logical switch is created on a host. Only one forwarding extension can be selected." Below this is a table titled "Virtual switch extensions:". The table has three columns: "Name", "Extension Type", and "Extension Manager". There are also "Move Up" and "Move Down" buttons to the right of the table. The table contains three rows: "Microsoft NDIS Capture" (Monitoring, N/A), "Microsoft Windows Fil..." (Filter, N/A), and "N1KV-VSM01" (Forwarding, Cisco Nexus 1000V Chassi...). The "N1KV-VSM01" row is selected. At the bottom are buttons for "Previous", "Next", and "Cancel".

Select the Team Uplink mode in the dropdown text box. Click Add to add the uplink port profile.



The wizard is titled "Create Logical Switch Wizard". The sidebar on the left has tabs: "Getting Started", "General", "Extensions", "Uplink", "Virtual Port", and "Summary". The "Uplink" tab is selected. The main area is titled "Specify the uplink port profiles that are part of this logical switch". It says: "The uplink port profiles configured here are available for use on hosts where an instance of this switch is created." There is a dropdown menu for "Uplink mode:" with "Team" selected. Below this is a section titled "Uplink port profiles:". It contains a table with columns: "Uplink Port Profile", "Host Groups", "Network Sites", and "Marked For Deleti...". To the right of the table are buttons for "Add...", "Edit...", and "Remove". At the bottom are buttons for "Previous", "Next", and "Cancel".

Select the **Port Profile** and click **OK**.



Add Uplink Port Profile

Select a port profile

The port profile selected here will be available for use by the host physical adapter that connect to this logical switch.

Port profile: N1KV-MF-Uplink

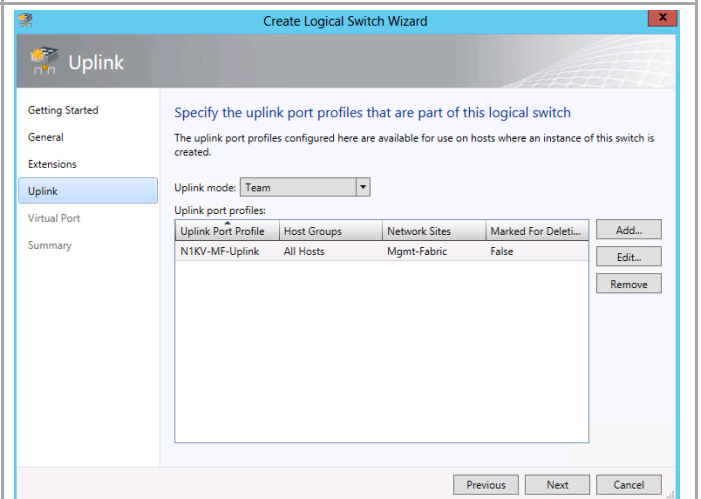
Summary

Host groups: All Hosts

Network sites: Mgmt-Fabric

OK Cancel

Review the added uplink port profile and click **Next** to continue.



Create Logical Switch Wizard

Uplink

Specify the uplink port profiles that are part of this logical switch

The uplink port profiles configured here are available for use on hosts where an instance of this switch is created.

Uplink mode: Team

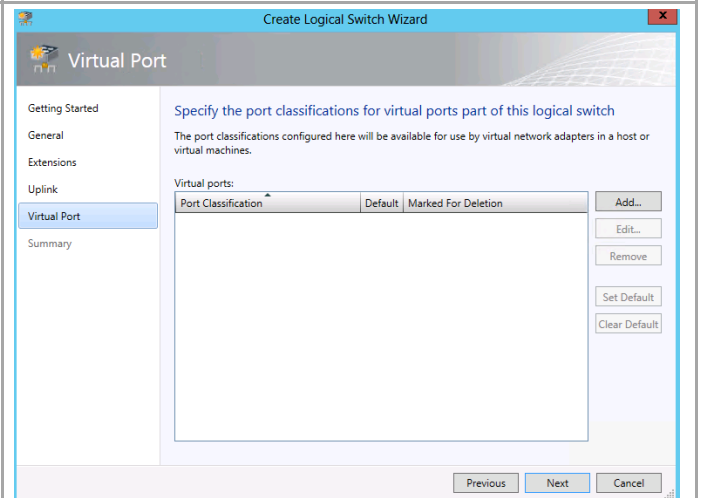
Uplink port profiles:

Uplink Port Profile	Host Groups	Network Sites	Marked For Deletion
N1KV-MF-Uplink	All Hosts	Mgmt-Fabric	False

Add... Edit... Remove

Previous Next Cancel

Click Add to add the virtual port classification.



Create Logical Switch Wizard

Virtual Port

Specify the port classifications for virtual ports part of this logical switch

The port classifications configured here will be available for use by virtual network adapters in a host or virtual machines.

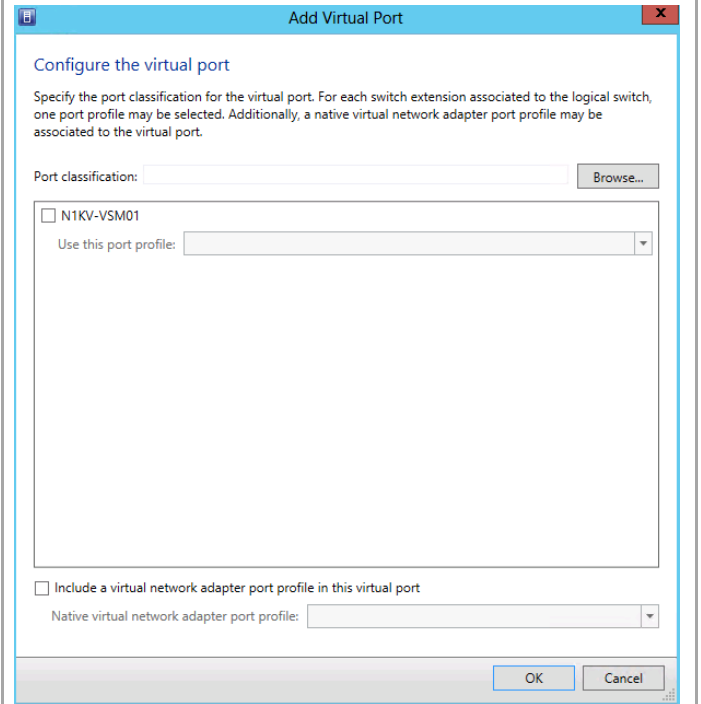
Virtual ports:

Port Classification	Default	Marked For Deletion
---------------------	---------	---------------------

Add... Edit... Remove Set Default Clear Default

Previous Next Cancel

Click Browse.



Add Virtual Port

Configure the virtual port

Specify the port classification for the virtual port. For each switch extension associated to the logical switch, one port profile may be selected. Additionally, a native virtual network adapter port profile may be associated to the virtual port.

Port classification:

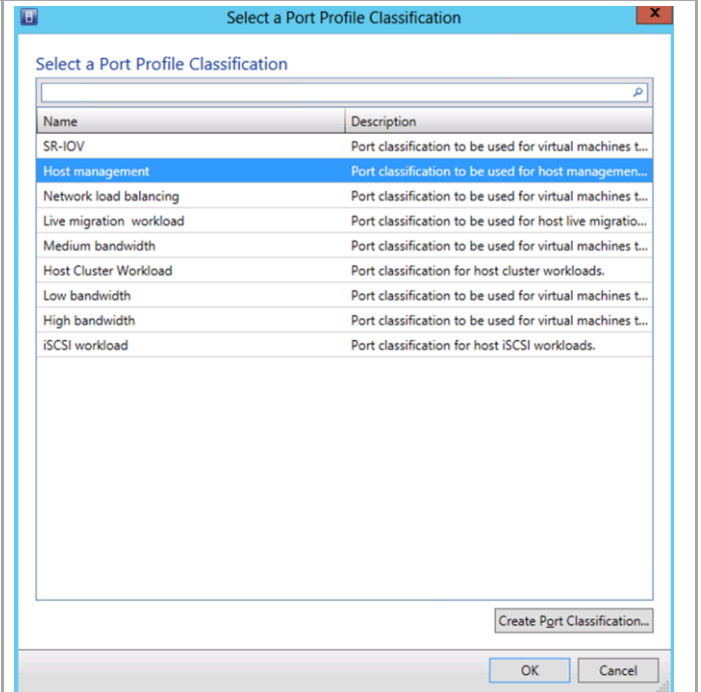
☐ N1KV-VSM01

Use this port profile:

☐ Include a virtual network adapter port profile in this virtual port

Native virtual network adapter port profile:

Click Create Port Classification.



Select a Port Profile Classification

Select a Port Profile Classification

Name	Description
SR-IOV	Port classification to be used for virtual machines t...
Host management	Port classification to be used for host managemen...
Network load balancing	Port classification to be used for virtual machines t...
Live migration workload	Port classification to be used for host live migratio...
Medium bandwidth	Port classification to be used for virtual machines t...
Host Cluster Workload	Port classification for host cluster workloads.
Low bandwidth	Port classification to be used for virtual machines t...
High bandwidth	Port classification to be used for virtual machines t...
iSCSI workload	Port classification for host iSCSI workloads.

Enter the port classification name and description.
Click **OK**.

Create Port Classification Wizard

Specify a name and description for the port classification

Name:Management Fabric

Description:Port Classification for Nexus 1000V Management Fabric

View Script

OK

Cancel

Select the new **Management Fabric** port classification and click **OK**.

Select a Port Profile Classification

Select a Port Profile Classification

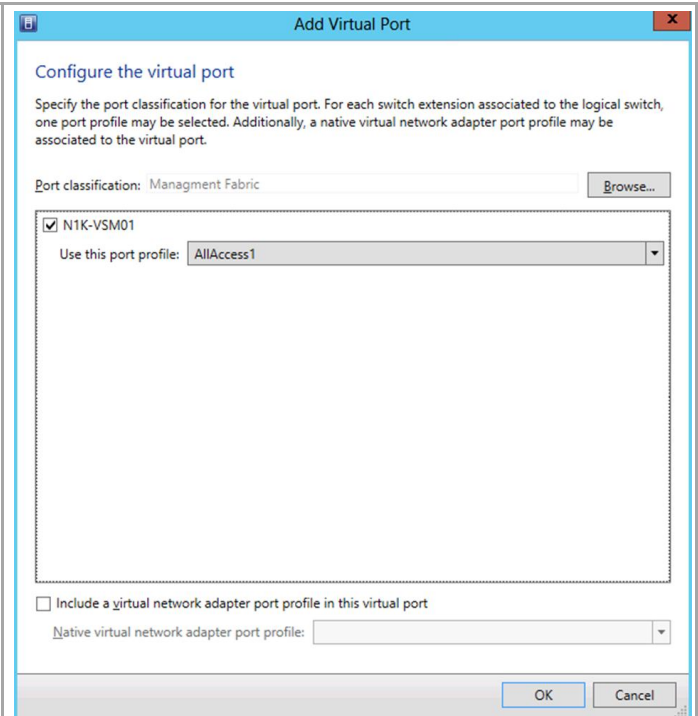
Name	Description
SR-IOV	Port classification to be used for virtual machines t...
Host management	Port classification to be used for host managemen...
Network load balancing	Port classification to be used for virtual machines t...
Live migration workload	Port classification to be used for host live migratio...
Management Fabric	Port Classification for Nexus 1000V Management F...
Medium bandwidth	Port classification to be used for virtual machines t...
Host Cluster Workload	Port classification for host cluster workloads.
Low bandwidth	Port classification to be used for virtual machines t...
High bandwidth	Port classification to be used for virtual machines t...
iSCSI workload	Port classification for host iSCSI workloads.

Create Port Classification...

OK

Cancel

Check N1KV-VSM01 and select the port profile from the dropdown text box. Click Ok.



Add Virtual Port

Configure the virtual port

Specify the port classification for the virtual port. For each switch extension associated to the logical switch, one port profile may be selected. Additionally, a native virtual network adapter port profile may be associated to the virtual port.

Port classification: Management Fabric Browse...

☒ N1KV-VSM01

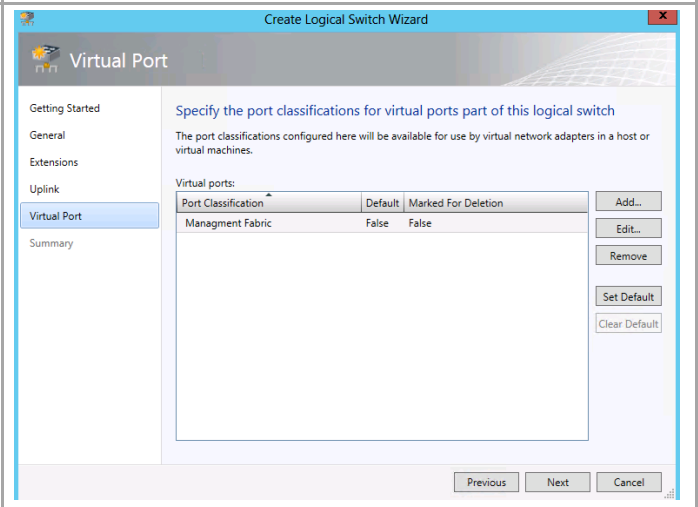
Use this port profile: AllAccess1

☐ Include a virtual network adapter port profile in this virtual port

Native virtual network adapter port profile:

OK Cancel

Click **Next** to proceed.



Create Logical Switch Wizard

Virtual Port

Specify the port classifications for virtual ports part of this logical switch

The port classifications configured here will be available for use by virtual network adapters in a host or virtual machines.

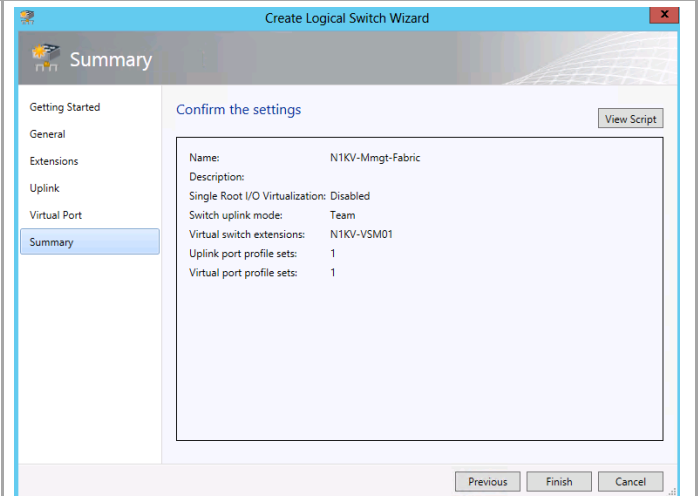
Virtual ports:

Port Classification	Default	Marked For Deletion
Management Fabric	False	False

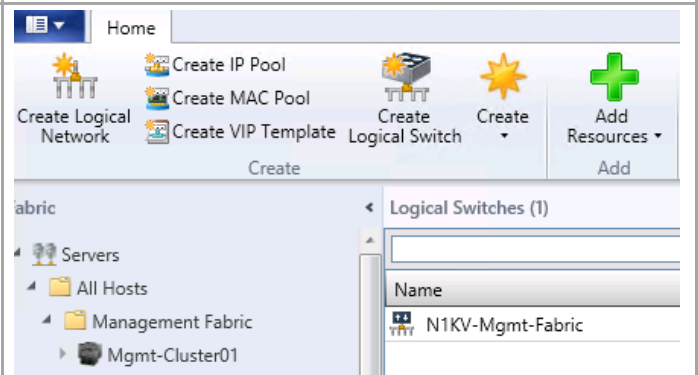
Add... Edit... Remove Set Default Clear Default

Previous Next Cancel

Confirm the configuration setting and click **Finish** to create the logical switch.



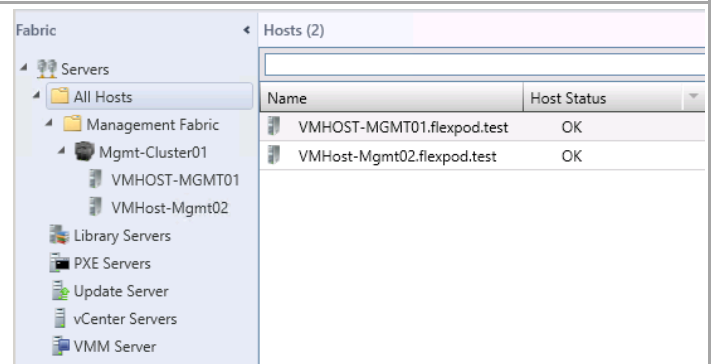
The Nexus 1000V virtual switch is created.



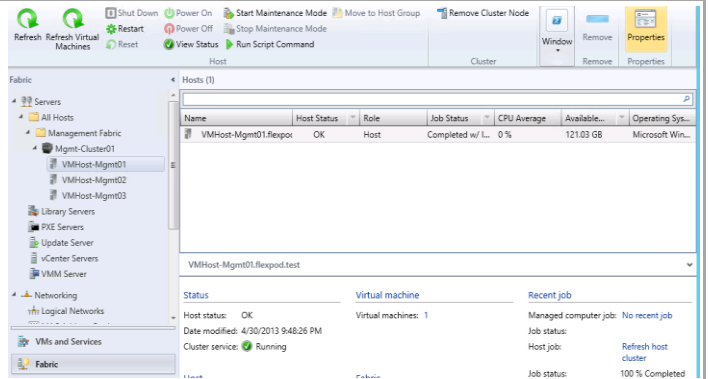
15.9 Create the Logical Switch on the Hyper-V Hosts

Perform the following procedure on each Management Fabric Cluster node.

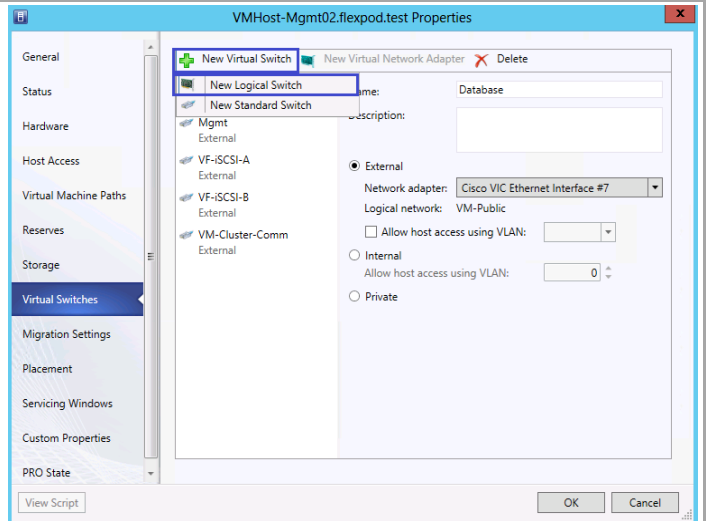
In the active Virtual Machine Manager instance, select Fabric. Expand All Hosts and Management Fabric.



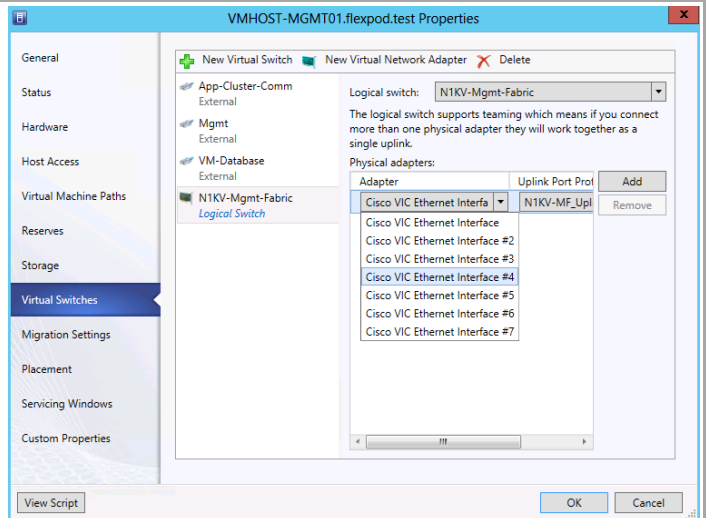
Select the first management fabric host and click **Properties**.



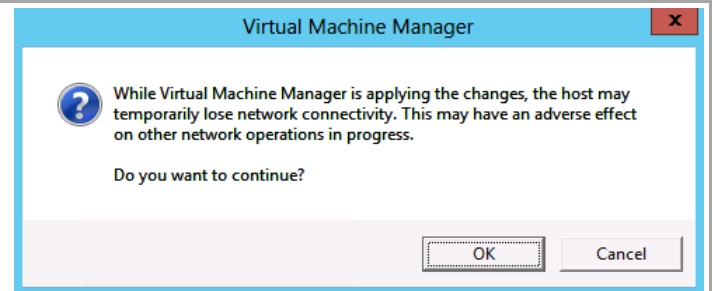
Select Virtual Switch in the left pane and New Virtual Switch. Select New Logical Switch.



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

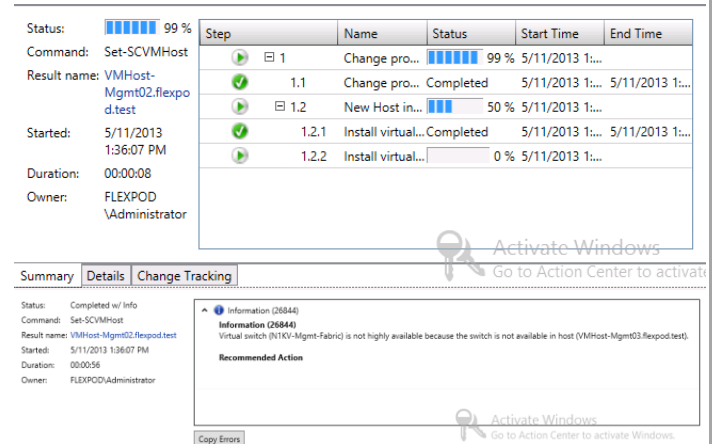


Click OK to invoke the configuration change.

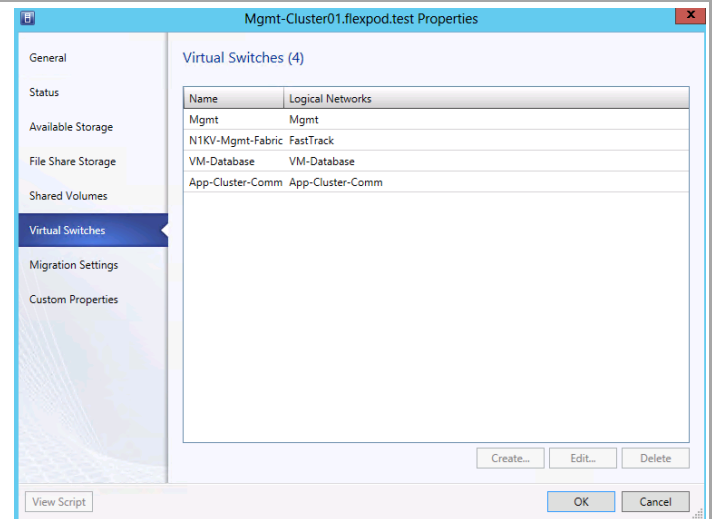


Click Jobs and monitor the job progress. The job will complete with info until the logical switch is installed on all of the hosts in the cluster.

Repeat this procedure on all cluster nodes.



Open the Mgmt-Cluster01 properties and verify that the N1KV-Mgmt-Fabric Switch is in the list of switch installed on all cluster nodes.



15.10 Create a VM Network

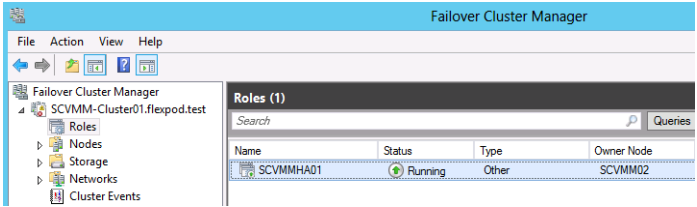
In Virtual Machine Manager, select **VMs and Services**. Right click **VM Networks** and click **Create VM Network**.

Enter the network name . Verify that the logical network FastTrack is selected and click Next .	
In the Isolation window, select Specify an externally supplied VM Network and select the External VM network N1KV-MF-Public . Click Next .	
In the Summary window, click Finish .	
The VM Network is created.	

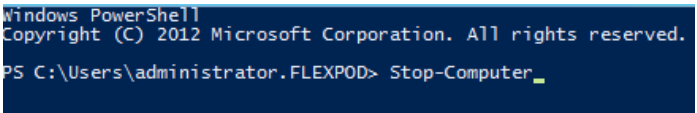
15.11 Configure the Virtual Machine Manager Virtual Machine Properties

Perform the following steps on the Virtual Machine Manager virtual machine.

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.

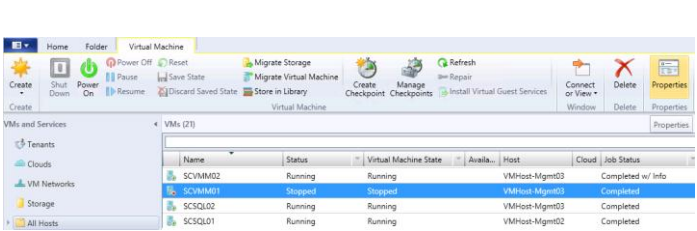


Shutdown the first Virtual Machine Manager virtual machine by running following powershell command.

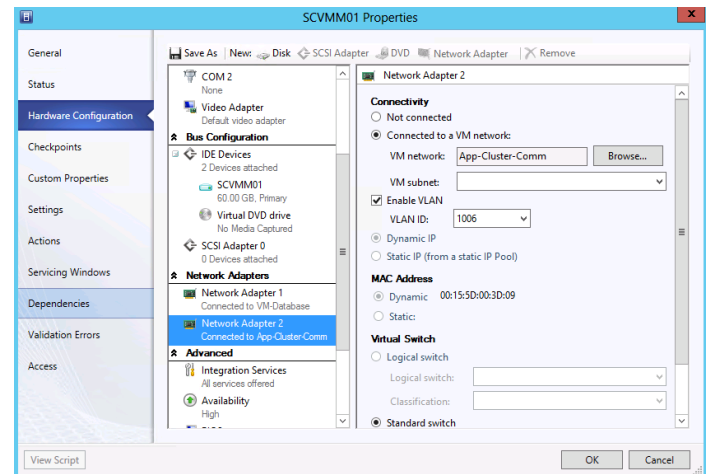
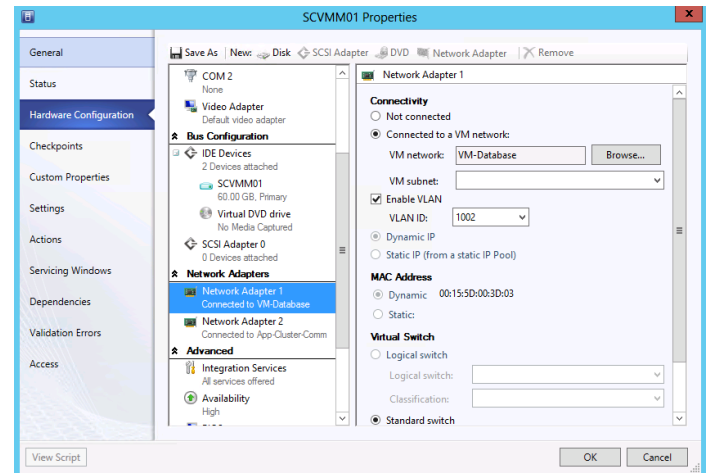


Stop-computer

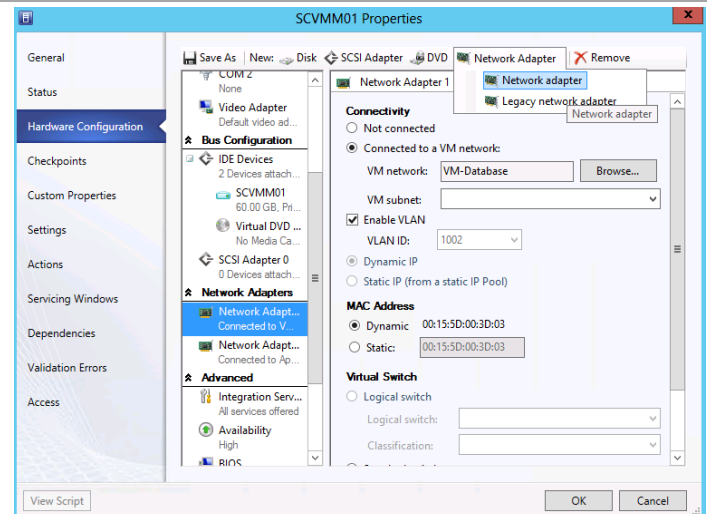
Log into the second Virtual Machine Manager virtual machine and start the Virtual Machine Manager console. Select VMs and Services. Click all hosts. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select properties.



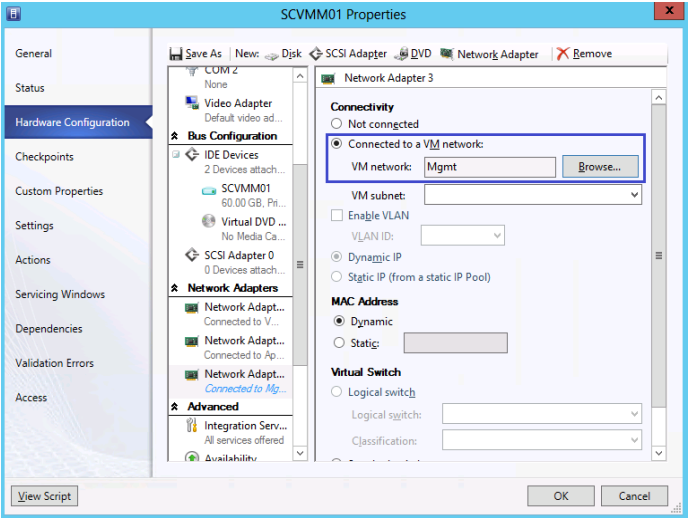
Select Hardware Configuraiton in the left pane and scroll down to the Network adapaters in the middle pane. Verify the all adapaters have the correct VM Networks specified. If any VM networks are listed as Not Specified, click browes and select the correct VM Network .



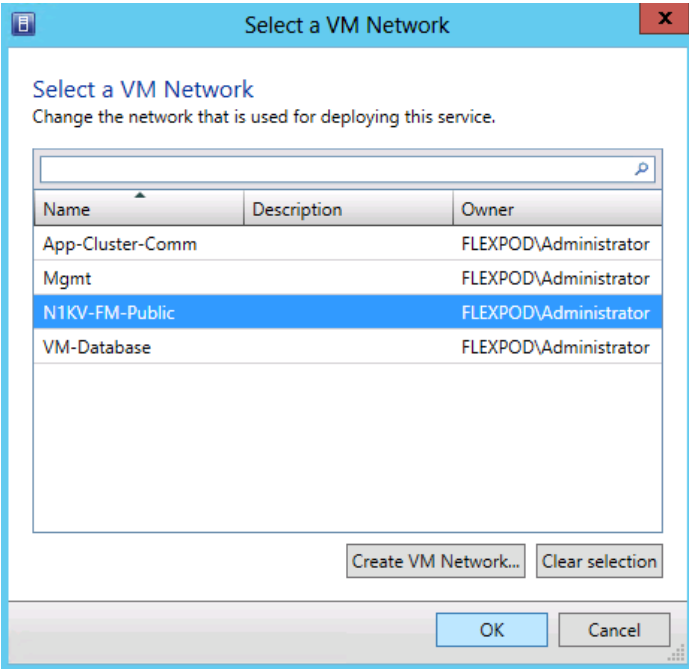
Click **Newtwork Addapter** and select **Network Addapter** to create the 3rd network addapter.



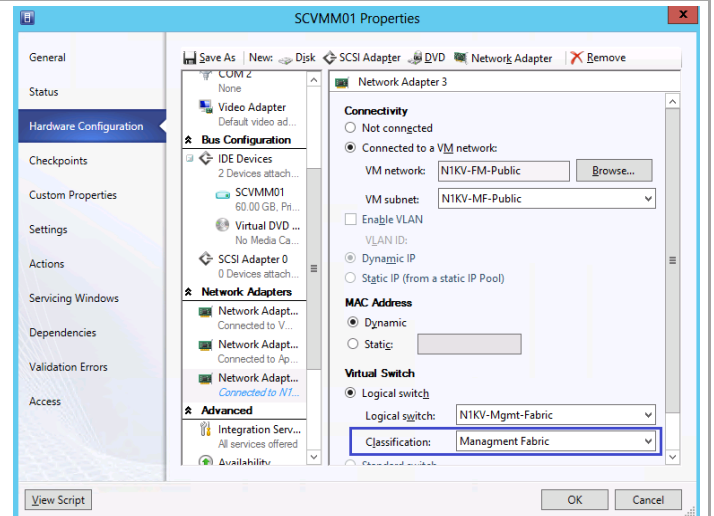
Select **Connect to a VM Network** and click **Browse** to select the VM Network.



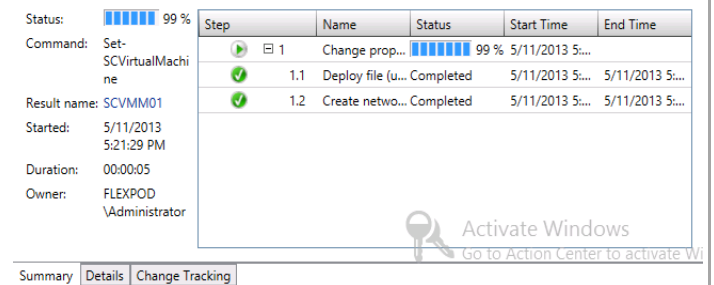
Select the N1KV-FM-Public VM Network and click **OK**.



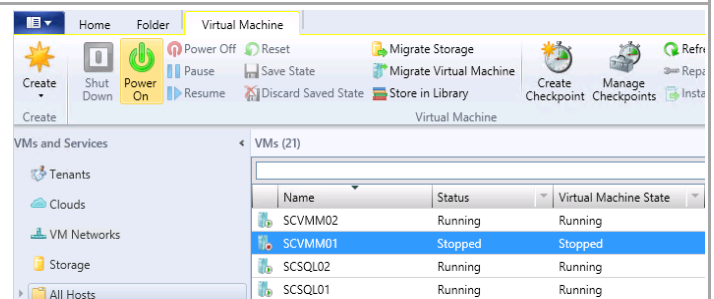
Select the Management Fabric Classification in the dropdown text box and click **OK**.



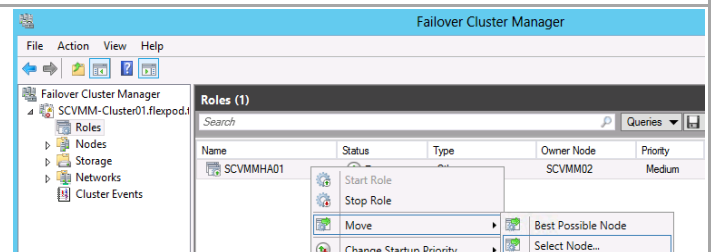
Select Jobs and monitor the job completion progress.



Start the Virtual 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.



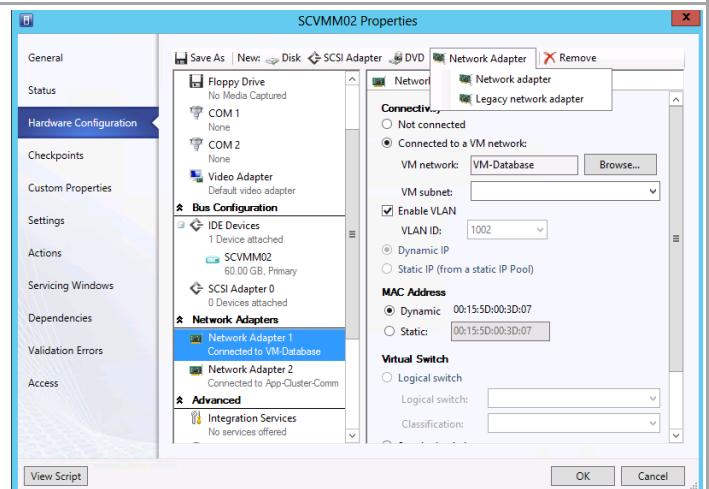
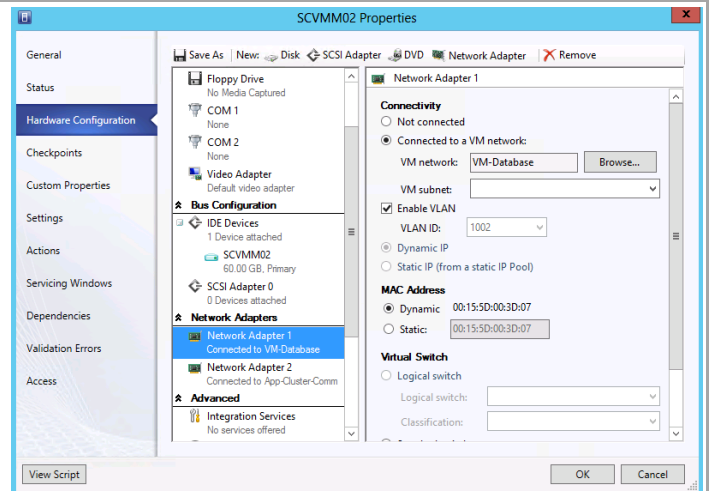
Shut down SCVMM02 virtual machine.

```
PS C:\Users\administrator.FLEXP0D>
PS C:\Users\administrator.FLEXP0D>
PS>Stop-Computer -ComputerName SCVMM02 -Force
```

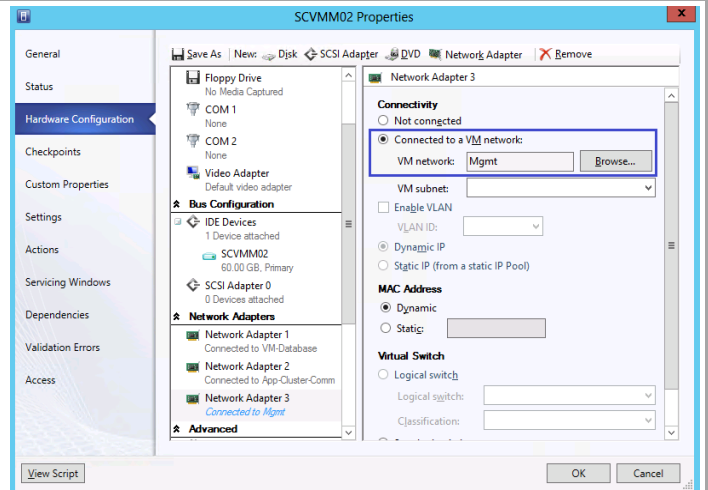
Start the Virtual Machine Manager console. Select VMs and Services. Click all hosts. Right click the first Virtual Machine Manager virtual machine that is in a stopped state and select properties.



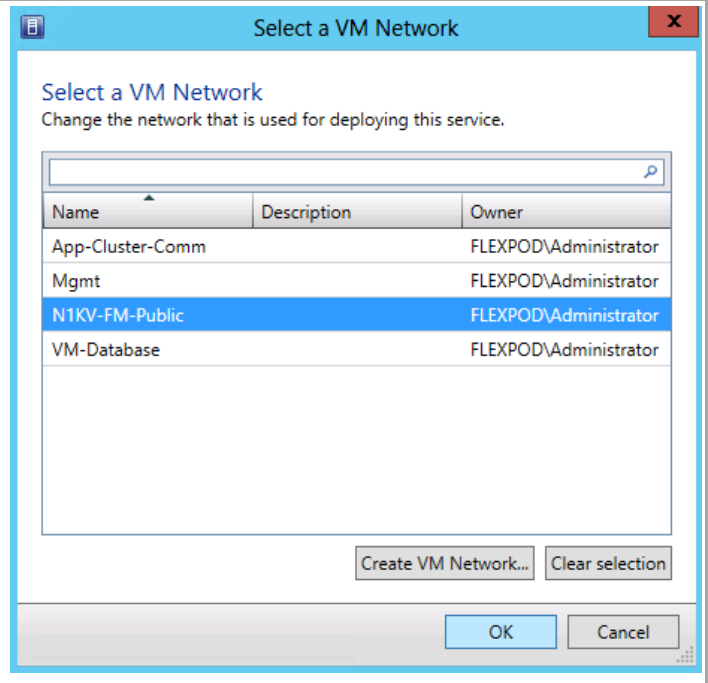
Select Hardware Configuraiton in the left pane and scroll down to the Network adapaters in the middle pane. Verify the all adapaters have the correct VM Networks specified. If any VM networks are listed as Not Specified, clickbrowes and select the correct VM Network .



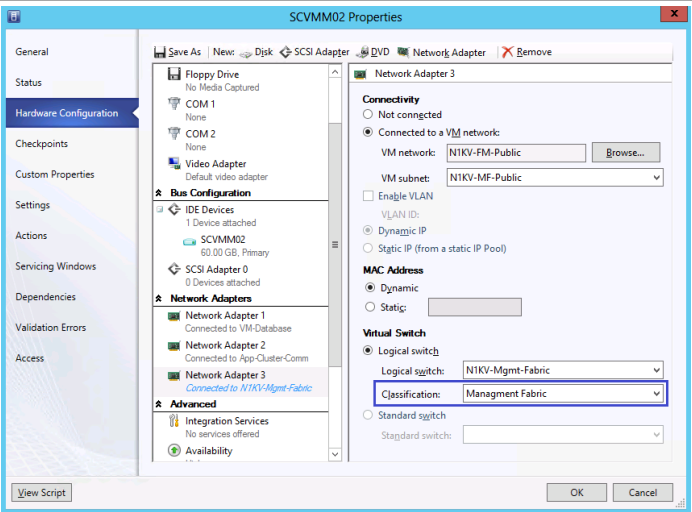
Select Connect to VM network radial button and click Browse.





Select the N1KV-FM-Public VM Network and click OK.






Select the Management Fabric Classification in the dropdown text box and click OK.



Select Jobs and monitor the job completion progress.

Status:  99 %	Step	Name	Status	Start Time	End Time
Command: Set-SCVirtualMachine	1	Change prop...	 99 %	5/11/2013 6:5...	5/11/2013 6:5...
Result name: SCVMM02	1.1	Deploy file (u...	Completed	5/11/2013 6:5...	5/11/2013 6:5...
Started: 5/11/2013 6:59:15 PM	1.2	Create netwo...	Completed	5/11/2013 6:5...	5/11/2013 6:5...
Duration: 00:00:05					
Owner: FLEXP0D \Administrator					
Summary	Details	Change Tracking			

Start the second Virtual Machine Manager virtual Machine.

Name	Status
SCVMM02	Stopped
SCVMM01	 Create
SCSQL02	 Shut Down
SCSQL01	 Power On

Login to the Cisco Nexus 1000V VSM and verify that the virtual adapters are connected to the Virtual Machine Manager virtual machines.

```
NIKU-USM01# show interface virtual
```

Port	Adapter	Owner	Mod	Host
Veth1	Net Adapter	SCVMM02	4	UMHOST-MGMT02
Veth2	Net Adapter	SCVMM01	3	UMHOST-MGMT01

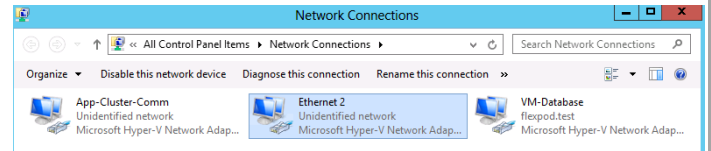
```
NIKU-USM01#
```

Show interfrace virtual

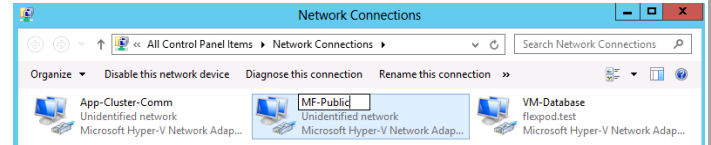
15.12 Configure Virtual Machine Manager Network Interfaces

Perform the following operation on both Virtual Machine Manager virtual machines.

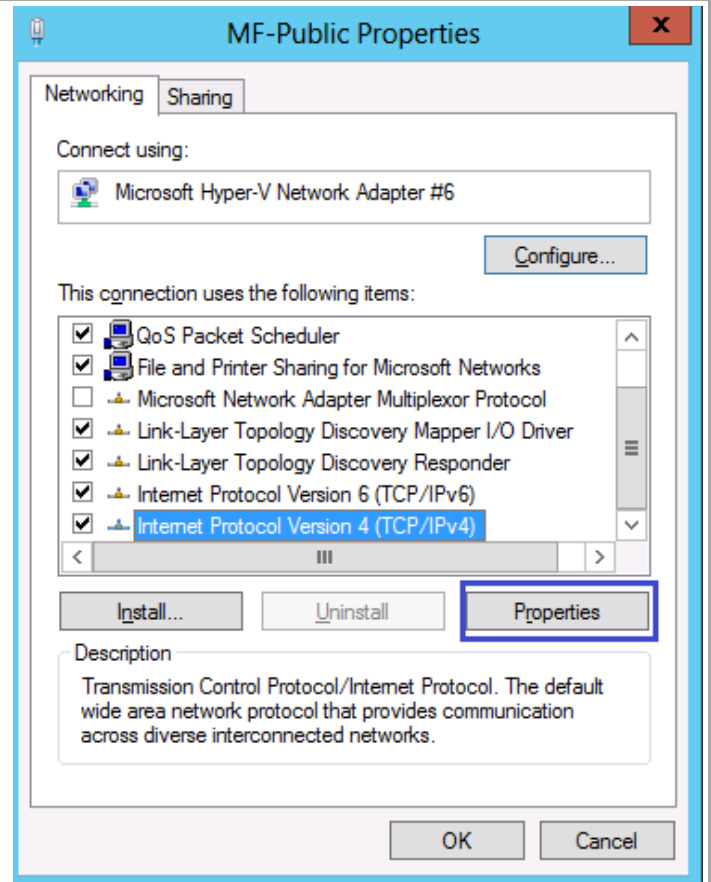
Open Network Connections.



Rename the new network interface to match the network infrace connection.



Right click on the new network interace, select properites. Select the TCP/IPv4 item and click properties.



Configure the TCP/IP properties. Specify the IP Address, Subnetmask, 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 . 1 . 10

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

Right click on the previously created VM-**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 . 2 . 10

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

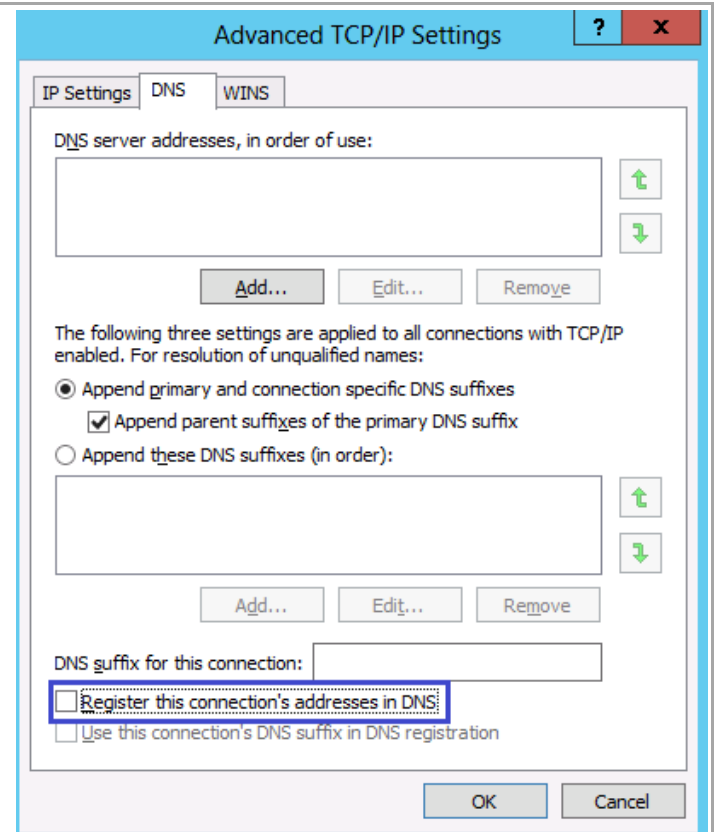
Alternate DNS server: 10 . 10 . 4 . 62

☐ Validate settings upon exit

Advanced...

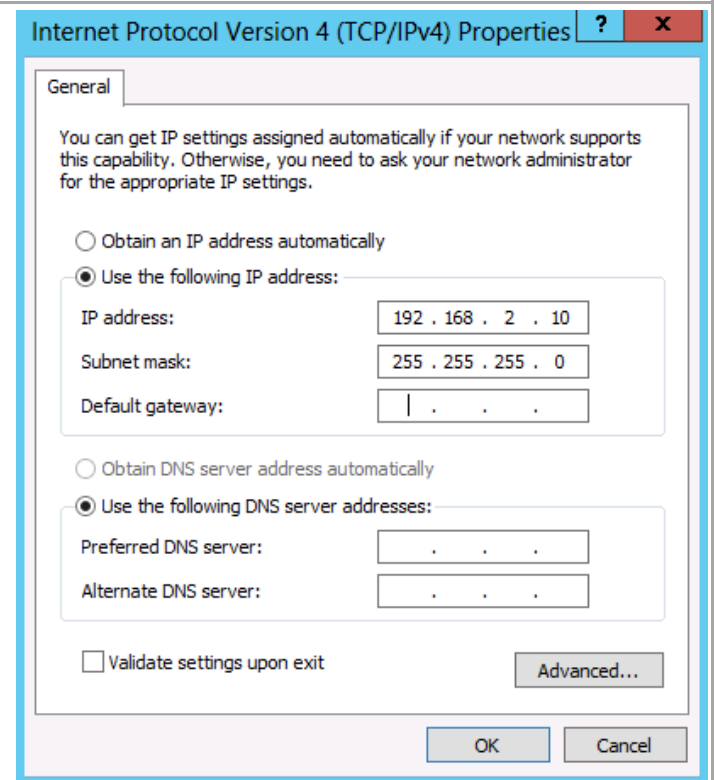
OK Cancel

Select the DNS tab. Uncheck Register this connection's address in DNS. Click OK to save the configuration.



The image 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. A note states: 'The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:'. There are 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 the third option is an empty list box with 'Add...', 'Edit...', and 'Remove' buttons. The 'DNS suffix for this connection:' field is empty. At the bottom, the checkbox 'Register this connection's addresses in DNS' is unchecked and highlighted with a red box. Below it is the checkbox 'Use this connection's DNS suffix in DNS registration', which is also unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

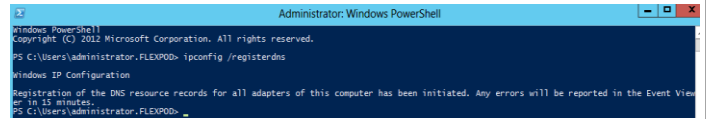
In the general IPv4 TCP/IP properties clear the default gateway and preferred DNS entries. Click OK to save the changes.



The image shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'General' tab selected. A note states: '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.' There are two radio button options: 'Obtain an IP address automatically' and 'Use the following IP address:' (selected). Below the second option are fields for 'IP address:' (192 . 168 . 2 . 10), 'Subnet mask:' (255 . 255 . 255 . 0), and 'Default gateway:' (| . . .). There are two radio button options: 'Obtain DNS server address automatically' and 'Use the following DNS server addresses:' (selected). Below the second option are fields for 'Preferred DNS server:' (. . .) and 'Alternate DNS server:' (. . .). At the bottom, the checkbox 'Validate settings upon exit' is unchecked. An 'Advanced...' button is to the right of the checkbox. 'OK' and 'Cancel' buttons are at the bottom right.

Open a command prompt. Run the following command.

```
Ipconfig /registerdns
```

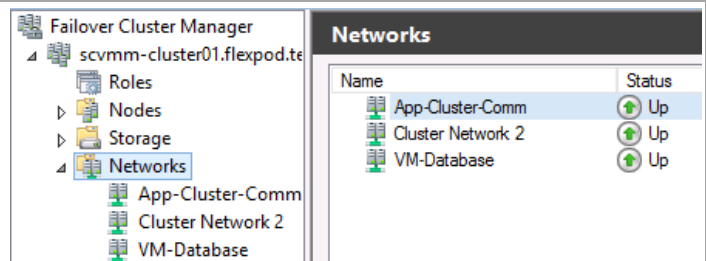


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator\FLEXPOD> ipconfig /registerdns
Windows IP Configuration
Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
PS C:\Users\Administrator\FLEXPOD>
```

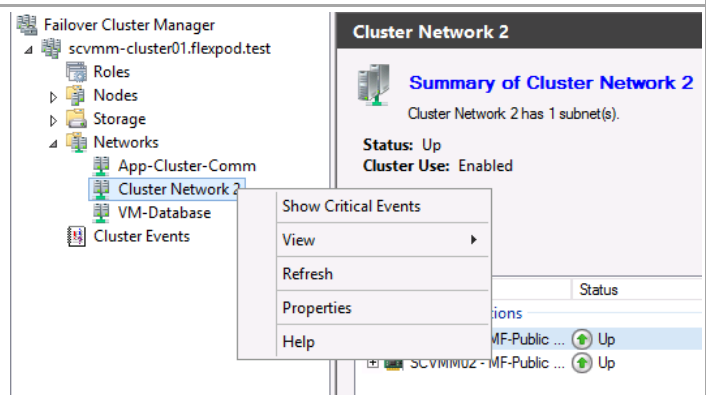
15.13 Rename the New Cluster Network

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.

Cluster Network 2 Properties

General

 Cluster Network 2

Name:

☐ Allow cluster network communication on this network
☒ Allow clients to connect through this network
☐ Do not allow cluster network communication on this network

Status: Up

Subnets:

OK

Cancel

Apply

Select **Roles** in the left pane and select the highly available Virtual Machine Manager instance in the top middle pane.

Failover Cluster Manager

scvmm-cluster01.flexpod.test

Roles

Nodes

Storage

Networks

App-Cluster-Comm

MF-Public

VM-Database

Cluster Events

Roles (1)

Search

Queries

Name	Status	Type	Owner Node	Priority
SCVMMHA01	Running	Other	SCVMM01	Medium

III

SCVMMHA01

Preferred Owners: [User Settings](#)

Status: Running

Priority: Medium

Owner Node: SCVMM01

Client Access Name: SCVMMHA01

IP Addresses: 192.168.2.72

Summary

Resources

In the middle lower pane click the **resource tab** and double click the IP address to open its perperities page.

Name

Status

Server Name

Name: SCVMMHA01

Online

IP Address: 192.168.2.72

Online

Roles

VMM Service SCVMMHA01

Online

Update the Name, Network, and static IP address to use the MF-Public network.

IP Address 192.168.2.72 Properties

General Dependencies Policies Advanced Policies

Name: IP Address 192.168.1.72

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 . 72

☒ 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.

Name	Status
Server Name	
 Name: SCVMMHA01	 Online
 IP Address: 192.168.1.72	 Online
Roles	
 VMM Service SCVMMHA01	 Online
<	
Summary	Resources

Open a command prompt. Run the following command.

Ipconfig /registerdns

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator\FLEXPOD> ipconfig /registerdns
Windows IP Configuration
Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
PS C:\Users\Administrator\FLEXPOD>
```

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.

Failover Cluster Manager

scvmm-cluster01.flexpod.test

Roles

Nodes

Storage

Networks

Cluster Events

Cluster scvmm-cluster01.flexpod.test

Summary of Cluster scvmm-cluster01

scvmm-cluster01 has 1 clustered roles and 2 nodes.

Name: scvmm-cluster01.flexpod.test

Current Host Server: SCVMM01







Quorum Configuration: Node and Disk Majority (Quorum Disk)

Recent Cluster Events: None in the last hour

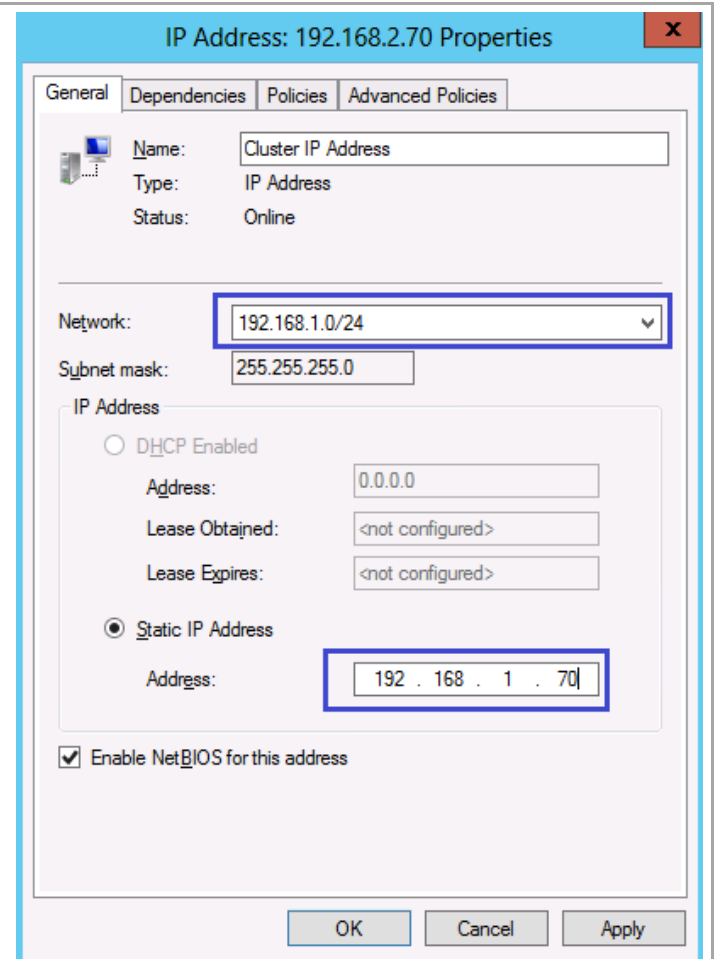
Configure

Navigate

Cluster Core Resources

Name	Status
Cluster Name	
 Name: scvmm-cluster01	 Online
 IP Address: 192.168.2.70	 Online
Storage	
 Quorum Disk	 Online

Update the Network and static IP address to use the MF-Public network.



IP Address: 192.168.2.70 Properties

General Dependencies Policies Advanced Policies

Name: Cluster IP Address
Type: IP Address
Status: Online

Network: 192.168.1.0/24
Subnet mask: 255.255.255.0

IP Address

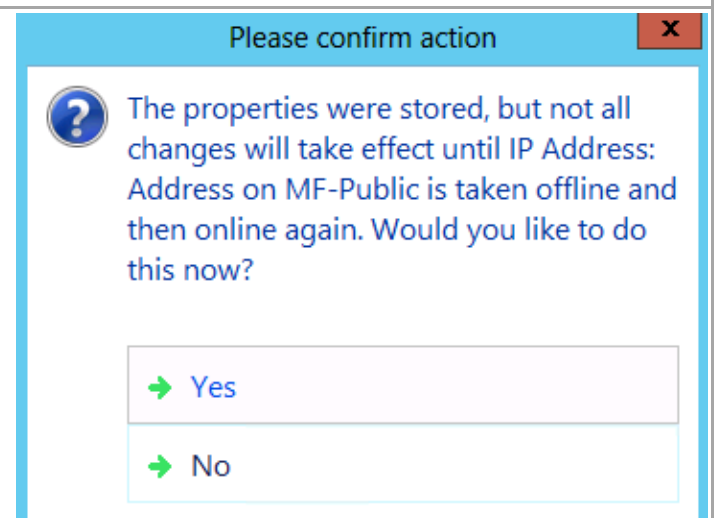
☐ DHCP Enabled
Address: 0.0.0.0
Lease Obtained: <not configured>
Lease Expires: <not configured>

☒ Static IP Address
Address: 192.168.1.70

☒ 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.



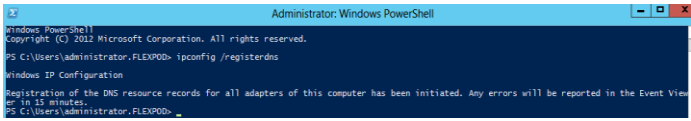
Please confirm action

?

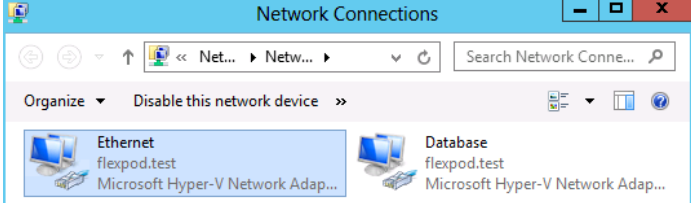
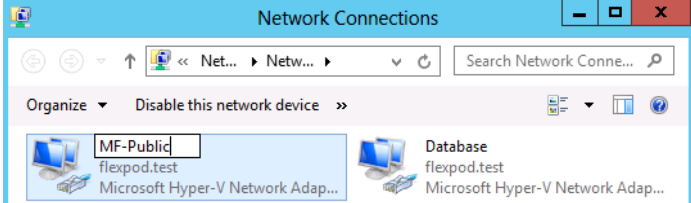
The properties were stored, but not all changes will take effect until IP Address: Address on MF-Public is taken offline and then online again. Would you like to do this now?

→ Yes

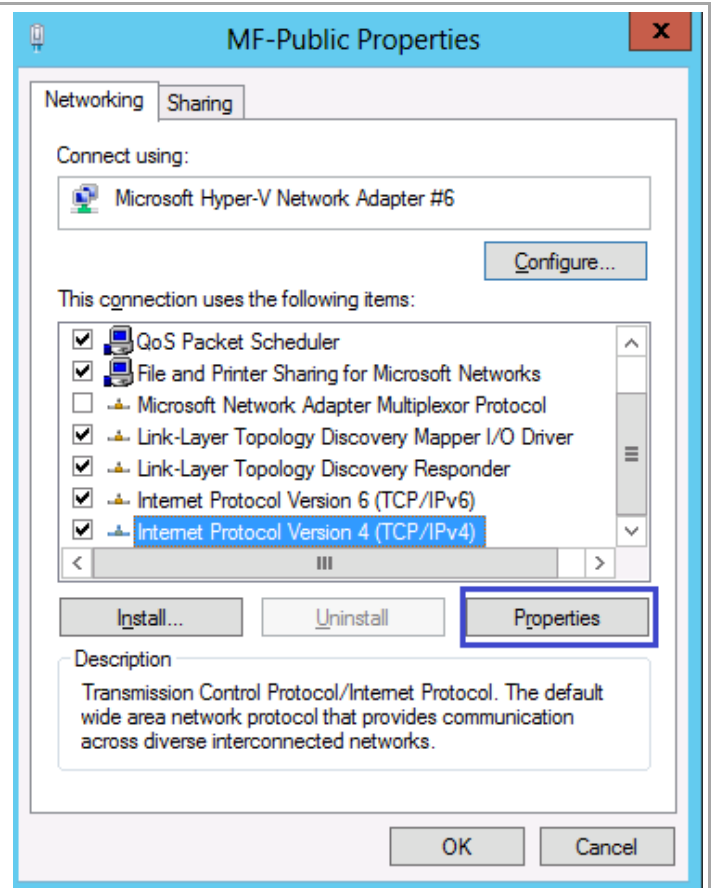
→ No

<p>Allow the IP Address resource to be brought offline. Bring the IP Address resource back online.</p> <p>Open a command prompt. Run the following command.</p>	
<pre>Ipconfig /registerdns</pre>	

15.14 Configure System Center Application Virtual Machine Network Interfaces

<p>Perform the following operation on the following System Center virtual machines.</p> <ul style="list-style-type: none"> • Operations Manager • Operations Manager Reporting Services • Service Manager • Orchestrator • Application Controller 	
<p>Open Network Connections.</p>	
<p>Rename the new network interface to match the network infrace connection.</p>	

Right click on the new network interace, select properites. Select the TCP/IPv4 item and click properties.



Configure the TCP/IP properties. Specify the IP Address, Subnetmask, 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 **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

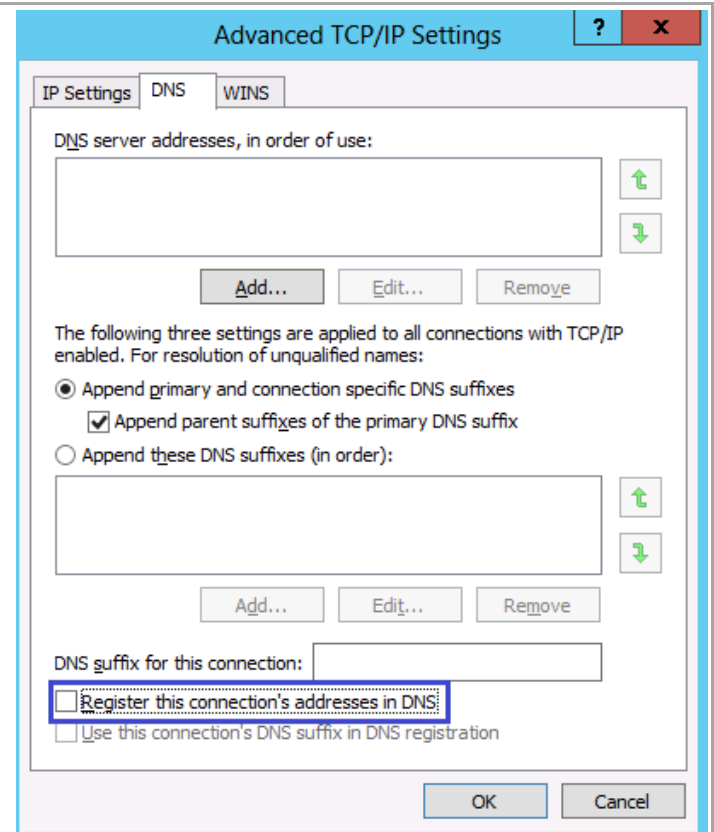
Alternate DNS server: 10 . 10 . 4 . 62

☐ Validate settings upon exit

Advanced...

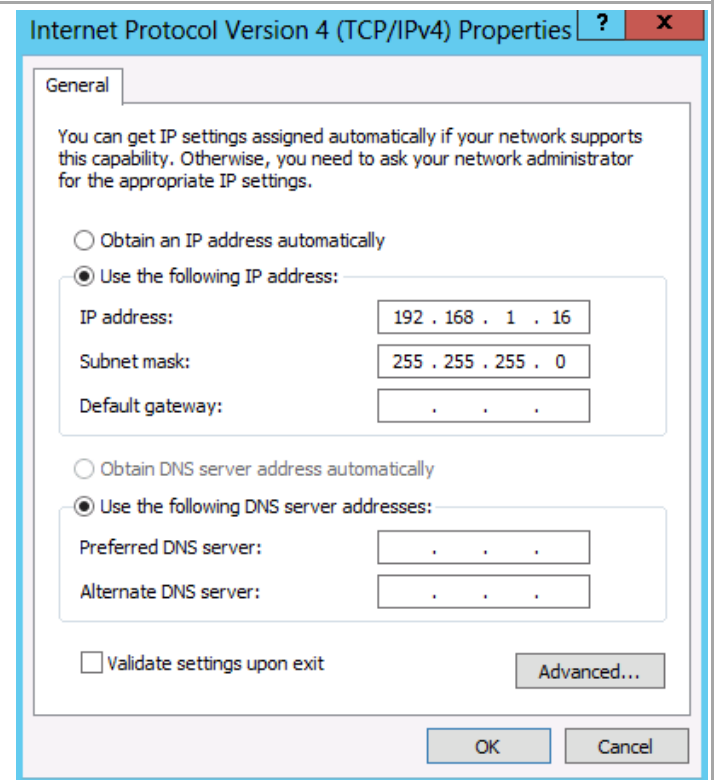
OK Cancel

Select the DNS tab. Uncheck Register this connection's address in DNS. Click OK to save the configuration.



The image 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. A note states: 'The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:'. There are 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 the third option is an empty list box with 'Add...', 'Edit...', and 'Remove' buttons. The 'DNS suffix for this connection:' field is empty. At the bottom, the checkbox 'Register this connection's addresses in DNS' is unchecked and highlighted with a red box. Other checkboxes include 'Use this connection's DNS suffix in DNS registration'. 'OK' and 'Cancel' buttons are at the bottom right.

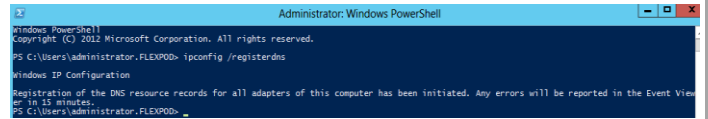
In the general IPv4 TCP/IP properties clear the default gateway and preferred DNS entries. Click OK to save the changes.



The image shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'General' tab selected. A note states: '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.' There are two radio button options: 'Obtain an IP address automatically' and 'Use the following IP address:' (selected). Below the second option are fields for 'IP address:' (192 . 168 . 1 . 16), 'Subnet mask:' (255 . 255 . 255 . 0), and 'Default gateway:' (empty). There are two more radio button options: 'Obtain DNS server address automatically' and 'Use the following DNS server addresses:' (selected). Below the second option are fields for 'Preferred DNS server:' (empty) and 'Alternate DNS server:' (empty). At the bottom, the checkbox 'Validate settings upon exit' is unchecked. An 'Advanced...' button is to the right of it. 'OK' and 'Cancel' buttons are at the bottom right.

Open a command prompt. Run the following command.

Ipconfig /registerdns



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator.FLEXPOD> ipconfig /registerdns
Windows IP Configuration
Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
PS C:\Users\Administrator.FLEXPOD>
```

16 Install and Configure the Data ONTAP SMI-S Agent

16.1 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following local account has been created:⁹

User name	Purpose	Permissions
FT-SMIS-User	SMI-S access account	This account will not need any special delegation.

16.2 Install the SMI-S Provider


The following steps need to be completed in order to install the NetApp SMI-S provider

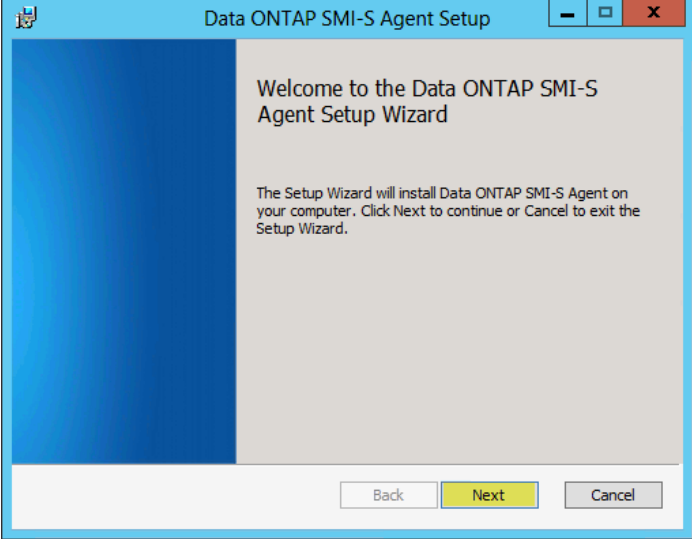
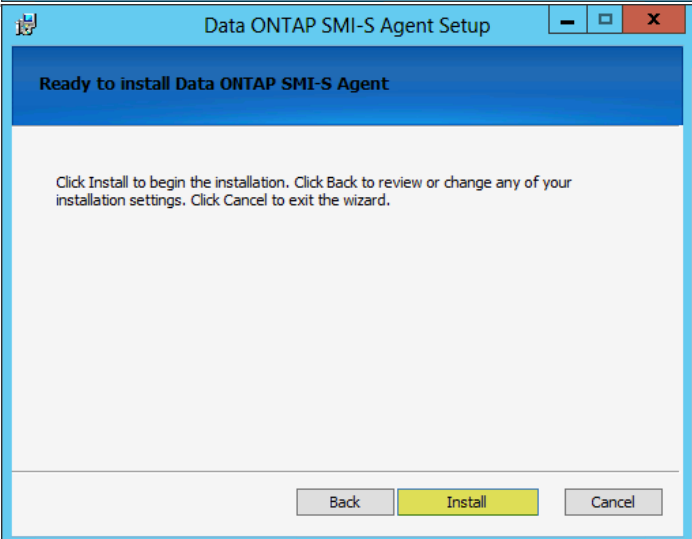
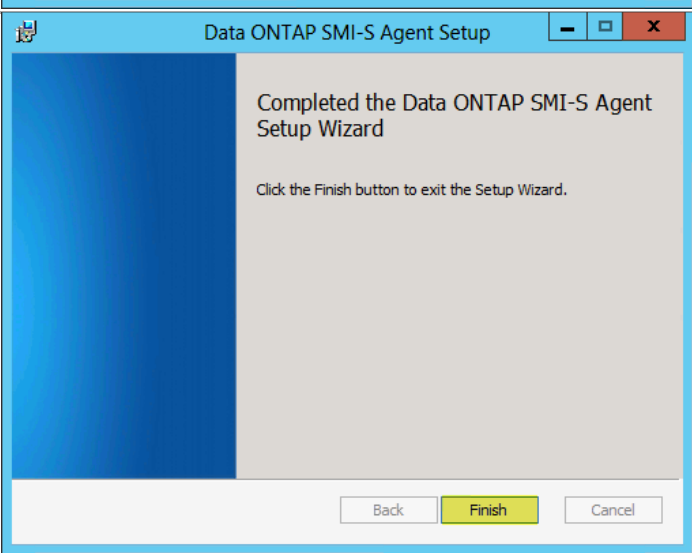
Download the installer from:

<http://support.netapp.com/NOW/download/software/smis/Windows/5.0/smisagent-5-0.msi>

► Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

Right-click **smisagent-5-0** and select **Install** from the context menu to begin setup.

Name	Date modified	Type
 smisagent-5-0		AM Win
<div><div>Install</div><div>Repair</div><div>Uninstall</div><div>Troubleshoot compatibility</div></div>		

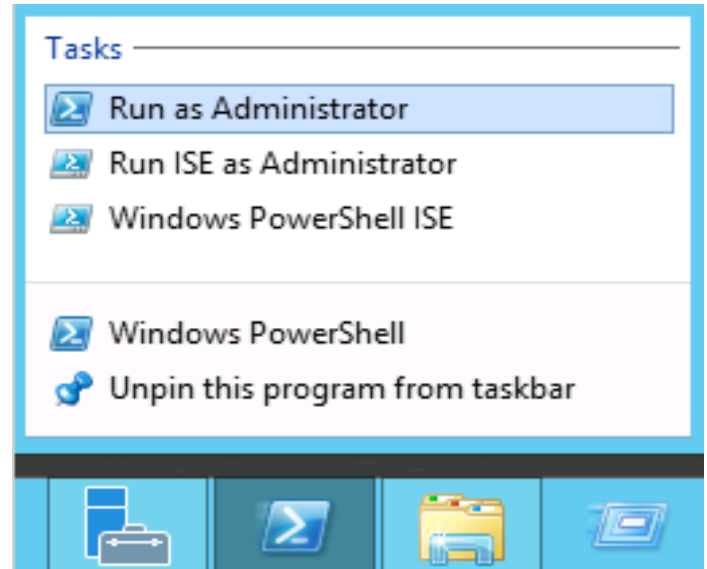
<p>On the “Welcome to the Data ONTAP SMI-S Agent Setup Wizard” page, click Next</p>	
<p>On the “Ready to install Data ONTAP SMI-S Agent” page, click Install.</p>	
<p>On the “Completed the Data ONTAP SMI-S Agent Setup Wizard”, click Finish to complete the installation.</p>	

16.3 Configure the SMI-S Provider

The following steps need to be completed in order to configure the NetApp SMI-S provider

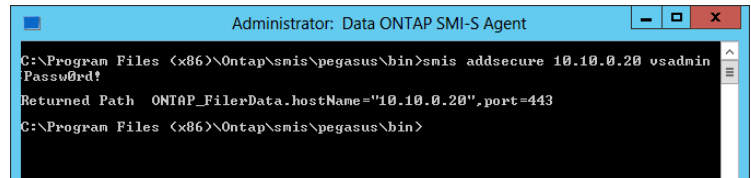
► Perform the following steps on the **Infrastructure SMI-S Server** virtual machine.

Open App screen, right-mouse click on **Data ONTAP SMI-S Agent** and select **Run as Administrator** at the bottom of the screen.



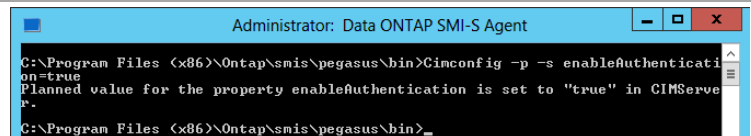
Add Vserver to the SMIS configuration.

```
Smis addsecure <VserverIpAddress>  
<VserverAdmin> <VserverAdminPassword>
```



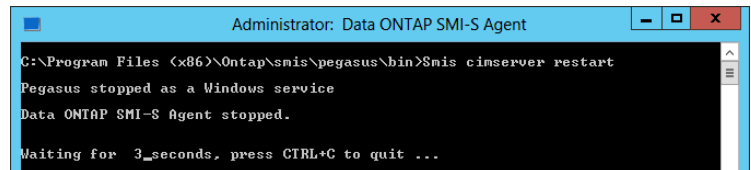
Enable user authentication using cimconfig command

```
Cimconfig -p -s enableAuthentication=true
```



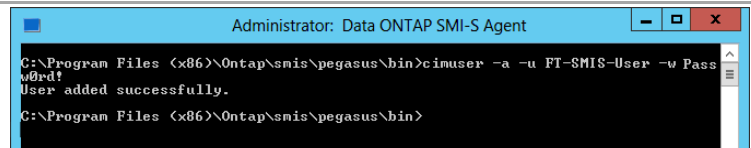
45. Restart the Agent/cimserver

```
Smis cimserver restart
```



Add SMI-S Run As account to the SMIS configuration.

```
cimuser -a -u FT-SMIS-User -w <password>
```



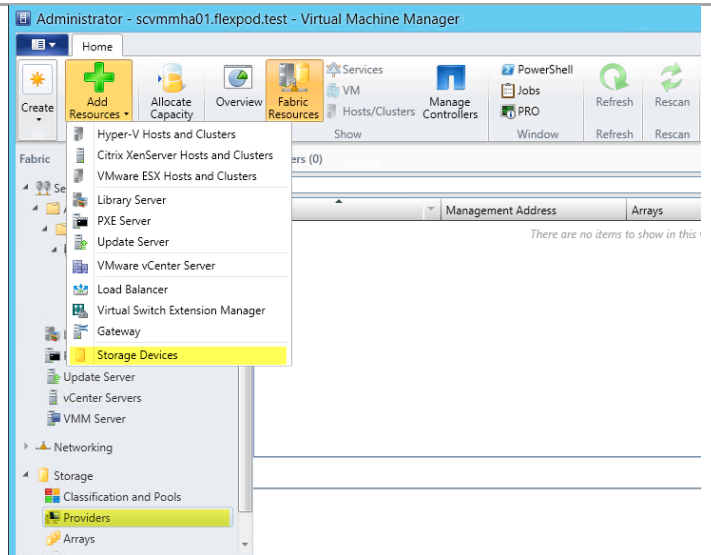
16.4 Register SMI-S in SCVMM

The following steps need to be completed in order to register the NetApp SMI-S provider in SCVMM.

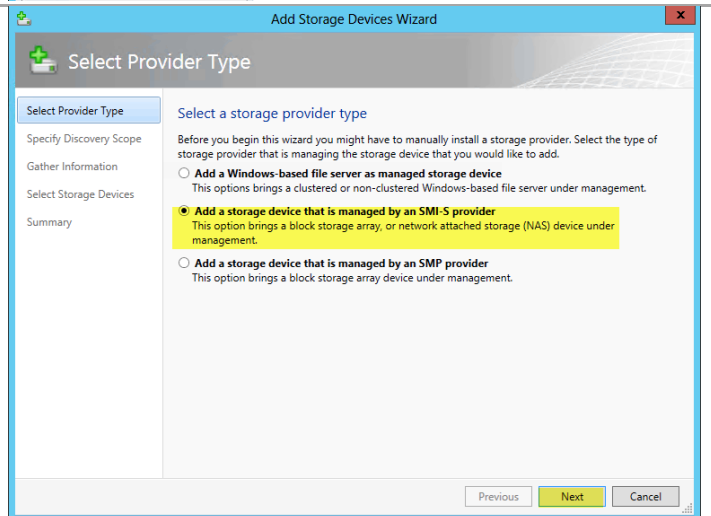
► Perform the following steps on both **Virtual Machine Manger** virtual machine.

In the **Virtual Machine Manger** 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 **Add a Storage device that is managed by a SMI-S provider**, and Click **Next**.



On the Specify Discovery Scope page.

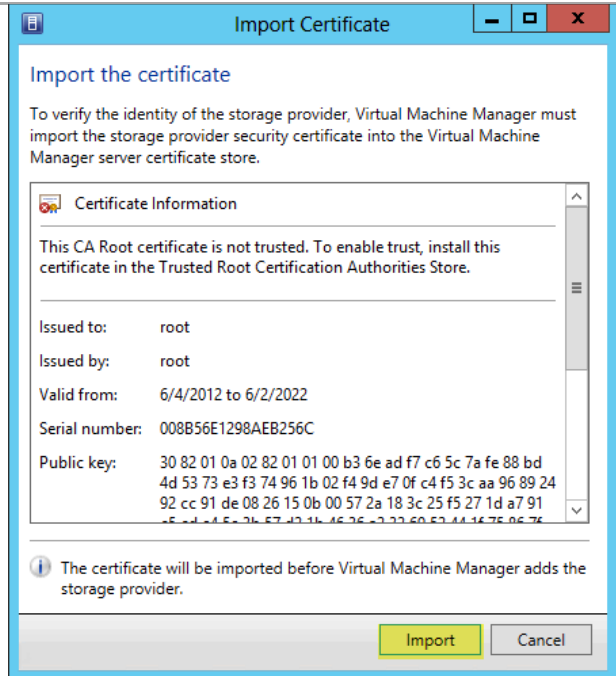
- Select **SMI-S CIMXML** for the Protocol
- Enter the **IP or FQDN** for the SMI-S provider
- Check the **Use Secure Sockets Layer** check box
- Click **Browse**, and in the resulting popup select **Create Run As Account**
 - Enter a **Display Name**
 - Enter the **User Name**
 - Enter the **Password**
 - Uncheck **Validate Domain Credentials**
 - Click **OK**.
- Click **Next**

The screenshot shows the 'Specify Discovery Scope' window. On the left, a sidebar lists 'Select Provider Type', 'Gather Information', 'Select Storage Devices', and 'Summary'. The 'Specify Discovery Scope' step is active. The main area is titled 'Specify protocol and address of the storage SMI-S provider'. It contains the following fields: 'Protocol' set to 'SMI-S CIMXML', 'Provider IP address or FQDN' set to 'SCInfra.flexpod.test', and 'TCP/IP port' set to '5989'. There is a checked checkbox for 'Use Secure Sockets Layer (SSL) connection'. The 'Run As account' field is set to 'NT AUTHORITY\NetworkService', with a 'Browse...' button next to it. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

The screenshot shows the 'Create Run As Account' window. The title bar says 'Create Run As Account'. The main area is titled 'Provide the details for this Run As account'. It contains the following fields: 'Name' set to 'SMI-S User', 'Description' (empty), 'User name' set to 'FT-SMIS-User' with a hint 'Example: contoso\domainuser or localuser', 'Password' (masked with dots), and 'Confirm password' (masked with dots). There is an unchecked checkbox for 'Validate domain credentials'. At the bottom left is a 'View Script' button, and at the bottom right are 'OK' and 'Cancel' buttons.

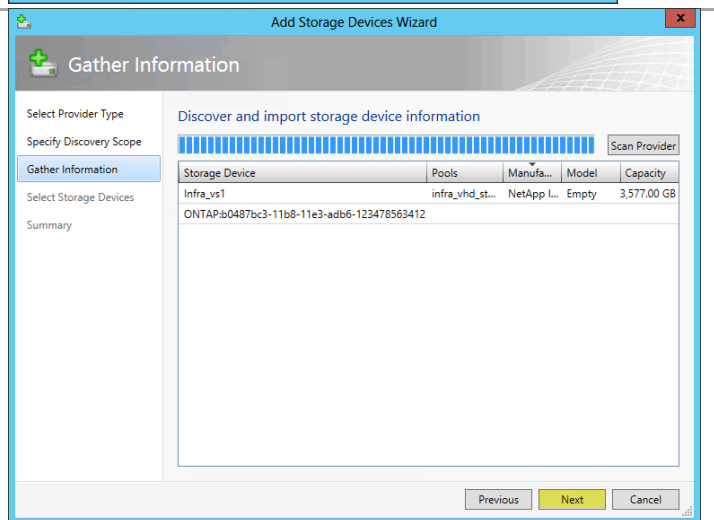
During the discovery phase a popup will open asking to Import the SMI-S providers Certificate.

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 **SCVMM_Lib** and set the **classification**.
- Click **Next**, and **Finish** to close out the wizard.

Add Storage Devices Wizard

Select Storage Devices

Select storage pools to place under management and assign a classification
Logical unit information will be imported from the selected storage pools. The assigned classification describes the capabilities of the selected storage pools.

Select Provider Type
Specify Discovery Scope
Gather Information
Select Storage Devices
Summary

Storage Device	P.	Classification	Total Capa...	Available Capa...
Infra_vs1				
<input type="checkbox"/> infra_vhd_store_1	O.		500.00 GB	192.85 GB
<input type="checkbox"/> quorum	O.		5.00 GB	3.72 GB
<input type="checkbox"/> sc_sql_db	O.		1,024.00 GB	953.75 GB
<input type="checkbox"/> scvmm_lib	O.		1,024.00 GB	1,010.19 GB
<input checked="" type="checkbox"/> scvmm_pool01	O.	Gold	4,096.00 GB	4,095.99 GB
<input type="checkbox"/> smhv_snapinfo	O.		190.00 GB	190.00 GB
<input type="checkbox"/> ucs_boot	O.		1,024.00 GB	827.29 GB

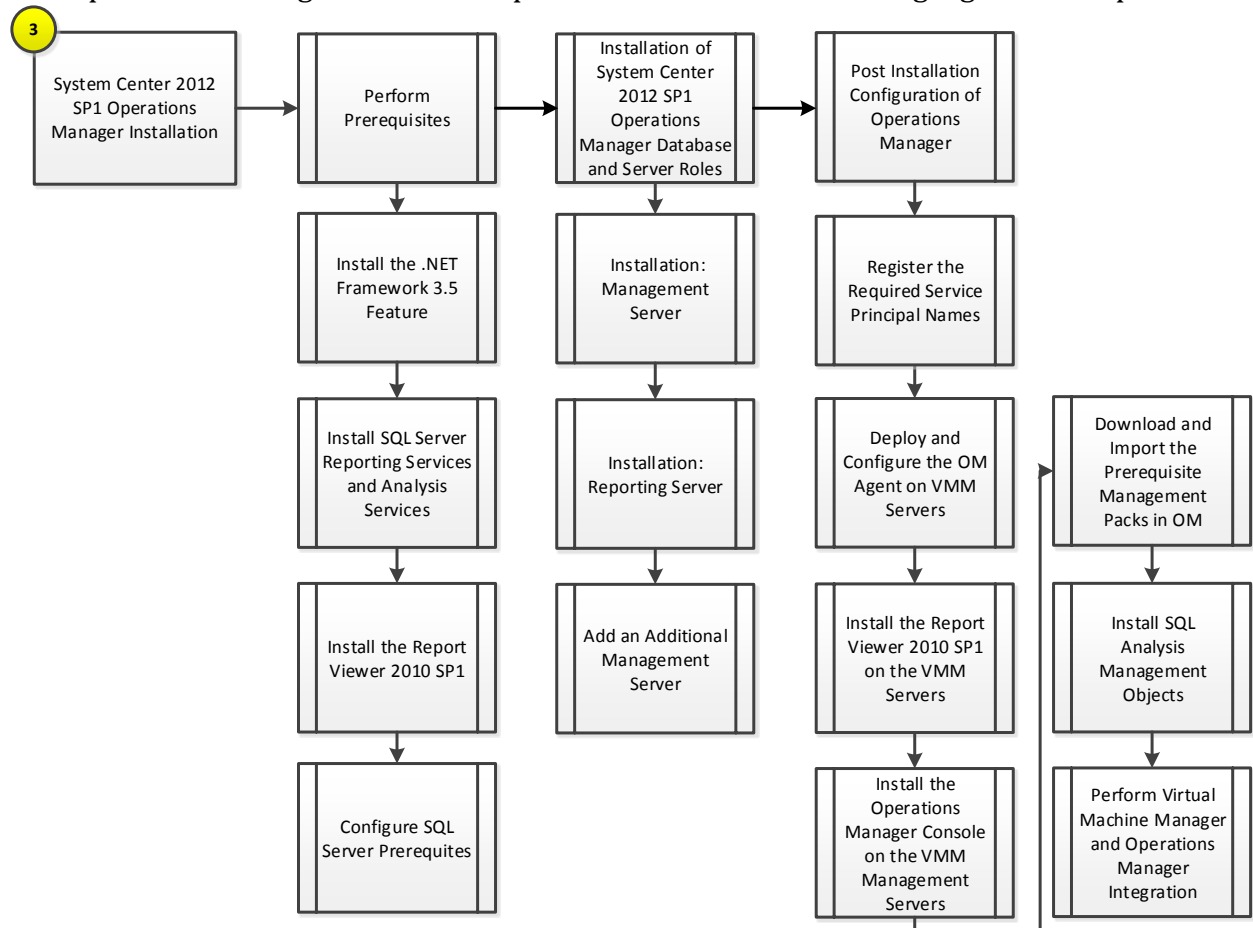
ONTAP:b0487bc3-11b8-11e3-adb6-12347856341

Create classification...

Previous Next Cancel

17 Operations Manger

The Operations Manager installation process includes the following high-level steps:



17.1 Overview

This section provides high-level walkthrough on deploying Operations Manager into the fabric management architecture. The following assumptions are made:

- A base virtual machine running Windows Server 2012 has been provisioned for Operations Manager
- A SQL Server 2012 cluster with dedicated instances has been established in previous steps:
 - The default SQL Server collation settings are required - SQL_Latin1_General_CP1_CI_AS.
 - SQL Server Full Text Search is required.
- The installation will follow a remote SQL Server configuration with multiple SQL Server instances:
 - SQL Server Reporting Services and SQL Server Analysis Services and associated databases will run on one instance locally on the Operations Manager management server.

- The Operations Manager databases will run on a separate SQL Server instance on the Fabric Management SQL cluster.

17.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created:¹⁰

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.

¹⁰ Specific rights for Operations Manager are outlined in http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin.

Groups

Verify that the following security groups have been created:

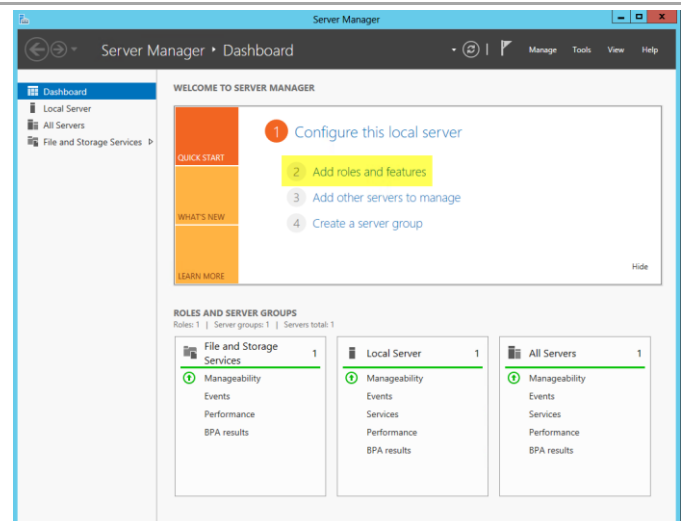
Security group name	Group scope	Members
<DOMAIN>\FT-SCOM-ADMINS	Global	<DOMAIN>\FT-SCOM-Action <DOMAIN>\FT-SCOM-SVC <DOMAIN>\FT-SCOM-DR <DOMAIN>\FT-SCOM-DW Operations Manager Administrators' privileged admin account Operations Manager computer account <DOMAIN>\FT-VMM-SVC
<DOMAIN>\FT-OM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>\FT-OM-AdvOperators	Global	Operations Manager Advanced Operators privileged admin accounts

Add the .NET Framework 3.5 Feature

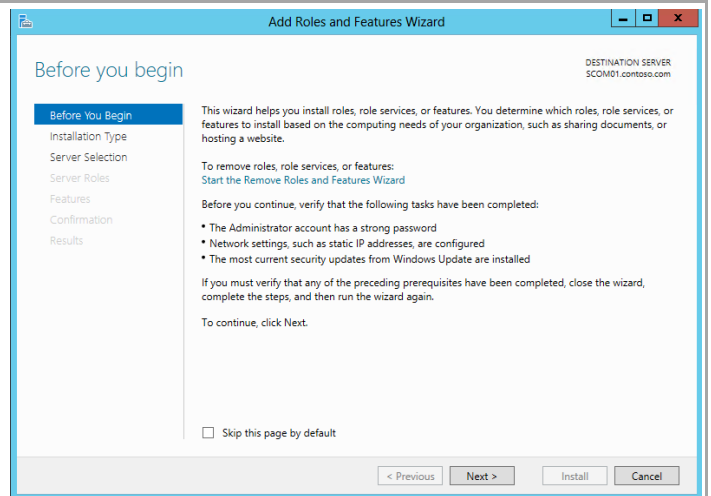
The Operations Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

► Perform the following steps on all **Operations Manager** virtual machines.

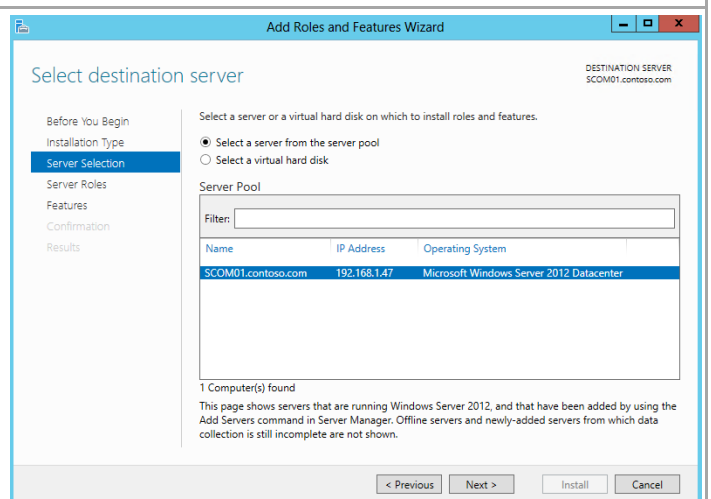
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



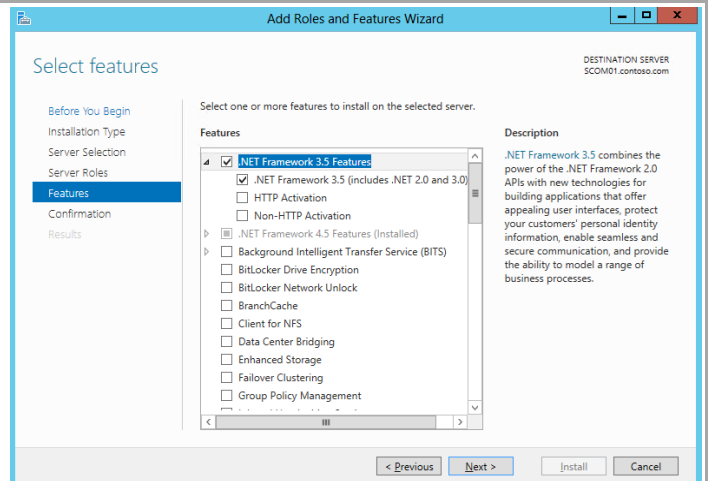
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



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.

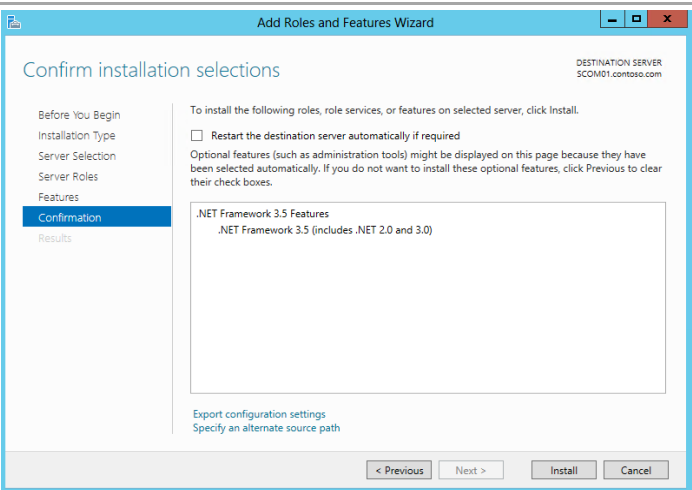


To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.

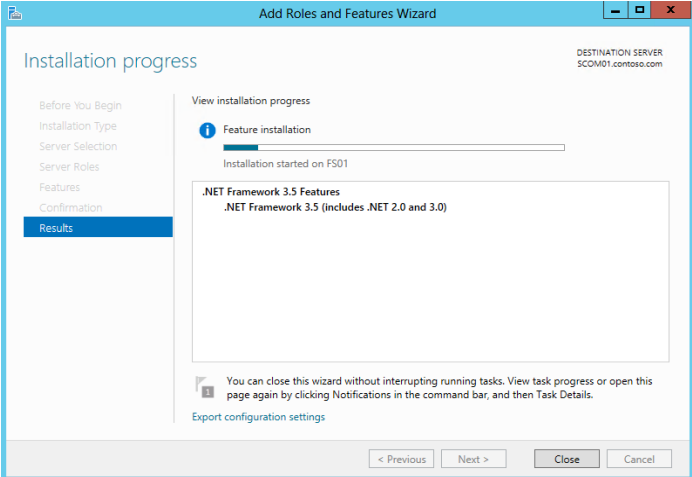


In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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



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



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



Install the SQL Server Reporting Services and Analysis Services (Split Configuration)

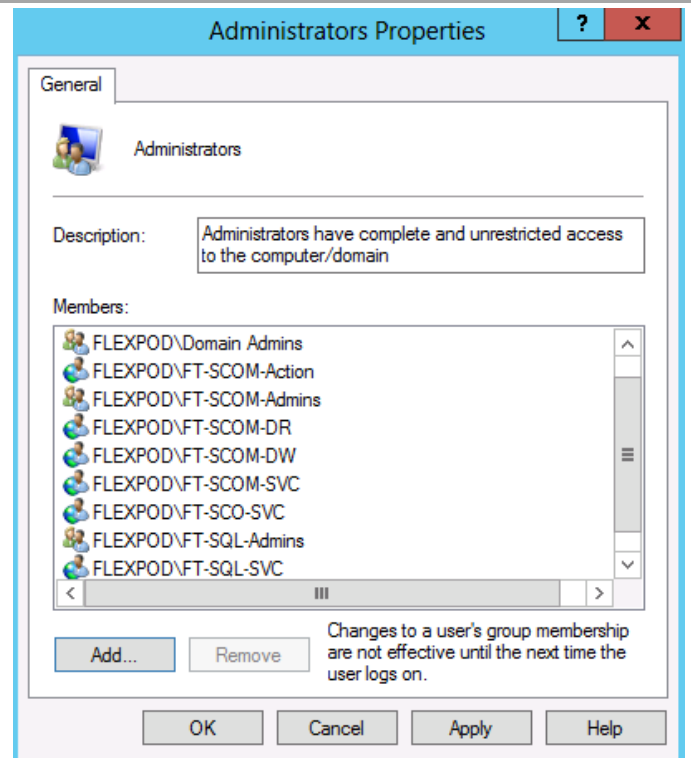
The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the provided steps to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

► Perform the following steps on the **Operations Manager Reporting Server** virtual machine only.

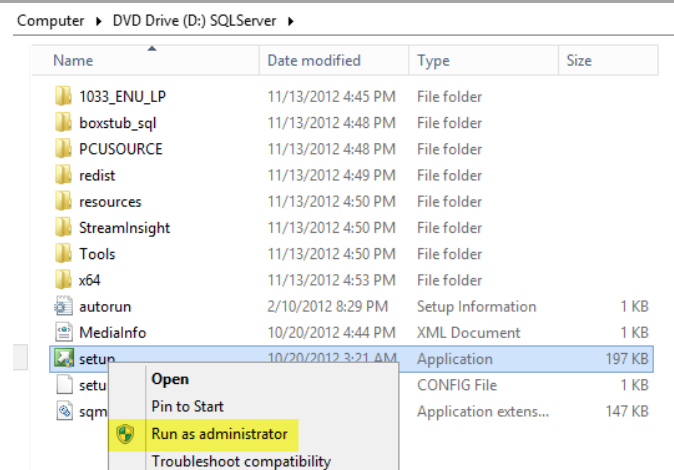
Log on to the Operations Manager Reporting Server virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager reporting server virtual machine:

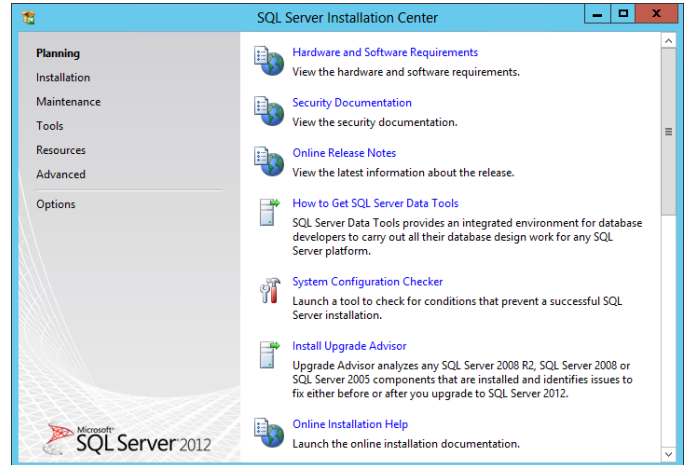
- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.
- SQL Server service account.
- SQL Server Admins group.



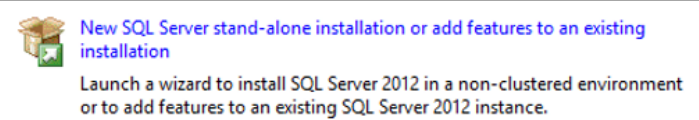
From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



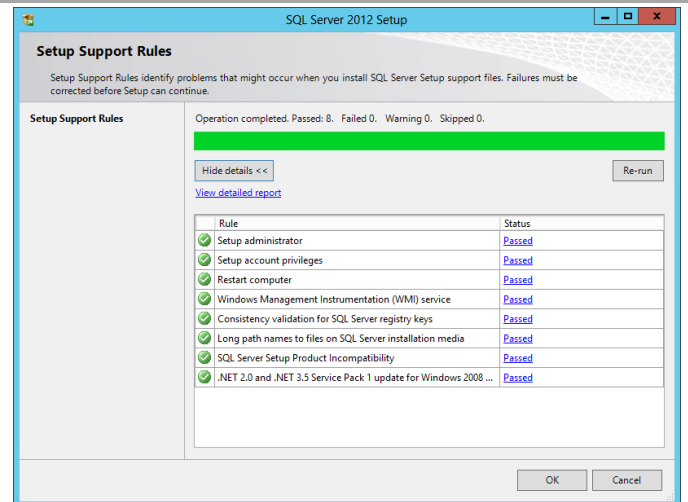
The **SQL Server Installation Center** will appear. Select the **Installation** menu option.



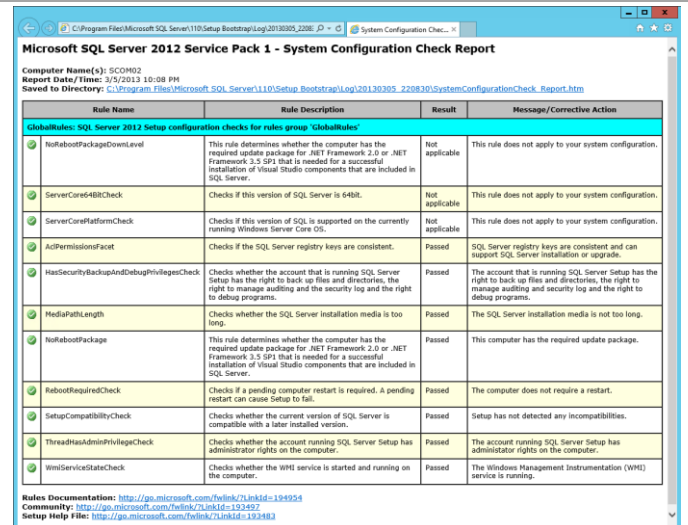
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.



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

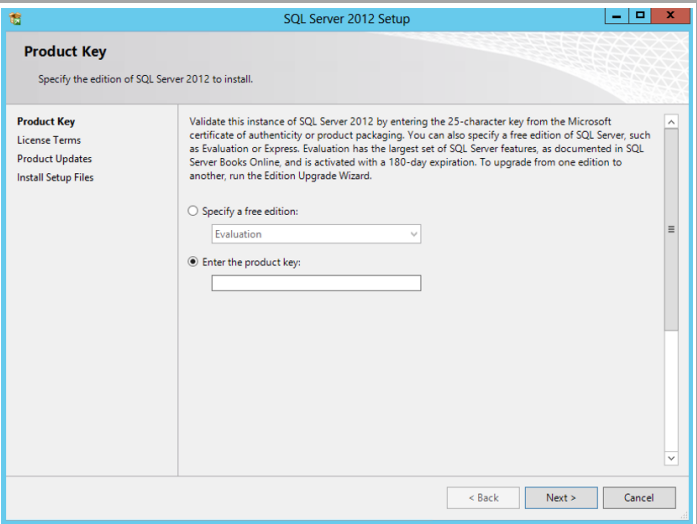


If the **View detailed report** link is selected, the following report is available.

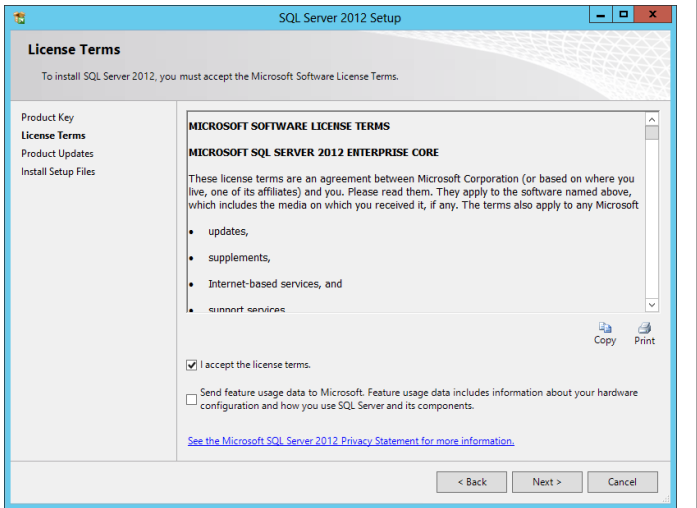


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

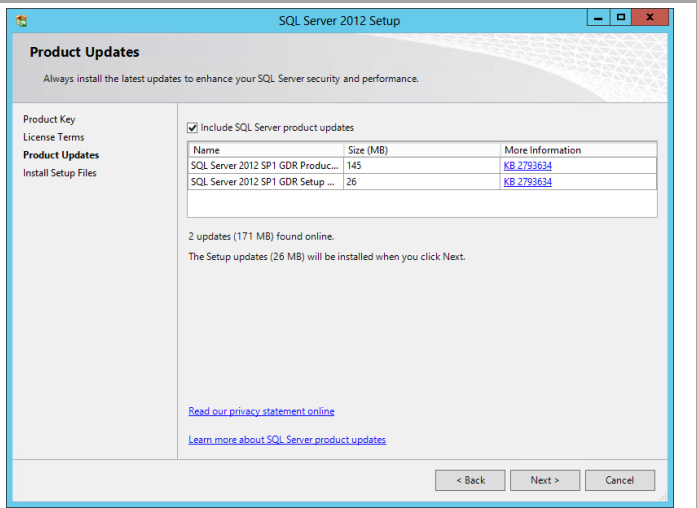
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



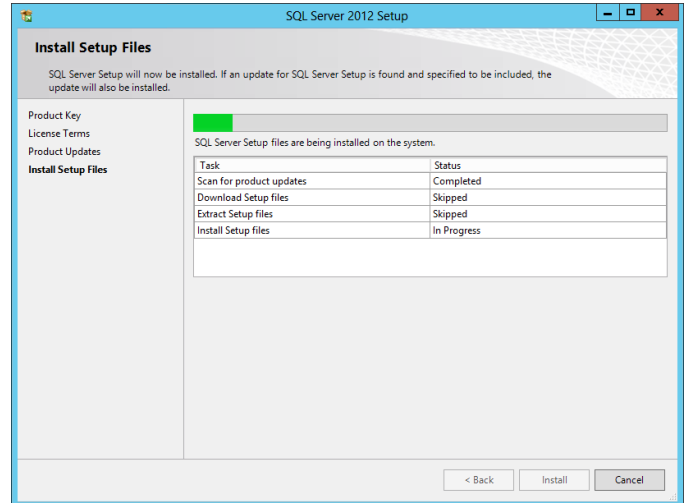
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization’s policies and click **Next** to continue.



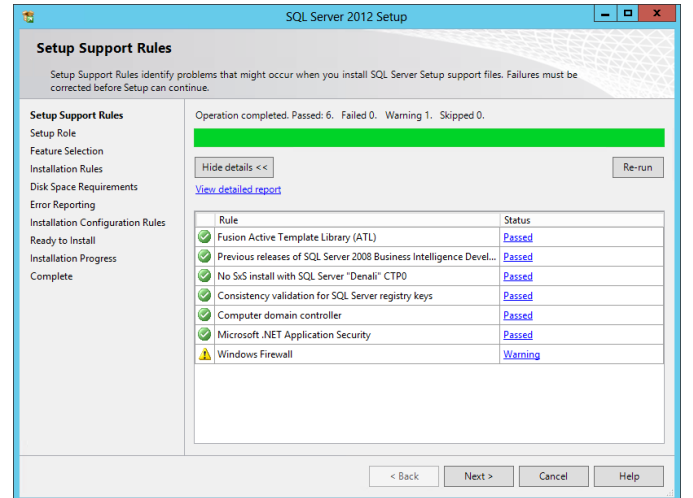
In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.



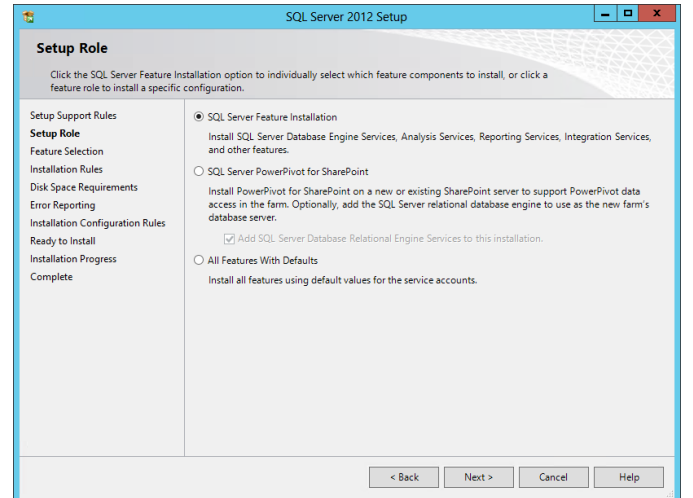
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.



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



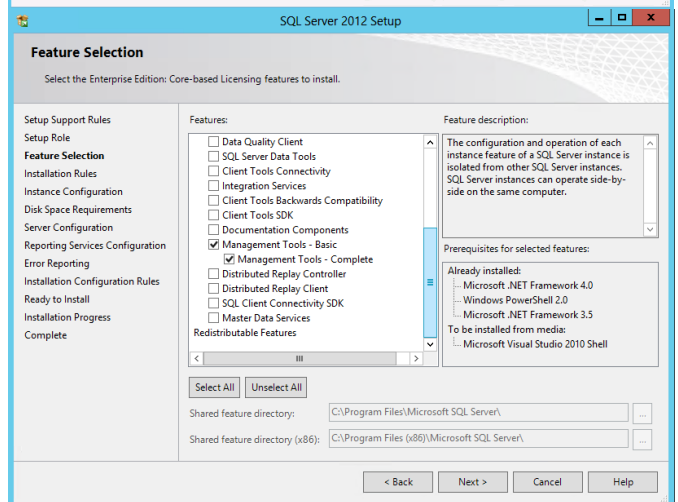
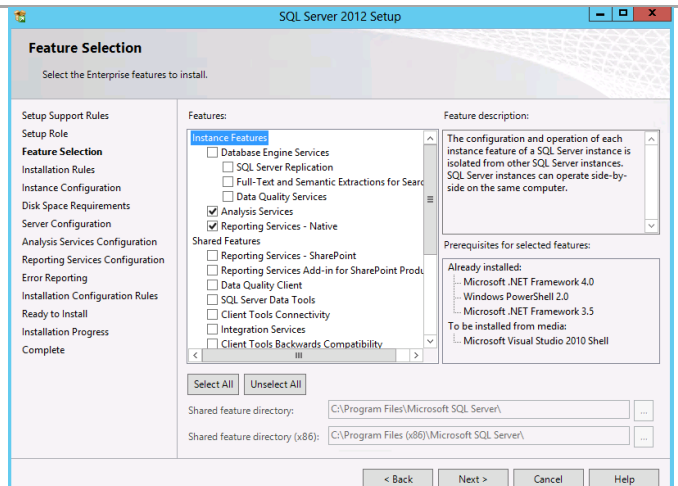
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.



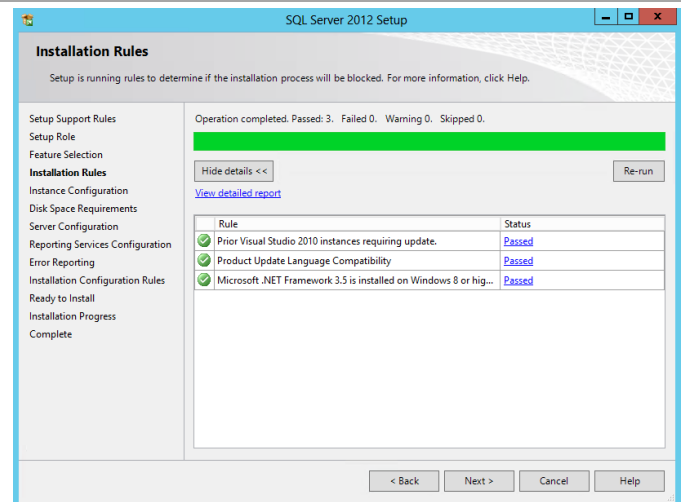
In the **Feature Selection** dialog, select the following features

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.

Note: A post-installation configuration process will occur to configure the reporting server database within the Operations Manager SQL Server instance

- **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.

The screenshot shows the 'Instance Configuration' dialog box in the SQL Server 2012 Setup wizard. The 'Named instance' radio button is selected, and the 'Instance ID' text box contains 'SCOMASRS'. The 'Instance root directory' is set to 'C:\Program Files\Microsoft SQL Server\'. The 'Analysis Services directory' is 'C:\Program Files\Microsoft SQL Server\MSAS11.SCOMASRS' and the 'Reporting Services directory' is 'C:\Program Files\Microsoft SQL Server\MSRS11.SCOMASRS'. The 'Installed instances' table is empty. The left sidebar shows the installation progress, with 'Instance Configuration' being the current step.

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

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

The screenshot shows the 'Disk Space Requirements' dialog box in the SQL Server 2012 Setup wizard. The 'Disk Usage Summary' section shows the following information: Drive C: 2788 MB required, 112679 MB available; System Drive (C:\): 1438 MB required; Instance Directory (C:\Program Files\Microsoft SQL Server\): 532 MB required; Shared Install Directory (C:\Program Files\Microsoft SQL Server\): 817 MB required. The left sidebar shows the installation progress, with 'Disk Space Requirements' being the current step.

In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NETWORK SERVICE** account for both the **SQL Server Reporting Services** and **SQL Server Analysis Services** service, . Click **Next** to continue.

Service	Account Name	Password	Startup Type
SQL Server Analysis Services	NT AUTHORITY\NETWORK SERVICE		Automatic
SQL Server Reporting Services	NT AUTHORITY\NETWORK SERVICE		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL SERVICE		Automatic

In the **Analysis Services Configuration** dialog, Click **Add**, Verify that the following accounts and/or groups are granted access to the Analysis Services:

- 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.

Server Mode:

☒ Multidimensional and Data Mining Mode

☐ Tabular Mode

Specify which users have administrative permissions for Analysis Services.

FLEXPOD\FT-SCOM-Action (FT-SCOM-Action)	Analysis Services administrators have unrestricted access to Analysis Services.
FLEXPOD\FT-SCOM-DR (FT-SCOM-DR)	
FLEXPOD\FT-SCOM-DW (FT-SCOM-DW)	
FLEXPOD\FT-SCOM-SVC (FT-SCOM-SVC)	
FLEXPOD\FT-SCOM-Admins (FT-SCOM-Admins)	

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.

Reporting Services Native Mode

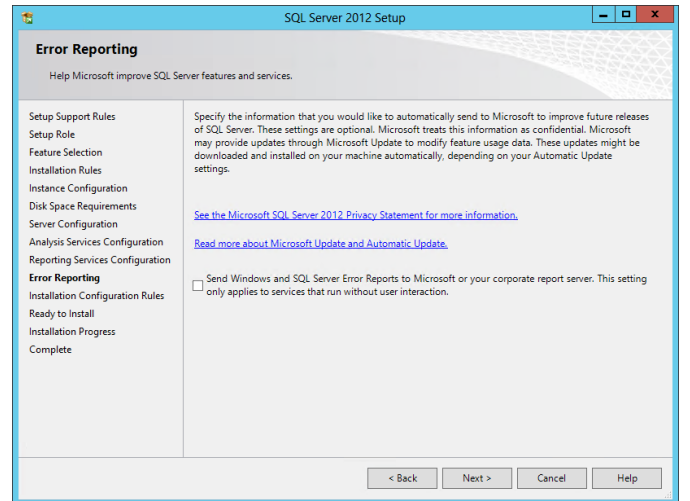
☐ Install and configure.
Installs and configures the report server in native mode. The report server is operational after setup completes.

☒ Install only.
Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.

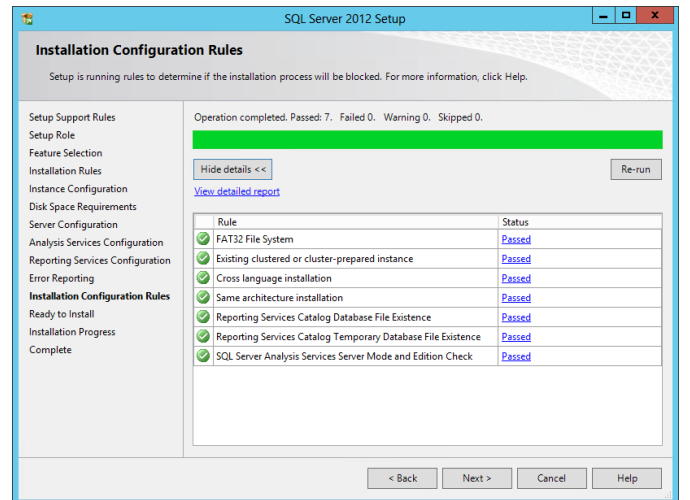
Reporting Services SharePoint Integrated Mode

☐ Install only.
Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.

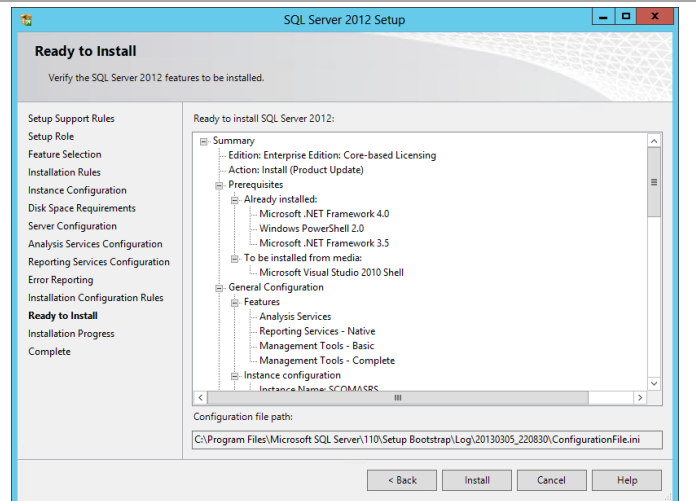
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



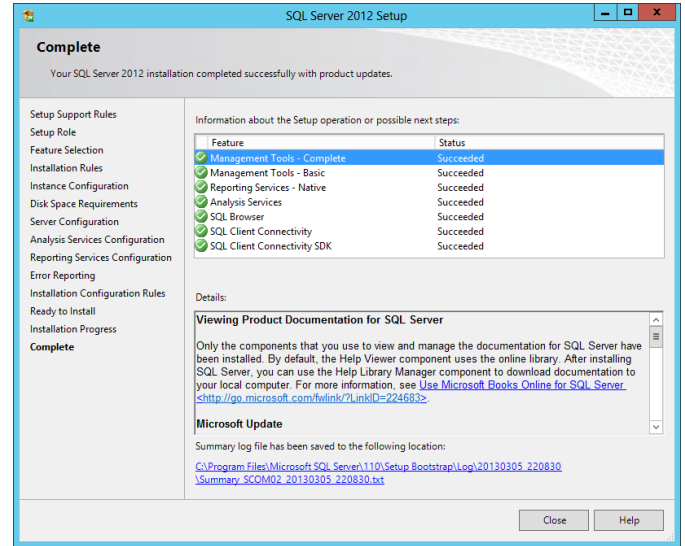
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



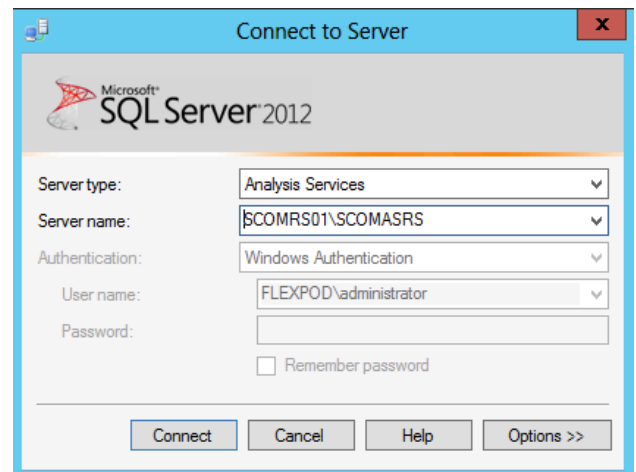
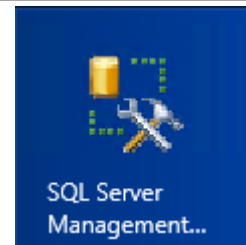
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



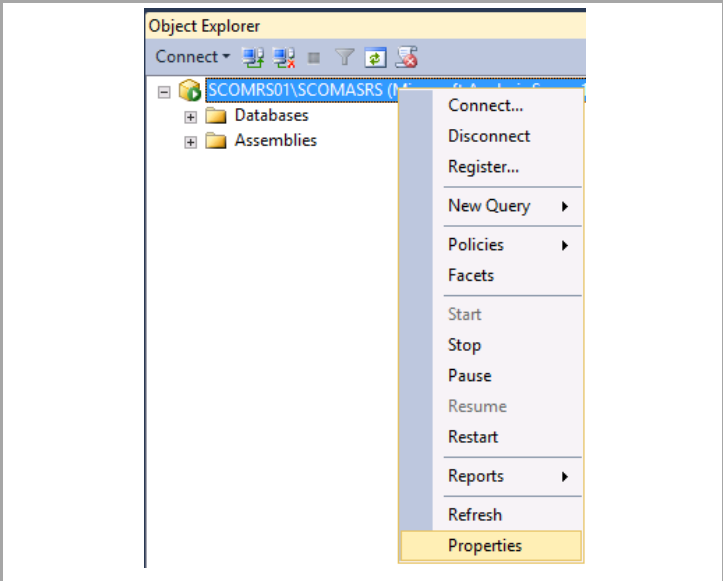
Once complete, the **Complete** dialog will appear. Click **Close** to complete the installation of this SQL Server database instance.



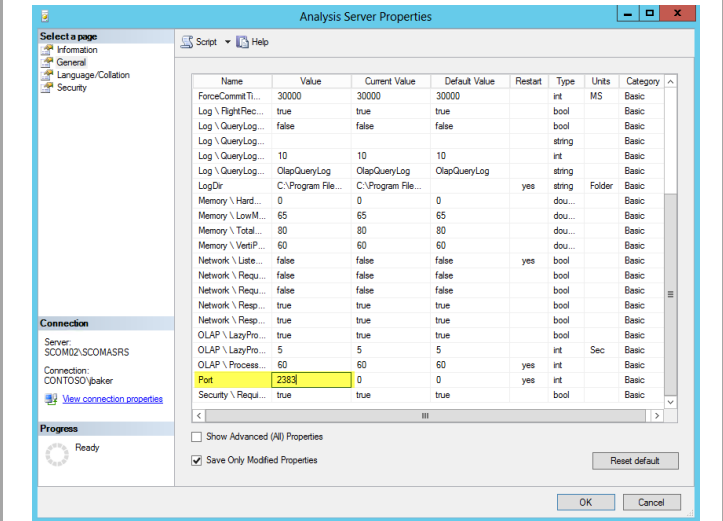
Verify the installation in SSMS prior to moving to the next step of installation. Launch **SQL Server Management Studio** and connect to Analysis Services at **ServerName\InstanceName**.



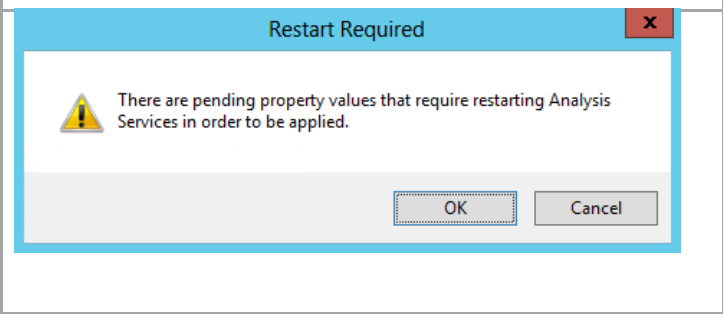
By default, named instances will use dynamic ports. In order to achieve better compatibility with firewalls the instance port should be set to static. Select the SSAS instance. Right-click on the instance and select **Properties**.

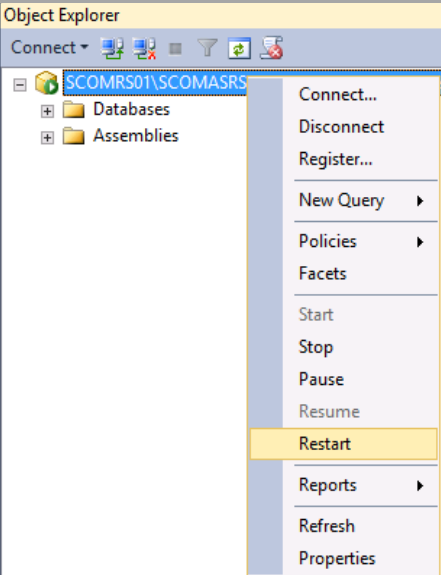
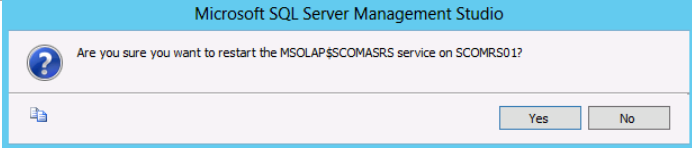
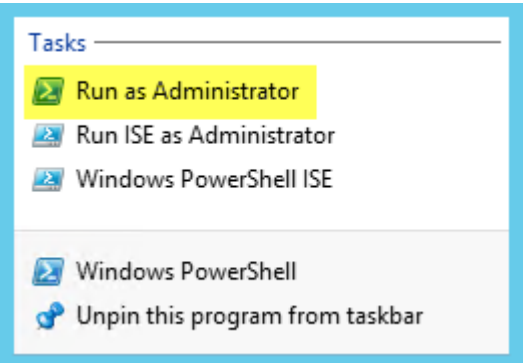


In the **Properties** dialog select the **General** tab. Scroll down to the **Port** value under the **Name** column. Select the value and change the value of 0 (zero) to 2383 or a port value of your choice. Once complete, click **OK** to continue.



When prompted by the Restart Required dialog, click **OK**.



<p>Within SQL Server ManagementStudio, in Object Explorer, select the SSAS instance, right-click and select Restart from the context menu.</p>	
<p>On the confirmation screen, click Yes. Close SQL Server Management Studio.</p>	
<p>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.</p>	

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-aab368ae0e05}
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

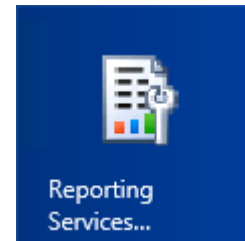
Name : {c713d65-9708-470a-837e-fd263bdf1d68}
DisplayName : SQL Analysis Services SCOMASRS Instance
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

Name : {fae137cf-a4a7-43ce-a6bd-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. Once verified, close the MMC console.

Inbound Rules						
Name	Group	Profile	Enabled	Action	Override	Pro
SQL Analysis Services Browser Service		All	Yes	Allow	No	Any
SQL Analysis Services SCOMASRS Instance		All	Yes	Allow	No	Any
SQL Reporting Services		All	Yes	Allow	No	Any
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

Once 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**.

Reporting Services Configuration Connection

Microsoft SQL Server 2012 Reporting Services

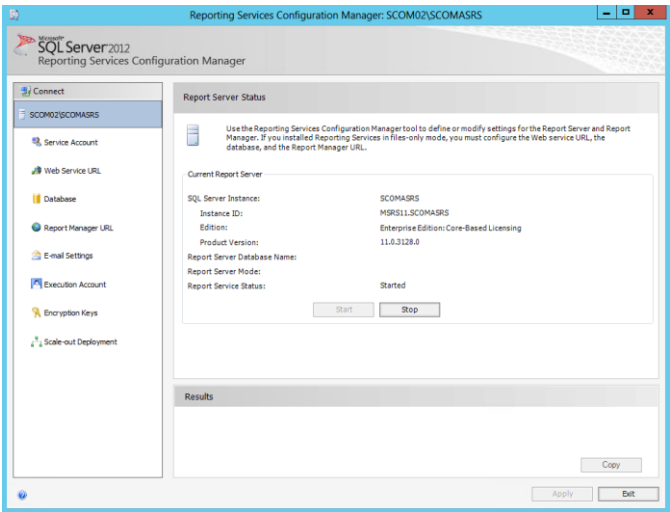
Please specify a server name, click the Find button, and select a report server instance to configure.

Server Name: SCOMRS01 Find

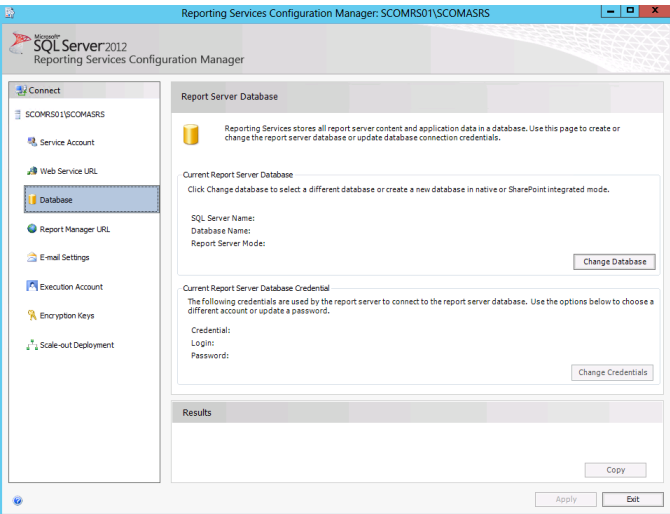
Report Server Instance: SCOMASRS

Connect Cancel

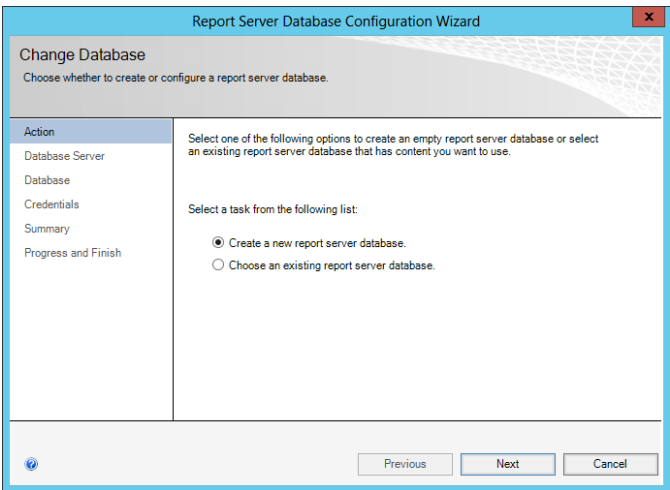
The **Reporting Services Configuration Manager** tool will appear.



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. Once verified, click **Next** to continue.

In the **Database** section, specify the following values:

- **Database Name** – *accept the default value of ReportServer.*
- **Language** – *specify the desired language option from the drop-down menu.*
- **Report Server Mode** – *select the **Native Mode** option.*

Click **Next** to continue.

In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.

In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.

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: SCOMDW\SCOMDW

Report Server Database: ReportServer

Temp Database: ReportServerTempDB

Report Server Language: English (United States)

Report Server Mode: Native

Authentication Type: Service Account

Username: FLEXPDI\FT-SCOM-DR

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**.

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

Please wait while the Report Server Database Configuration wizard configures the database. This might take several minutes to complete.

Verifying database sku	Success
Generating database script	Success
Running database script	Success
Generating rights scripts	Success
Applying connection rights	Success
Setting DSN	Success

Previous Finish Cancel

In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.

Reporting Services Configuration Manager: SCOMRS01\SCOMASRS

SQL Server 2012
Reporting Services Configuration Manager

Connect

SCOMRS01\SCOMASRS

Service Account

Web Service URL

Database

Report Manager URL

E-mail Settings

Execution Account

Encryption Keys

Scale-out Deployment

Report Server Database

Reporting Services stores all report server content and application data in a database. Use this page to create or change the report server database or update database connection credentials.

Current Report Server Database
Click Change database to select a different database or create a new database in native or SharePoint integrated mode.

SQL Server Name: SCOMDW\SCOMDW

Database Name: ReportServer

Report Server Mode: Native

Change Database

Current Report Server Database Credential
The following credentials are used by the report server to connect to the report server database. Use the options below to choose a different account or update a password.

Credential: Service Account

Login: FLEXPDI\FT-SCOM-DR

Password: *****

Change Credentials

Results

Copy

Apply Exit

In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer_SCOMASRS** in the provided text box.
- In the **Report Server Web Service Site Identification** section, set the following values:
 - **IP Address** – set the **All Assigned** drop-down menu value.
 - **TCP Port** – specify the desired TCP Port (default 80).
 - **SSL Certificate** – select the available certificate or choose the default of (Not Selected).

Click the **Apply** button to save the settings and create the Web Service URL.

The screenshot shows the 'Web Service URL' configuration window in the Reporting Services Configuration Manager. The left sidebar has 'Web Service URL' selected. The main pane shows the 'Report Server Web Service Site Identification' section. The 'Virtual Directory' is set to 'ReportServer_SCOMASRS'. The 'IP Address' is set to 'All Assigned (Recommended)', 'TCP Port' is '80', and 'SSL Certificate' is '(Not Selected)'. The 'Report Server Web Service URLs' section shows a single URL: 'http://SCOMRS01:80/ReportServer_SCOMASRS'. The 'Results' section is empty. At the bottom, there are 'Apply' and 'Exit' buttons.

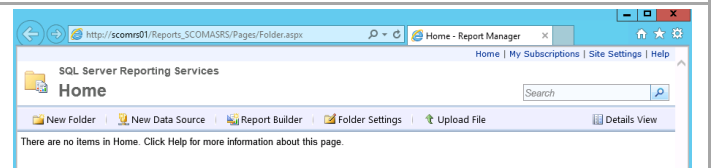
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

- In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports_SCOMASRS** in the provided text box.

Click the **Apply** button to save the settings and create the Report Manager URL.

The screenshot shows the 'Report Manager URL' configuration window in the Reporting Services Configuration Manager. The left sidebar has 'Report Manager URL' selected. The main pane shows the 'Report Manager Site Identification' section. The 'Virtual Directory' is set to 'Reports_SCOMASRS' and the 'URLs' section shows 'http://SCOMRS01:80/Reports_SCOMASRS'. The 'Results' section is empty. At the bottom, there are 'Apply' and 'Exit' buttons.

Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.

Note that in order to test the URL directory from the Operations Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.



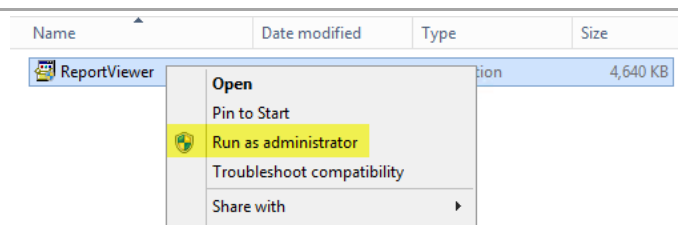
Close the Reporting Server Configuration Manager.

Install Microsoft Report Viewer 2010 SP1

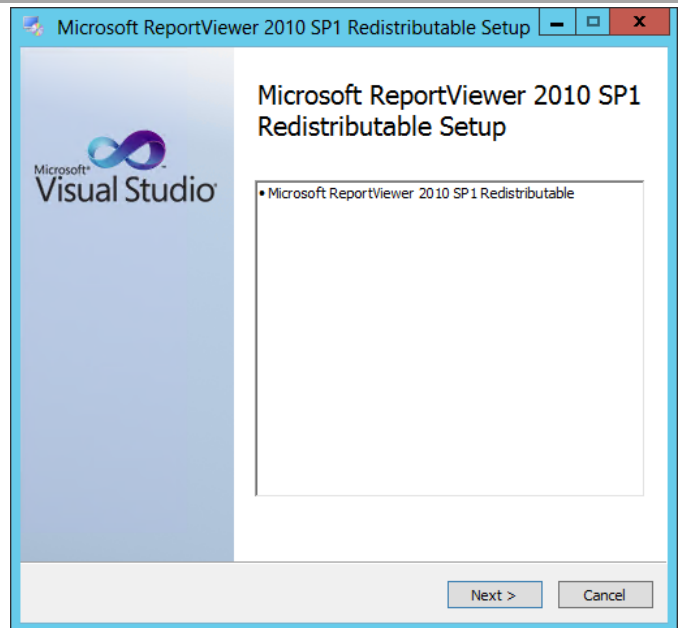
Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package to be installed prior to the installation of Operations Manager.¹¹ Follow the provided steps to install Microsoft Report Viewer 2010 SP1.

► Perform the following steps on the **Operations Manager management server** virtual machine.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

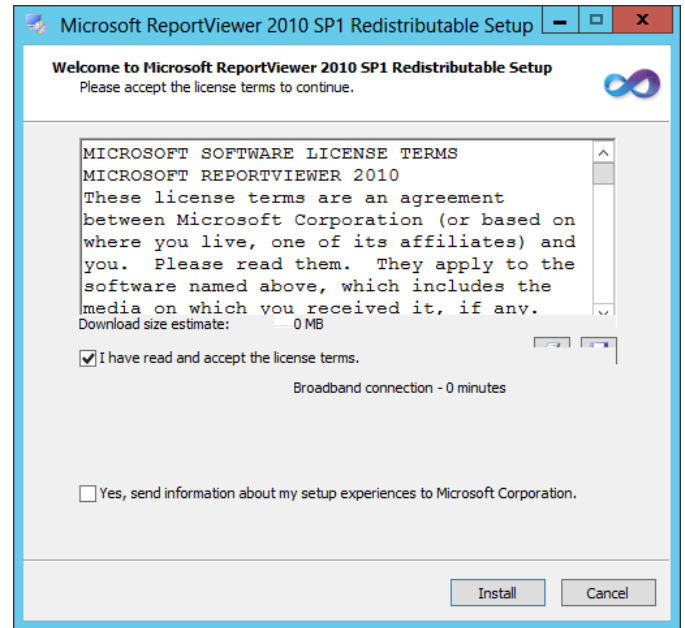


Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.

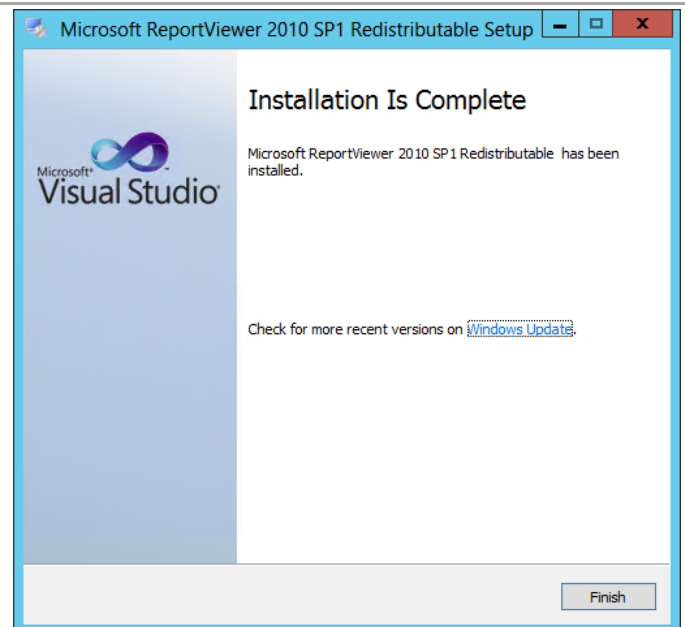


¹¹ Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en>.

Select the **I have read and accept the license terms** check box and click **Install**.



The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.



Configuration of Operations Manager SQL Server Prerequisites

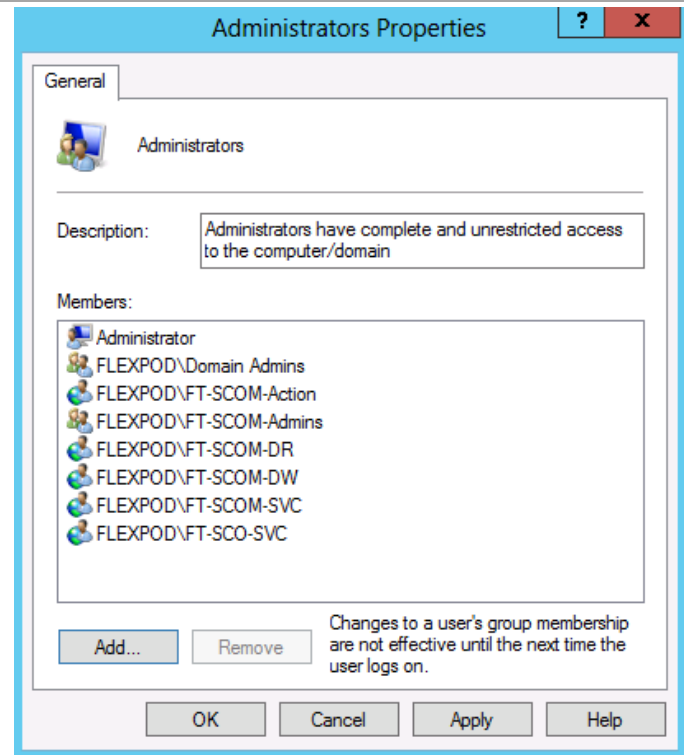
The following prerequisite steps must be completed prior to the installation of Operations Manager roles.¹²

► Perform the following steps on the **Operations Manager management server** virtual machines.

Log on to the Operations Manager virtual machine as a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager virtual machine:

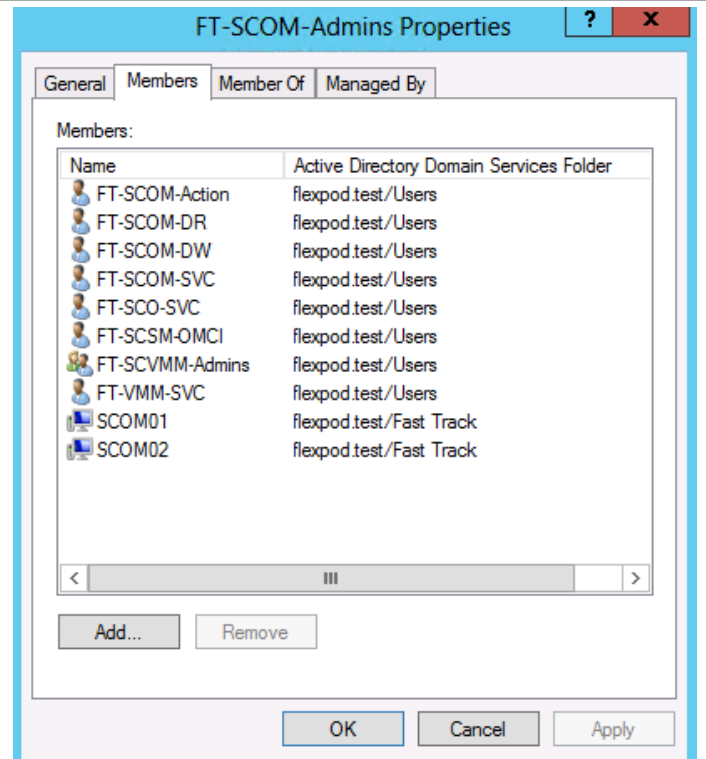
- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.
- Operations configuration service and data access service account.



► Perform the following step on an **Active Directory Domain Controller** in the target environment.

¹² Deploying System Center 2012 - Operations Manager - http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin.

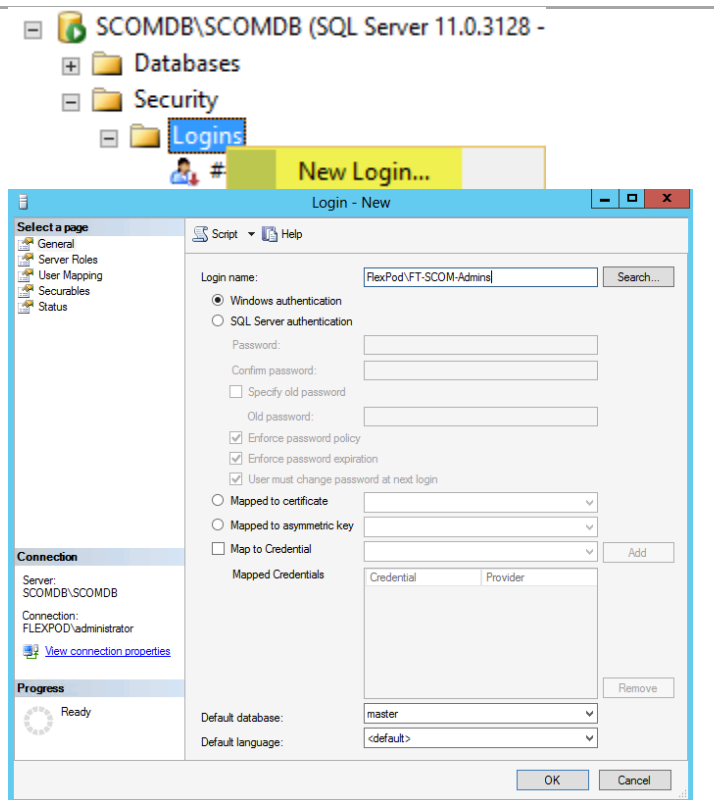
In the domain where Operations Manager will be installed, verify that the Operations Manager computer account and the groups outlined in the table above are members of the OM Admins group created earlier.



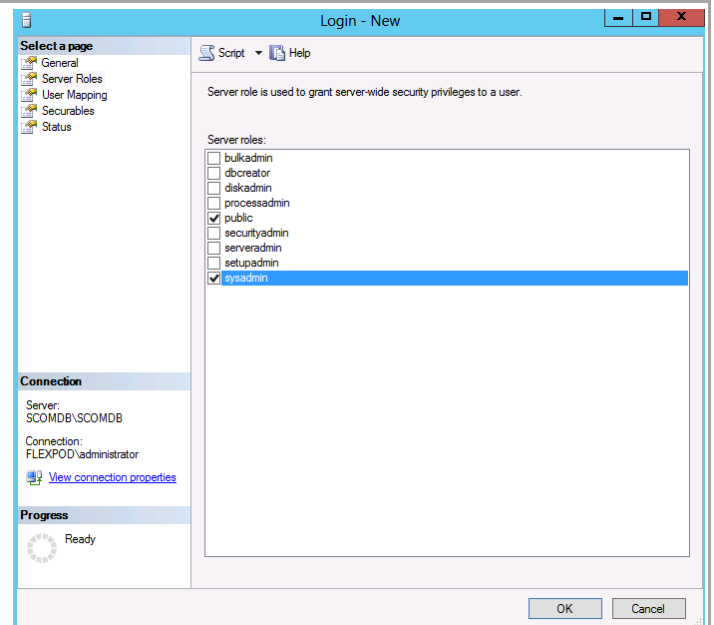
► Perform the following steps on the **primary SQL Server cluster node**.

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.

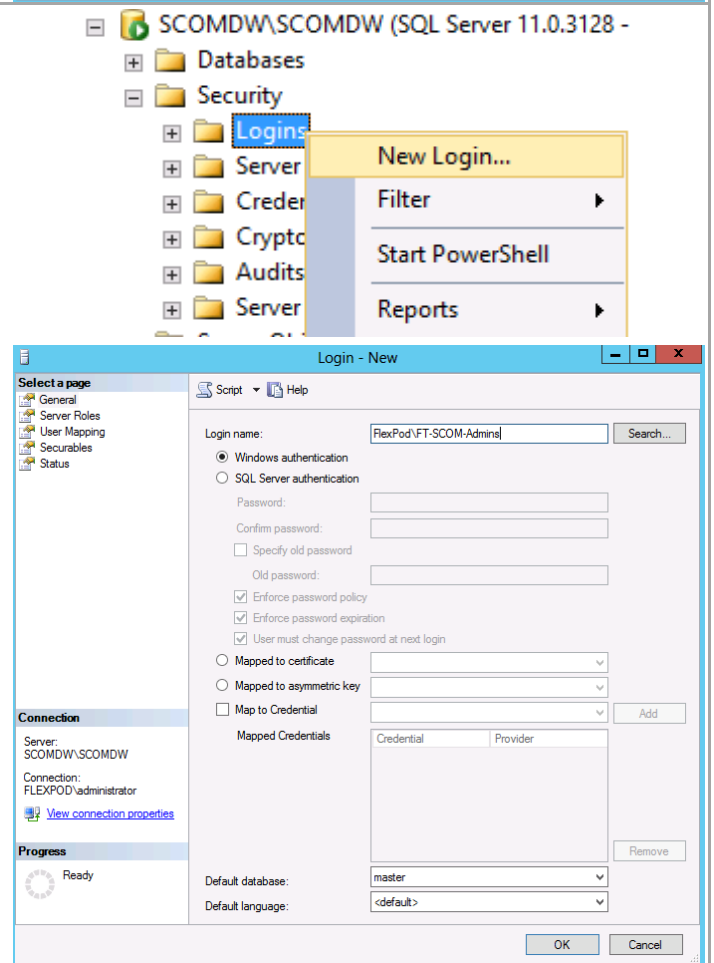
In the **Login - New** dialog, specify the Operations Manager Admins group created earlier as the new **Login name**.



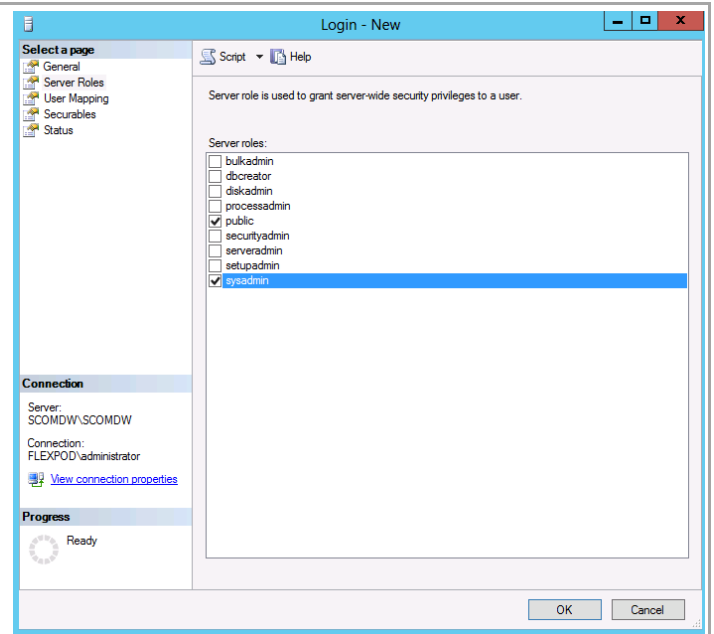
While still in the **Login - New** dialog, select the **Server Roles** page. Select the **sysadmin** role and click **OK** to add this login to the sysadmin role of the instance.



Repeat this procedure for the Operations Manager Data Warehouse SQL Server instance



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.



17.3 Installation

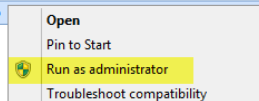
Install the Operations Manager Management Server

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.

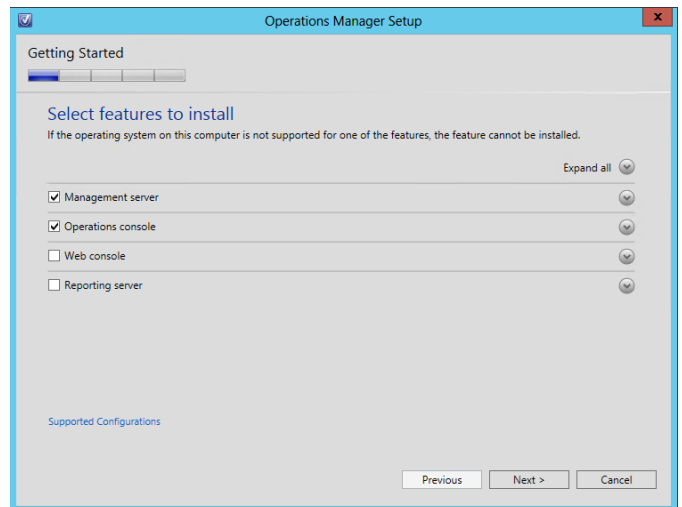
Name	Date modified	Type	Size
acs	11/23/2012 3:04 AM	File folder	
agent	11/23/2012 3:04 AM	File folder	
gateway	11/23/2012 3:04 AM	File folder	
HelperObjects	11/23/2012 3:04 AM	File folder	
Licenses	11/23/2012 3:04 AM	File folder	
ManagementPacks	11/23/2012 3:05 AM	File folder	
msxml	11/23/2012 3:05 AM	File folder	
ProductDocumentation	11/23/2012 3:05 AM	File folder	
ReportModels	11/23/2012 3:05 AM	File folder	
SCXACS	11/23/2012 3:05 AM	File folder	
Setup	11/23/2012 3:05 AM	File folder	
SupportTools	11/23/2012 3:05 AM	File folder	
autorun	10/16/2012 8:01 PM	Setup Information	1 KB
Setup	11/23/2012 6:52 PM	Application	1,571 KB



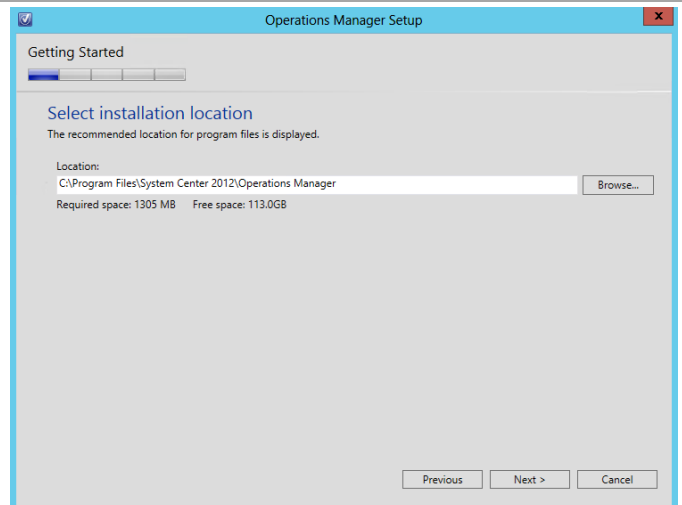
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.



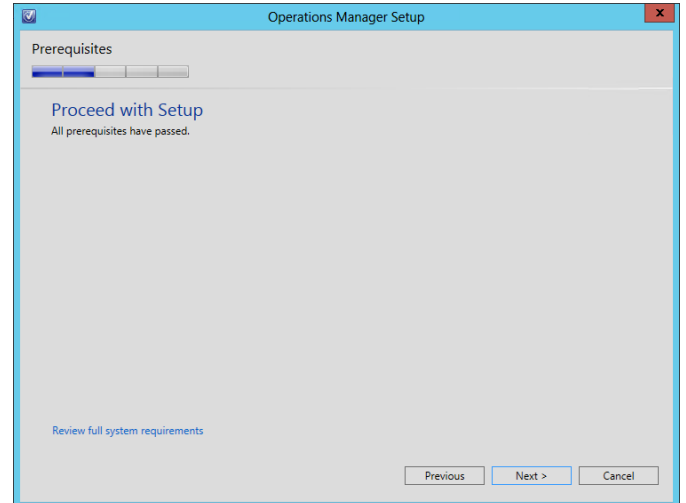
In the **Select features to install** dialog, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system pre-requisites are met in the **Proceed with Setup** dialog. If any pre-requisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.

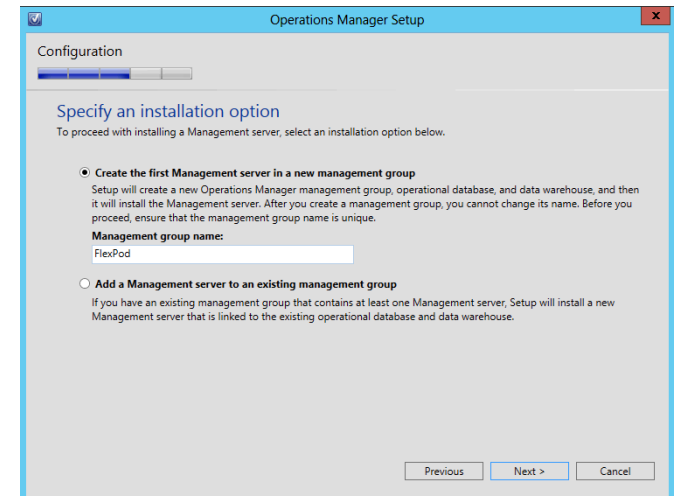


In the **Specify an installation option** dialog, two installation options are provided:

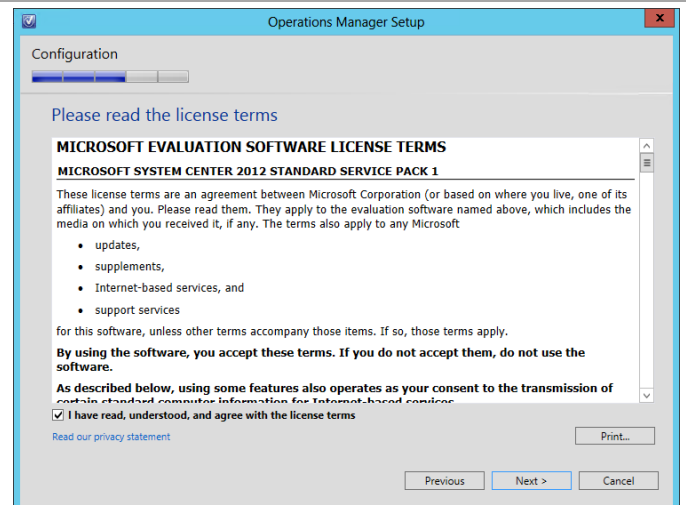
- **Create the first management server in a new management group.**
- **Add a Management server to an existing management group.**

Select the **Create the first Management server in a new management group** option and supply a unique name in the **Management group name** text box. Note that this name must be unique across System Center products.

Click **Next** to continue.



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



In the **Configure the operational database** dialog, Specify the following information in the provided text boxes:

- **Server name and instance name** – *specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.*
- **SQL Server port** – *specify the TCP port used for SQL Server connectivity (1433 is the default, however this may be different based on instance requirements outlined earlier).*
- **Database name** – *specify the name of the Operations Manager database. In most cases the default value of OperationsManager should be used.*
- **Database size (MB)** – *specify the initial database size.*¹³ *The following values can be used as a general guideline:*
 - Up to 500 agents: 12 GB.
 - Up to 1000 agents: 24 GB.
- **Data file folder** – *specify the drive letter associated in the SQL Server cluster for the database data files for the Operations Manager database. This should be cross-checked with the work sheet 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 work sheet identified earlier.*

Click **Next** to continue.

The screenshot shows the 'Operations Manager Setup' window with the 'Configuration' tab selected. The title bar reads 'Operations Manager Setup'. Below the title bar, there's a progress bar with four steps, the second of which is highlighted. The main heading is 'Configure the operational database'. A note states: '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 configuration fields are as follows:

- Server name and instance name:** scomdb/scomdb (Format: server name\instance name)
- SQL Server port:** 10435
- Database name:** OperationsManager
- Database size (MB):** 6000
- Data file folder:** O:\MSSQL11.SCOMDB\MSSQL\DATA\ (with a 'Browse...' button)
- Log file folder:** P:\MSSQL11.SCOMDB\MSSQL\Data (with a 'Browse...' button)

At the bottom right, there are three buttons: 'Previous', 'Next >', and 'Cancel'.

¹³ System Center 2012 - Operations Manager Component Add – On - <http://www.microsoft.com/en-us/download/details.aspx?id=29270> provides general guidance for database sizing.

In the **Configure the data warehouse database** dialog, specify the following information in the provided text boxes:

- **Server name and instance name** – specify the name of the SQL Server cluster network name (CNO) and the database instance created for the Operations Manager installation.
- **SQL Server port** – specify the TCP port used for SQL Server connectivity (1433 by default, however this may be different based on instance requirements outlined earlier).
- **Database name** – specify the name of the Operations Manager Data Warehouse database. In most cases the default value of OperationsManagerDW should be used.
- **Database size (MB)** – specify the initial database size.¹⁴ The following values can be used as a general guideline:
 - Up to 500 agents: 356 GB.
 - Up to 1000 agents: 720 GB.
- **Data file folder** – specify the drive letter associated in the SQL Service cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the work sheet 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 work sheet identified earlier.

Click **Next** to continue.

The screenshot shows the 'Operations Manager Setup' window with the 'Configuration' tab selected. The 'Configure the data warehouse database' section is active. It includes a progress bar at the top. Below the title, a note states: '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 form contains several input fields: 'Server name and instance name' (containing 'scomdw\scomdw'), 'SQL Server port' (containing '10436'), 'Database name' (containing 'OperationsManagerDW'), and 'Database size (MB)' (containing '14000'). There are two radio buttons: 'Create a new data warehouse database' (selected) and 'Use an existing data warehouse from a different management group'. Below these are two 'Browse...' buttons for 'Data file folder' (containing 'Q:\MSSQL11.SCOMDW\MSSQL\DATA\') and 'Log file folder' (containing 'R:\MSSQL11.SCOMDW\MSSQL\Data'). At the bottom right are 'Previous', 'Next >', and 'Cancel' buttons.

¹⁴ System Center 2012 - Operations Manager Component Add – On - <http://www.microsoft.com/en-us/download/details.aspx?id=29270> provides general guidance for database sizing.

In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- **Management server action account.**
- **System Center Configuration service and System Center Data Access service.**
- **Data Reader account.**
- **Data Writer account.**

If the use of a Domain Account is specified, enter the user account information as `<DOMAIN>\<USERNAME>` and enter the appropriate password.

Once completed, click **Next** to continue.

Account Name	Local System	Domain Account	Domain/User Name	Password
Management server action account	<input type="radio"/>	<input checked="" type="radio"/>	FLEXPOD\FT-SCOM-Actio	*****
System Center Configuration service and System Center Data Access service	<input type="radio"/>	<input checked="" type="radio"/>	FLEXPOD\FT-SCOM-SVC	*****
Data Reader account	<input type="radio"/>	<input checked="" type="radio"/>	FLEXPOD\FT-SCOM-DR	*****
Data Writer account	<input type="radio"/>	<input checked="" type="radio"/>	FLEXPOD\FT-SCOM-DW	*****

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.

Customer Experience Improvement Program

The Customer Experience Improvement Program collects data about your use of Microsoft applications to identify possible improvements for Microsoft products.

☒ Yes, I am willing to participate anonymously in the Customer Experience Improvement Program

☐ No, I am not willing to participate

Error Reporting

When a program error occurs, information about the error can be anonymously reported to Microsoft. This information is used to help identify and resolve common issues with Operations Manager.

☒ Yes, I am willing to participate anonymously. Please automatically send my error reports.

☐ Yes, I am willing to participate anonymously. Please queue the reports so that I can choose when to send them.

☐ No, I am not willing to participate

The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

Note: Ensure you set the database sizes appropriately for your particular deployment.

Installation Summary

Review your selections for the features that you are installing. To continue, click **Install**. To change your selections, click **Previous**.

Installation location:
C:\Program Files\System Center 2012\Operations Manager

Management group name:
SCOMMG01

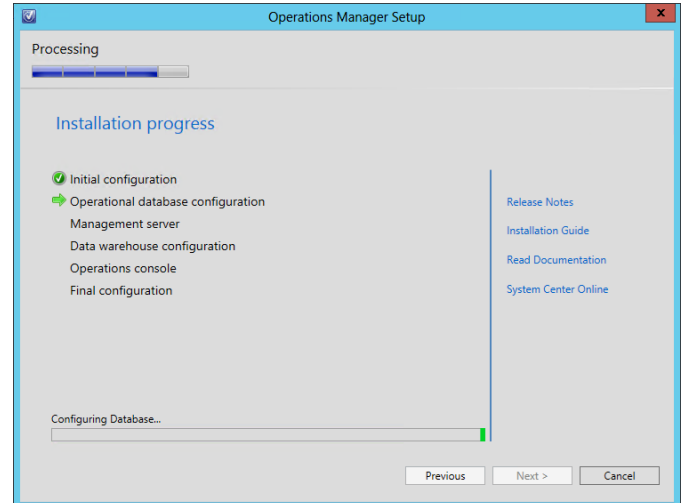
Operational database:
OperationsManager will be created on SCOMDB\SCOMDB

Database size (MB):
6000

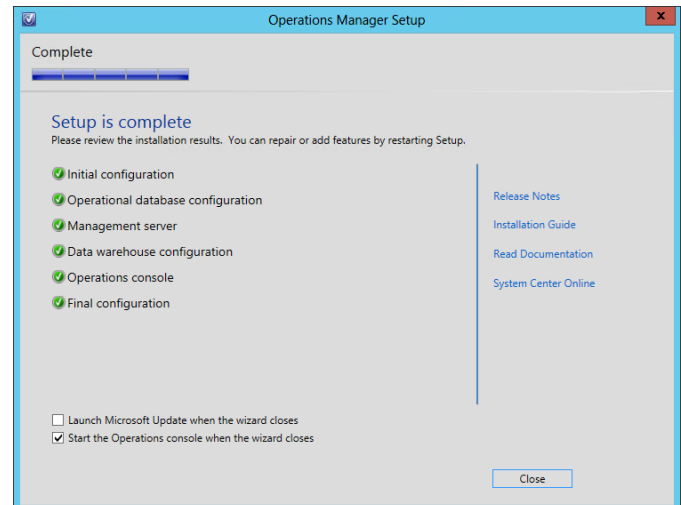
Data warehouse database:
OperationsManagerDW will be created on SCOMDW\SCOMDW

Data warehouse database size (MB):
14000

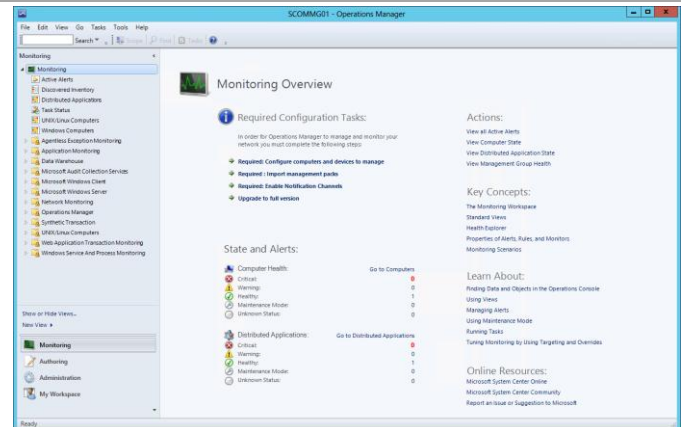
The wizard will display the progress while installing features.



Once 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.



Once completed, the **Operations Manager** console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



Install the Operations Manager Reporting Server

The following steps must be completed in order to install and configure the Operations Manager reporting server role.

► Perform the following steps on the **Operations Manager reporting server** virtual machine.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

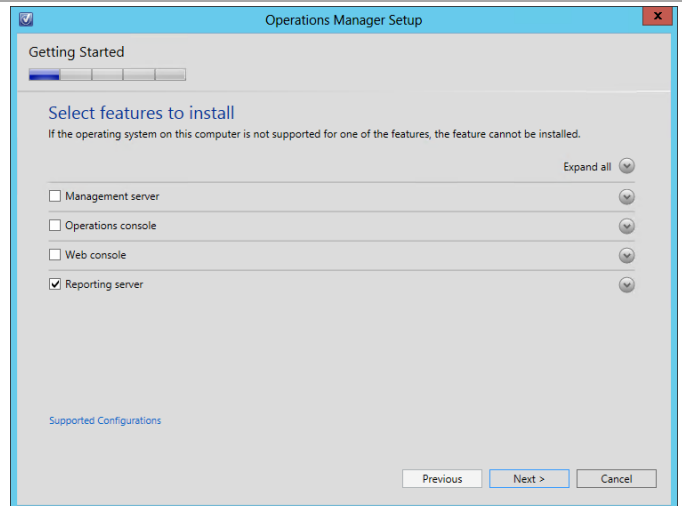
Name	Date modified	Type	Size
acs	11/23/2012 3:04 AM	File folder	
agent	11/23/2012 3:04 AM	File folder	
gateway	11/23/2012 3:04 AM	File folder	
HelperObjects	11/23/2012 3:04 AM	File folder	
Licenses	11/23/2012 3:04 AM	File folder	
ManagementPacks	11/23/2012 3:05 AM	File folder	
msxml	11/23/2012 3:05 AM	File folder	
ProductDocumentation	11/23/2012 3:05 AM	File folder	
ReportModels	11/23/2012 3:05 AM	File folder	
SCXACS	11/23/2012 3:05 AM	File folder	
Setup	11/23/2012 3:05 AM	File folder	
SupportTools	11/23/2012 3:05 AM	File folder	
autorun	10/16/2012 8:01 PM	Setup Information	1 KB
Setup	11/23/2012 6:52 PM	Application	1,571 KB

Open
Pin to Start
Run as administrator
Troubleshoot compatibility

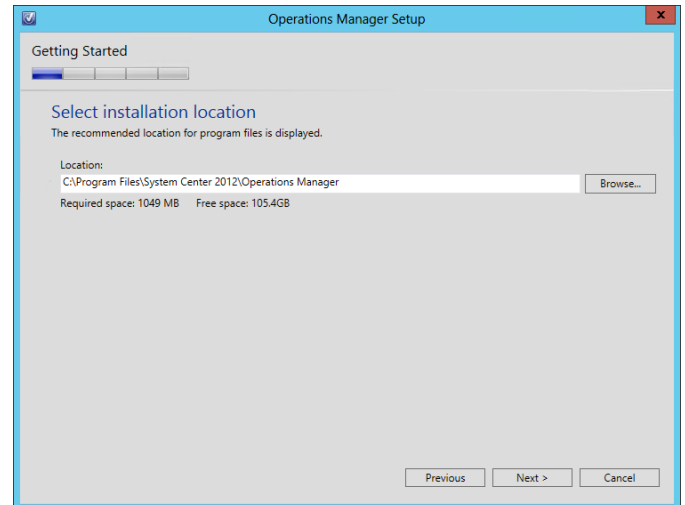
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.



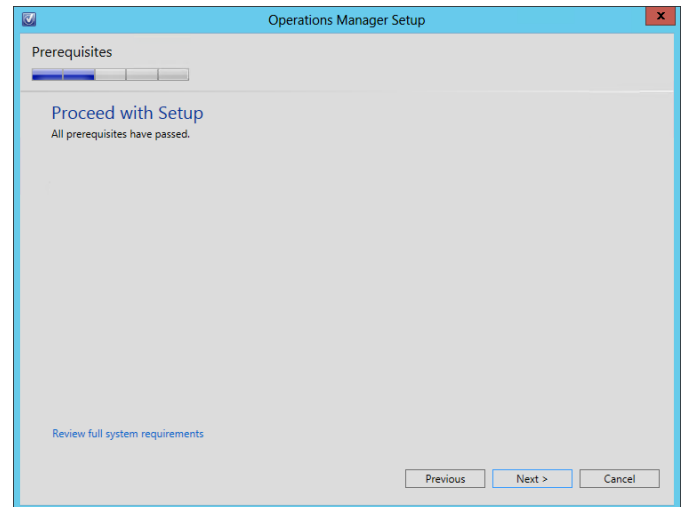
In the **Select features to install** dialog, verify that the **Reporting server** check boxes are selected. Click **Next** to continue.



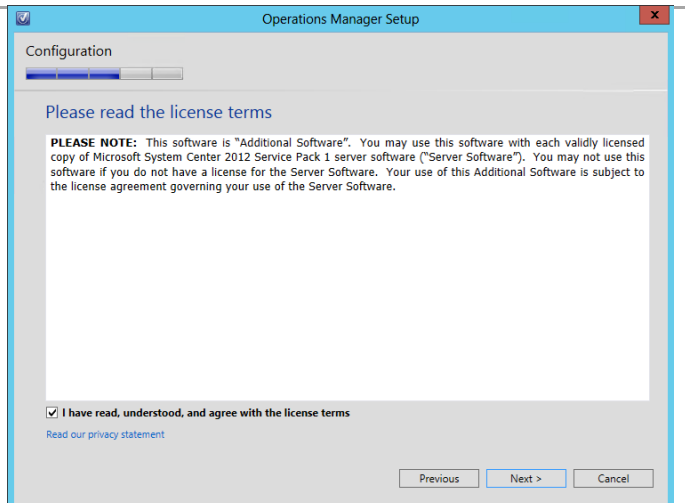
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.



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. Once verified, click **Next** to continue.



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



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.

The screenshot shows the 'Specify a Management server' dialog within the 'Operations Manager Setup' window. The dialog has a title bar with a checkmark icon and a close button. Below the title bar is a progress bar with four steps, the second of which is highlighted. The main heading is 'Specify a Management server'. Below this is a descriptive paragraph: 'Enter the name of a Management server to be used by the Web console and reporting features only. The Management server that you specify will handle data associated with specific Management servers or management groups.' There is a text input field labeled 'Management server name:' containing the text 'SCOM01'. At the bottom right are three buttons: 'Previous', 'Next >', and 'Cancel'.

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.

The screenshot shows the 'SQL Server instance for reporting services' dialog within the 'Operations Manager Setup' window. The dialog has a title bar with a checkmark icon and a close button. Below the title bar is a progress bar with four steps, the third of which is highlighted. The main heading is 'SQL Server instance for reporting services'. Below this is a descriptive paragraph: 'Select the SQL Server instance on which you want to host SQL Server Reporting Services (SSRS). This installation of a SQL Server Report Server will integrate the security of the selected SSRS instance with Operations Manager role-based security. Any reports that were previously installed on this SQL Server instance might become inaccessible. Only SQL server instances which meet the supported configuration are shown.' There is a drop-down menu labeled 'SQL Server instance' with the text 'SCOMRS01\SCOMASRS' selected. At the bottom right are three buttons: 'Previous', 'Next >', and 'Cancel'.

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.

Once completed, click **Next** to continue.

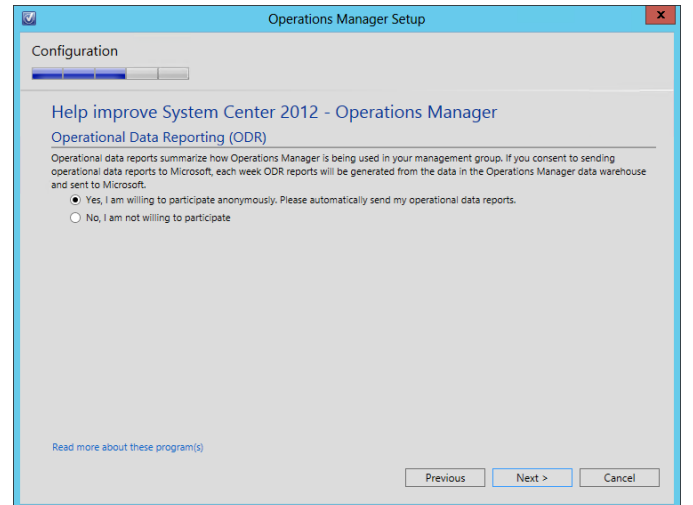
The screenshot shows the 'Configure Operations Manager accounts' dialog within the 'Operations Manager Setup' window. The dialog has a title bar with a checkmark icon and a close button. Below the title bar is a progress bar with four steps, the fourth of which is highlighted. The main heading is 'Configure Operations Manager accounts'. Below this is a descriptive paragraph: 'If you want to use a single account for all services, verify that the account has all the required rights. For more information, see the Operations Manager deployment documentation.' There is a table with the following columns: 'Account Name', 'Local System', 'Domain Account', 'Domain/User Name', and 'Password'. The table has one row with the following values: 'Data Reader account', a radio button selected under 'Domain Account', 'FlexPod\FT-SCOM-DR', and a masked password field. At the bottom right are three buttons: 'Previous', 'Next >', and 'Cancel'.

Account Name	Local System	Domain Account	Domain/User Name	Password
Data Reader account	<input type="radio"/>	<input checked="" type="radio"/>	FlexPod\FT-SCOM-DR	••••••••

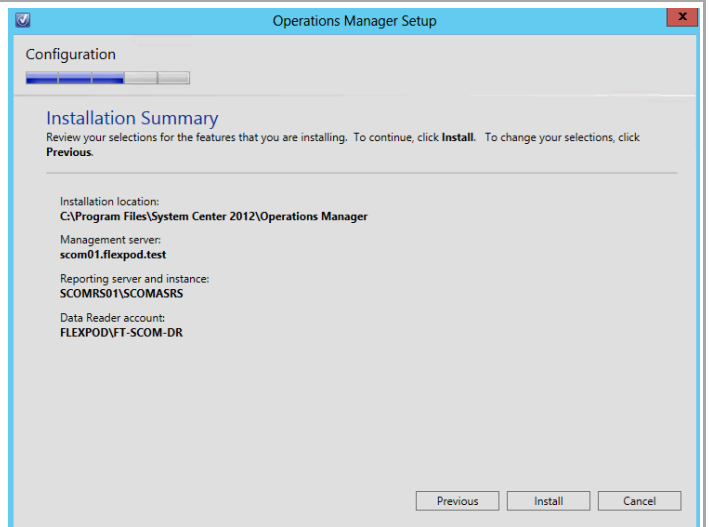
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. This includes:

- **Operational Data Reporting (ODR).**

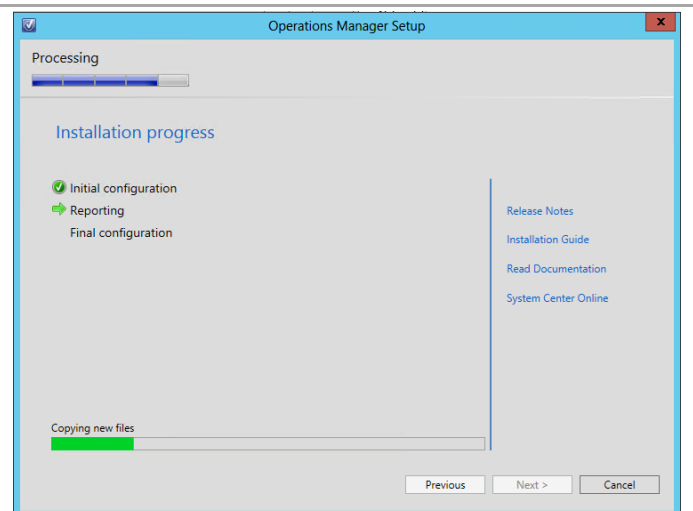
Select the appropriate option based on your organization's policies and click **Next** to continue.



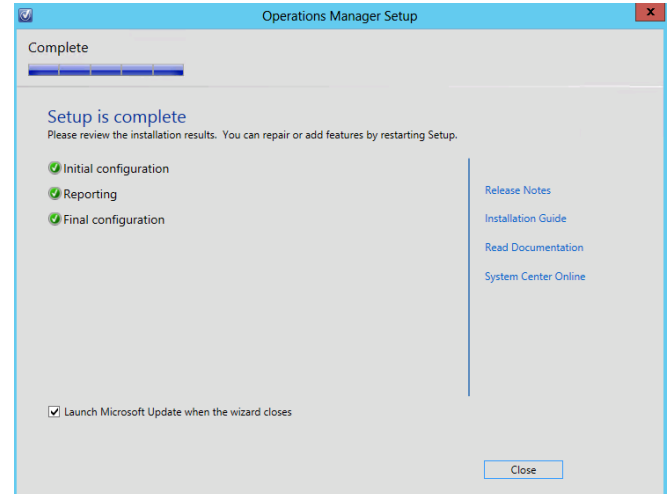
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



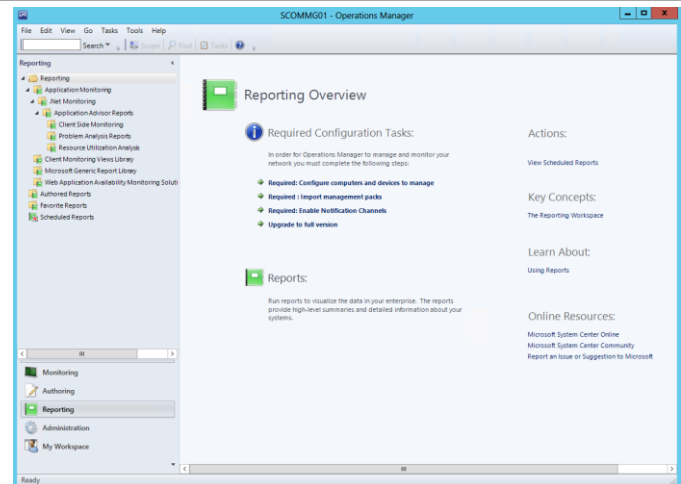
The wizard will display the progress while installing features.



Once 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.



Once 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.



17.4 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.

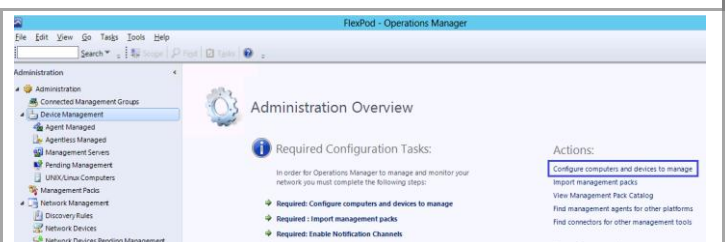
- Perform the following steps on a **Domain Controller** in the domain where Operations Manager is installed.

<p>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.</p>	
<p>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.</p> <p>To set the SPN run the following commands from an administrative command prompt: SETSPN.exe -S MSOMSdkSvc/<ManagementServerFQDN> <domain>\<SDKServiceAccount></p> <p>SETSPN.exe -S MSOMSdkSvc/<ManagementServerNetBIOS> <domain>\<SDKServiceAccount> Where <ManagementServerFQDN> is the name of the Operations Manager management server and <SDKServiceAccount> is the name of the Operations Manager Service Account.</p> <p>If there is more than one Management Server being deployed then these commands must be run for each Management Server.</p>	
<p>Once complete the SPNs can be confirmed with the following command: SETSPN -L <DOMAIN>\<SDKServiceAccount></p>	

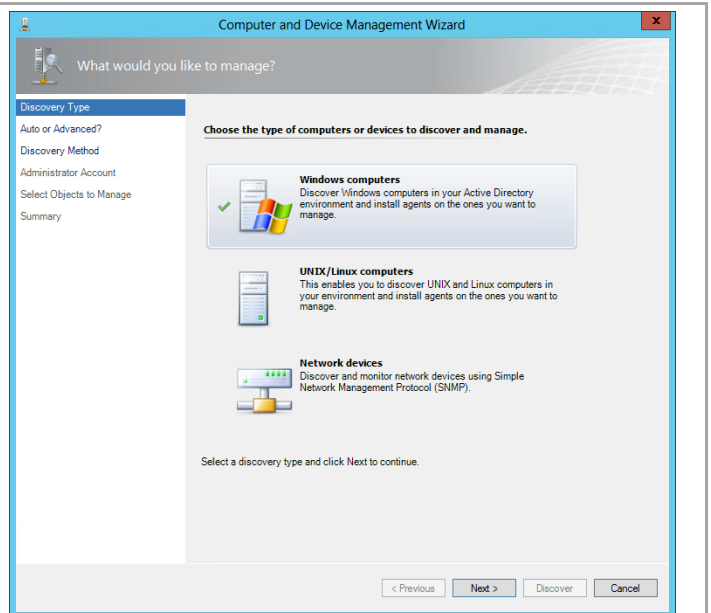
Deploy and Configure the operations Manager Agent on the Virtual Machine Manager Management Server Nodes

► Perform the following steps on the **Operations Manager management server** virtual machine.

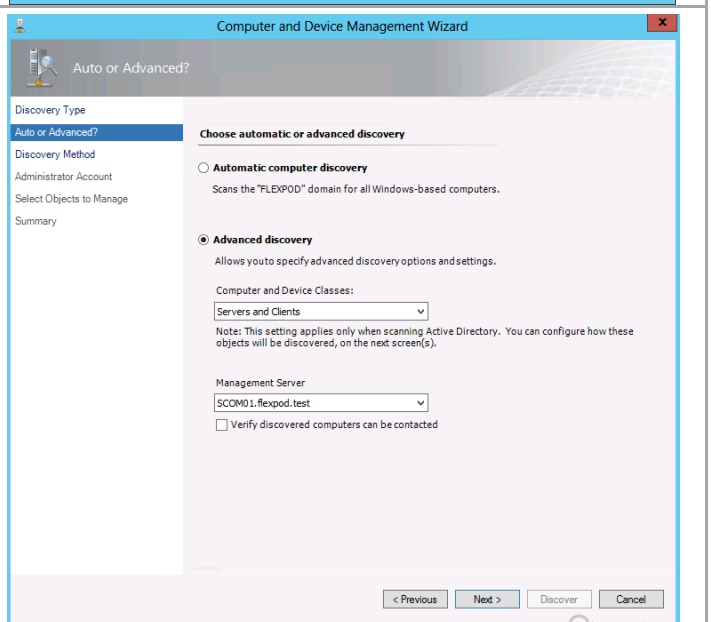
In **Operations Manager** console, navigate to the **Administration** workspace. Under **Actions**, select **Configure computers and devices to manage**.



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.



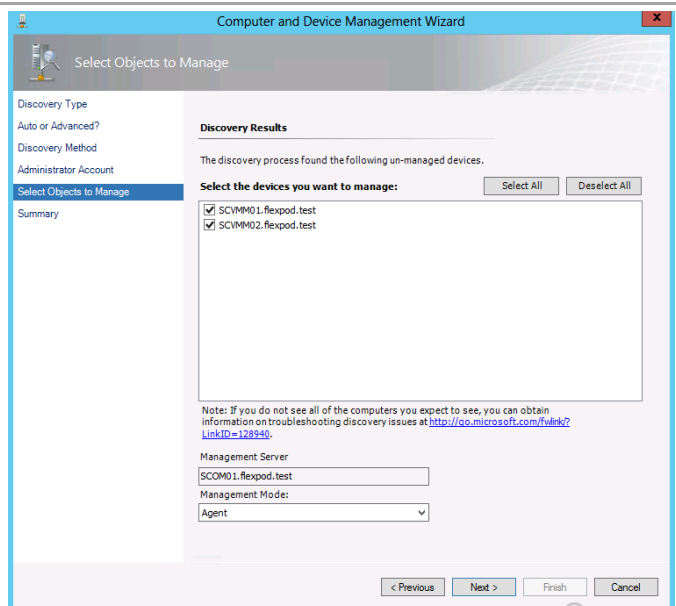
In the **Discovery Method** dialog box, under **Browse for, or type-in computer names**, input the names of both VMM servers. Click **Next** to continue.

The screenshot shows the 'Discovery Method' dialog box within the 'Computer and Device Management Wizard'. The left sidebar contains a list of steps: 'Discovery Type', 'Auto or Advanced?', 'Discovery Method' (which is highlighted), 'Administrator Account', 'Select Objects to Manage', and 'Summary'. The main area is titled 'How do you want to discover computers?'. It has two radio button options: 'Scan Active Directory' and 'Browse for, or type-in computer names'. The 'Browse for, or type-in computer names' option is selected. Below this, there is a text box containing 'SCVMM01.flexpod.test' and 'SCVMM02.flexpod.test'. To the right of this text box is a 'Browse...' button. At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Discover', and 'Cancel'.

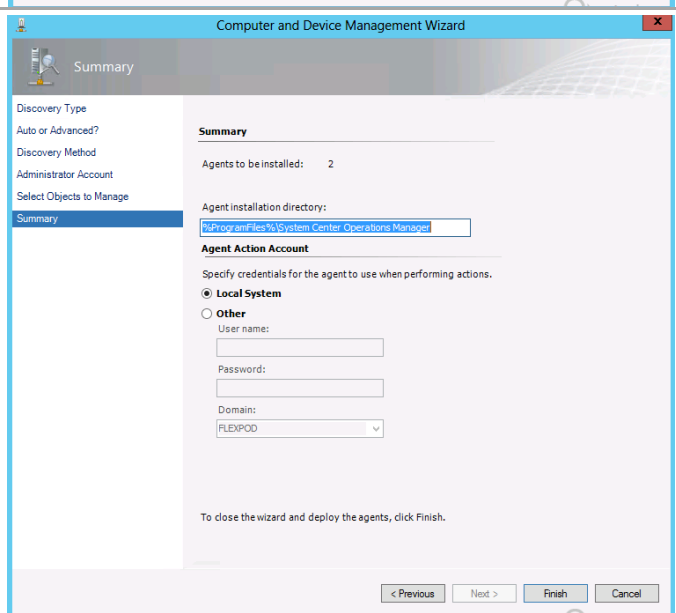
In the **Administrator Account** dialog, select the **Other user account** option and provide the credentials required to access Active Directory and perform discovery in your environment. Verify that the **This is a local computer account, not a domain account** check box is clear and click **Discover** to continue.

The screenshot shows the 'Administrator Account' dialog box within the 'Computer and Device Management Wizard'. The left sidebar contains a list of steps: 'Discovery Type', 'Auto or Advanced?', 'Discovery Method', 'Administrator Account' (which is highlighted), 'Select Objects to Manage', and 'Summary'. The main area is titled 'Administrator Account'. It contains a text box for 'Select a user account with Administrator rights on the computers you will scan. These credentials will also be used when installing the agents on managed computers.' Below this, there are two radio button options: 'Use selected Management Server Action Account' and 'Other user account'. The 'Other user account' option is selected. Below this, there are three text boxes: 'User name:', 'Password:', and 'Domain:'. The 'Domain:' dropdown menu is set to 'FLEXPOD'. At the bottom, there is a checkbox labeled 'This is a local computer account, not a domain account', which is currently unchecked. Below the checkbox, there is a note: 'Note: When selecting the local account option, the agent installation task will be run as the local account, while the Discovery task will be run using the Management Server Action Account.' At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Discover', and 'Cancel'.

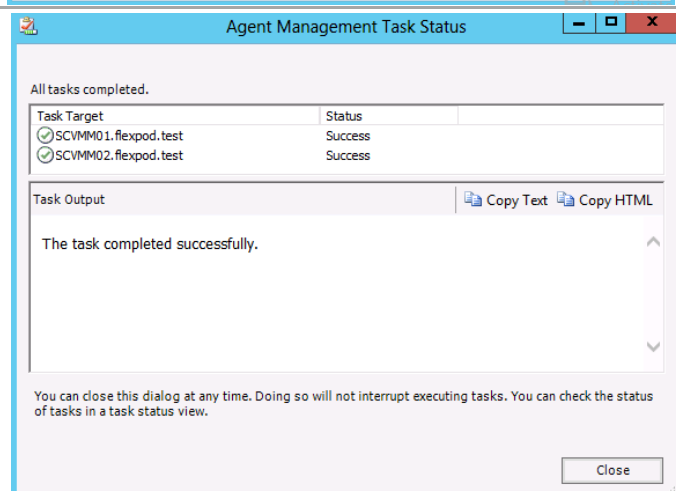
In the **Select Objects to Manage** dialog, review the Discovery Results and select the VMM server. From the **Management Mode** drop-down menu, select **Agent** and click **Next** to continue.

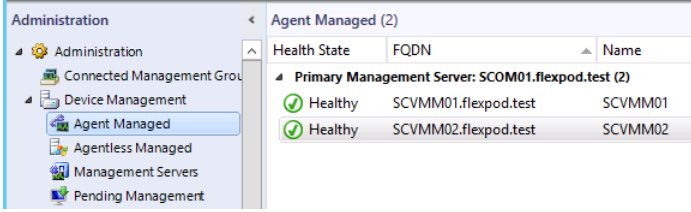
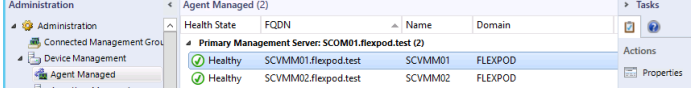
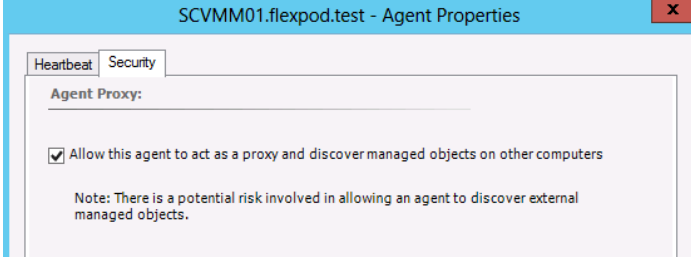


In the **Summary** dialog, accept the default **Agent installation directory** as `%ProgramFiles%\System Center Operations Manager`. In the **Agent Action Account** section, select the **Local System** option. Once complete, click **Finish** to perform the agent installation.



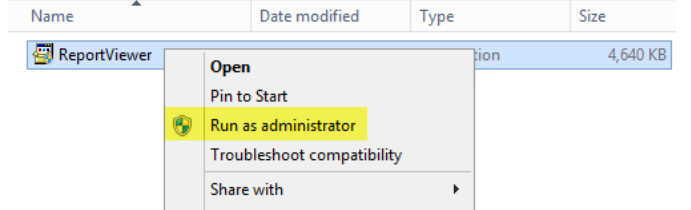
In the **Agent Management Task Status** dialog, verify that the agent installation completes successfully. Once successful, click **Close** to complete the operation.



<p>The next step is to enable the Operations Manager agent deployed to the Virtual Machine Manager management server to be a proxy agent.</p> <p>In Operations Manager console, navigate to the Administration workspace, expand the Device Management node and select the Agent Managed view.</p> <p><i>Note: It can take a few minutes for the Health State to transition from Not Monitored to Healthy.</i></p>	
<p>In the Agent Managed pane, select the agent associated with the VMM Management Server and click Properties in the task pane.</p>	
<p>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 checkbox is selected then click OK to save the changes.</p>	

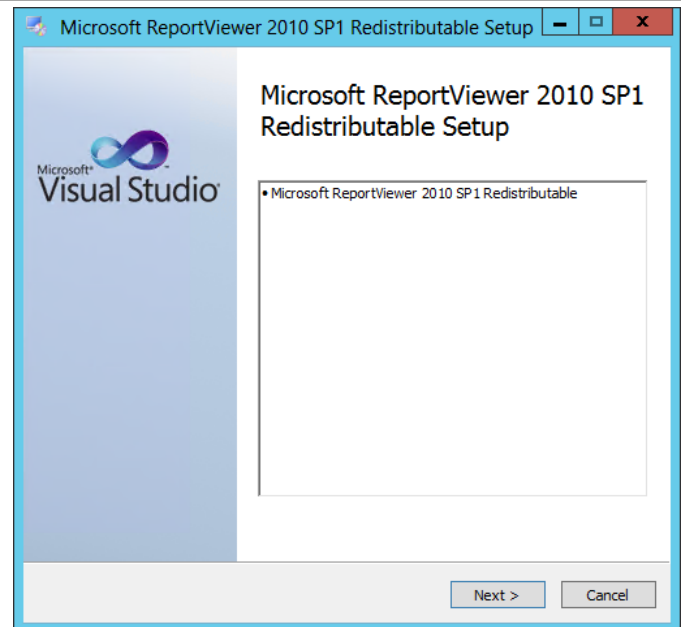
Install Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.¹⁵ Follow the provided steps to install the Microsoft Report Viewer 2010 SP1 package.

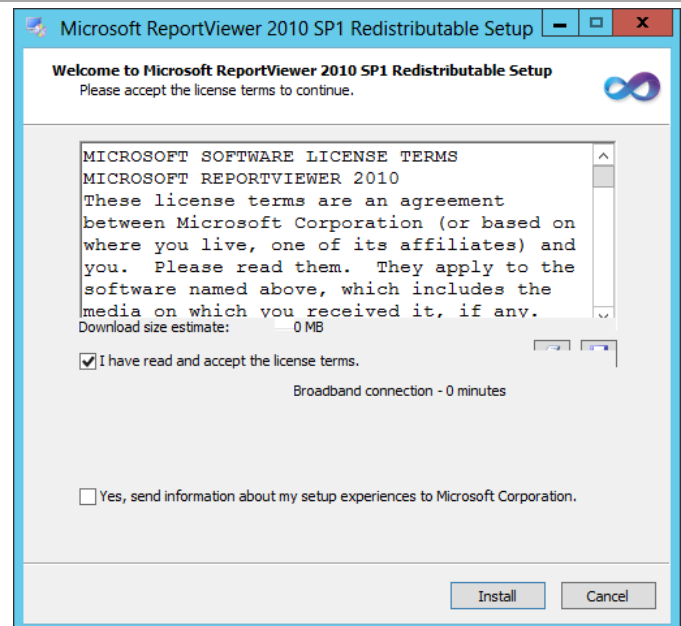
<p>► Perform the following steps on <u>each</u> Virtual Machine Manager virtual machine.</p>	
<p>From the installation media source, right-click ReportViewer.exe and select Run as administrator from the context menu to begin setup.</p>	

¹⁵ Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&amp;displaylang=r&displaylang=en>.

Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.



Select the **I have read and accept the license terms** check box and click **Install**.



The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.



Install Operations Manager Console on the Virtual Machine Manager Management Server

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

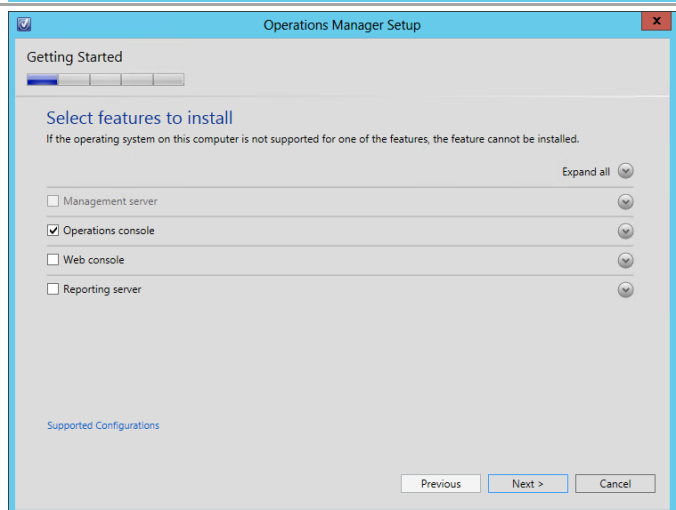
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

Name	Date modified	Type	Size
acs	11/23/2012 3:04 AM	File folder	
agent	11/23/2012 3:04 AM	File folder	
gateway	11/23/2012 3:04 AM	File folder	
HelperObjects	11/23/2012 3:04 AM	File folder	
Licenses	11/23/2012 3:04 AM	File folder	
ManagementPacks	11/23/2012 3:05 AM	File folder	
msxml	11/23/2012 3:05 AM	File folder	
ProductDocumentation	11/23/2012 3:05 AM	File folder	
ReportModels	11/23/2012 3:05 AM	File folder	
SCXACS	11/23/2012 3:05 AM	File folder	
Setup	11/23/2012 3:05 AM	File folder	
SupportTools	11/23/2012 3:05 AM	File folder	
autorun	10/16/2012 8:01 PM	Setup Information	1 KB
Setup	11/23/2012 3:05 PM	Application	1,571 KB

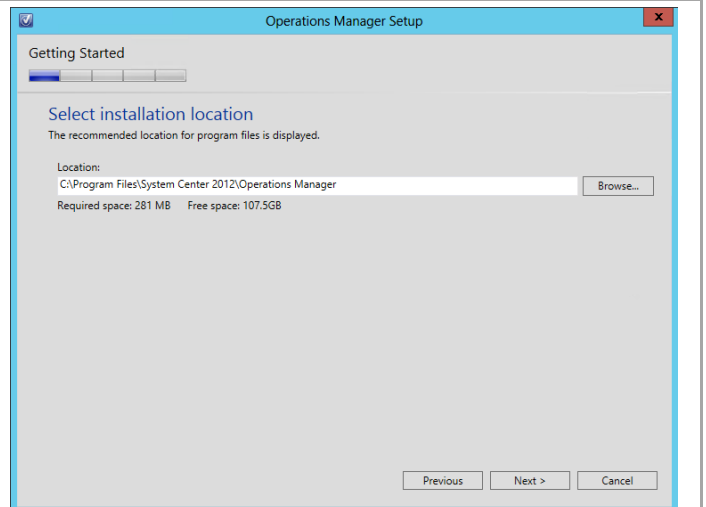
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



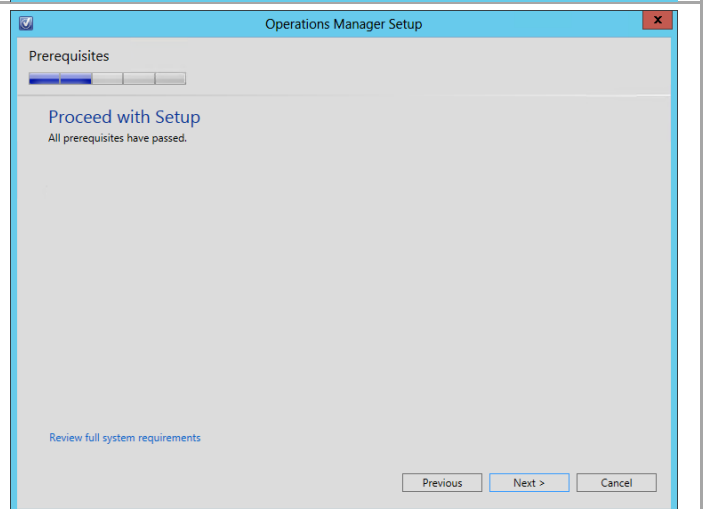
In the **Select features to install** dialog, verify that the **Operations console** checkbox is selected. Click **Next** to continue.



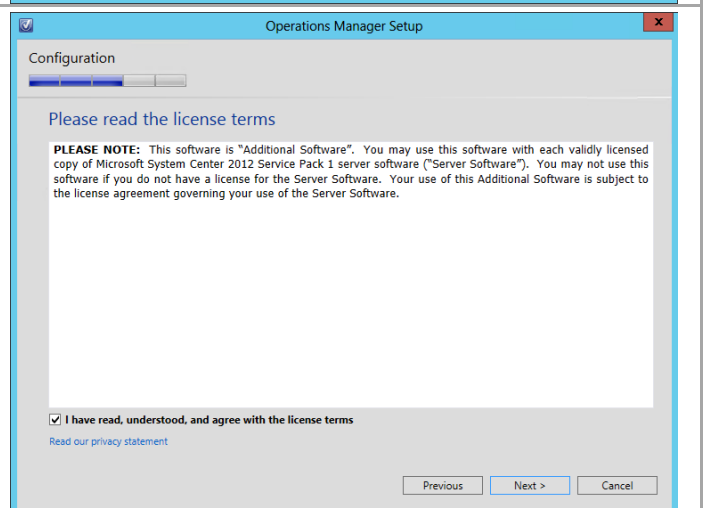
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.



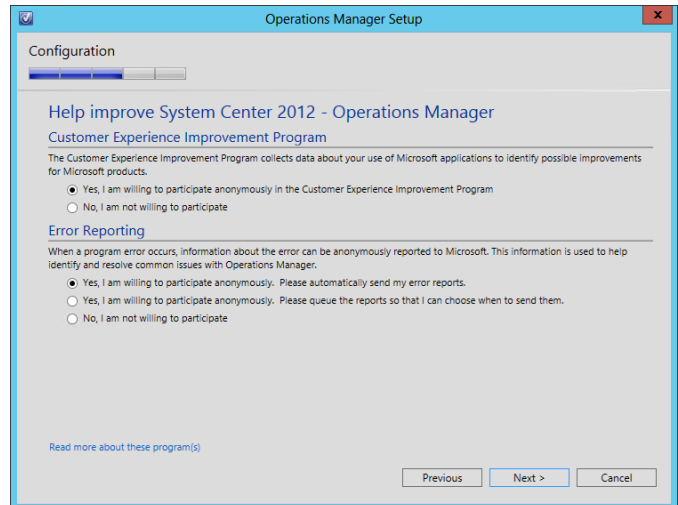
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the license terms** installation option check box is selected and click **Next** to continue.



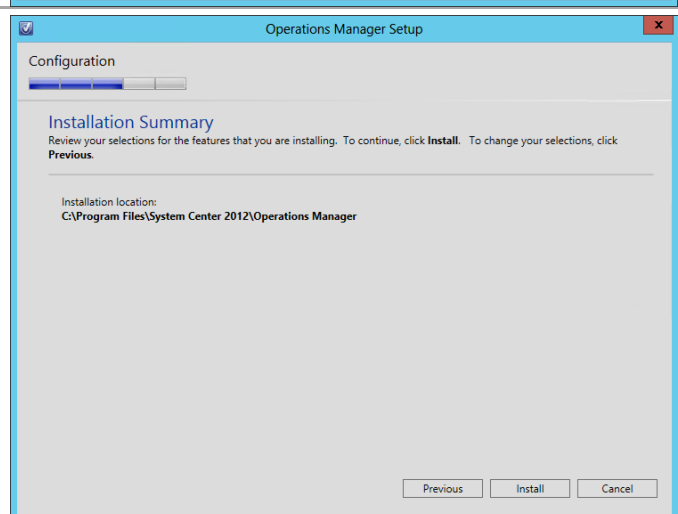
The **Help Improve System Center 2012 – Operations Manager** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program.**
- **Error Reporting.**

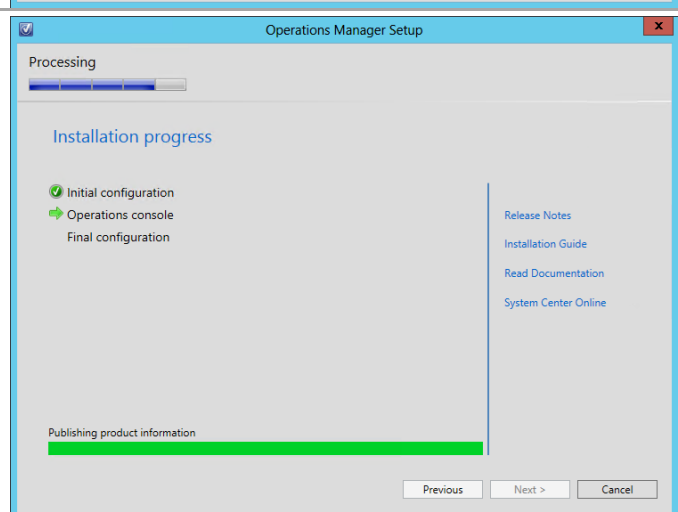
Select the appropriate option based on your organization's policies and click **Next** to continue.



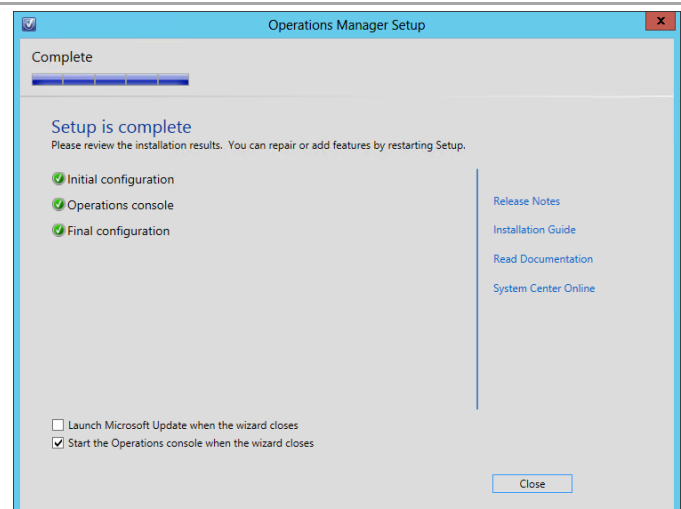
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



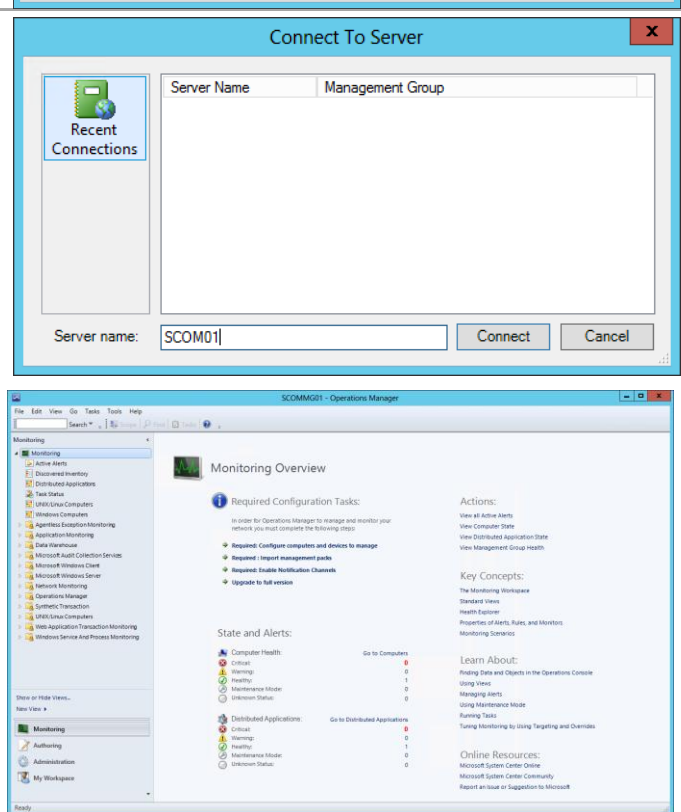
The wizard will display the progress while performing the installation.



Once 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.



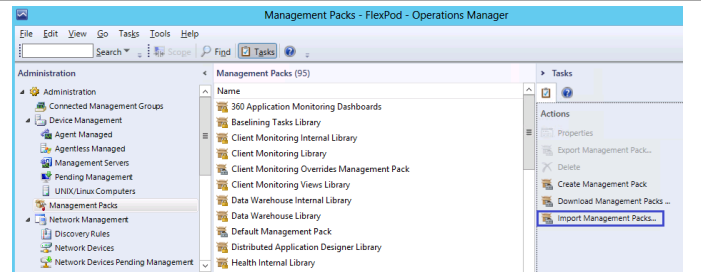
Once completed, the **Operations Manager console** will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



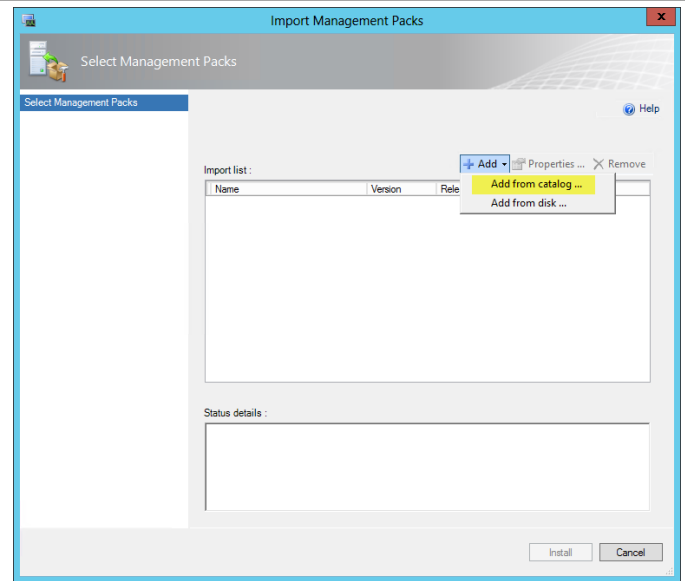
Download and Import the Required Prerequisite Management Packs in Operations Manager

► 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...**



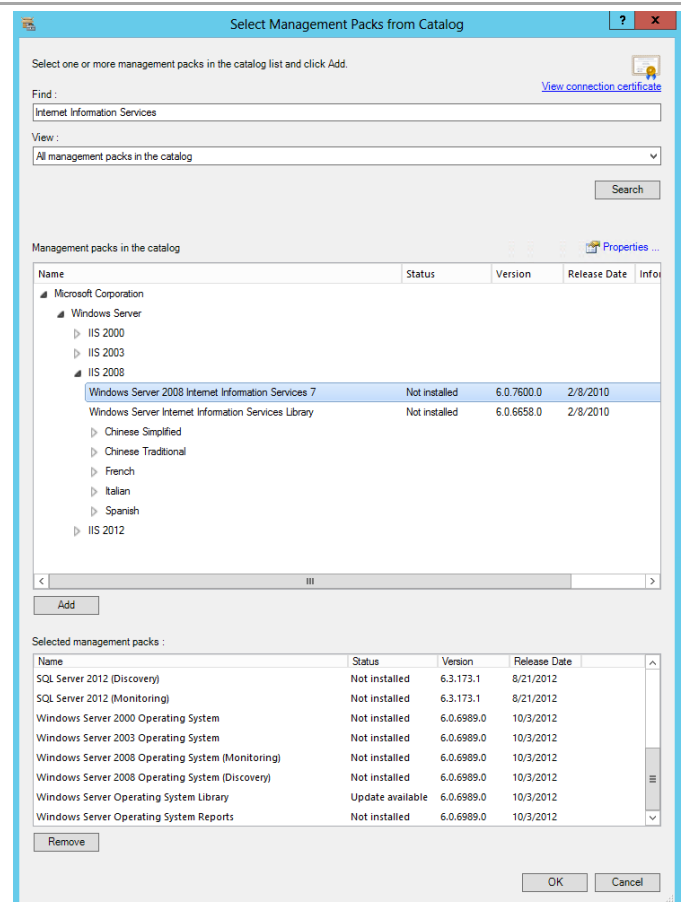
In the **Select Management Packs** dialog, click the **Add** button and select **Add from catalog...** in the drop-down menu.



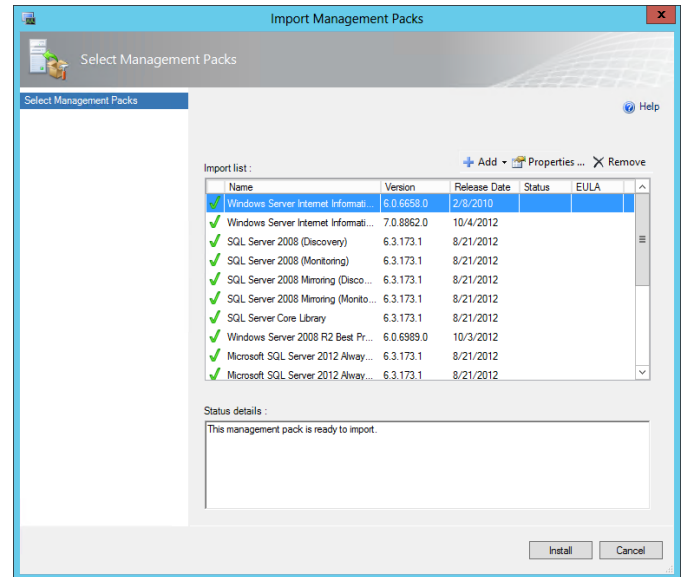
In the **Select Management Packs from Catalog** dialog, find and add the following management packs:

- Windows Server Internet Information Services Library Version 6.0.6658.0
- Windows Server Internet Information Services Library Version 7.0.8862.0
- Windows Server Internet Information Services 2000 Version 6.0.6658.0
- Windows Server Internet Information Services 2003 Version 6.0.6658.0
- Windows Server 2008 Internet Information Services 7 Version 6.0.6658.0
- SQL Server 2008 (Discovery) version 6.3.173.1
- SQL Server 2008 (Monitoring) version 6.3.173.1
- SQL Server 2008 Mirroring (Discovery) version 6.3.173.1
- SQL Server 2008 Mirroring (Monitoring) version 6.3.173.1
- SQL Server Core Library version 6.3.173.1
- SQL Server 2012 (Discovery) version 6.3.173.1
- SQL Server 2012 (Monitoring) version 6.3.173.1
- Windows Server 2008 R2 Best Practice Analyzer Monitoring version 6.0.6989.0
- Windows Server 2000 Operating System version 6.0.6989.0
- Windows Server 2003 Operating System version 6.0.6989.0
- Windows Server 2008 Operating System (Discovery) version 6.0.6989.0
- Windows Server 2008 Operating System (Monitoring) version 6.0.6989.0
- Windows Server Operating System Library version 6.0.6989.0
- Windows Server Operating System Reports version 6.0.6989.0
- Windows Server 2012 Operating System (Discovery) version 6.0.6989.0
- Windows Server 2012 Operating System (Monitoring) version 6.0.6989.0

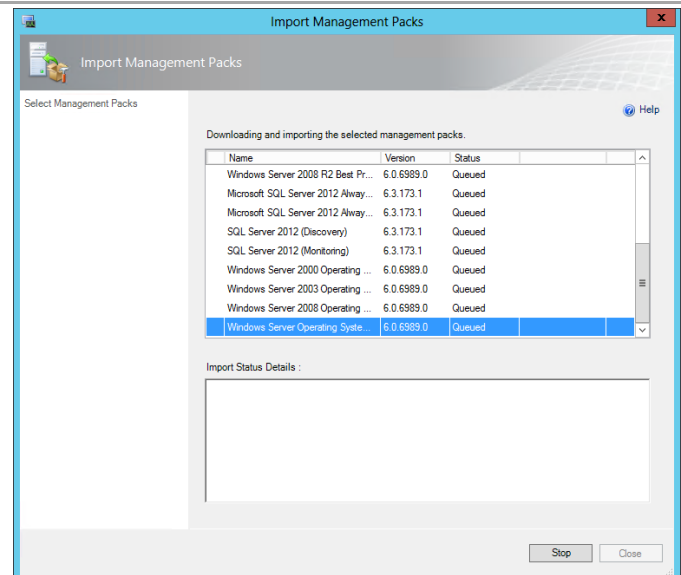
Once added, click **OK** to continue.



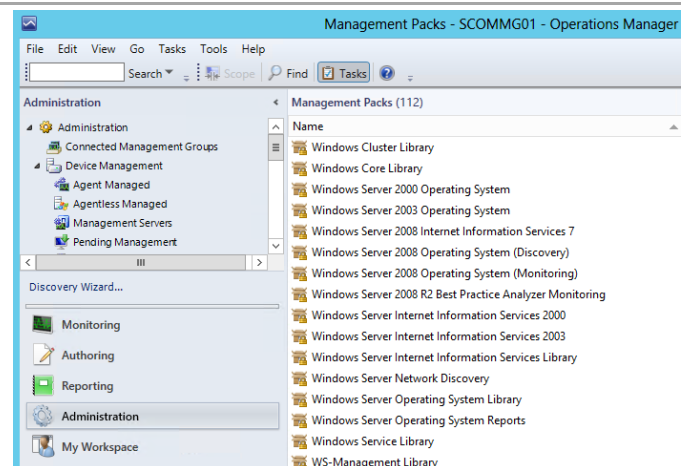
At the **Select Management Packs** dialog, click **Install** to import the selected management packs.



The management packs will download and import into Operations Manager. Once complete, verify that the imports were successful and click **Close** to exit the Import Management Packs wizard.



In the **Operations Manager** console, go to the **Administration** workspace and verify the previously selected management packs are now installed.



Install SQL Analysis Management Objects

For full functionality of Virtual Machine Manager 2012 SP1 integration with Operations Manager 2012 SP1, SQL Server 2008 R2 SP1 AMO and SQL Server 2012 SP1 AMO must be installed on all VMM management servers.

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

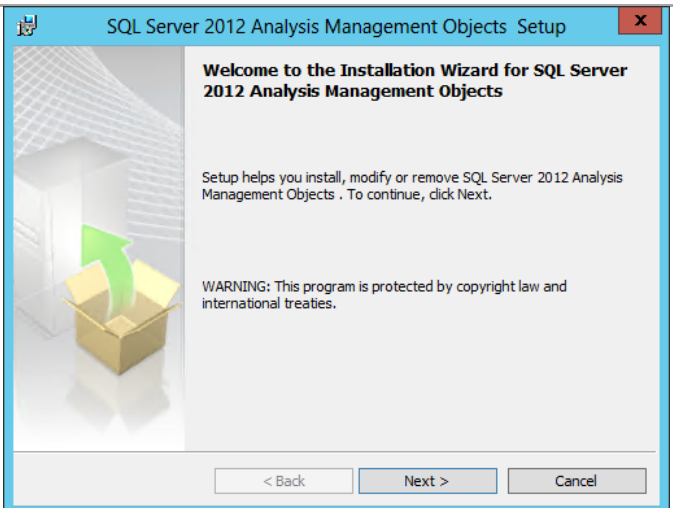
From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.

Note: The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI**, can be downloaded from

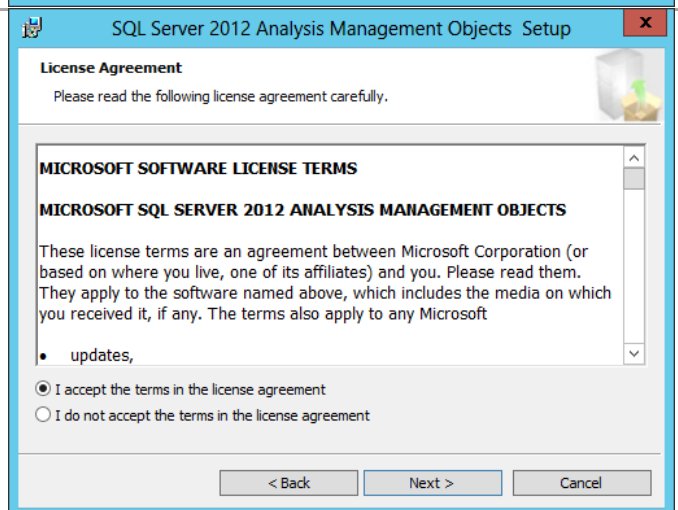
<http://www.microsoft.com/en-us/download/details.aspx?id=35580>.

Name	Date modified	Type	Size
SQL_AS_AMO	3/7/2013 11:04 AM	Windows Installer Package	3,604 KB

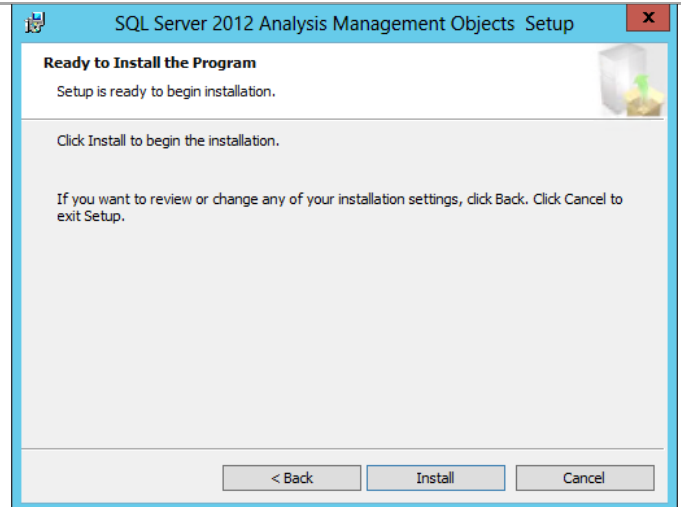
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



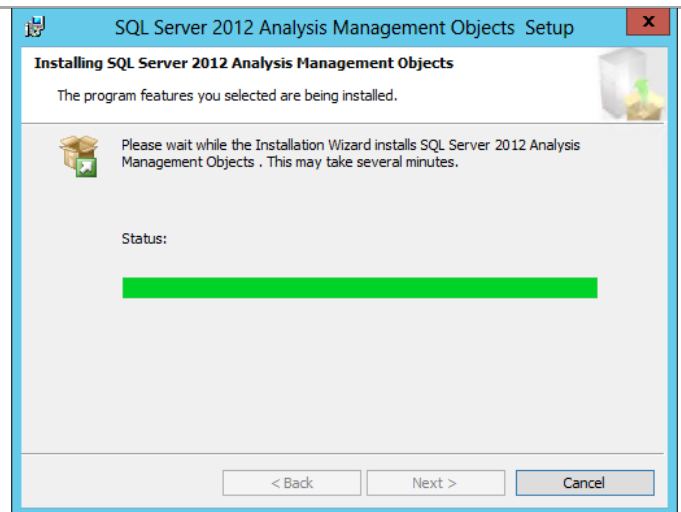
In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.



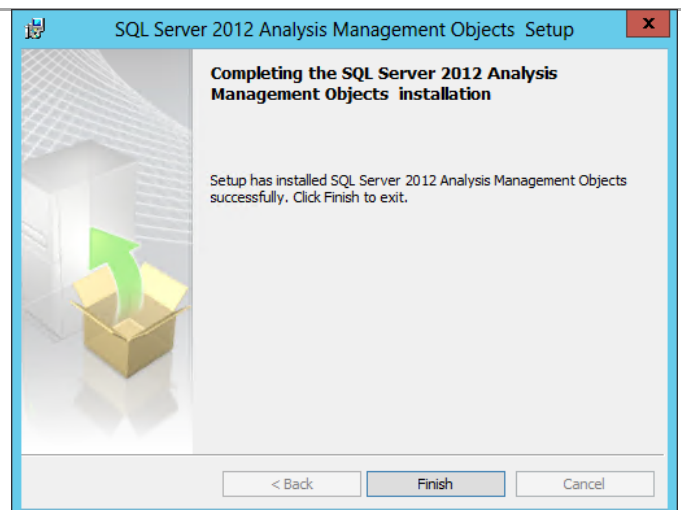
In the **Ready to Install the Program** dialog, click **Install** to begin the installation.




The installation process may take several minutes to complete. The progress is displayed on the status dialog.



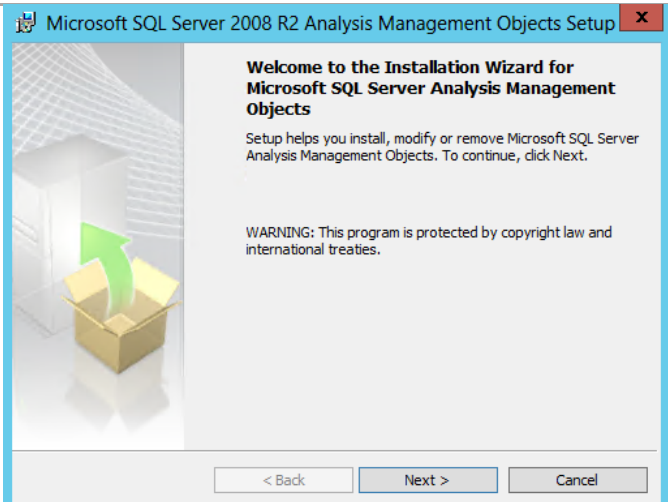
In the **Completing the SQL Server 2012 Analysis Management Objects installation** dialog, click **Finish** to exit the installation.



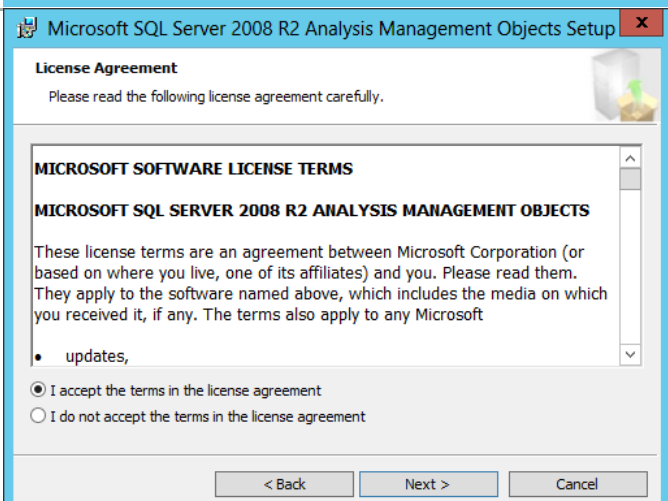
The SQL Server 2008 R2 SP1 Analysis Management Objects package must be installed as well to allow for the integration wizard to complete. From the **SQL Server 2008 R2 SP1 Analysis Management Objects** installation media source, double-click **SQLSERVER2008_ASAMO10.MSI** to begin setup. **Note:** The SQL Server 2008 R2 SP1 Analysis Management Objects installer, **1033\x64\SQLSERVER2008_ASAMO10.msi**, can be downloaded from <http://www.microsoft.com/download/en/details.aspx?id=26728>.

Name	Date modified	Type	Size
 SQLSERVER2008_ASAMO10	3/7/2013 11:06 AM	Windows Installer ...	4,650 KB

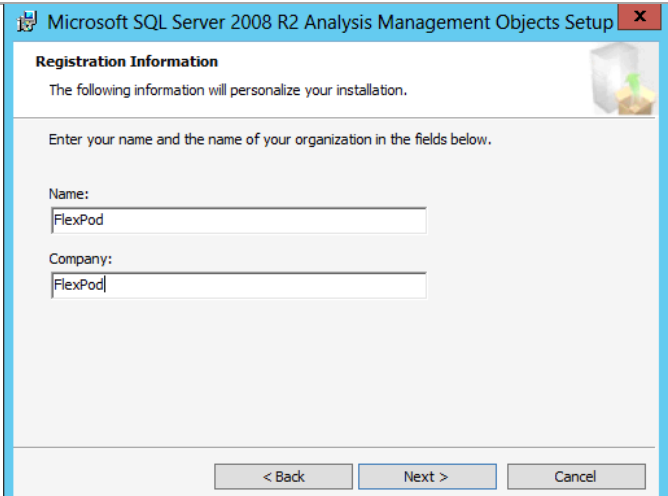
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



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 **Registration Information** dialog, provide values in the **Name** and **Company** textboxes and then click **Next** to continue.



Microsoft SQL Server 2008 R2 Analysis Management Objects Setup

Registration Information

The following information will personalize your installation.

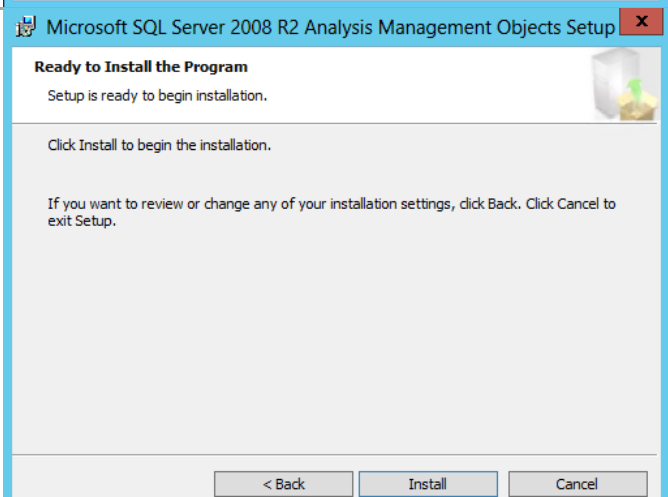
Enter your name and the name of your organization in the fields below.

Name:
FlexPod

Company:
FlexPod

< Back Next > Cancel

On the **Ready to Install the Program** screen, click **Install** to begin the installation.



Microsoft SQL Server 2008 R2 Analysis Management Objects Setup

Ready to Install the Program

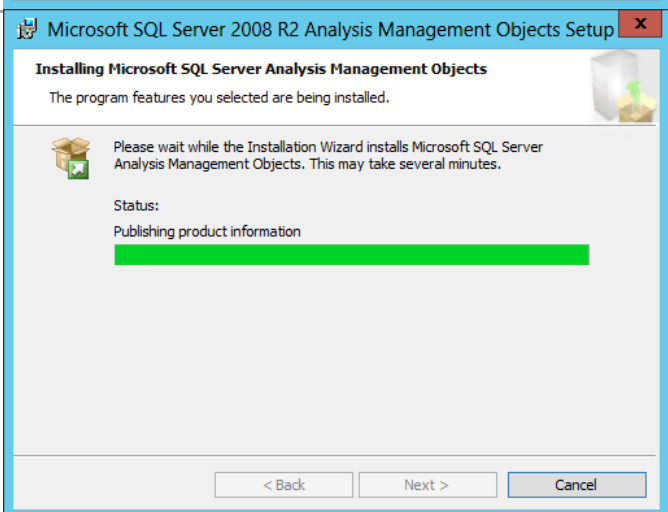
Setup is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit Setup.

< Back Install Cancel

The installation process may take several minutes to complete. The progress is displayed on the **Status** screen.



Microsoft SQL Server 2008 R2 Analysis Management Objects Setup

Installing Microsoft SQL Server Analysis Management Objects

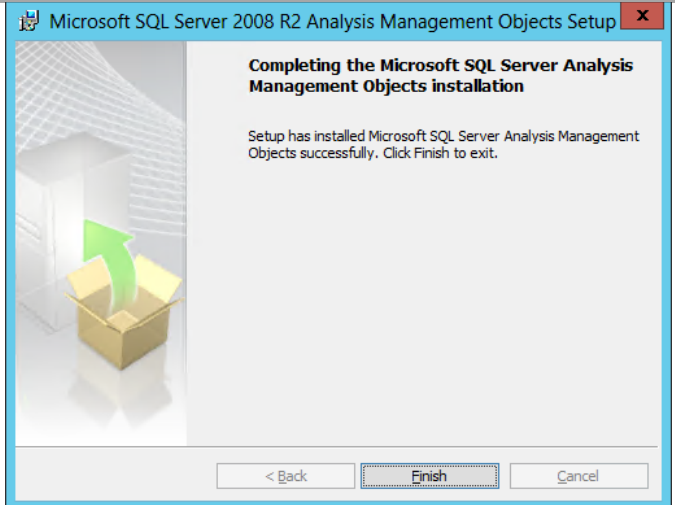
The program features you selected are being installed.

Please wait while the Installation Wizard installs Microsoft SQL Server Analysis Management Objects. This may take several minutes.

Status:
Publishing product information

< Back Next > Cancel

On the **Completing the SQL Server 2008 Analysis Management Objects** installation screen, click **Finish** to exit the installation.

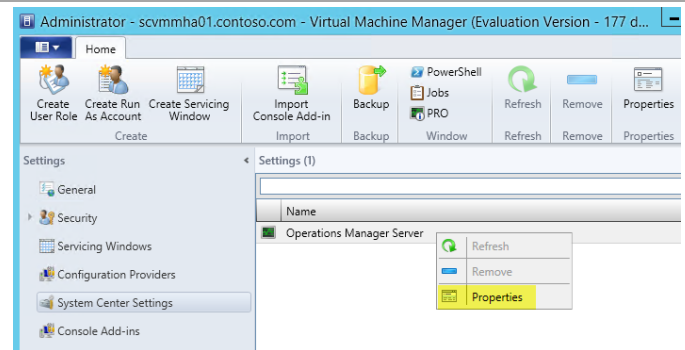


Perform Virtual Machine Manager and Operations Manager Integration

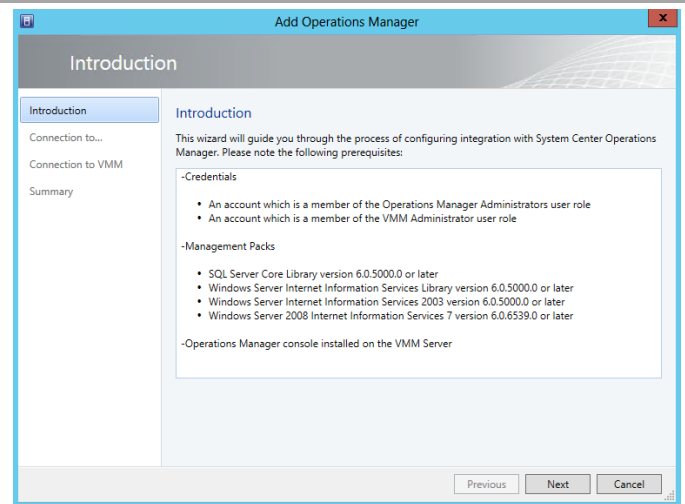
When all pre-requisite configurations and installations are performed, the integration of Virtual Machine Manager and Operations Manager can be completed.

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

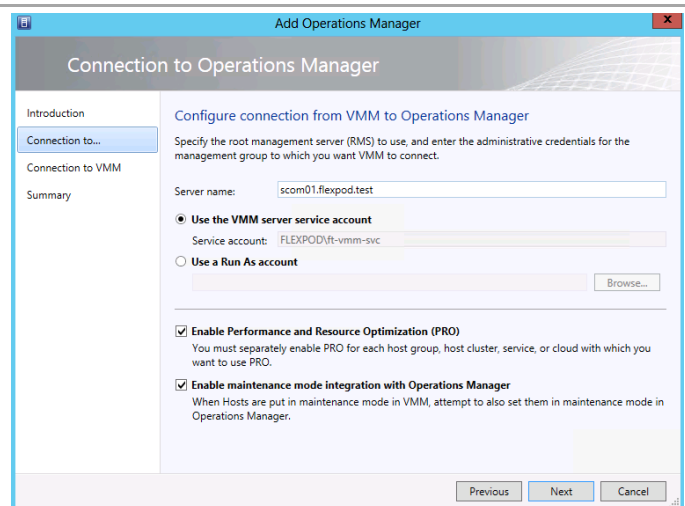
In the **Virtual Machine Manager** console, navigate to **Settings** pane and select **System Center Settings**, right-click **Operations Manager Server** and select **Properties** from the context menu.



The **Add Operations Manager** dialog will appear. In the **Introduction** dialog, verify the prerequisites have been met and click **Next** to continue.



In the **Connection to Operations Manager** dialog type the FQDN of the Operations Manager server in the **Server name** text box. Select the **Use the VMM server service account** option. Select the **Enable Performance and Resource Optimization (PRO)** and **Enable maintenance mode integration with Operations Manager** check boxes. Once 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.

The screenshot shows the 'Add Operations Manager' dialog box with the 'Connection to VMM' tab selected. The 'Introduction' pane on the left lists 'Connection to...', 'Connection to VMM', and 'Summary'. The main area is titled 'Configure connection from Operations Manager to VMM' and contains instructions: 'Specify credentials for Operations Manager to use to connect to the VMM server. The account will be assigned Administrator rights on the VMM server.' Below this, there are two text boxes: 'User name' with the value 'FlexPod\FT-VMM-SVC' and an example 'contoso\domainuser', and 'Password' with masked characters. At the bottom right are 'Previous', 'Next', and 'Cancel' buttons.

In the **Summary** dialog, verify the options selected click **Finish** to begin the Operations Manager integration process.

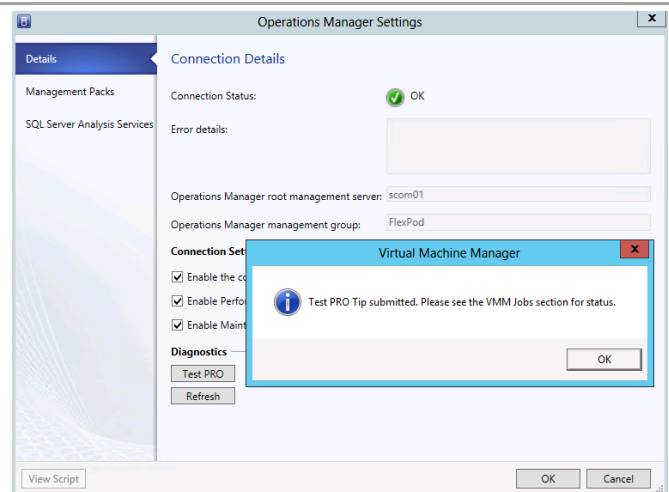
The screenshot shows the 'Add Operations Manager' dialog box with the 'Summary' tab selected. The 'Introduction' pane on the left lists 'Introduction', 'Connection to...', 'Connection to VMM', and 'Summary'. The main area is titled 'Confirm the settings' and contains a list of configuration details: 'RMS name: scom01.flexpod.test', 'Operations Manager credentials: FLEXPOD\ft-vmm-svc', 'VMM credentials: flexpod\ft-vmm-svc', 'Enable PRO: Yes', and 'Maintenance mode integration: Yes'. A 'View Script' button is in the top right. At the bottom right are 'Previous', 'Finish', and 'Cancel' buttons.

The **Jobs** pane will appear. Before moving forward, wait for the job to complete successfully.

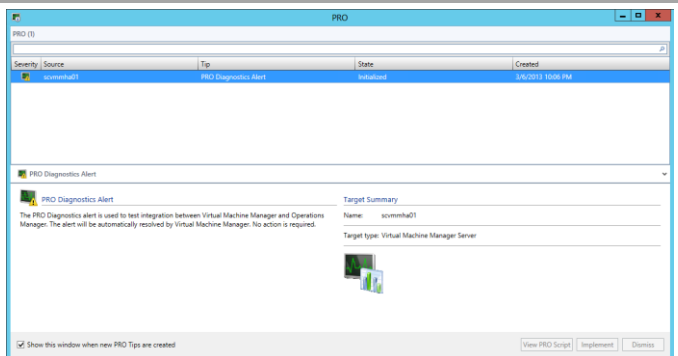
The screenshot shows the 'Jobs' pane with a table of recent jobs. The table has columns for Name, Status, Start Time, Result Name, and Owner. A single job is listed with a status of 'Completed'.

Name	Status	Start Time	Result Name	Owner
New Operations Ma...	Completed	5/22/2013 10:56:58...	scom01.flexpod.test	FLEXPOD\Administr...

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.



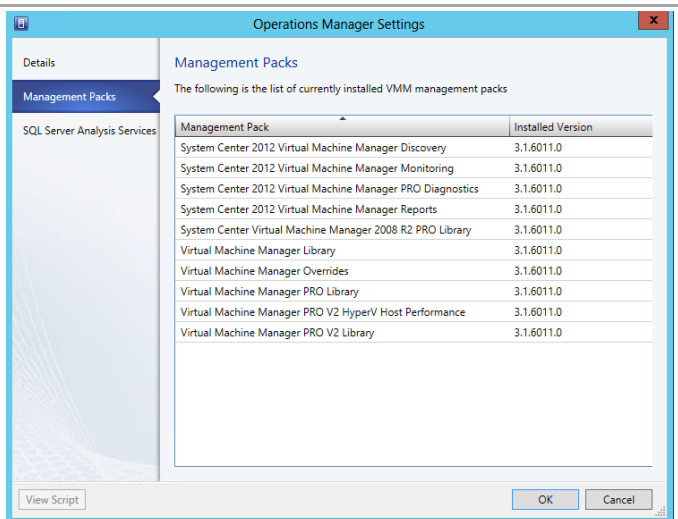
As part of the test, PRO will generate a diagnostics alert.



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	
✓ PRO diagnostics	Completed	3/6/2013 10:06:58 PM	PRO Diagnostics Alert	
✓ Set state of a PRO tip	Completed	3/6/2013 10:06:00 PM	PRO Diagnostics Alert	
✓ Set state of a PRO tip	Completed	3/6/2013 10:05:59 PM	PRO Diagnostics Alert	
✓ PRO diagnostics	Completed	3/6/2013 10:05:32 PM	PRO Diagnostics Alert	
✓ New Operations Manager connec...	Completed	3/6/2013 9:59:56 PM	SCOM01.CONTOSO.COM	
✓ PRO diagnostics				
Step	Name	Status	Start Time	End Time
✓ 1	PRO diagnostics	Completed	3/6/2013 10:06:58 PM	3/6/2013 10:08:22 PM
✓ 1.1	Create new PRO tip	Completed	3/6/2013 10:06:58 PM	3/6/2013 10:07:45 PM
✓ 1.2	Implement the fix for a PRO tip	Completed	3/6/2013 10:07:45 PM	3/6/2013 10:08:22 PM
✓ 1.2.1	Invoke remediation	Completed	3/6/2013 10:07:45 PM	3/6/2013 10:07:45 PM
✓ 1.2.2	Wait for remediation	Completed	3/6/2013 10:07:45 PM	3/6/2013 10:08:22 PM

In the **Management Packs** dialog, verify all Virtual Machine Manager Management Packs were successfully installed.

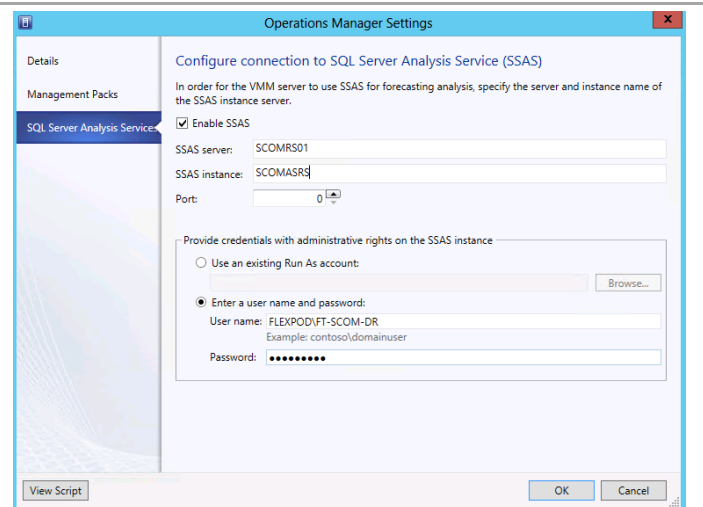


In the **Configure connection to SQL Server Analysis Services (SSAS)** dialog, provide the following information.

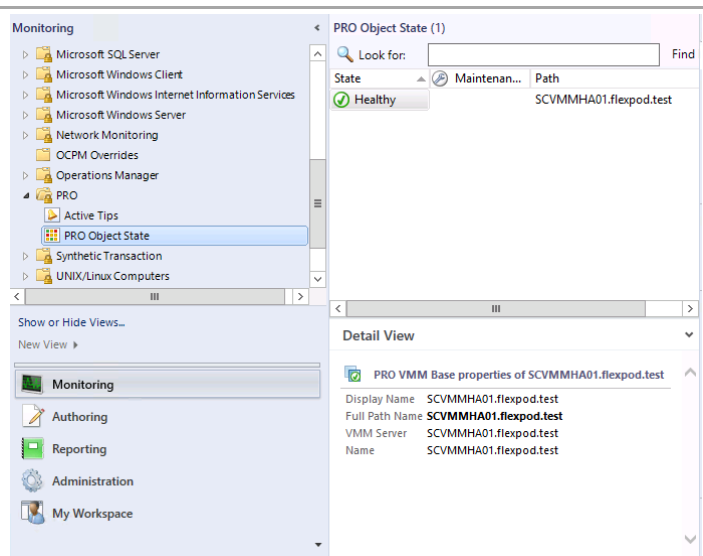
Select the **Enable SSAS** checkbox. Provide the following information on the text boxes provided:

- **SSAS server** – *Specify the Operations Manager database server instance.*
- **SSAS Instance** – *Specify the SSAS instance name created earlier.*

In the **Provide credentials with administrative rights on the SSAS instance**, select the **Enter a user name and password** option and provide the supplied credentials for the Operations Manager Data Reader account. Click **OK** to save these settings.



On the **Operations Manager** console, go to **Monitoring** workspace, navigate to the **PRO** node and select **PRO Object State**. Verify the VMM server is listed with a health state other than “*Not Monitored*.”



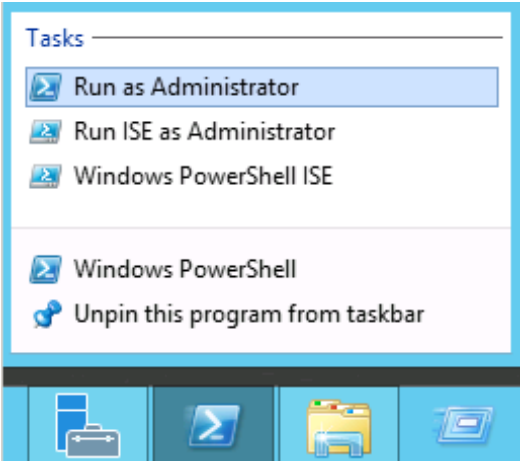
17.5 Install NetApp Management Pack

The following steps must be completed in order to install and configure the NetApp OnCommand SCOM Management Pack.

Install and configure SNMP.

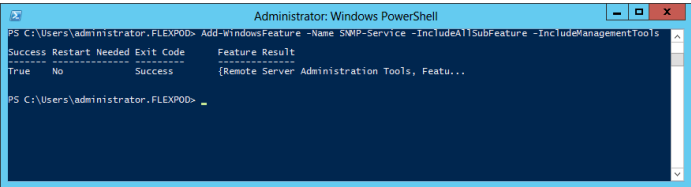
- Perform the following steps on the **Operations Manager management server** virtual machine.

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

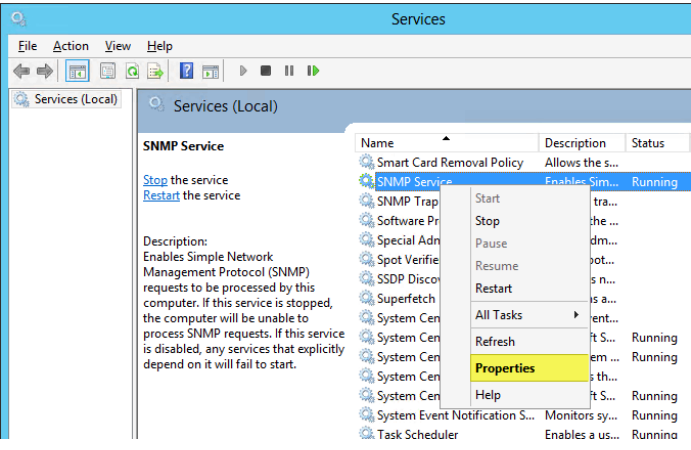


Add the SNMP feature by entering the following command:

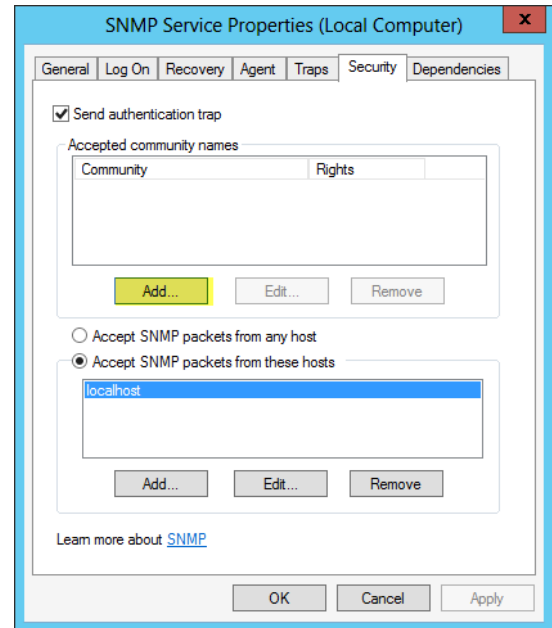
```
Add-WindowsFeature -Name SNMP-Service -IncludeAllSubFeatures -IncludeManagementTools
```



Open the Services management console, right-click **SNMP Service**, and select **Properties**

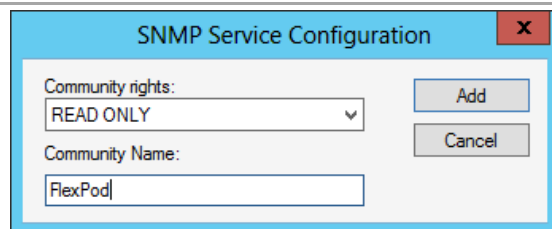


On the SNMP Service Properties page, select the **Security** tab, and under Accepted Community Names, click **Add**.



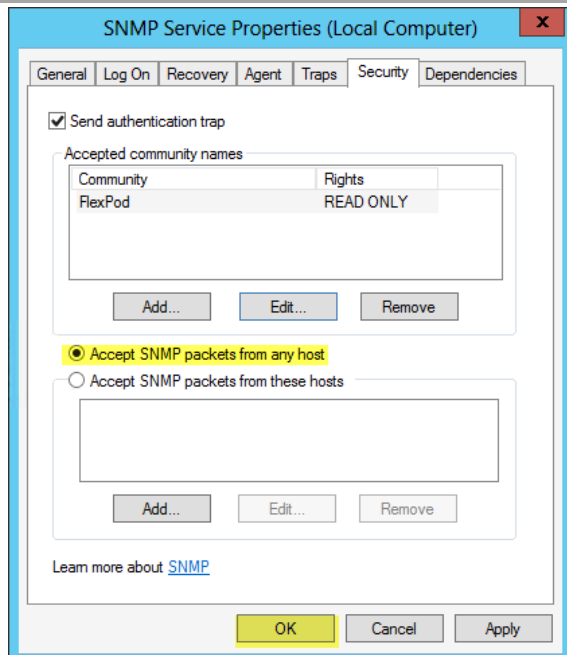
The screenshot shows the 'SNMP Service Properties (Local Computer)' dialog box with the 'Security' tab selected. The 'Send authentication trap' checkbox is checked. Under 'Accepted community names', there is a table with columns 'Community' and 'Rights'. Below the table are 'Add...', 'Edit...', and 'Remove' buttons. The 'Accept SNMP packets from these hosts' radio button is selected, and 'localhost' is listed in the host list. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

In the SNMP Service Configuration dialog box, set the following values and then click **Add**:



The screenshot shows the 'SNMP Service Configuration' dialog box. The 'Community rights:' dropdown is set to 'READ ONLY'. The 'Community Name:' text box contains 'FlexPod'. There are 'Add' and 'Cancel' buttons.

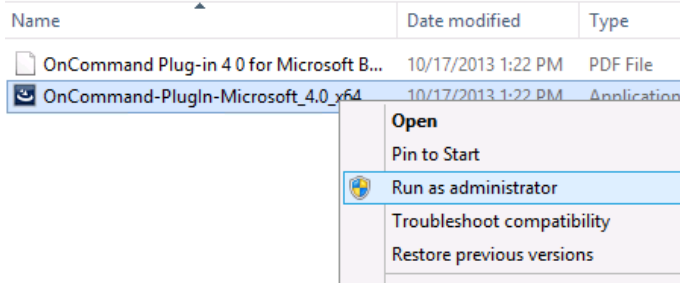
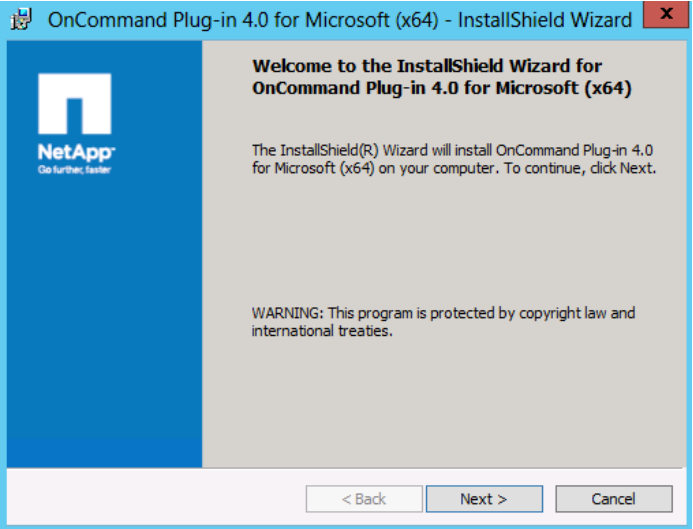
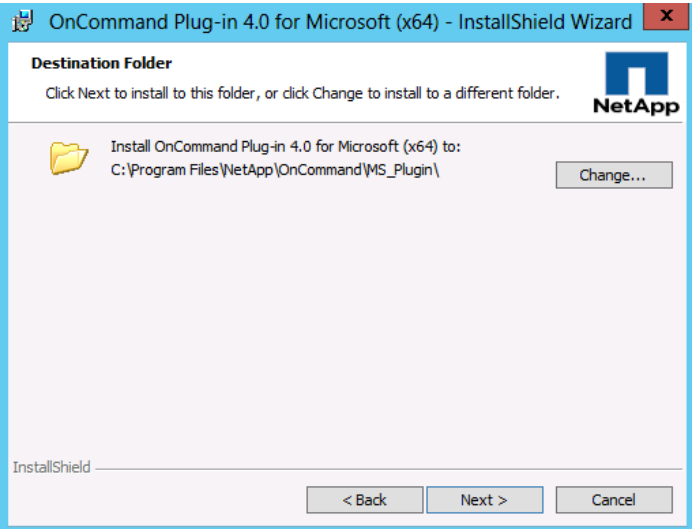
On the Security tab,, select **Accept SNMP Packets from any Host**. Click **OK** to complete the configuration.



The screenshot shows the 'SNMP Service Properties (Local Computer)' dialog box with the 'Security' tab selected. The 'Send authentication trap' checkbox is checked. Under 'Accepted community names', the table now shows 'FlexPod' with 'READ ONLY' rights. The 'Accept SNMP packets from any host' radio button is selected and highlighted in yellow. The 'Accept SNMP packets from these hosts' section is empty. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

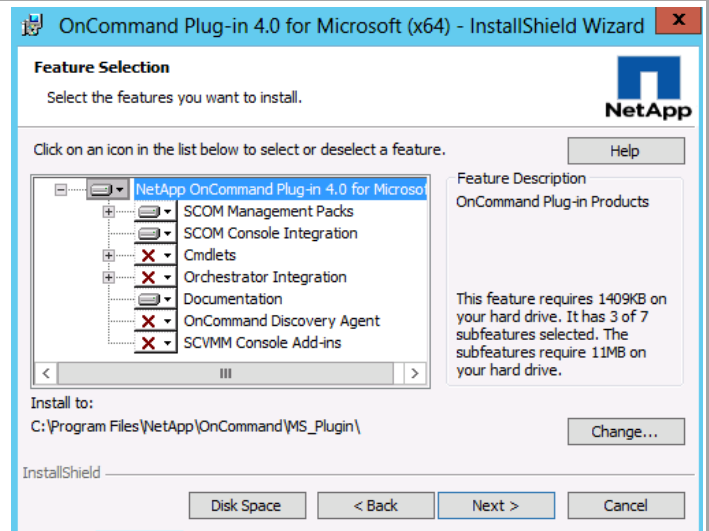
Install NetApp OnCommand Plug-IN Mangement Pack.

- Perform the following steps on the **Operations Manager management server** virtual machine.

<DOMAIN>\FT-OCPM-SVC	<p>This account will need:</p> <ul style="list-style-type: none"> • Full admin permissions on all Hyper-V hosts to be managed. • Full admin on the Operation Mangement servers.
<p>Log in to the SCO management server, right-click the OCPM 4.0 installation package, and select Run as Administrator to start the OCPM installation wizard.</p>	
<p>On the Welcome Page click Next.</p>	
<p>On the Destination Folder page, click Next to keep the default installation folder</p>	

65. On the Feature Selection page, select the following features and click Next:

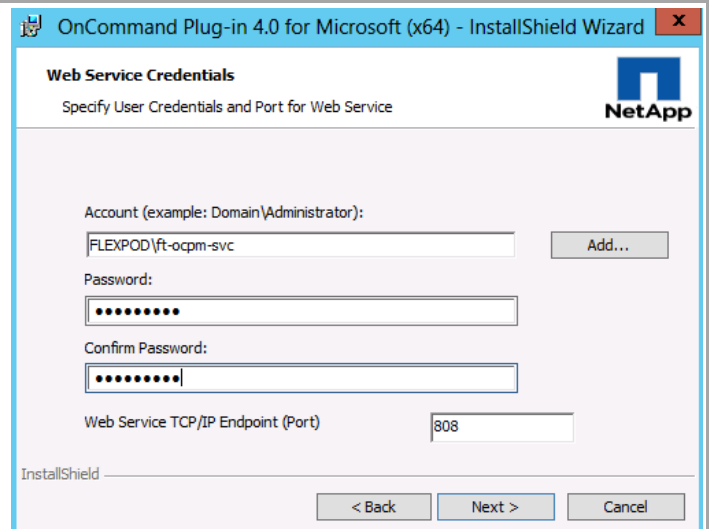
- SCOM Management Packs
- SCOM Console Integration
- Documentation



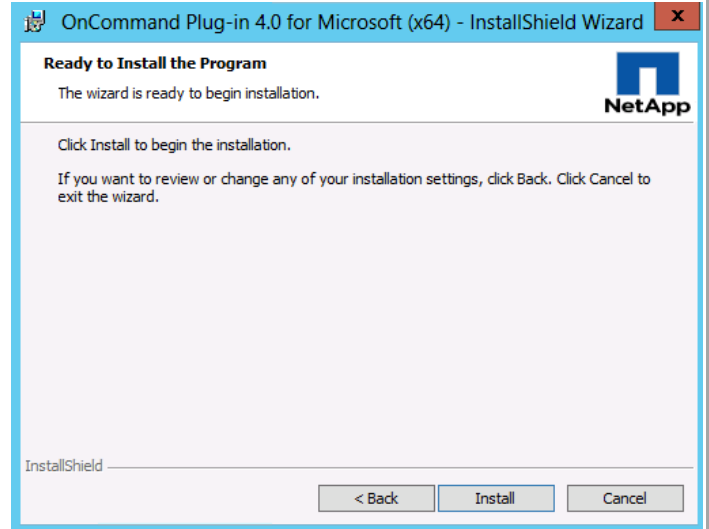
On the Web Service Credentials page, enter the following credentials and click Next:

- 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.

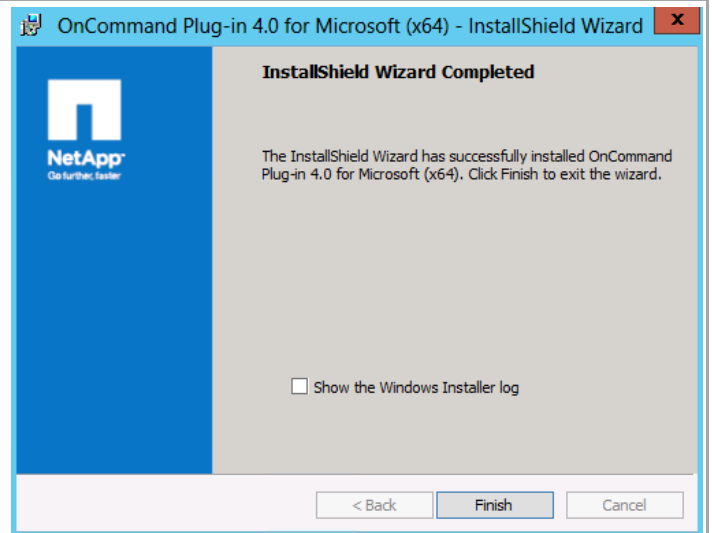


Click **Install** to continue the installation.



On the InstallShield Wizard Completed page, click **Finish** to complete the installation.

Note: It may be necessary to reboot the server to completely register the Management Pack, and it's associated tasks.

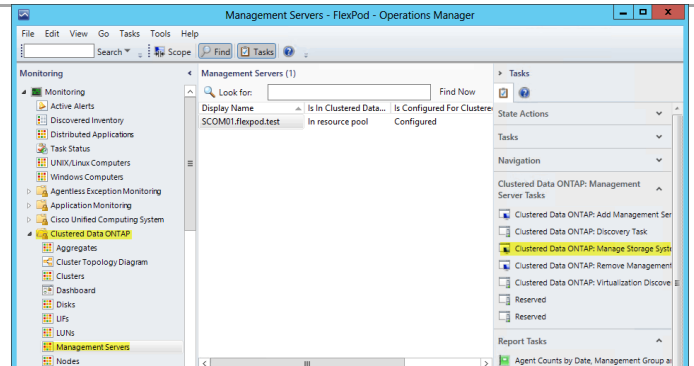


Configure NetApp OnCommand Plug-IN Mangement Pack.

► Perform the following steps on the **Operations Manager** virtual machine.

In the **Operations Manager** console, navigate to the **Monitoring** pane and select the **Clustered Data ONTAP -> ManagementServer**

On the tasks pane select **Data ONTAP Add Controller**

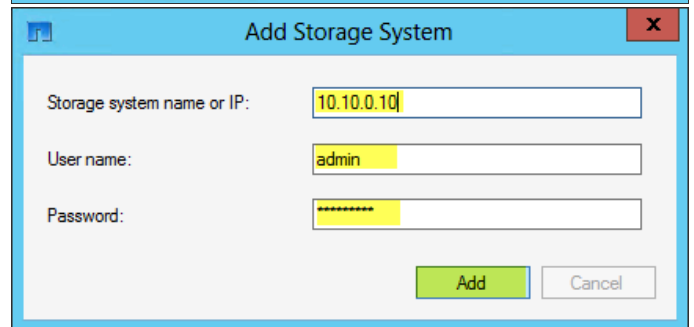
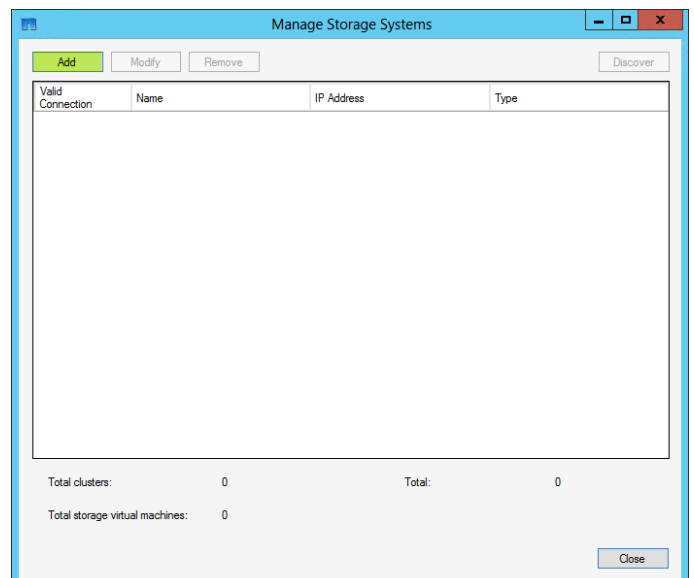


Click the **Add** button on the Manage Storage Systems.

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.



17.6 Install the Cisco UCS Management Pack

Verify the following Components are installed in the virtual machine where management pack will be installed

- Windows PowerShell 2.0
- .NET Framework 4

- Microsoft XM Core Services 6.0 (with latest Service Pack)
- System Center 2012 Operations Manager

Cisco UCS Manager Management Pack for Microsoft System Center Operations Manager can be downloaded at the following link:

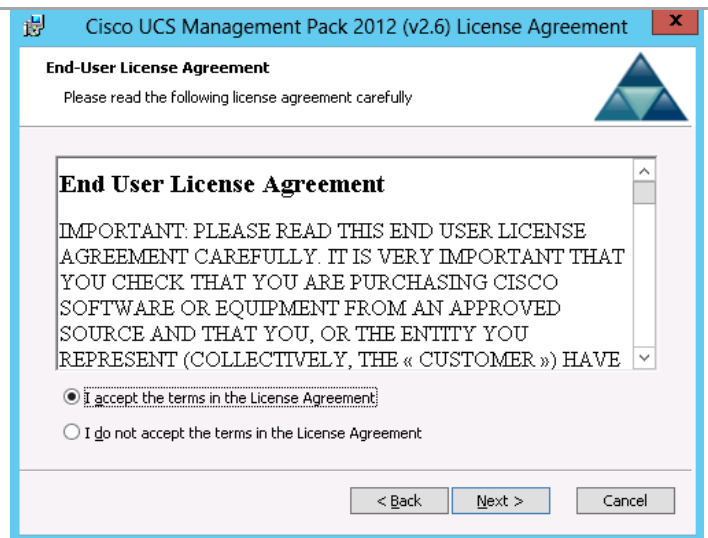
<http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=283034298&release=2.6.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

Perform the following steps on all the Operations Manager virtual machine

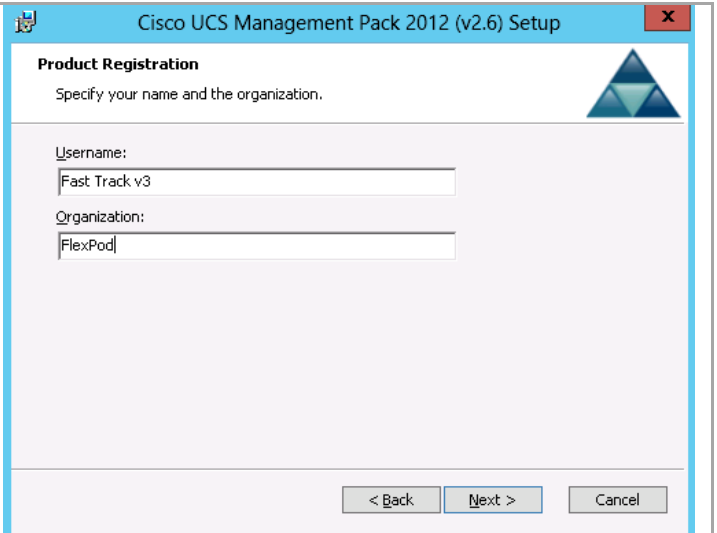
Launch the Management Pack Installer. The **Setup Wizard** screen appears.



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**.



The screenshot shows the 'Product Registration' window of the Cisco UCS Management Pack 2012 (v2.6) Setup. The window has a blue title bar and a Cisco logo in the top right. The main area is light blue with a white border. It contains two text input fields: 'Username:' with the value 'Fast Track v3' and 'Organization:' with the value 'FlexPod'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Cisco UCS Management Pack 2012 (v2.6) Setup

Product Registration

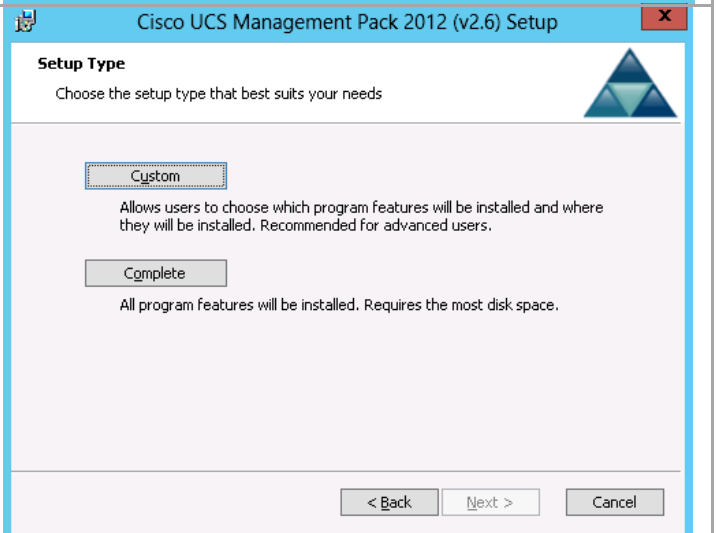
Specify your name and the organization.

Username:
Fast Track v3

Organization:
FlexPod

< Back Next > Cancel

Select the **Complete** installation option.



The screenshot shows the 'Setup Type' window of the Cisco UCS Management Pack 2012 (v2.6) Setup. The window has a blue title bar and a Cisco logo in the top right. The main area is light blue with a white border. It contains two radio button options: 'Custom' and 'Complete'. The 'Complete' option is selected. Below each option is a description. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Cisco UCS Management Pack 2012 (v2.6) Setup

Setup Type

Choose the setup type that best suits your needs

Custom

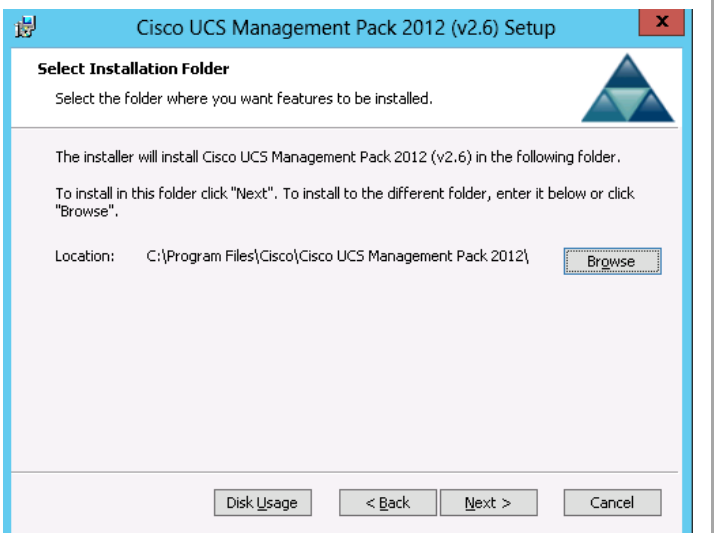
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete

All program features will be installed. Requires the most disk space.

< Back Next > Cancel

The **Select Installation Folder** Screen appears. Specify the folder location to install the Management Pack, in the **Location** field and click the **Next** button.



The screenshot shows the 'Select Installation Folder' window of the Cisco UCS Management Pack 2012 (v2.6) Setup. The window has a blue title bar and a Cisco logo in the top right. The main area is light blue with a white border. It contains a text input field for 'Location' with the value 'C:\Program Files\Cisco\Cisco UCS Management Pack 2012\'. To the right of the input field is a 'Browse' button. At the bottom, there are four buttons: 'Disk Usage', '< Back', 'Next >', and 'Cancel'.

Cisco UCS Management Pack 2012 (v2.6) Setup

Select Installation Folder

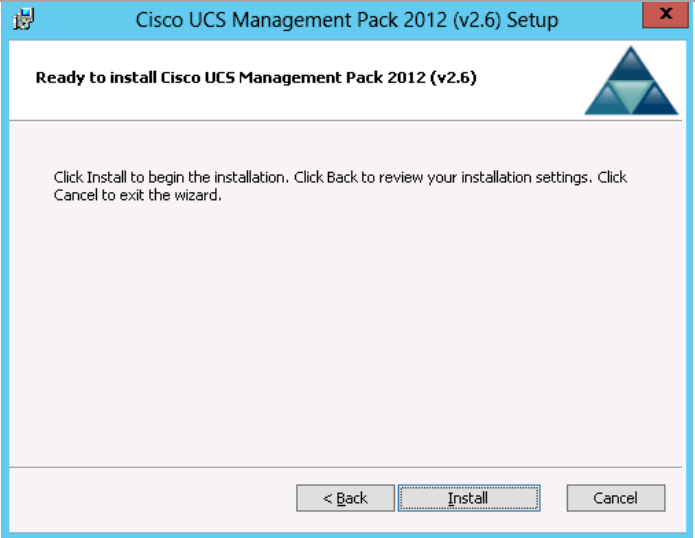
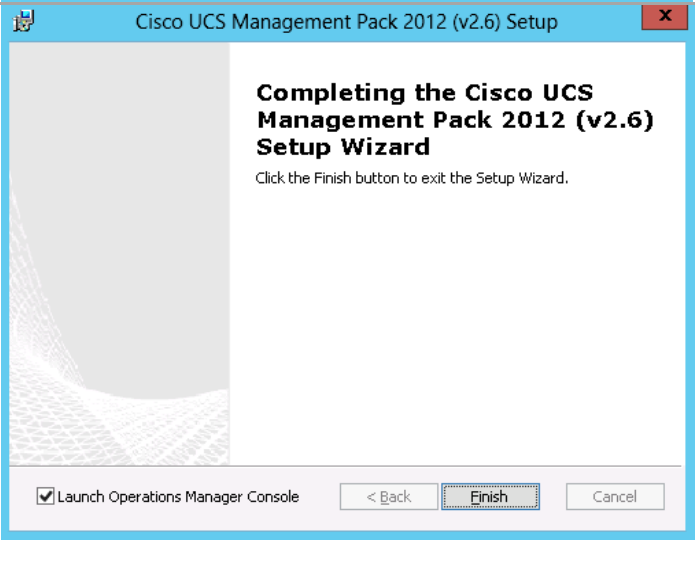
Select the folder where you want features to be installed.

The installer will install Cisco UCS Management Pack 2012 (v2.6) in the following folder.

To install in this folder click "Next". To install to the different folder, enter it below or click "Browse".

Location: C:\Program Files\Cisco\Cisco UCS Management Pack 2012\ Browse

Disk Usage < Back Next > Cancel

<p>Click the Install button to start the installation.</p>	
<p>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.</p>	

Configuring SCOM to Monitor Cisco Unified Computing System

After the Cisco UCS Management Pack is successfully installed on the Operation Manager virtual machine it must be configured for accessing configuration and event data on the Cisco Unified Compute System. The following procedures provide guidance for this process.

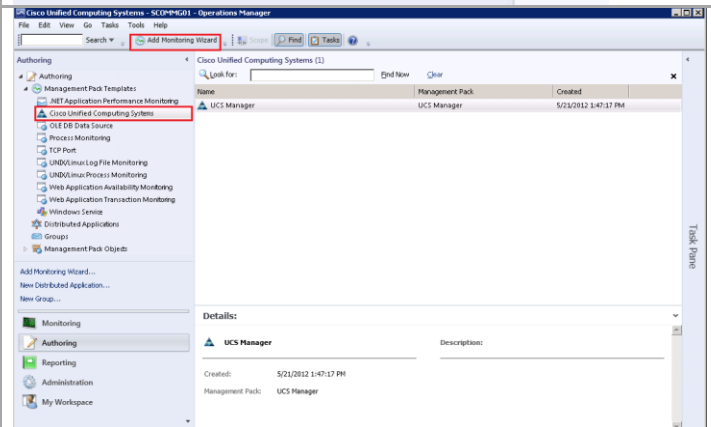
Perform the following steps on all the Operations Manager virtual Machine.

In the **Operations Manager** console, click the **Go** tab in the menu bar.

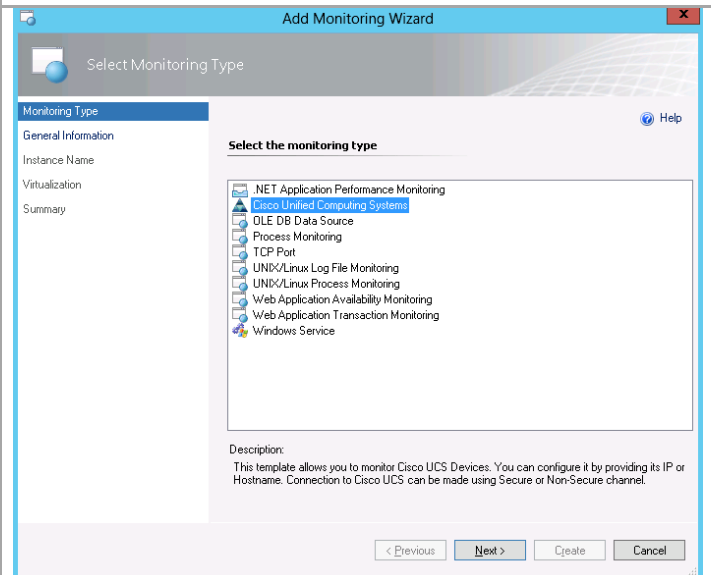
Select **Authoring** from the drop-down menu. The **Authoring** column options appear.



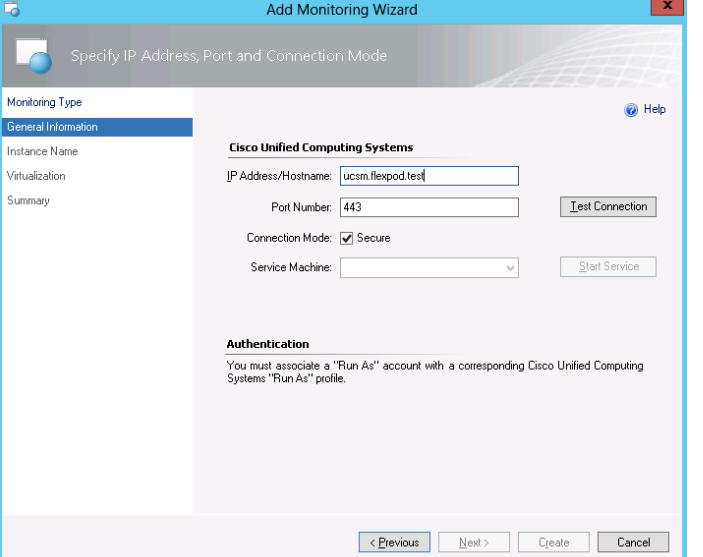
In the **Authoring** column, expand **Management Pack Templates** and select **Cisco Unified Computing Systems**. In the **Tasks** panel, click the **Add Monitoring Wizard**.



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**, **Port Number** and **Connection Mode**. Click the **Test connection** button.



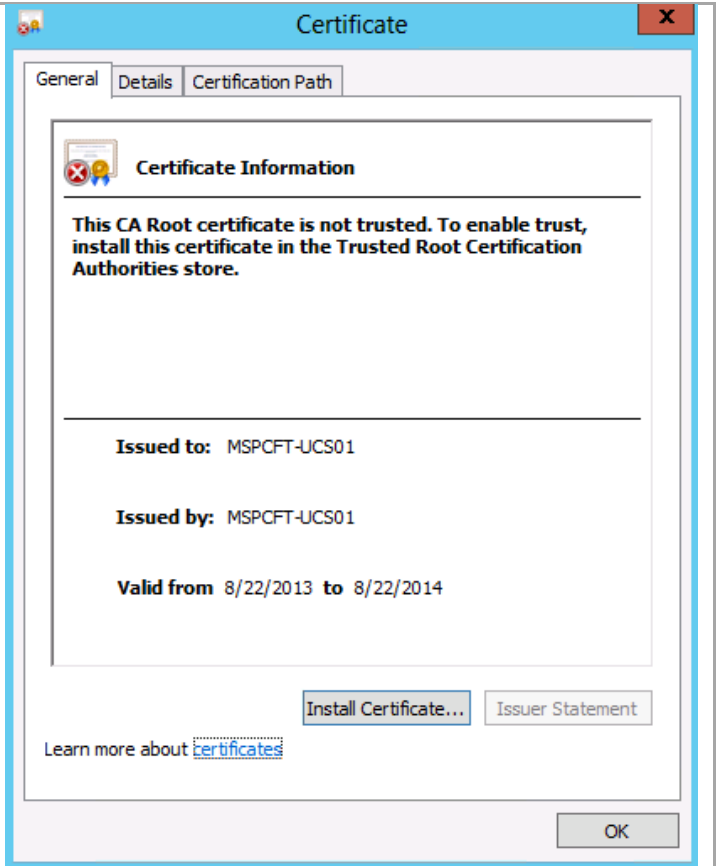
The screenshot shows the 'Add Monitoring Wizard' window with the 'Specify IP Address, Port and Connection Mode' step. On the left, a 'Monitoring Type' sidebar lists 'General Information' (selected), 'Instance Name', 'Virtualization', and 'Summary'. The main area is titled 'Cisco Unified Computing Systems' and contains the following fields: 'IP Address/Hostname' with the value 'ucsm.flexpod.test', 'Port Number' with the value '443', 'Connection Mode' with a checked 'Secure' option, and a 'Service Machine' dropdown menu. There are 'Test Connection' and 'Start Service' buttons. Below this, an 'Authentication' section contains a warning message: 'You must associate a "Run As" account with a corresponding Cisco Unified Computing Systems "Run As" profile.' At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Create', and 'Cancel'.

Click **View Certificate**.

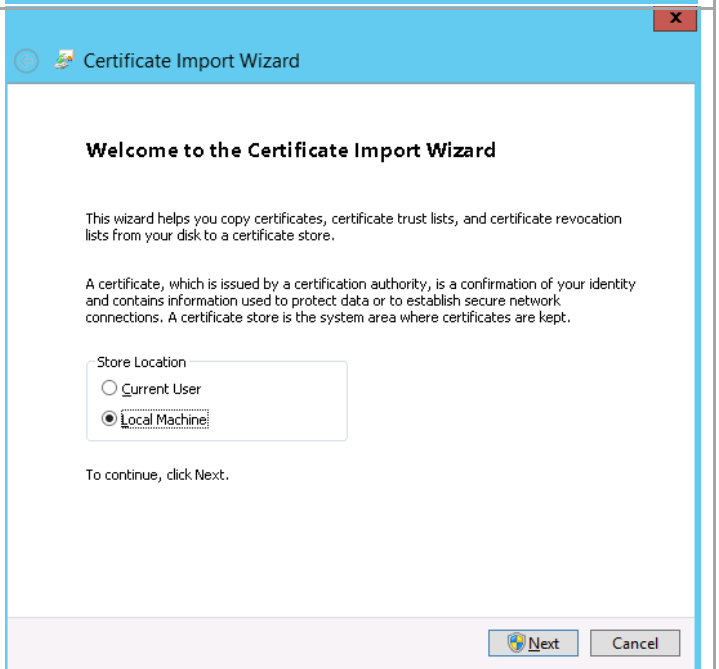


The screenshot shows a 'Security Alert' dialog box. It features a yellow warning icon with an exclamation mark. The main text reads: 'Information you exchange with this site cannot be viewed or changed by others. However, there is problem with the site's security certificate.' Below this, there are three items in a list: 1. A yellow warning icon followed by the text 'The security certificate was issued by a company you have no chosen to trust. View the certificate to determine whether you want to trust the certifying authority.' 2. A green checkmark icon followed by the text 'The security certificate date is valid.' 3. A yellow warning icon followed by the text 'The name on the security certificate is invalid or does not match the name of the site.' At the bottom, it asks 'Do you want to proceed?' and provides three buttons: 'Yes', 'No', and '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**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

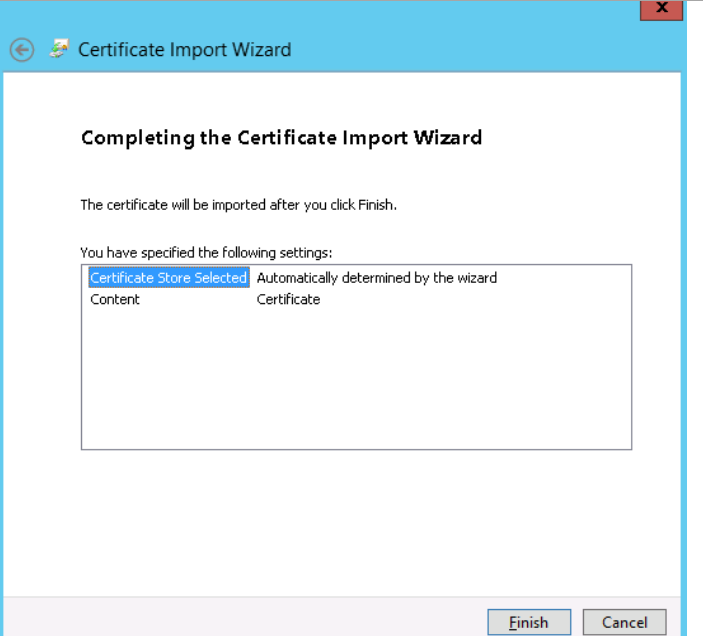
☒ Automatically select the certificate store based on the type of certificate

☐ Place all certificates in the following store

Certificate store:

Learn more about: [certificate stores](#)

Select the default location and click **Finish**.


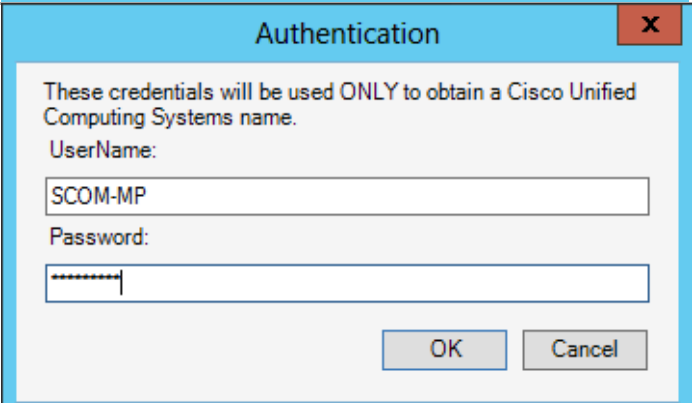
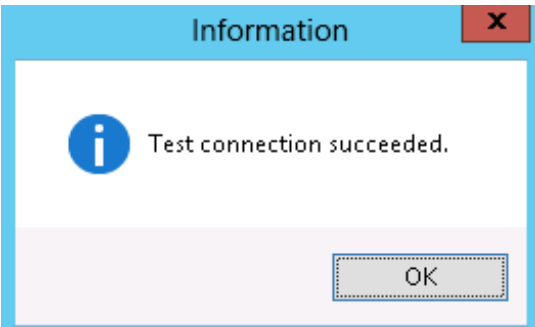


Completing the Certificate Import Wizard

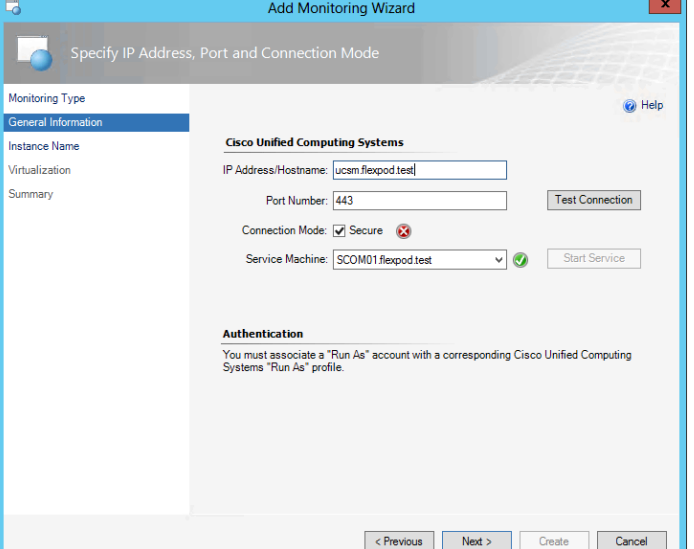
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

<p>Click Yes to proceed.</p>	 <p>Security Alert</p> <p>Information you exchange with this site cannot be viewed or changed by others. However, there is problem with the site's security certificate.</p> <ul style="list-style-type: none"> The security certificate was issued by a company you have no chosen to trust. View the certificate to determine whether you want to trust the certifying authority. The security certificate date is valid. The name on the security certificate is invalid or does not match the name of the site. <p>Do you want to proceed?</p> <p>Yes No View Certificate</p>
<p>Enter the Cisco UCS Manager SCOM Management Pack account created earlier. Enter the account password and click Next.</p>	 <p>Authentication</p> <p>These credentials will be used ONLY to obtain a Cisco Unified Computing Systems name.</p> <p>UserName: SCOM-MP</p> <p>Password: *****</p> <p>OK Cancel</p>
<p>Click OK to close the information window</p>	 <p>Information</p> <p>Test connection succeeded.</p> <p>OK</p>

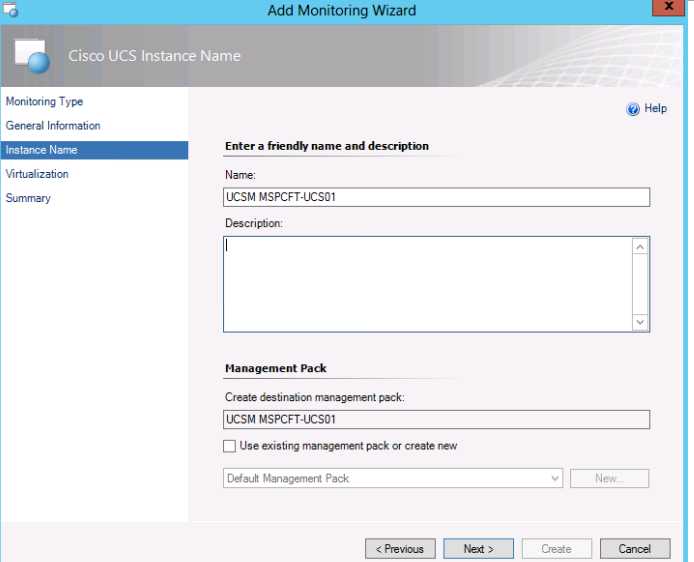
Click **Next** to proceed.



The screenshot shows the 'Add Monitoring Wizard' window, specifically the 'Specify IP Address, Port and Connection Mode' step. The left sidebar has 'Monitoring Type' expanded, with 'General Information' selected. The main area is titled 'Cisco Unified Computing Systems'. It contains the following fields and controls:

- IP Address/Hostname:** A text box containing 'ucsm.flexpod.test'.
- Port Number:** A text box containing '443'.
- Connection Mode:** A checkbox labeled 'Secure' which is checked.
- Service Machine:** A dropdown menu showing 'SCOM01.flexpod.test'.
- Buttons:** 'Test Connection' and 'Start Service'.
- Authentication:** A section with the text: 'You must associate a "Run As" account with a corresponding Cisco Unified Computing Systems "Run As" profile.'
- Navigation:** '< Previous', 'Next >', 'Create', and 'Cancel' buttons at the bottom.

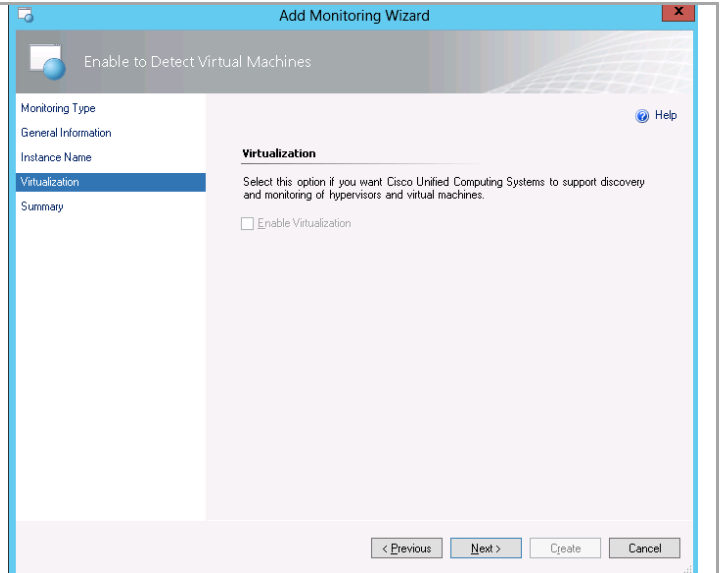
Enter the **Cisco UCS Manager** instance name and click **Next**.



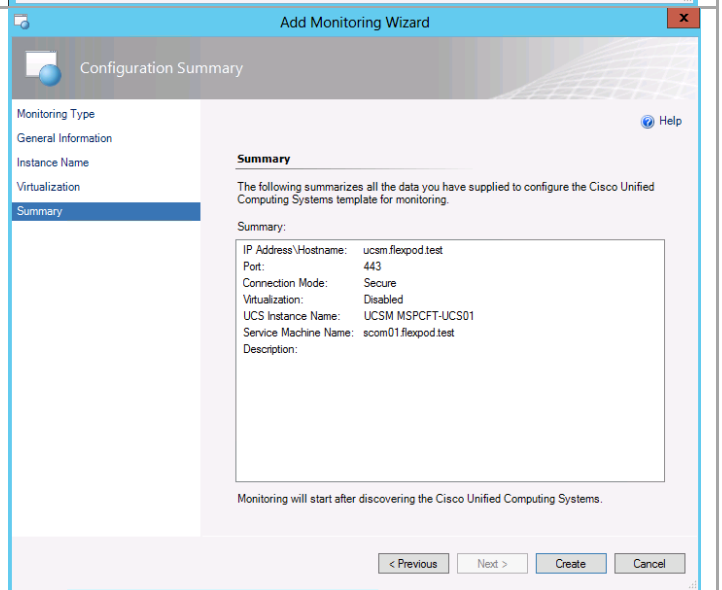
The screenshot shows the 'Add Monitoring Wizard' window, specifically the 'Cisco UCS Instance Name' step. The left sidebar has 'Monitoring Type' expanded, with 'Instance Name' selected. The main area is titled 'Cisco UCS Instance Name'. It contains the following fields and controls:

- Enter a friendly name and description:**
 - Name:** A text box containing 'UCSM MSPCFT-UCS01'.
 - Description:** A large text area.
- Management Pack:**
 - Create destination management pack:** A text box containing 'UCSM MSPCFT-UCS01'.
 - ☐ Use existing management pack or create new
 - Default Management Pack:** A dropdown menu.
 - Buttons:** 'New...'.
- Navigation:** '< Previous', 'Next >', 'Create', and 'Cancel' buttons at the bottom.

In the Enable to Detect Virtual Machines window the Enable Virtualization selection is disabled. Click **Next** to proceed.



Review the configuration summary and click the **Create** button to complete the wizard.



Creating an Administration Account

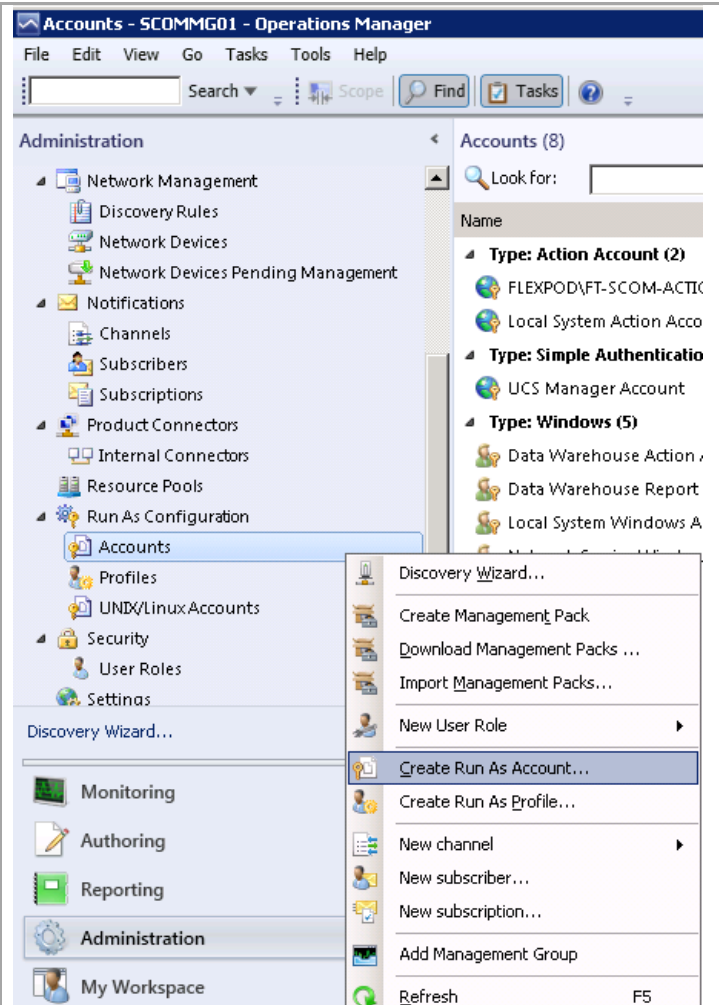
Perform the following steps on all the Operations Manager virtual machine.

In the Operations Manager console, click the **Go** tab in the menu bar.

Select **Administration** from the drop-down menu.

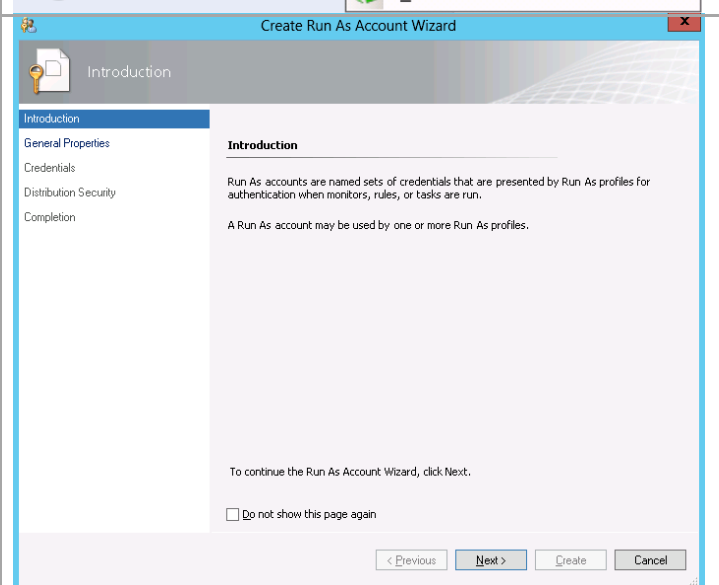


In the Administration column, right click on **Accounts**. Select **Create Run as Accounts** from the drop-down menu.



The **Create Run as Accounts Wizard** screen appears. Click the **Next** button.

Note: Operations Manager uses Run as Accounts to establish connection to Cisco Unified Computing System.



The **General Properties** screen appears. Select **Run as Account Type** as **Simple Authentication** from the drop down menu. Specify **Display name** and **Description**. Click the **Next** button.

The screenshot shows the 'Create Run As Account Wizard' window with the 'General Properties' tab selected. The left sidebar lists the steps: Introduction, General Properties, Credentials, Distribution Security, and Completion. The main area is titled 'Specify general properties for the Run As account'. It contains a dropdown menu for 'Run As account type' set to 'Simple Authentication', a text field for 'Display name' containing 'UCS Manager Account', and a text area for 'Description (optional)'. At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

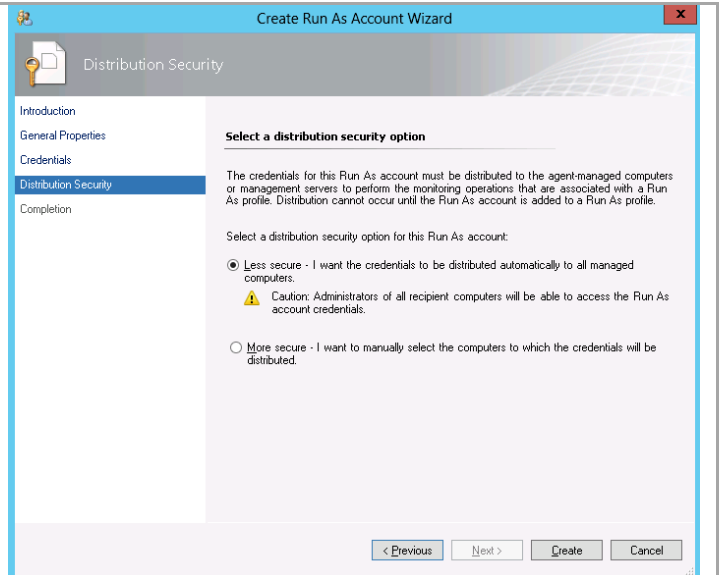
The **Credentials** screen appears. Specify **Account name**, **Password** and **Confirm Password**. Click the **Next** button.

Note: These credentials are used for all communication with Cisco Unified Computing System.

The screenshot shows the 'Create Run As Account Wizard' window with the 'Credentials' tab selected. The left sidebar lists the steps: Introduction, General Properties, Credentials, Distribution Security, and Completion. The main area is titled 'Simple Run As Account' and says 'Provide credentials for this Simple account type.' It contains three text fields: 'Account name' with 'SCOM-MP', 'Password' with masked characters, and 'Confirm password' with masked characters. At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

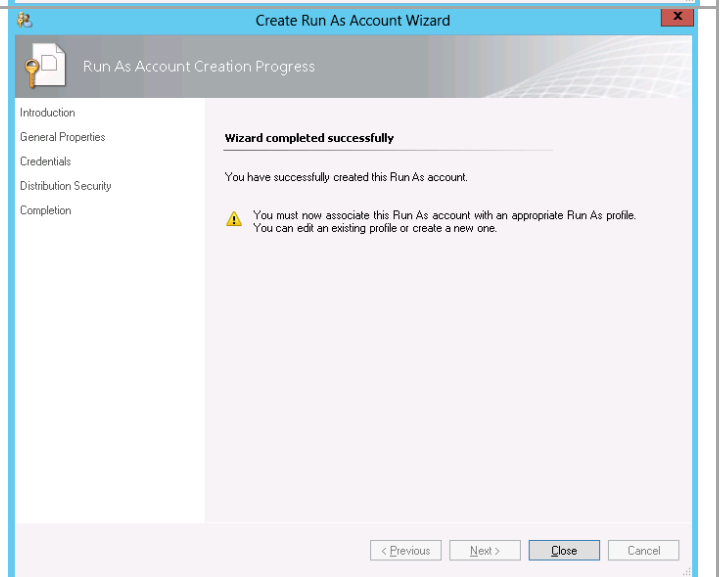
The **Distribution Security** screen appears. Select a distribution security option as **Less Secure**. Click the **Create** button.

Note: More Secure feature is provided to management packs for managing computers or devices running the Windows operating system. Cisco UCS does not run Windows. Cisco recommends using the **Less Secure** option.



The **Create Run as Account Wizard - Completion** screen appears. Click the **Close** button.

The Administrator Account is created. Proceed to associating a Run As Profile with this account.



Associating a Run As Account with a Run As Profile

The Run As account that was created in the previous step must not be associated with a Run As profile.

Perform the following steps on the Operations Manager virtual machine.

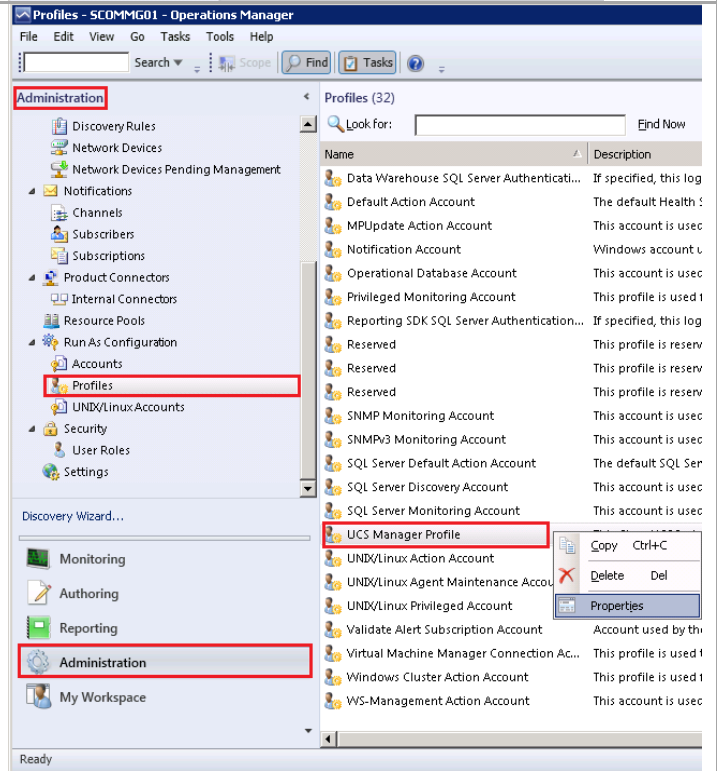
In the Operations Manager console, click the **Go** tab in the menu bar.

Select **Administration** from the drop-down menu.

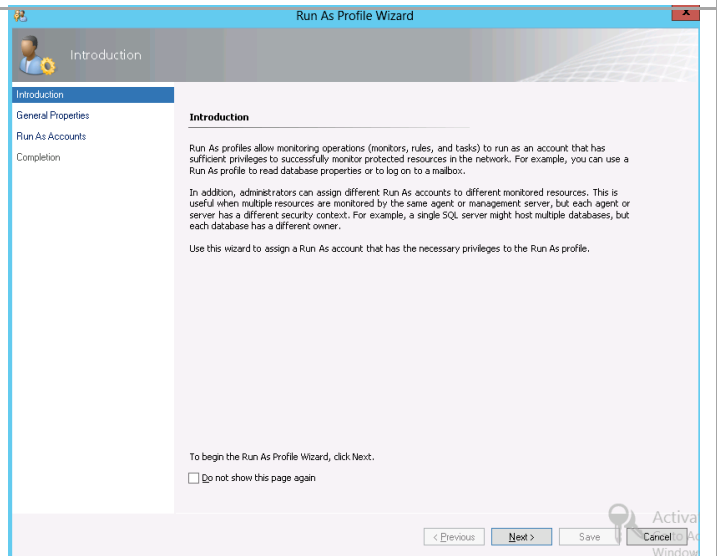


In the Administration column, click on **Profiles**. A list of profiles is displayed on the window. Choose a profile and select **Properties** from its right click menu.

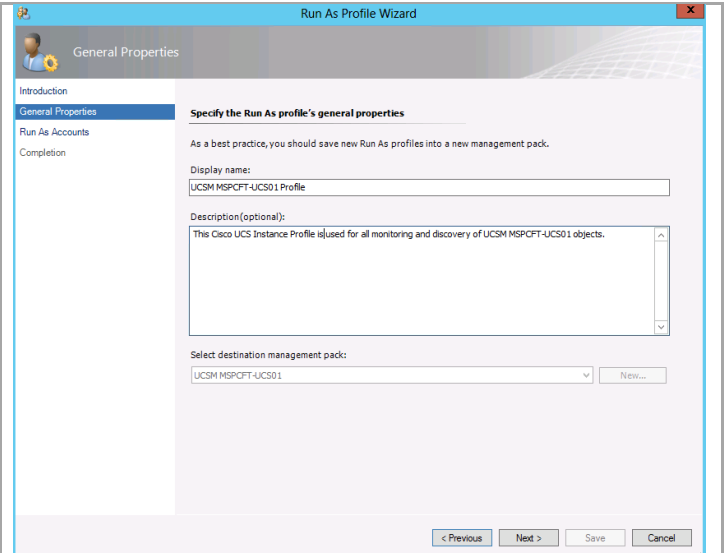
Note: The Cisco UCS Manager Profile is used in this example.



The **Run as Profile Wizard** opens. Click **Next** to continue on to the next screen.

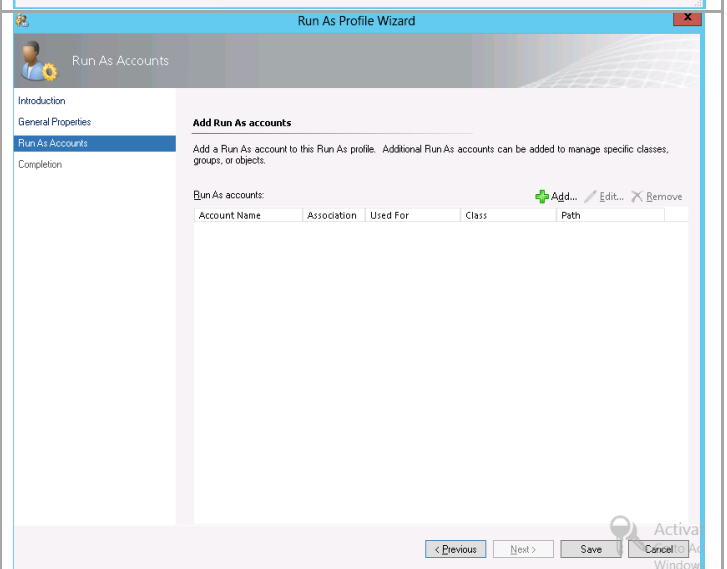


Click **Next** again to continue on to the next screen.



The screenshot shows the 'Run As Profile Wizard' window, specifically the 'General Properties' tab. The left sidebar has 'General Properties' selected. The main area is titled 'Specify the Run As profile's general properties'. It includes a 'Display name' field with 'UCSM MSPCFT-UCS01 Profile' and a 'Description (optional)' text area with 'This Cisco UCS Instance Profile is used for all monitoring and discovery of UCSM MSPCFT-UCS01 objects.' Below these is a 'Select destination management pack:' dropdown menu showing 'UCSM MSPCFT-UCS01'. At the bottom are buttons for '< Previous', 'Next >', 'Save', and 'Cancel'.

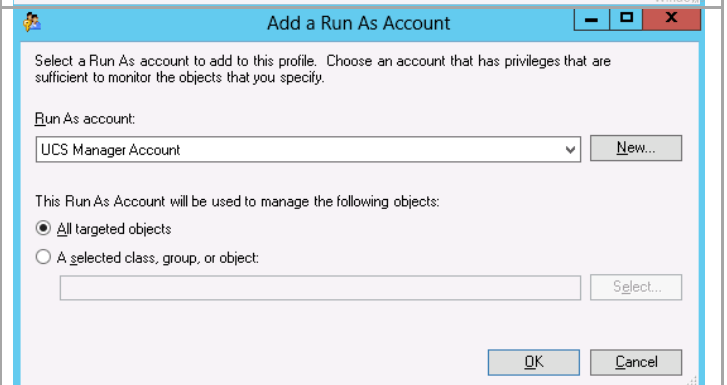
Click **Add** to add the Run As account.



The screenshot shows the 'Run As Profile Wizard' window, specifically the 'Run As Accounts' tab. The left sidebar has 'Run As Accounts' selected. The main area is titled 'Add Run As accounts'. It includes a table with columns: 'Account Name', 'Association', 'Used For', 'Class', and 'Path'. Above the table are buttons for '+ Add...', 'Edit...', and 'Remove'. At the bottom are buttons for '< Previous', 'Next >', 'Save', and 'Cancel'. An 'Active Window' watermark is visible in the bottom right corner.

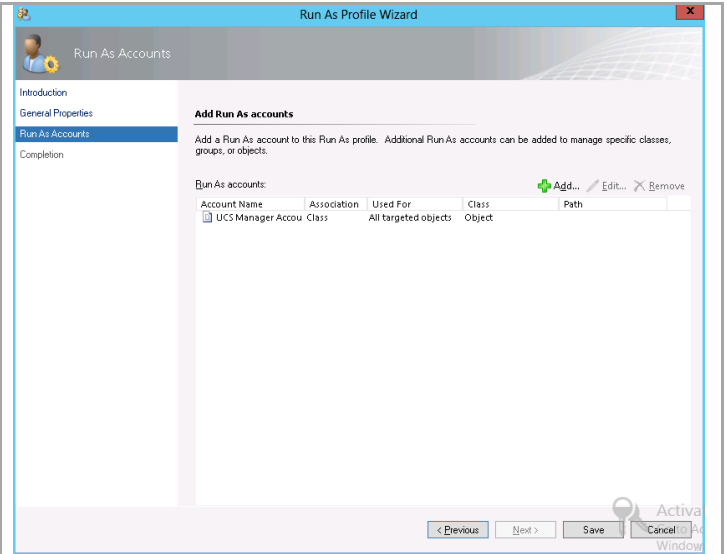
Select the **Cisco UCS Manager Account** from the **Run As Account** drop-down menu. This is the account created in the previous section.

Select the **All targeted objects** options and click **OK**.

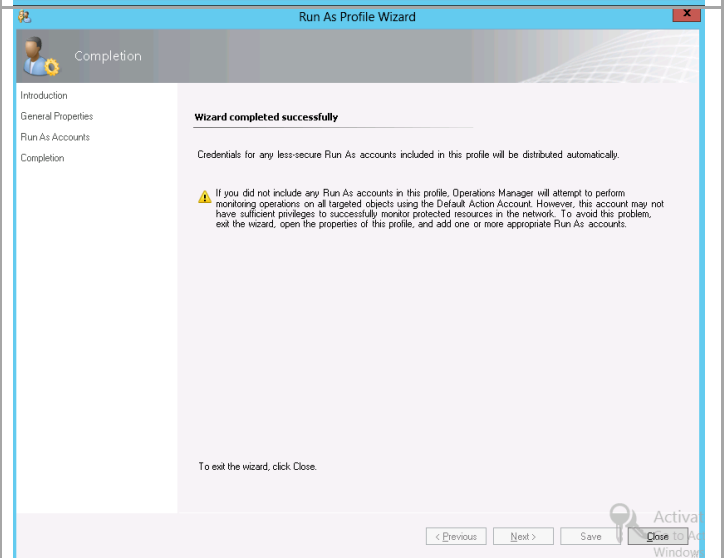


The screenshot shows the 'Add a Run As Account' dialog box. It has a title bar with standard window controls. The main text says 'Select a Run As account to add to this profile. Choose an account that has privileges that are sufficient to monitor the objects that you specify.' Below this is a 'Run As account:' dropdown menu with 'UCS Manager Account' selected and a 'New...' button. Further down, it says 'This Run As Account will be used to manage the following objects:' with two radio button options: 'All targeted objects' (which is selected) and 'A selected class, group, or object:'. Below the second option is a text field and a 'Select...' button. At the bottom are 'OK' and 'Cancel' buttons.

Click the **Save** button to save the account configuration.



The **Completion** screen appears. Click the **Close** button to close the wizard.

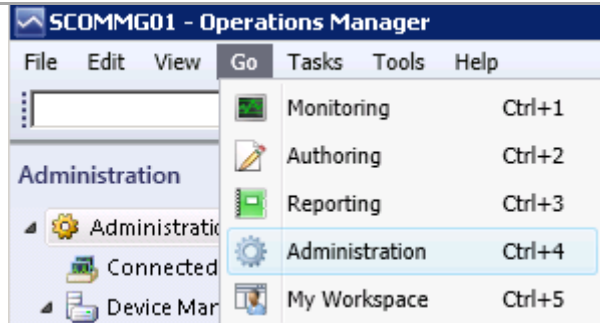


Configuring Bidirectional Communication

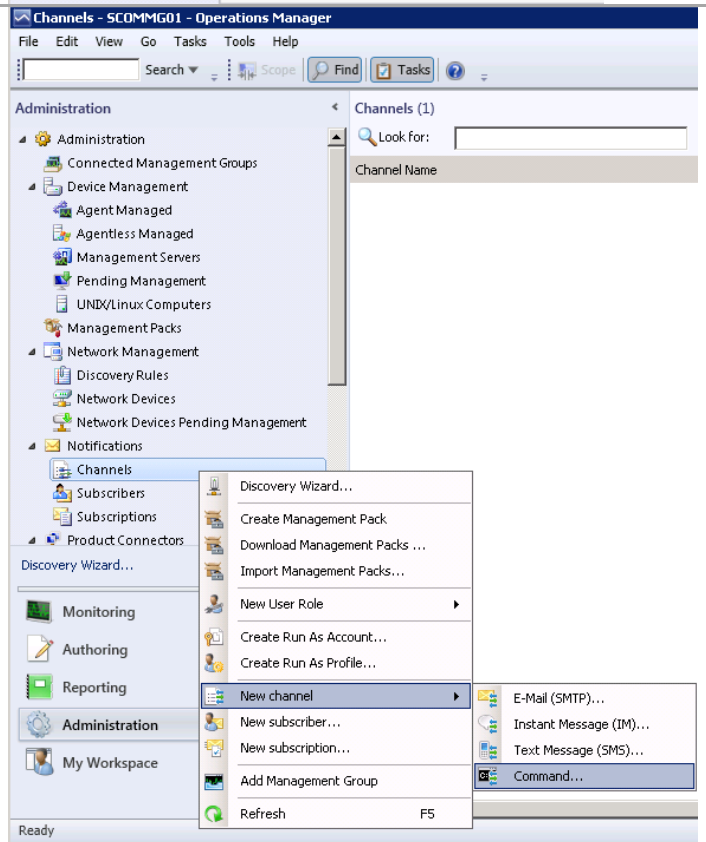
The following procedure describes the required configuration to communicate with Cisco UCS for acknowledging alerts from the Operations Manager Console.

Note: The Bidirectional feature is currently limited to Management Servers on which SCOM 2012 Console and Cisco UCS MP are both installed.

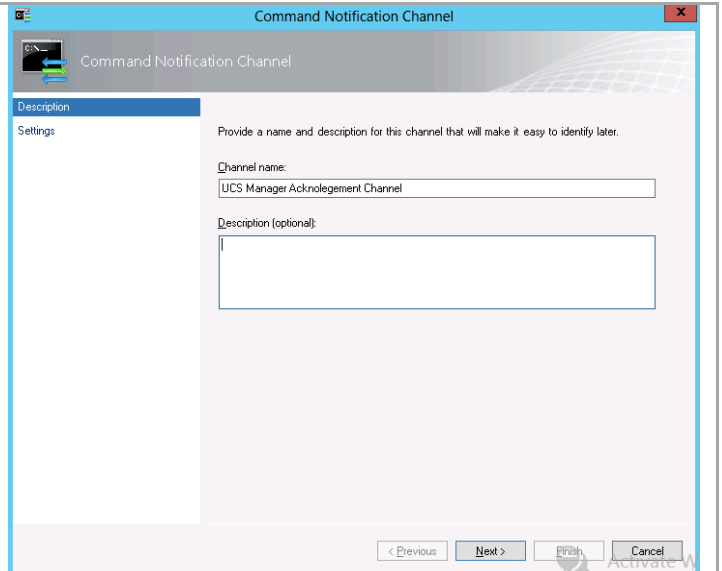
In the Operations Manager console, click the **Go** tab in the menu bar. Select **Administration** from the drop-down menu.



In the Administration column, 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 screenshot shows the 'Command Notification Channel' window with the 'Description' tab selected. The 'Settings' section on the left is empty. The main area contains a 'Channel name' field with the text 'UCS Manager Acknowledgement Channel' and a 'Description (optional)' text area. At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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** as

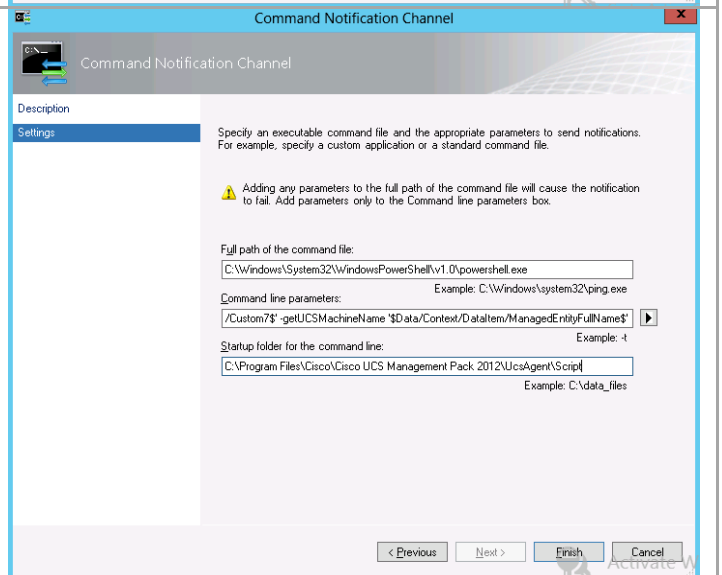
-Command "& "C:\Program Files\Cisco\Cisco UCS Management Pack 2012\UcsAgent\Script\Bidirectional.ps1" - getFaultID '\$Data/Context/DataItem/Custom7\$' - getUCSMachineName '\$Data/Context/DataItem/ManagedEntityFullName\$'

Specify **Start up folder for the command line** as

C:\Program Files\Cisco\Cisco UCS Management Pack 2012\UcsAgent\Script

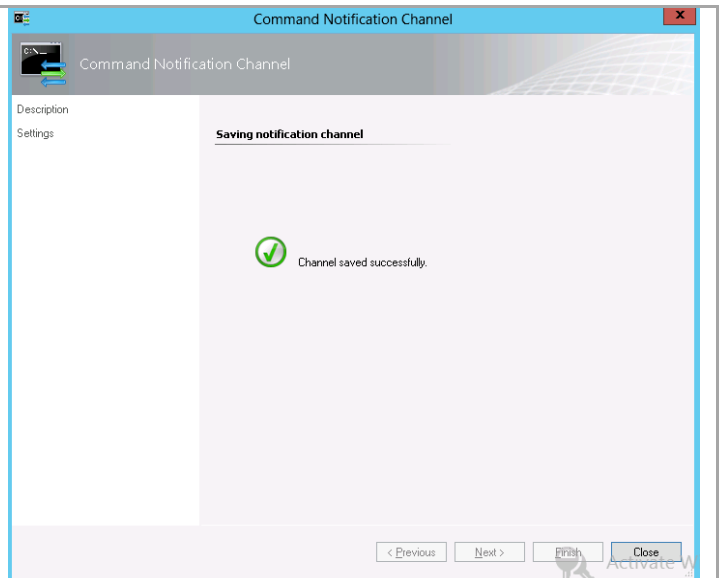
Note: Verify the path for script is valid.

Click the **Finish** button.

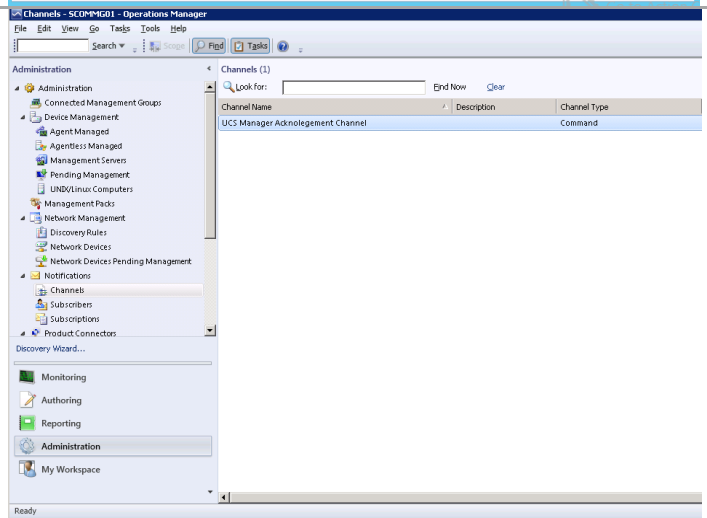


The screenshot shows the 'Command Notification Channel' window with the 'Settings' tab selected. The 'Description' section on the left is empty. The main area contains instructions to specify an executable command file and parameters. It includes a warning icon and text: 'Adding any parameters to the full path of the command file will cause the notification to fail. Add parameters only to the Command line parameters box.' There are three input fields: 'Full path of the command file' (containing 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe'), 'Command line parameters' (containing '/Custom7\$ -getUCSMachineName \$Data/Context/DataItem/ManagedEntityFullName\$'), and 'Startup folder for the command line' (containing 'C:\Program Files\Cisco\Cisco UCS Management Pack 2012\UcsAgent\Script'). At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

The new Channel is saved successfully. Click **Close** to close the wizard.

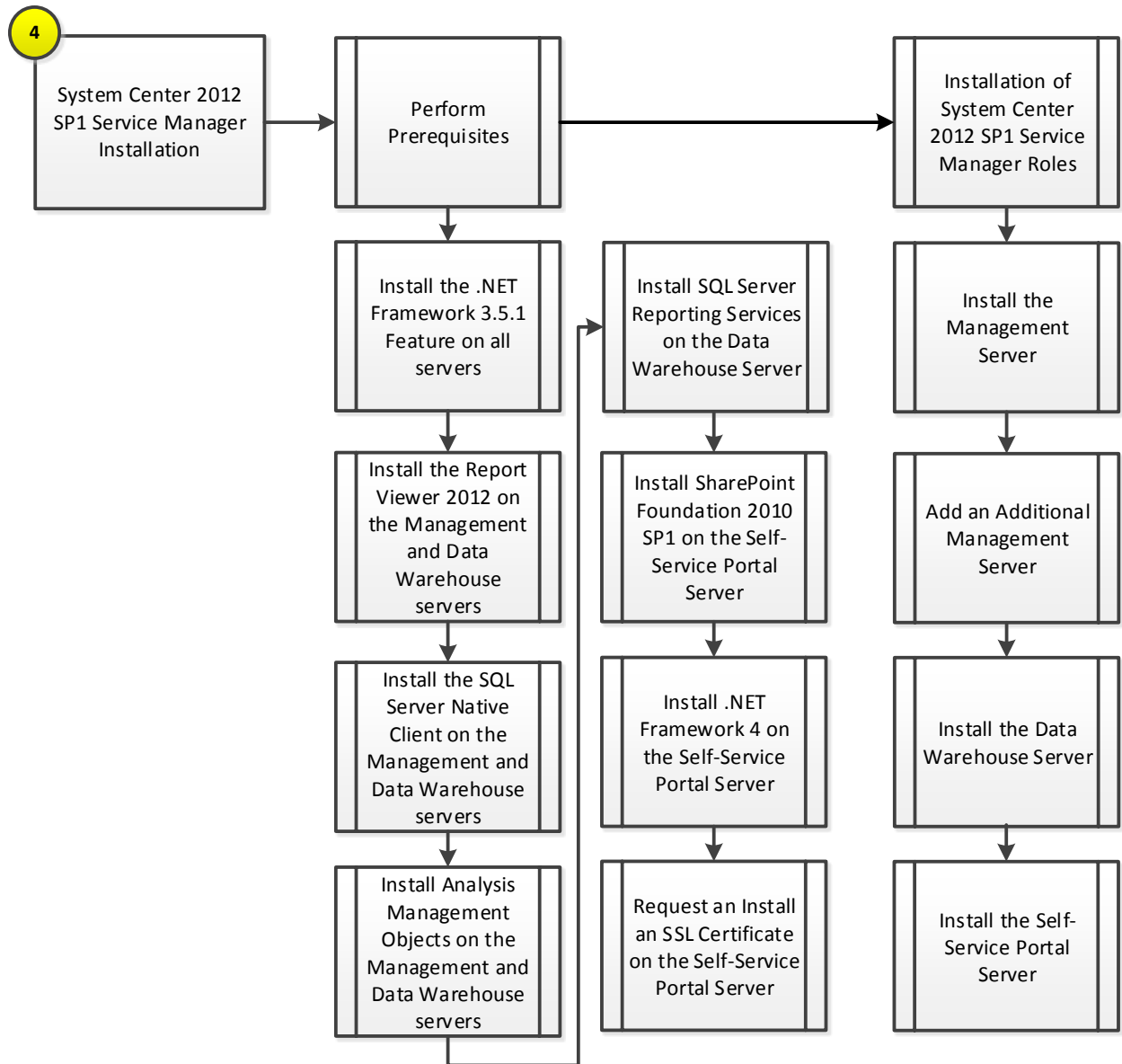


The new channel appears in the **Channel** view.



18 Service Manager

The Service Manager installation process includes the following high-level steps:



Overview

This section provides a high-level walkthrough on deploying Service Manager into the Fast Track fabric management architecture. The following assumptions are made:

Management Server

- A base virtual machine running Windows Server 2012 has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with dedicated Service Manager instances that has been established in previous steps for Service Manager.
 - Service Manager database – instance for Service Manager management database.
- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.
- The Microsoft SQL Server 2012 Analysis Management Objects is installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.

Data Warehouse Server

- A base virtual machine running Windows Server 2012 has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with dedicated instance that has been established in previous steps for Service Manager.
 - SCSMAS – instance for SQL Server 2012 Analysis Services and SQL Server Reporting Services databases.
 - SCSMDW – instance for Service Manager Data Warehouse databases.
- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.
- The Microsoft SQL Server 2012 Analysis Management Objects are installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.
- The Microsoft SQL Server 2012 Reporting Services (split configuration) is installed.
- The Microsoft SQL Server 2012 Management tools are installed.

Self-Service Portal Server

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role.
- A multi-node, SQL Server 2012 cluster with dedicated instance that has been established in previous steps for Service Manager.
 - SCSPFarm – instance for Self Service Portal SharePoint Farm databases.
- The .NET Framework 3.5 Feature is installed.
- The Microsoft Report Viewer 2008 Service Pack 1 Redistributable (KB971119) is installed
- The Microsoft SQL Server 2012 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.

- The Microsoft SQL Server 2012 Analysis Management Objects is installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.
- SharePoint Foundation 2010 Service Pack 1 is installed.
- The .NET Framework 4 Redistributable is installed.

18.1 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User name	Purpose	Permissions
<DOMAIN>\FT-SCSM-SVC	SCSM services account	Add the account to the local Administrators group on the all SCSM servers. Must be a local admin on all SQL Server nodes.
<DOMAIN>\FT-SCSM-WF	SCSM workflow account	Must have permissions to send e-mail and must have a mailbox on the SMTP server (required for the E-mail Incident feature). Must be member of Users local security group on all SCSM servers. Must be made a member of the Service Manager Administrators user role in order for e-mail Must be a local admin on all SQL Server nodes.
<DOMAIN>\FT-SCSM-SSRS	SCSM reporting account	Must be a local admin on all SQL Server nodes.
<DOMAIN>\FT-SCSM-OMCI	SCSM Operations Manager CI connector account	Must be a member of the Users local security group on all SCSM servers. Must be an Operations Manager Operator.
<DOMAIN>\FT-SCSM-ADCI	SCSM Active Directory CI connector account	Must be a member of the Users local security group on the Service Manager management server. Must have permissions to bind to the domain controller that the connector will read data from. Needs generic read rights on the objects that are being

User name	Purpose	Permissions
		synchronized into the Service Manager database from Active Directory.
<DOMAIN>\ FT-SCSM-OMAlert	SCSM Operations Manager alert connector account	Must be a member of the Users local security group on the Service Manager management server. Must be a member of FT-SCSM-Admins
DOMAIN>\ FT-SCSM-VMMCI	Virtual Machine Manager CI connector account	Member of the VMM Admin domain group. The account must also be in the Service Manager Advanced Operator role
DOMAIN>\ FT-SCSM-OCI	Orchestrator CI connector	Member of SCO Operators (Users) domain group. The account must also be in the Service Manager Advanced Operator role
<DOMAIN>\ FT-SCSM-OLAP	Service Manager Analysis Services account	Must be a local admin on all SQL Server nodes.

Groups

Verify that the following security groups have been created:

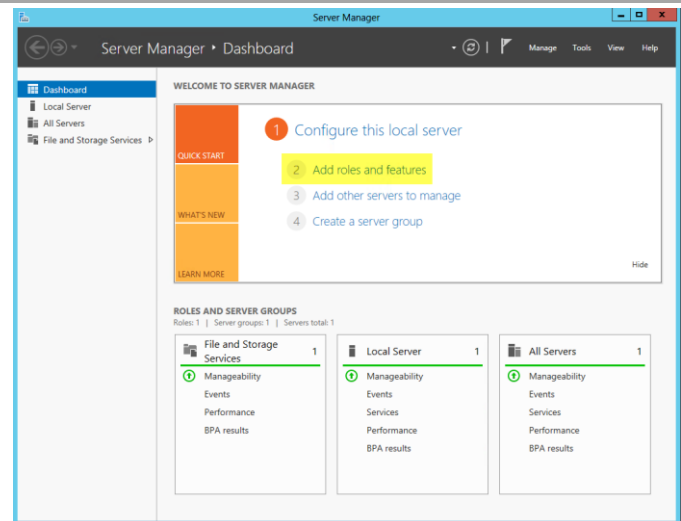
Security group name	Group scope	Members	Member of
<DOMAIN>\ FT-SCSM-ADMINS	Global	DOMAIN\ FT-SCSM-SVC	Must be added to the Service Manager Administrators user role and added to the Operations Manager Administrators role in Operations Manager and a member of the Administrators group on each SQL Server.

Add the .NET Framework 3.5 Feature on all Server Manager Servers

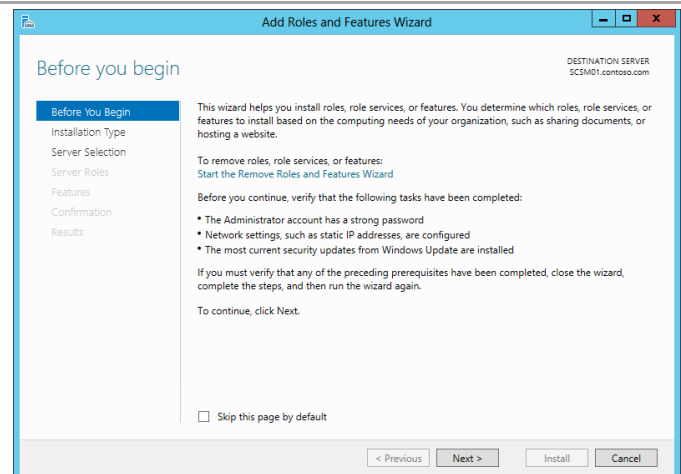
The Service Manager installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5 Feature.

- Perform the following steps on the **Service Manager management server (SCSM01)** and **data warehouse (SCSM02)** virtual machines.

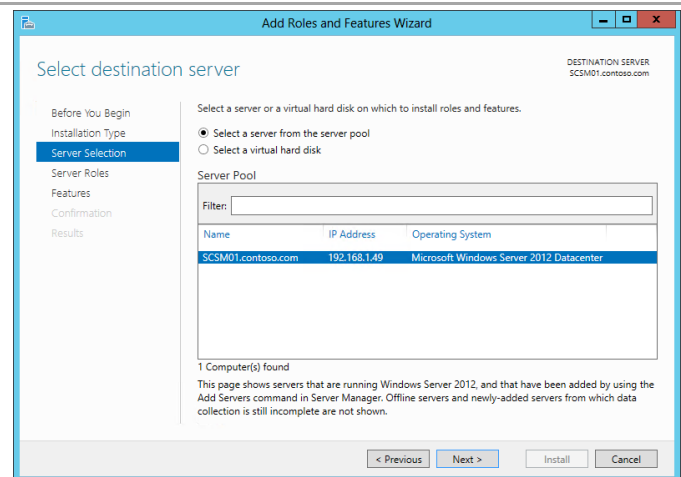
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



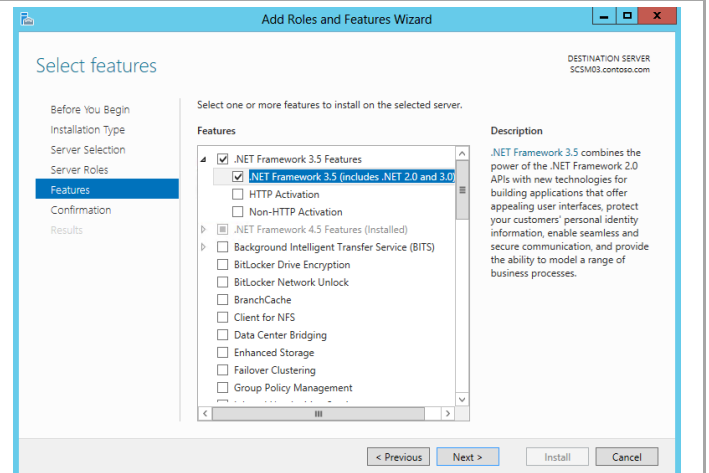
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



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.



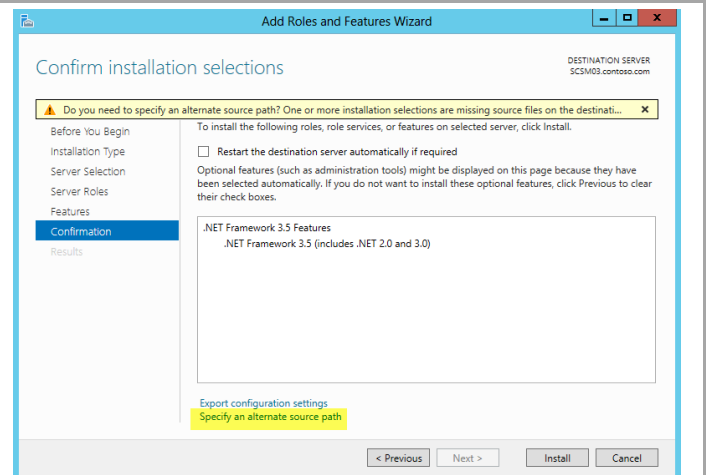
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



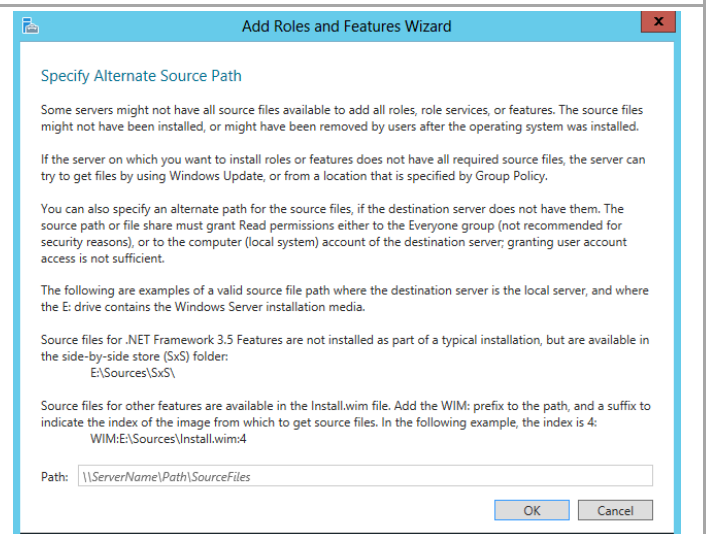
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

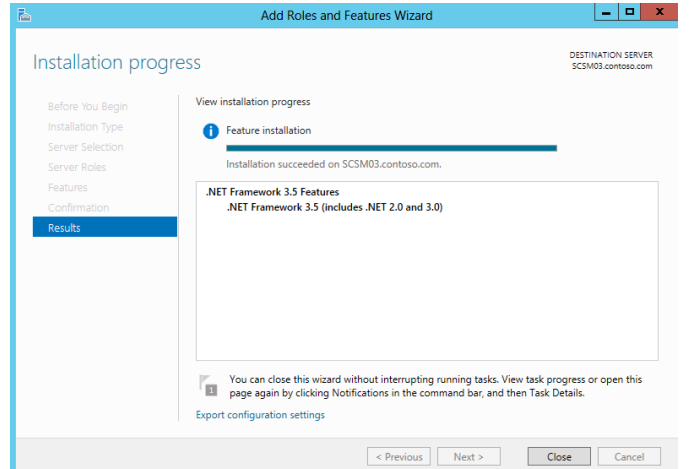
*Also, If the server does not have internet access an alternate source path can be specified by clicking the **Specify** and **alternate source patch** link.*



For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location be specified for the installation.

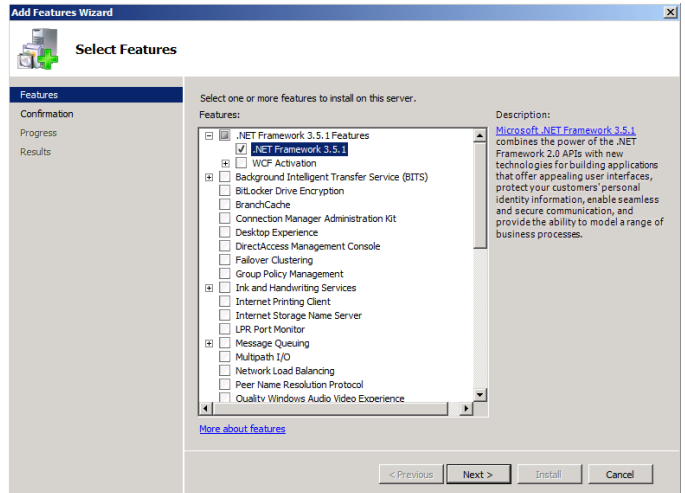


The **Installation Progress** dialog will show the progress of the feature installation. Click **Close** when the installation process completes.

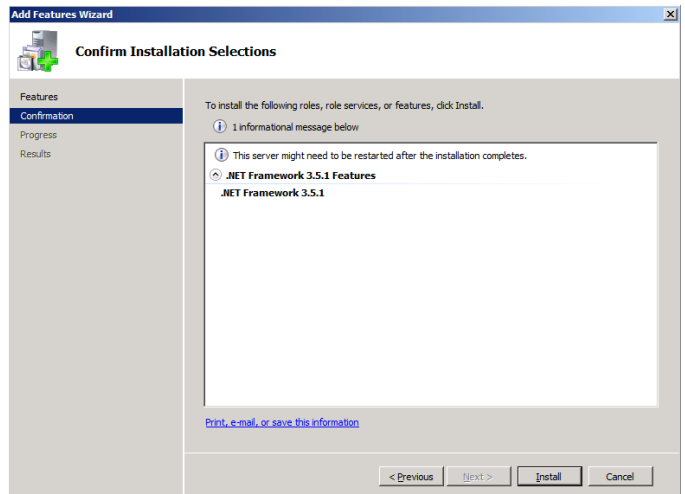


- Perform the following steps on the **Service Manager Self-Service Portal** virtual machine running Windows Server 2008 R2.

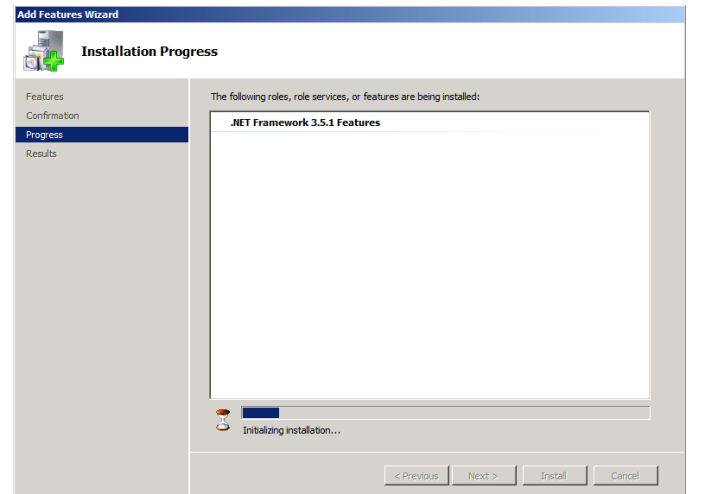
To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features**, and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.



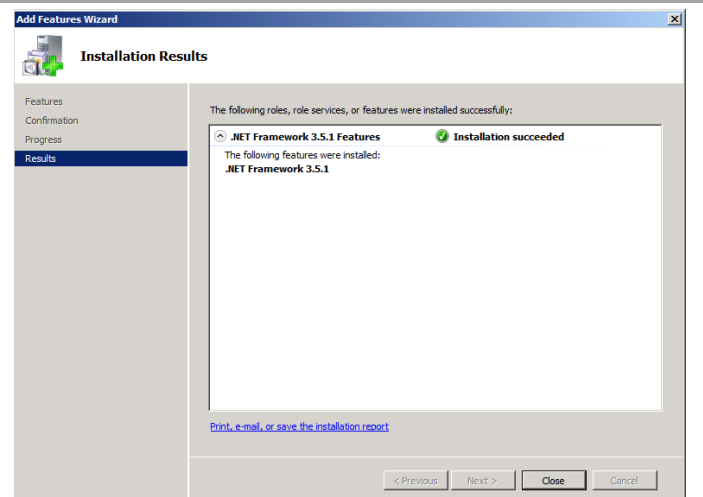
In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.



The **Installation Progress** dialog will show the progress of the feature install.



Once complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. Once verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.



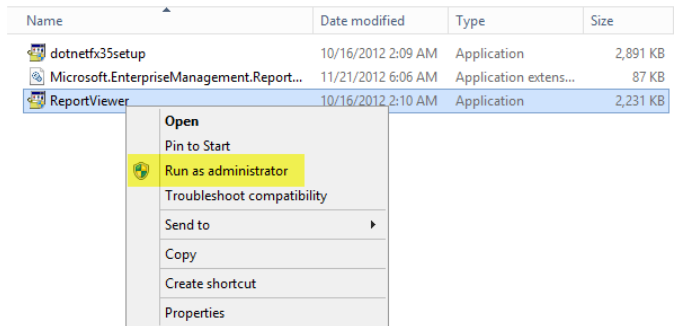
Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers

The Server Manager management and Data Warehouse server installations also require the **Microsoft Report Viewer 2008 SP1** Redistributable be installed prior to installation. The following steps are provided to help install the Microsoft Report Viewer 2008 SP1 Redistributable.

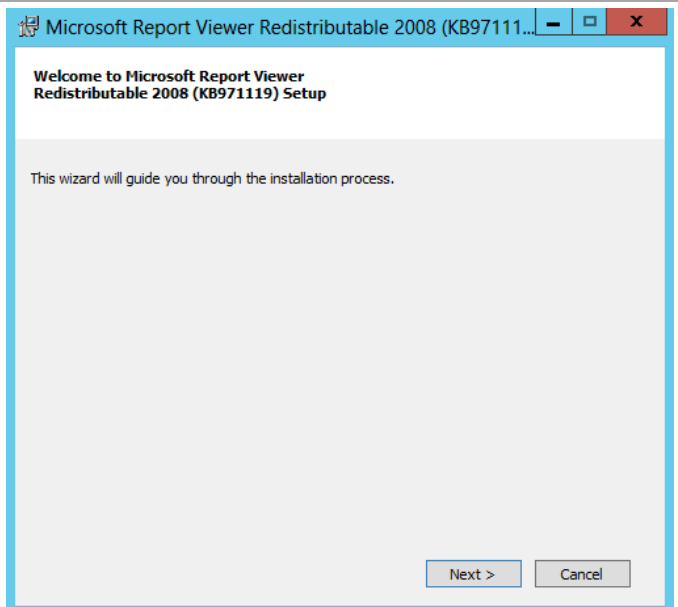
- Perform the following steps on the **Server Manager management (SCSM01) and Data Warehouse server (SCSM02)** virtual machines.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

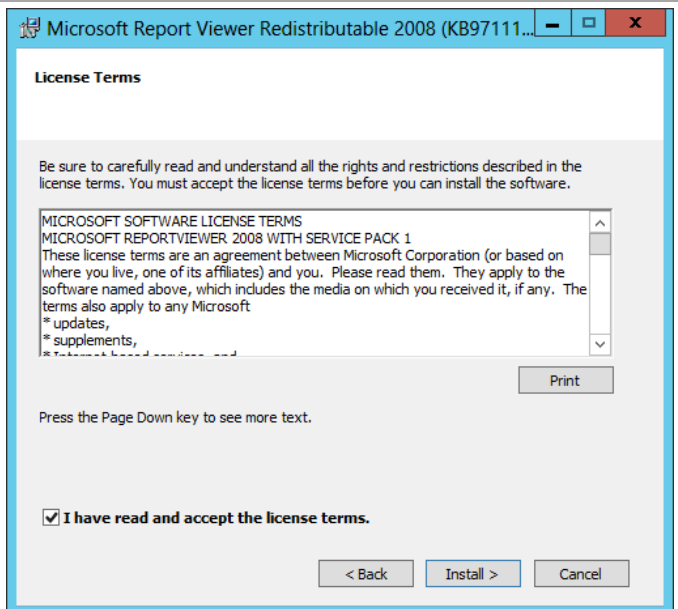
Note: Report Viewer can be found in the prerequisites folder of the Service Manager 2012 SP1 installation media or it can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=3203>



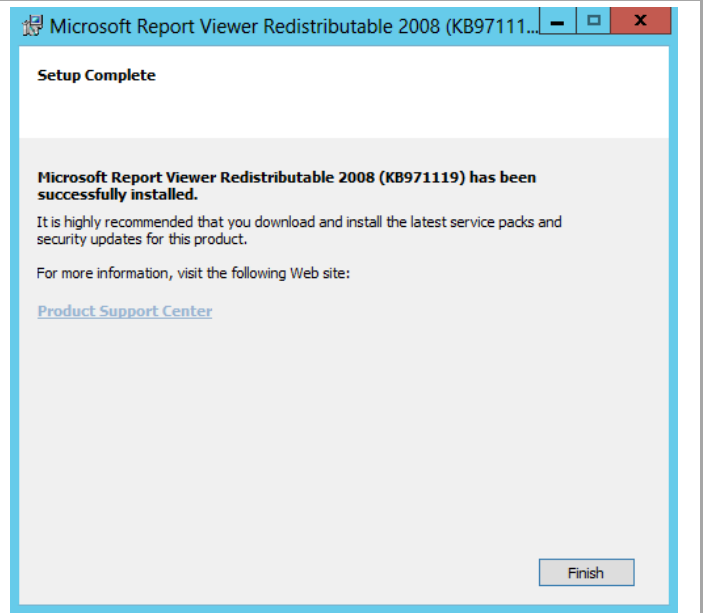
The setup wizard will appear. Click **Next** to continue.



Within the **License Terms** dialog, select the **I have read and accept the license terms** checkbox. Click **Install** to begin the installation.



Once completed, click **Finish** to exit the installation.



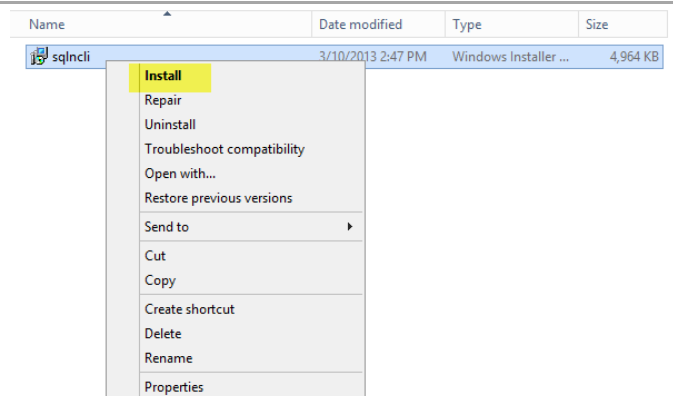
Install SQL Server 2012 Native Client on the on the Management and Data Warehouse Servers

The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 Native Client be installed prior to installation. Follow the provided steps to install the SQL Server 2012 Native Client.

- Perform the following steps on the **Server Manager management (SCSM01)** and **Data Warehouse server (SCSM02)** virtual machines.

From the installation media source, right-click **SQLNCLI.MSI** and select **Install** from the context menu to begin setup.

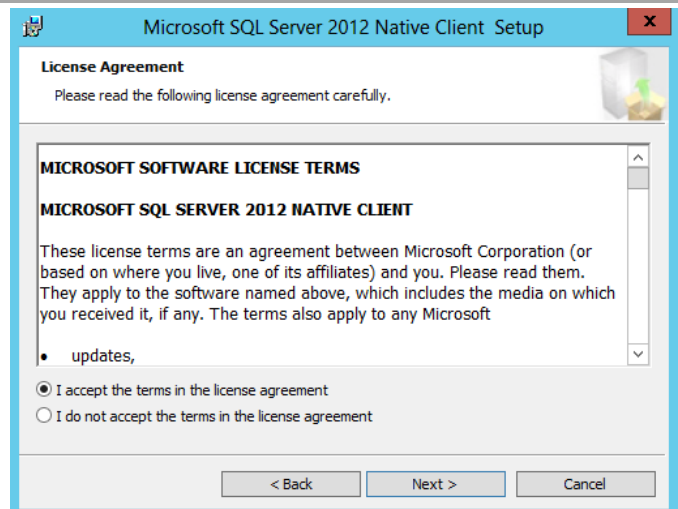
Note: the SQL Server 2012 SP1 Native Client installer, **1033\x64\sqlncli.msi**, can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=35580>.



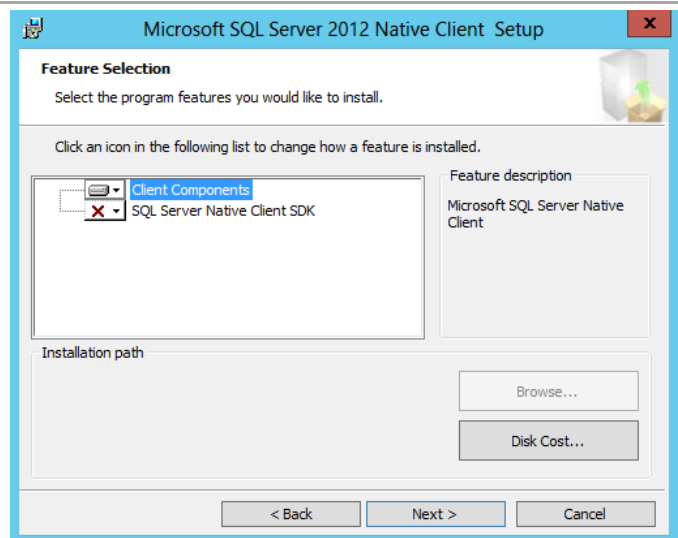
The setup wizard will appear. Click **Next** to continue.



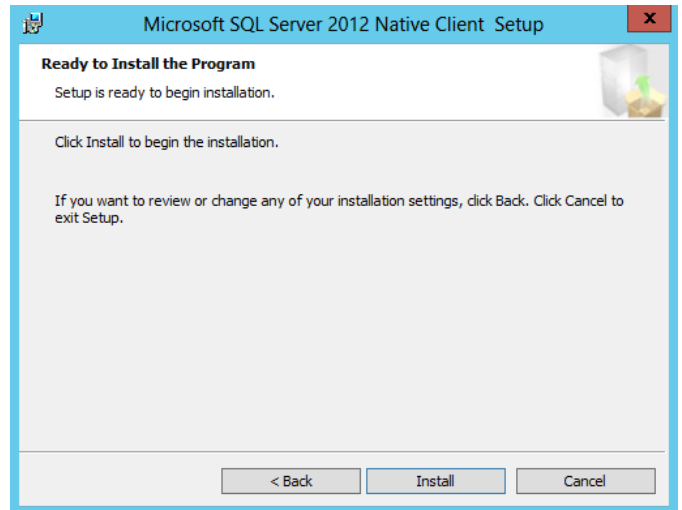
Within the **License Terms** dialog, select the **I accept the terms in the license agreement** check box. Click **Next** to continue.



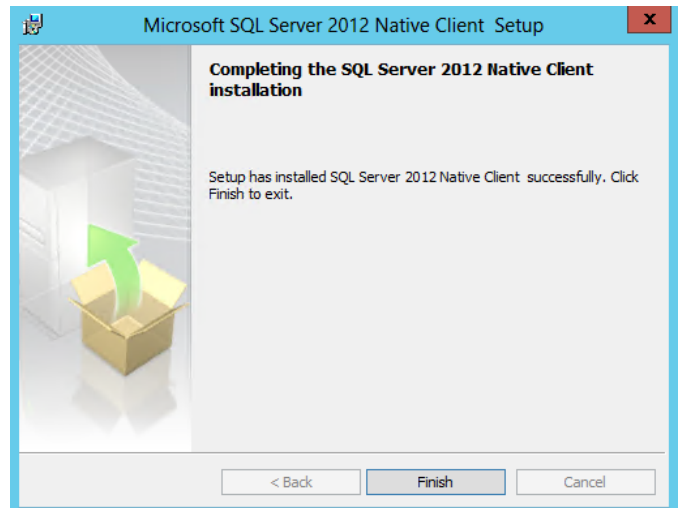
In the **Feature Selection** dialog, verify that the **Client Components** feature is selected for installation. Click **Next** to continue.



In the **Ready to Install the Program** dialog, click **Install** to begin the installation.



Once completed, click **Finish** to exit the installation.



Install SQL Server 2012 SP1 Analysis Management Objects

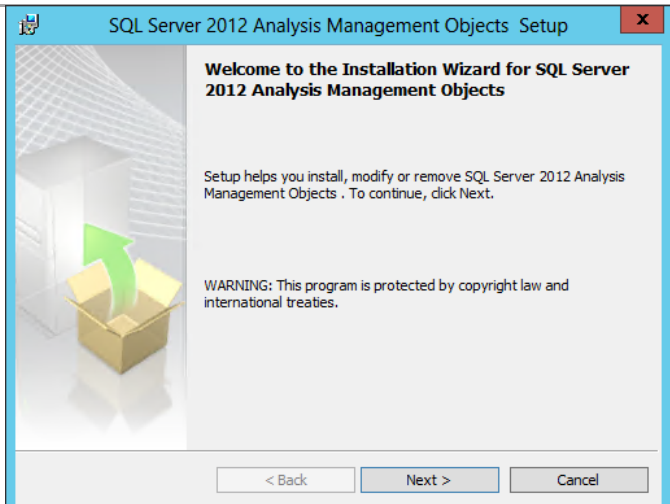
The Server Manager management and Data Warehouse server installations also require the SQL Server 2012 SP1 Analysis Management Object be installed prior to installation. Follow the provided steps to install the SQL Server 2012 SP1 Analysis Management Objects.

- Perform the following steps on the **Server Manager management (SCSM01)** and **Data Warehouse server (SCSM02)** virtual machines.

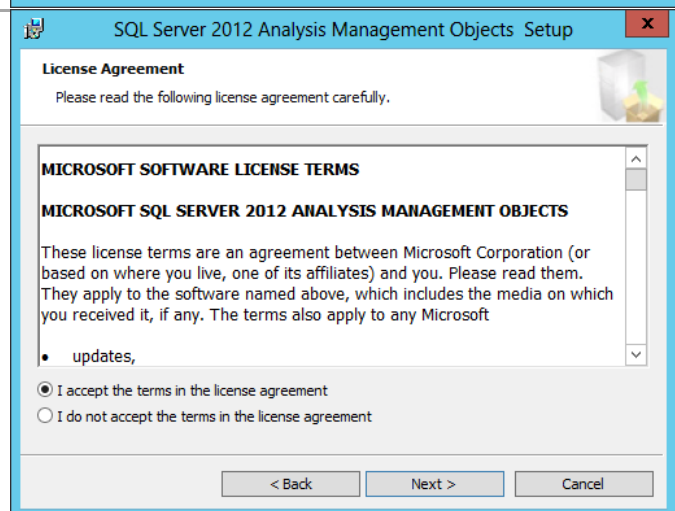
From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.
Note: The SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI**, can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=35580>.

Name	Date modified	Type	Size
SQL_AS_AMO	3/7/2013 11:04 AM	Windows Installer Package	3,604 KB

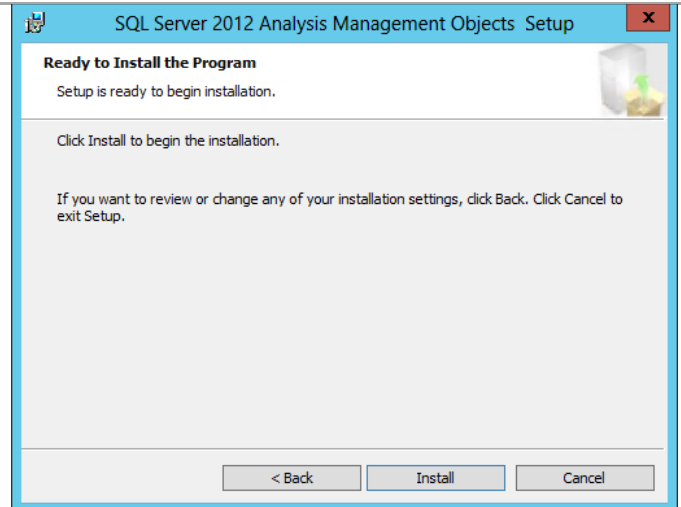
The setup wizard will launch. On the **Welcome** dialog, click **Next** to continue.



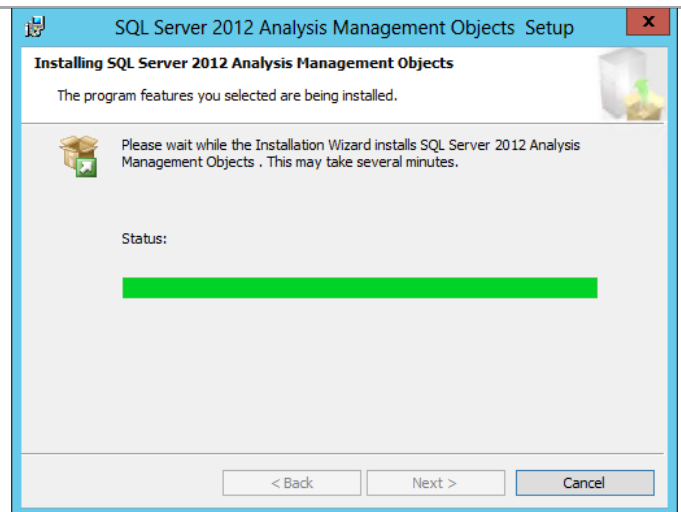
In the **License Agreement** dialog, review the license agreement and select the **I accept the terms in the license agreement** radio button and then click **Next** to continue.



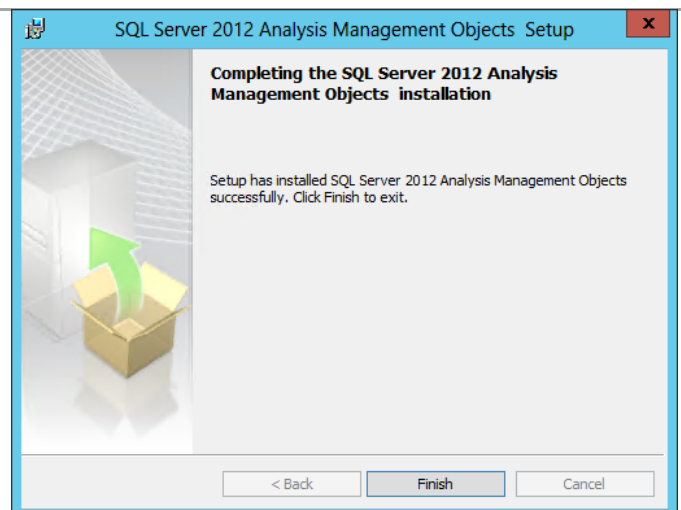
In the **Ready to Install the Program** dialog, click **Install** to begin the installation.



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.

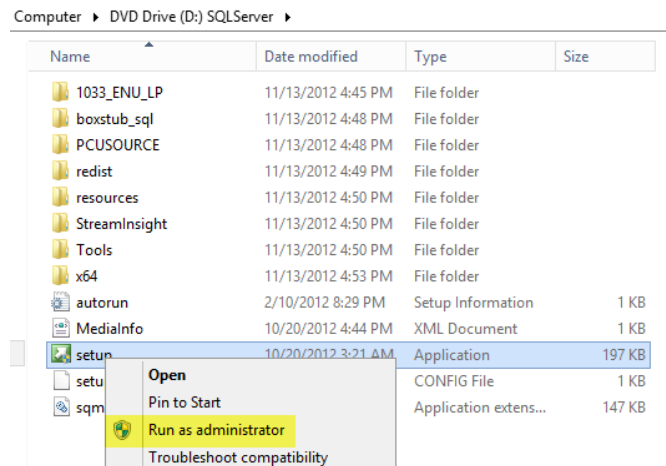


Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

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 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.



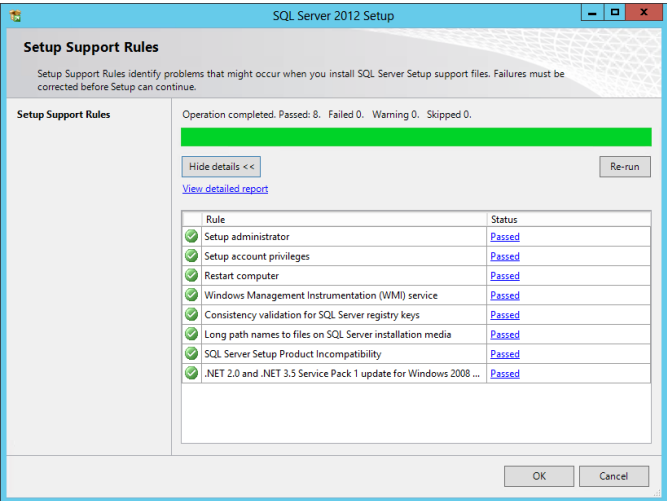
From the **SQL Server Installation Center** click the **New SQL Server stand-alone installation or add features to an existing installation** link.



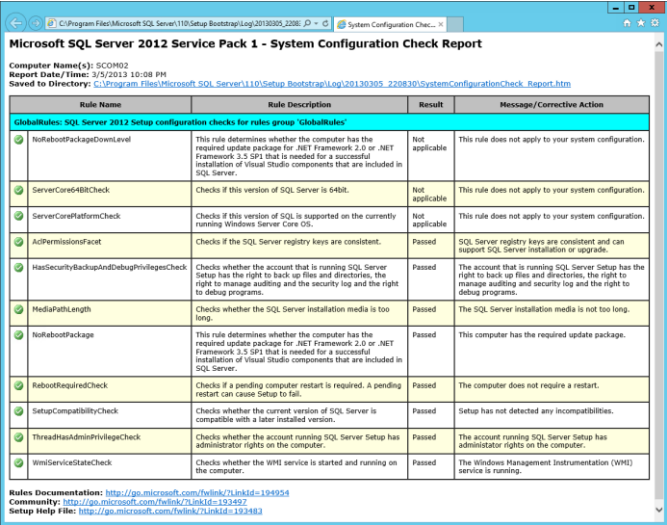
New SQL Server stand-alone installation or add features to an existing installation

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.

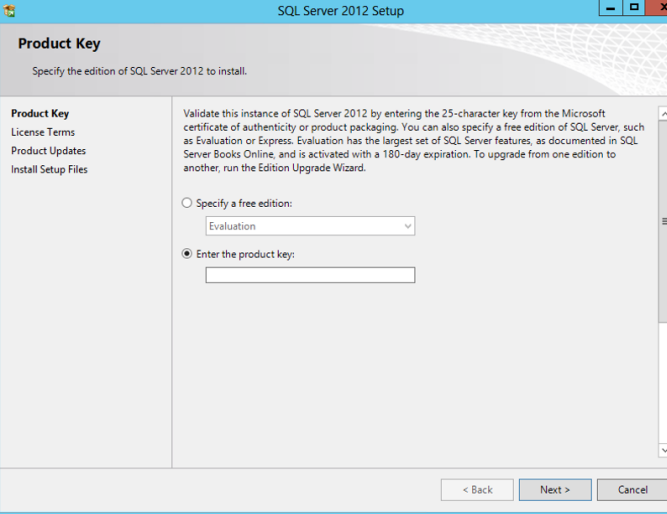


If the **View detailed report** link is selected, the following report is available.

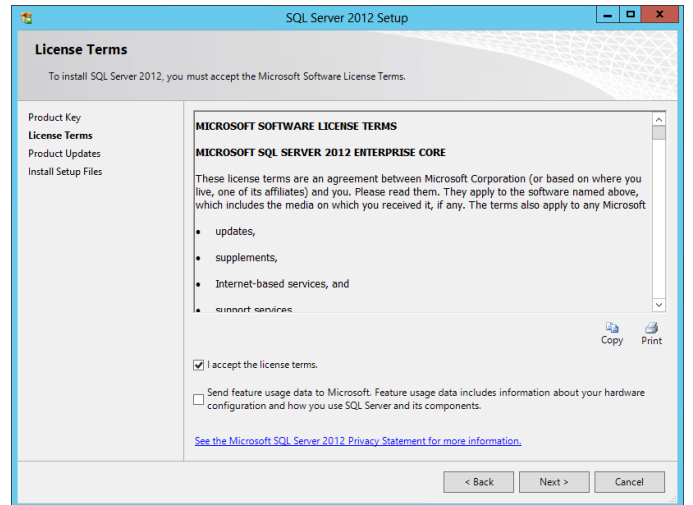


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

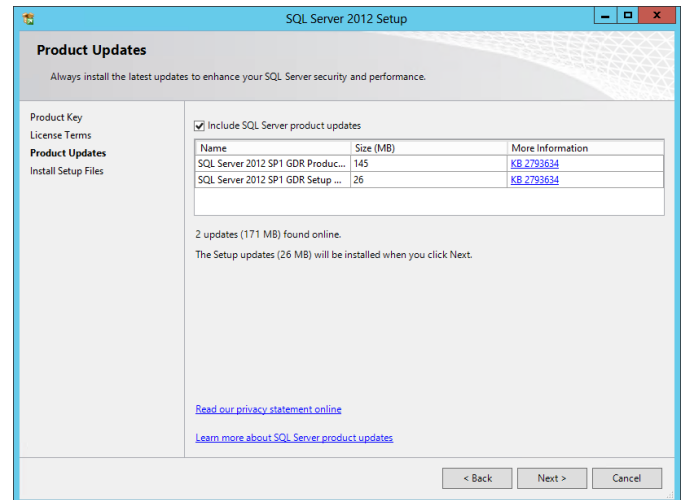
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



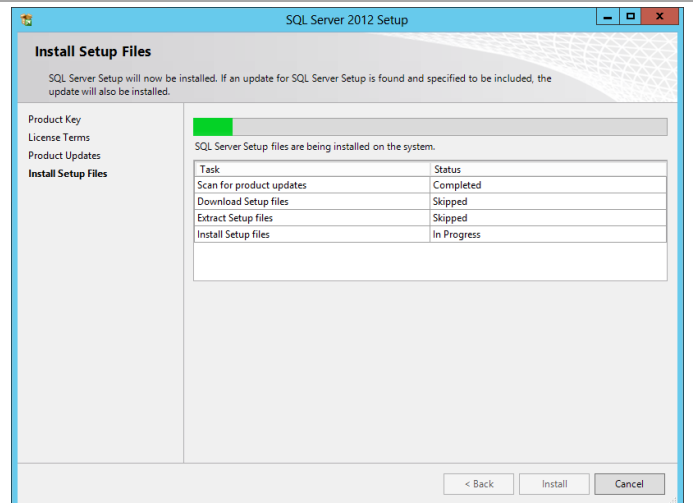
In the **License Terms** dialog, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box based on your organization's policies and click **Next** to continue.



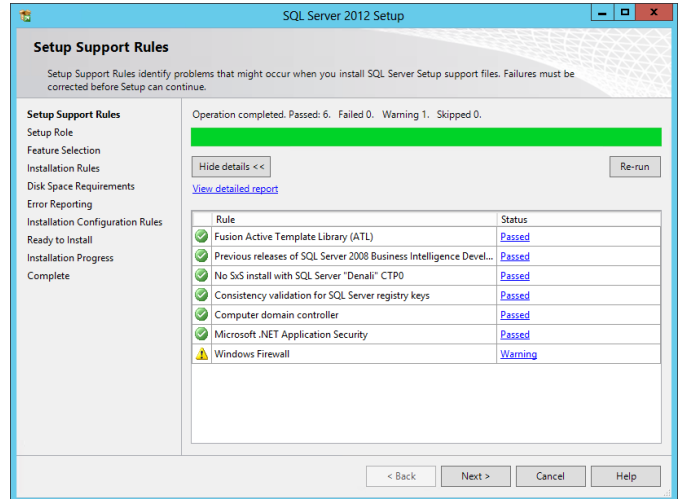
In the **Product Updates** dialog, select the **Include SQL Server product updates** checkbox and click **Next** to continue.



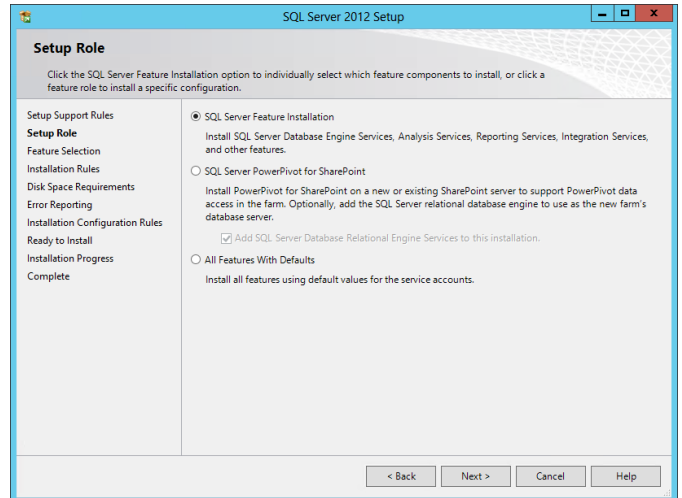
In the **Install Setup Files** dialog, click **Install** and allow the support files to install.



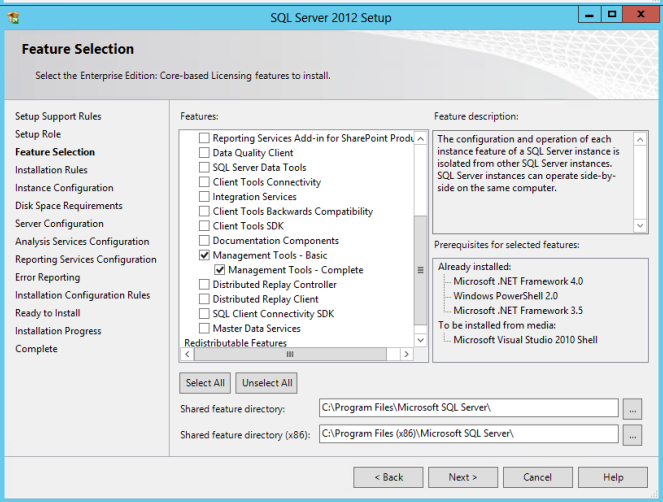
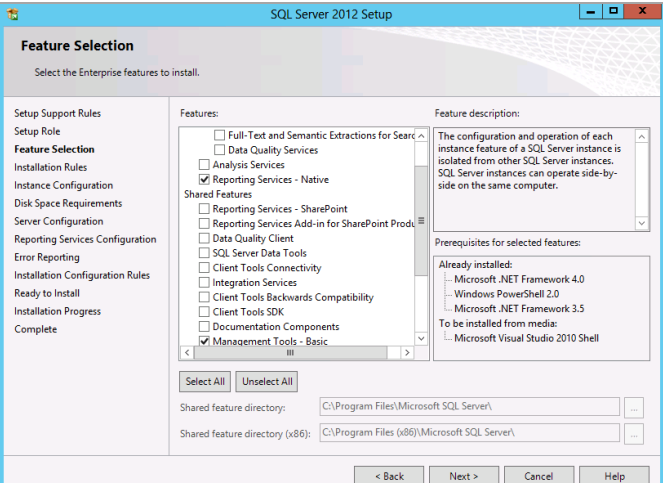
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Note that common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System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



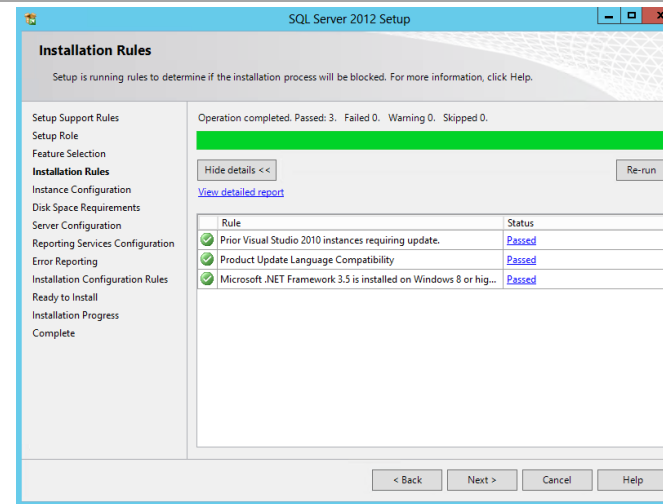
In the **Setup Role** dialog, select the **SQL Server Feature Installation** radio button and click **Next** to continue.



In the **Feature Selection** dialog, select the **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.

SQL Server 2012 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

☒ Default instance
☐ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\ ...

Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS11.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back Next > Cancel Help

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

SQL Server 2012 Setup

Disk Space Requirements

Review the disk space summary for the SQL Server features you selected.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

Disk Usage Summary:

- Drive C: 2788 MB required, 112679 MB available
 - System Drive (C:\): 1439 MB required
 - Instance Directory (C:\Program Files\Microsoft SQL Server\): 532 MB required
 - Shared Install Directory (C:\Program Files\Microsoft SQL Server\): 817 MB required

< Back Next > Cancel Help

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.

SQL Server 2012 Setup

Server Configuration

Specify the service accounts and collation configuration.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

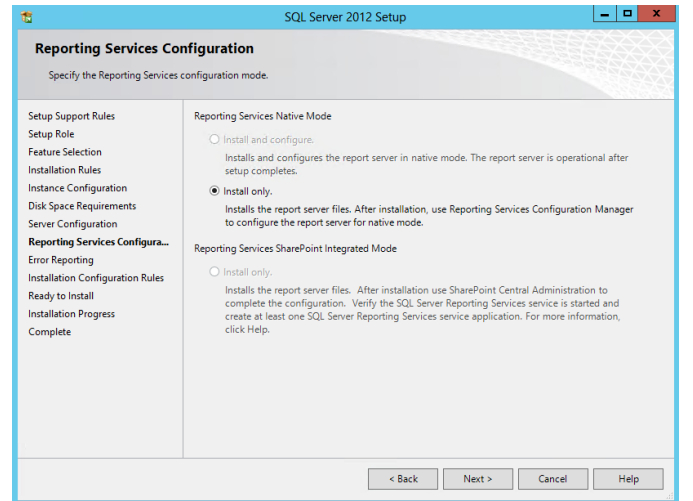
Service Accounts

Microsoft recommends that you use a separate account for each SQL Server service.

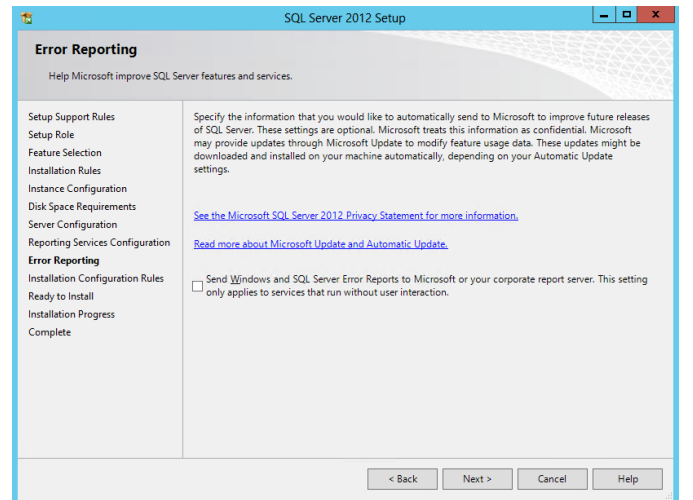
Service	Account Name	Password	Startup Type
SQL Server Reporting Services	NETWORK SERVICE		Automatic

< Back Next > Cancel Help

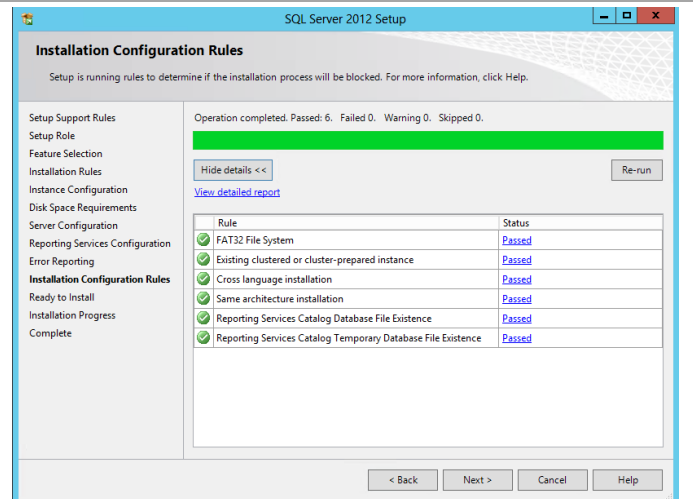
In the **Reporting Services Configuration** dialog, select the **Install only** option. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.



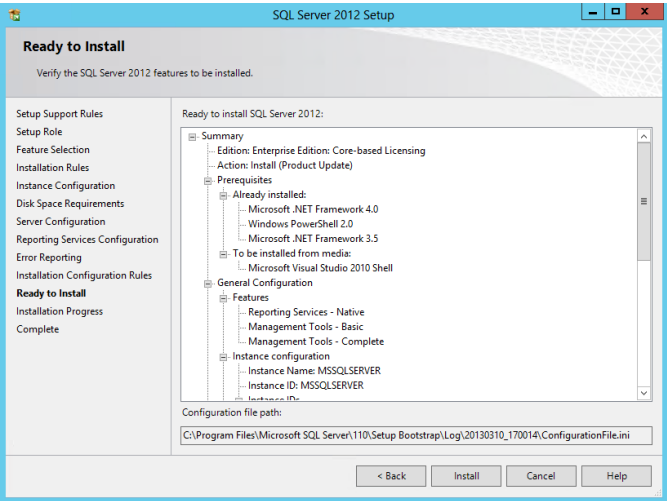
In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box based on your organization's policies and click **Next** to continue.



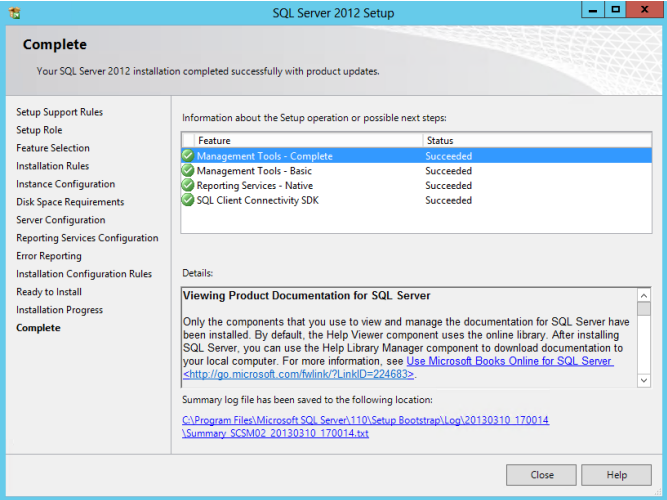
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



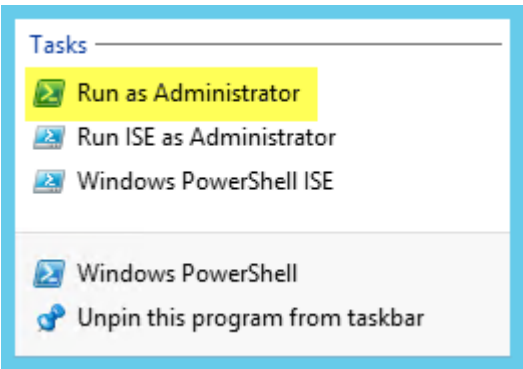
In the **Ready to Install** dialog, verify all of the settings that were entered during the setup process and click **Install** to begin the installation of the SQL Server instance.



Once 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

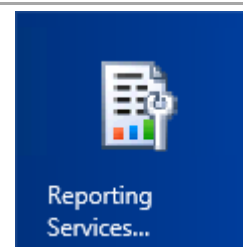
Name                : (26898efb-90e5-4c43-825b-3e36404b9258)
DisplayName          : SQL Reporting Services
Description          :
DisplayGroup         :
Group               :
Enabled              : True
Profile              : Any
Platform             : {}
Direction           : Inbound
Action              : Allow
EdgeTraversalPolicy  : Block
LoadSourceMapping    : 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. Once verified, close the MMC console.

Inbound Rules						
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	

Once 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.



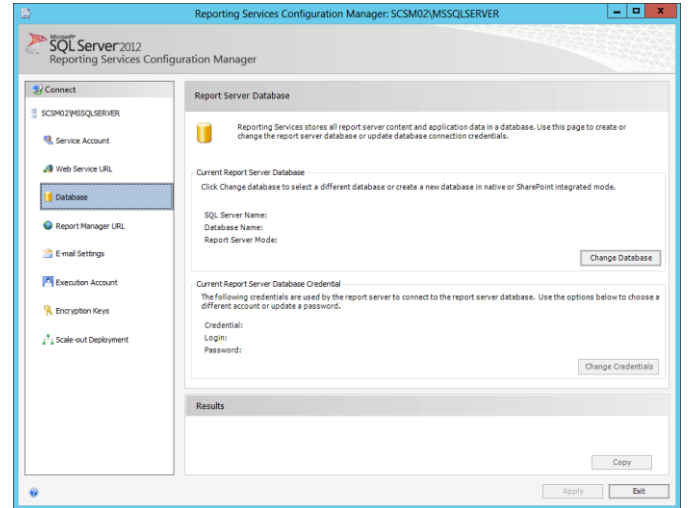
The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** text box, specify the name of the Service Manager server. In the **Report Server Instance** text box, use the default **MSSQLSERVER** drop-down menu value. Click **Connect**.

 A dialog box titled "Reporting Services Configuration Connection" with a Microsoft SQL Server 2012 Reporting Services logo. It contains a "Server Name" text box with "SCSM02" and a "Find" button. Below it is a "Report Server Instance" dropdown menu with "MSSQLSERVER" selected. At the bottom are "Connect" and "Cancel" buttons.

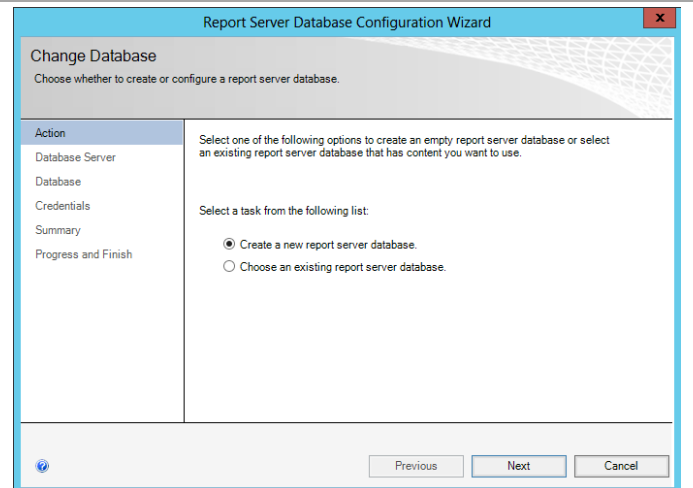
The **Reporting Services Configuration Manager** tool will appear.

 The Reporting Services Configuration Manager console window. The left pane shows a tree view with "Connect" selected. The right pane shows the "Report Server Status" for "SCSM02\MSSQLSERVER". It displays details like "SQL Server Instance: MSSQLSERVER", "Instance ID: MRSR11\MSSQLSERVER", "Edition: Enterprise Edition: Core-Based Licensing", "Product Version: 11.0.3128.0", "Report Server Database Name", "Report Server Mode", and "Report Service Status: Started". There are "Start" and "Stop" buttons. At the bottom are "Apply" and "Exit" buttons.

In the **Reporting Services Configuration Manager** tool, click the **Database** option from the toolbar. Within the **Current Report Server Database** section, click the **Change Database** button.



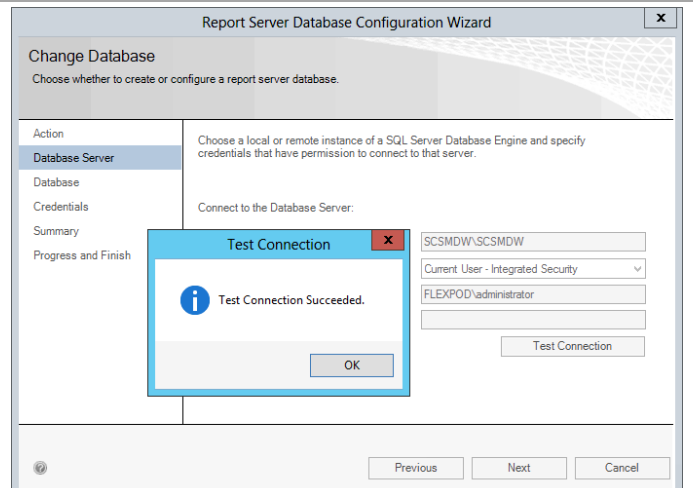
The **Reporting Services Database Configuration Wizard** will appear. In the **Action** section, choose the **Create a new report server database** option. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – *specify the name of the SQL Server Cluster SCSMDW Instance CNO and the database instance created for the Service Manager Data Warehouse installation.*
- **Authentication Type** – *specify **Current User** – **Integrated Security** from the drop-down menu.*

Click the **Test Connection** button to verify the credentials and database connectivity. Once verified, click **Next** to continue.



In the **Database** section, specify the following values:

- **Database Name** – *accept the default value of ReportServer.*
- **Language** – *specify the desired language option from the drop-down menu.*
- **Report Server Mode** – *select the **Native Mode** option.*

Click **Next** to continue.

Report Server Database Configuration Wizard

Change Database

Choose whether to create or configure a report server database.

Action	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 Server	
Database	
Credentials	
Summary	
Progress and Finish	

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 **Windows Credentials** from the drop-down menu. Enter the **System Center Service Manager Service account** and password. Click **Next** to continue.

Report Server Database Configuration Wizard

Change Database

Choose whether to create or configure a report server database.

Action	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.
Database Server	
Database	
Credentials	
Summary	
Progress and Finish	

Credentials:

Authentication Type: Windows Credentials

User name (Domain\user): FLEXPOD\FT-SCSM-SVC

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.

The following information will be used to create a new report server database. Verify this information is correct before you continue.

Action	
Database Server	
Database	
Credentials	
Summary	
Progress and Finish	

SQL Server Instance: scsmdw/scsmdw

Report Server Database: ReportServer

Temp Database: ReportServerTempDB

Report Server Language: English (United States)

Report Server Mode: Native

Authentication Type: Windows Account

Username: FLEXPOD\FT-SCSM-SVC

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**.

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

Please wait while the Report Server Database Configuration wizard configures the database. This might take several minutes to complete.

Verifying database sku	Success
Generating database script	Success
Running database script	Success
Generating rights scripts	Success
Applying connection rights	Success
Setting DSN	Success

Previous

Finish

Cancel

In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and report server database credentials specified in the wizard.

Reporting Services Configuration Manager: SCSDM02\MSSQLSERVER

SQL Server 2012

Reporting Services Configuration Manager

Connect

SCSDM02\MSSQLSERVER

Service Account

Web Service URL

Database

Report Manager URL

E-mail Settings

Execution Account

Encryption Keys

Scale-out Deployment

Report Server Database

Reporting Services stores all report server content and application data in a database. Use this page to create or change the report server database or update database connection credentials.

Current Report Server Database

Click Change database to select a different database or create a new database in native or SharePoint integrated mode.

SQL Server Name:scsdm02\scsdm02

Database Name:ReportServer

Report Server Mode:Native

Change Database

Current Report Server Database Credential

The following credentials are used by the report server to connect to the report server database. Use the options below to choose a different account or update a password.

Credential:Windows Account

Login:FLEXPD01FT-SCSM-SVC

Password:*****

Change Credentials

Results

Copy

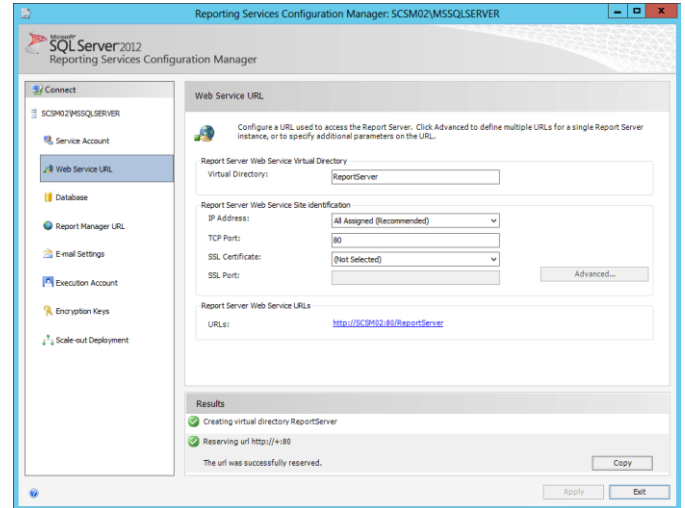
Apply

Exit

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).

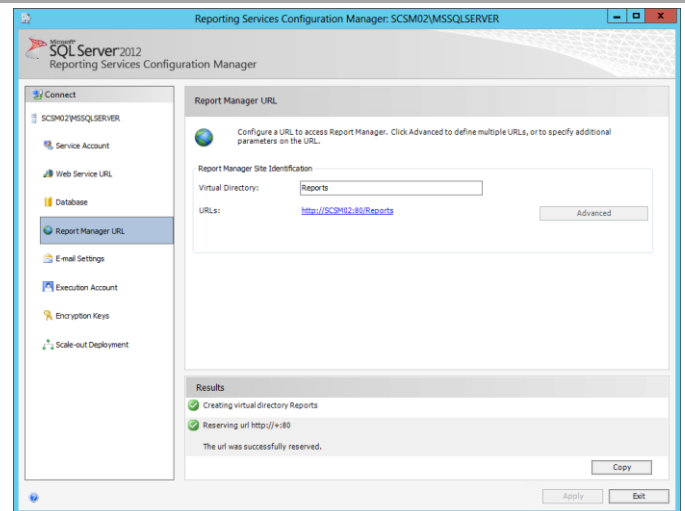
Click the **Apply** button to save the settings and create the Web Service URL.



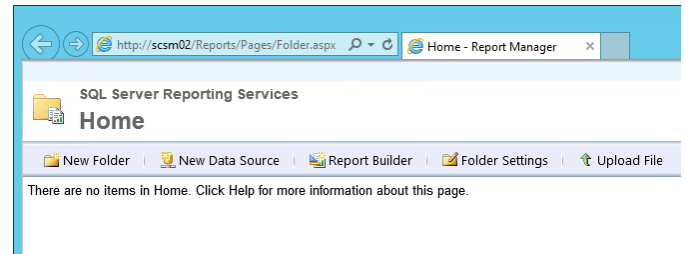
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

- 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.

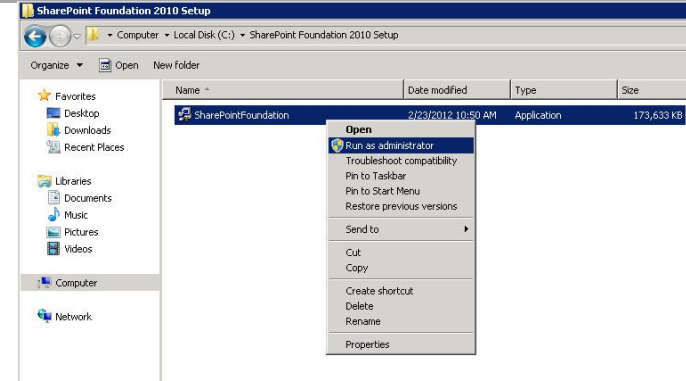


<p>Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.</p> <p><i>Note that in order to test the URL directory from the Service Manager server, Internet Explorer Enhanced Security Configuration will need to be temporarily disabled.</i></p>	
<p>Close the Reporting Server Configuration Manager.</p>	

Install SharePoint Foundation 2010 Service Pack 1 on the Self-Service Portal Server

SharePoint Foundation 2010 SP1 must be installed to allow for configuration of SharePoint with the SQL Server 2012 installation. The following steps must to be completed in order to install SharePoint Foundation 2010 SP1 on the Service Manager self-service portal server only.

► Perform the following steps on the **Service Manager self-service portal (SCSM03)** virtual machine.

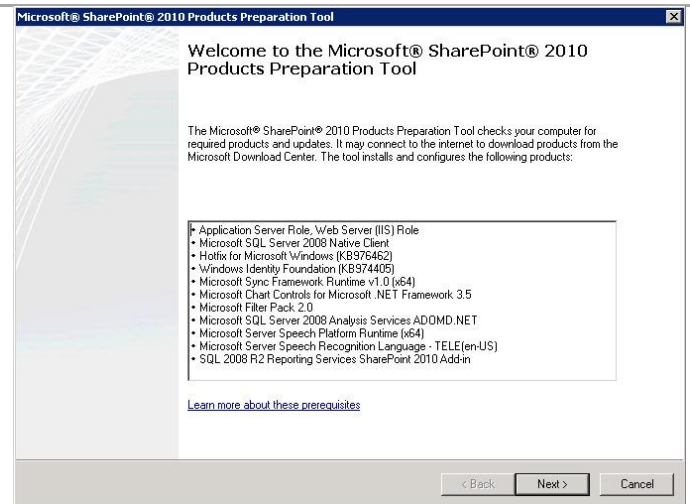
<p>Log on to Service Manager self-service portal server (NOT a Service Manager management server or the Data Warehouse server). Locate the SharePoint Foundation 2010 installation file. Right-click SharePointFoundation.exe and select Run as administrator from the context menu to begin setup.¹⁶</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

¹⁶ Microsoft SharePoint Foundation 2010 - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5970>.

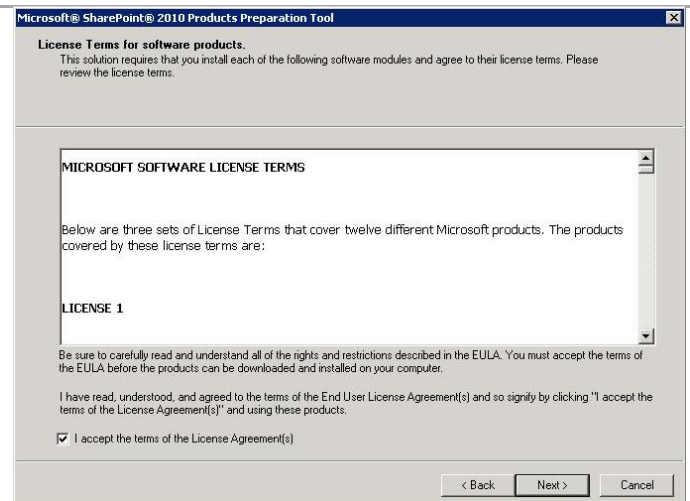
The **SharePoint Foundation 2010** setup dialog will appear. In the **Install** section, select **Install software prerequisites**.



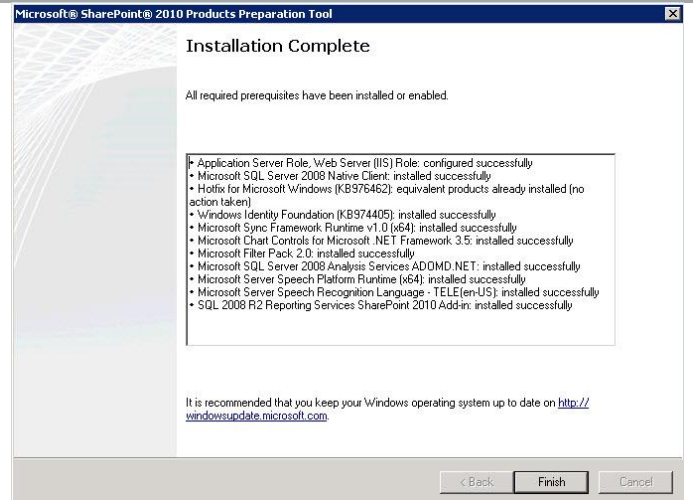
The **Microsoft SharePoint 2010 Products Preparation Tool** will open. Click **Next** to continue.



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.



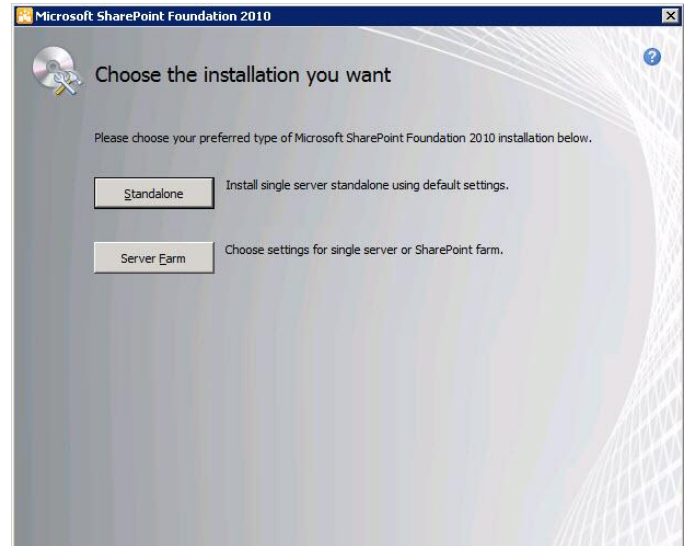
After the system restart, log back on with an account with administrative privileges. Re-launch the SharePoint Foundation 2010 installation. In the **SharePoint Foundation 2010** setup dialog, navigate to the **Install** section and select **Install SharePoint Foundation**.



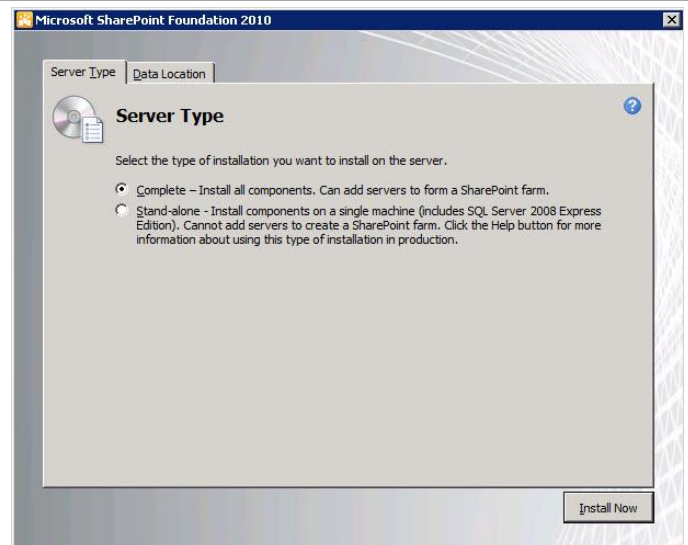
In the **Read the Microsoft Software License Terms** dialog, verify that the **I accept the terms of this Agreement** installation option checkbox is selected and click **Continue**.



In the **Choose the installation you want** dialog, click the **Server Farm** button.

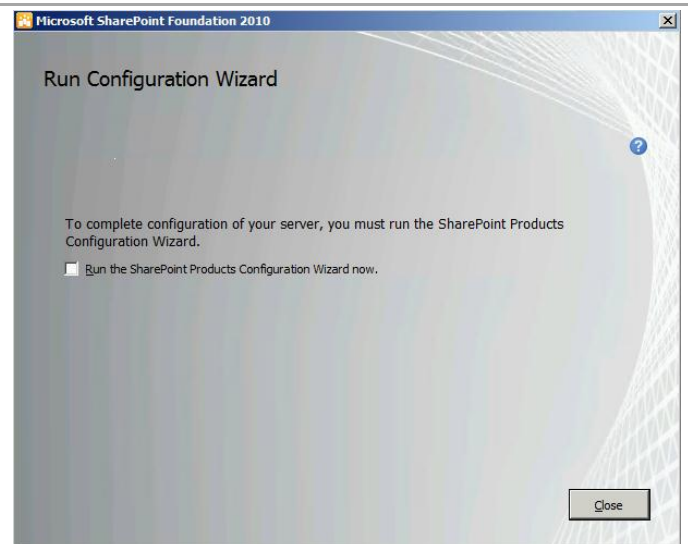


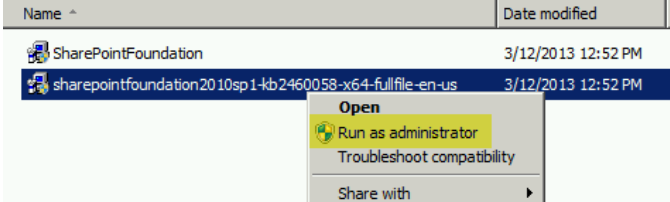
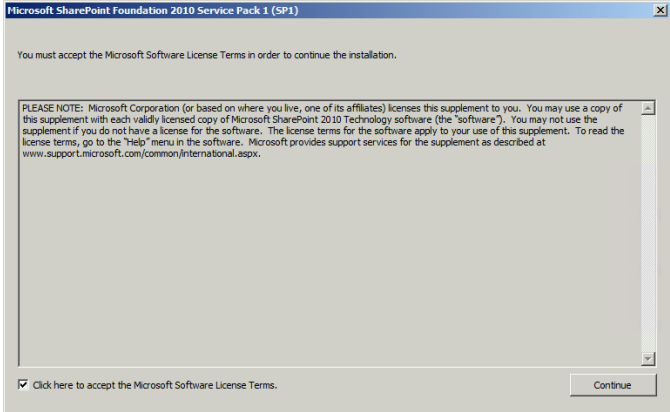
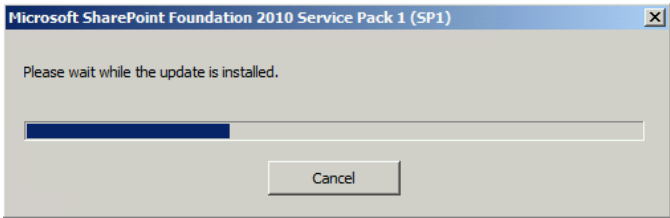
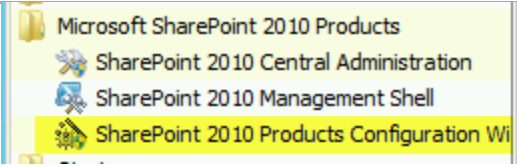
In the **Server Type** dialog, select the **Complete** option and click **Install Now**.



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**.

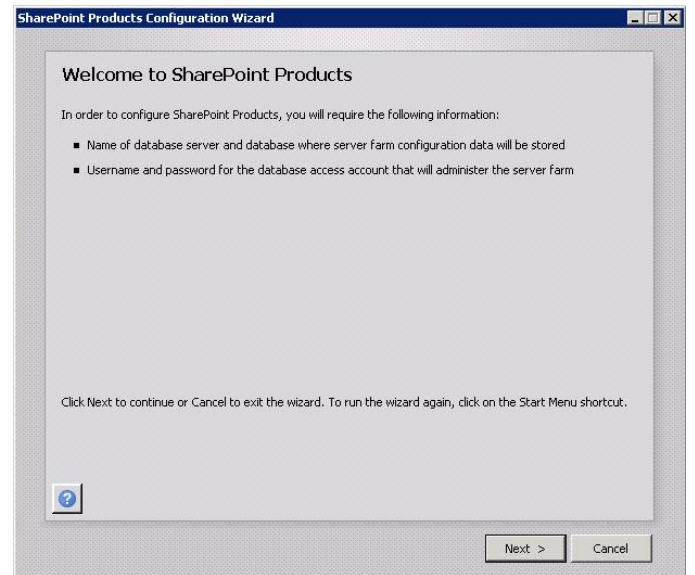
Important Note: SharePoint Foundation Server 2010 Service Pack 1 must be installed prior to the configuration wizard being run.



<p>Service Pack 1 <u>must</u> be applied to SharePoint Foundation server after this installation.¹⁷</p> <p>Locate the Service Pack 1 for SharePoint Foundation 2010 installation file, right-click the installation file and select Run as administrator from the context menu to begin the Service Pack setup.</p>	
<p>The Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1) wizard will appear. Verify that the Click here to accept the Microsoft Software License Terms installation option check box is selected and click Continue.</p>	
<p>The installation will continue without interaction until it completes. When prompted, click OK to complete the installation. You must restart the system after the service pack installation.</p>	
<p>From the Start menu, expand the Microsoft SharePoint 2010 Products program folder and select SharePoint 2010 Products Configuration Wizard.</p>	

¹⁷ Microsoft SharePoint Foundation 2010 SP1 - <http://www.microsoft.com/download/en/details.aspx?id=26640>.

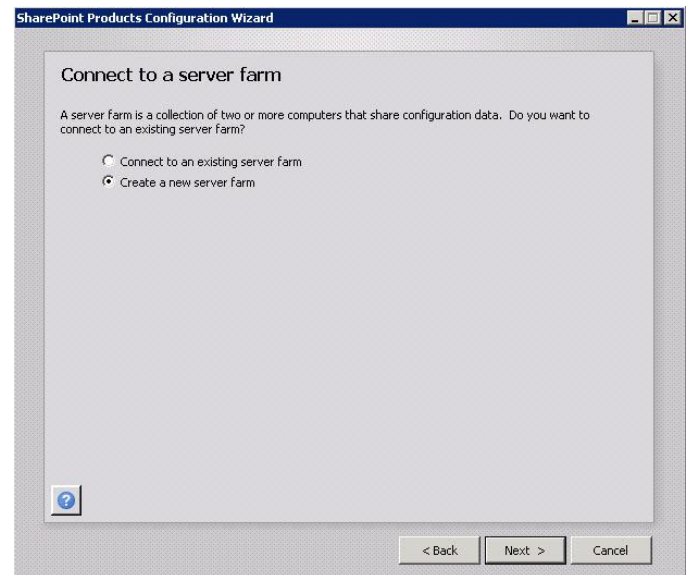
The **SharePoint Products Configuration Wizard** will appear. Click **Next** to continue with the wizard.



A dialog will appear that states that some services require restart as part of the installation. Click **Yes** to perform the services restart.



The **Connect to a server farm** dialog will appear. Select the **Create a new server farm** option and click **Next** to continue.



In the **Specify Configuration Database Settings** dialog, specify the following information in the provided text boxes:

- **Database server** – *specify the name of the SQL Server CNO and the database instance created for the Service Manager installation.*
- **Database name** – *specify the name of the SharePoint database. In most cases the default value of SharePoint_Config should be used.*

In the **Specify Database Access Account** section, specify the Username (<DOMAIN>\<USERNAME>) and associated password for the Service Manager service account. Once complete, click **Next** to continue.

In the **Specify Farm Security Settings** dialog, enter a unique passphrase in the **Passphrase** text box. Re-type the passphrase in the **Confirm passphrase** text box and click **Next** to continue.

The screenshot shows the 'Specify Configuration Database Settings' dialog box within the 'SharePoint Products Configuration Wizard'. It contains two text input fields: 'Database server' with the value 'SCDB\SCDB' and 'Database name' with the value 'SharePoint_Config'. Below these is the 'Specify Database Access Account' section, which includes a 'Username' field with 'FLEXPOD\FT-SQL-SVC' and a 'Password' field with masked characters. A help icon is in the bottom left, and '< Back', 'Next >', and 'Cancel' buttons are in the bottom right.

The screenshot shows the 'Specify Farm Security Settings' dialog box within the 'SharePoint Products Configuration Wizard'. It contains two text input fields: 'Passphrase' and 'Confirm passphrase', both with masked characters. A help icon is in the bottom left, and '< Back', 'Next >', and 'Cancel' buttons are in the bottom right.

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.

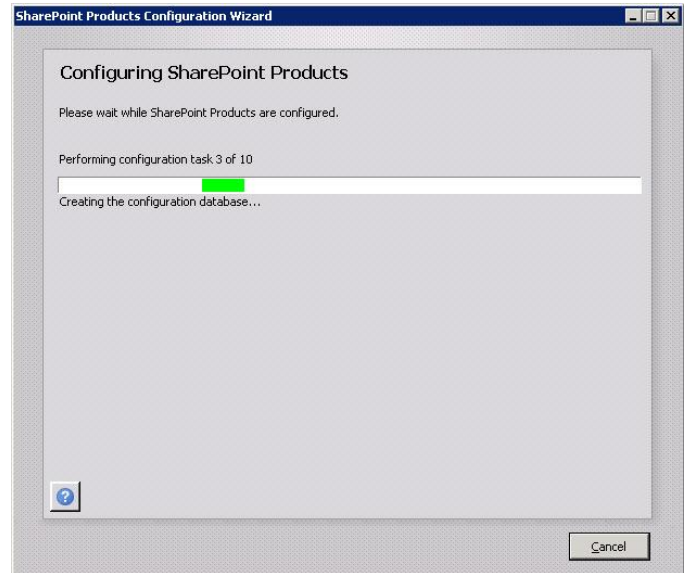
Once completed, click **Next** to continue.

The screenshot shows the 'SharePoint Products Configuration Wizard' window. The main title is 'Configure SharePoint Central Administration Web Application'. Below the title, there is a descriptive paragraph about the web application. A checkbox labeled 'Specify port number:' is checked, and the text box next to it contains '21902'. Below this, the 'Configure Security Settings' section is visible. It explains that Kerberos is the recommended security configuration but that NTLM authentication will be used. There are two radio buttons: 'NTLM' (which is selected) and 'Negotiate (Kerberos)'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

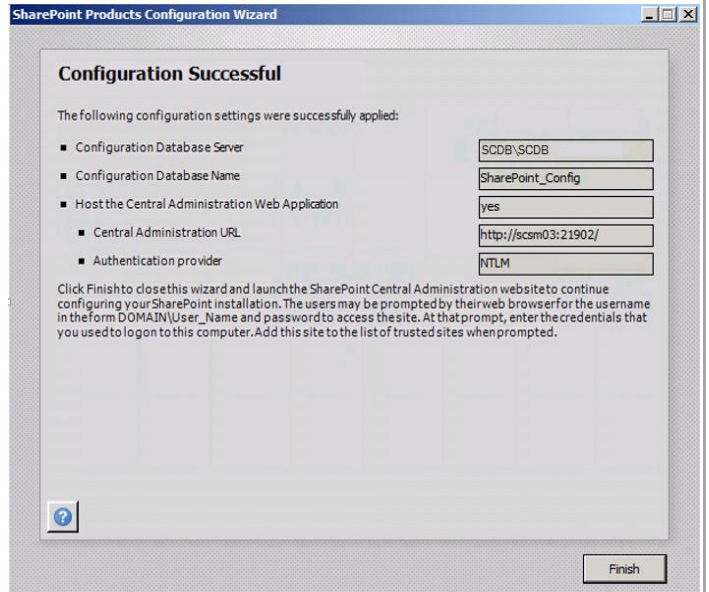
The **Completing the SharePoint Products Configuration Wizard** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Next** to continue.

The screenshot shows the 'SharePoint Products Configuration Wizard' window. The main title is 'Completing the SharePoint Products Configuration Wizard'. Below the title, it states 'The following configuration settings will be applied:'. There is a list of settings with their corresponding values in text boxes: 'Configuration Database Server' is 'SCDB\SCDB', 'Configuration Database Name' is 'SharePoint_Config', 'Host the Central Administration Web Application' is 'yes', 'Central Administration URL' is 'http://scsm03:21902/', and 'Authentication provider' is 'NTLM'. Below the list, there is a button labeled 'Advanced Settings'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

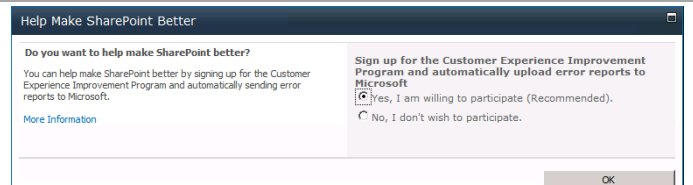
The wizard will display the progress while performing the SharePoint configuration.



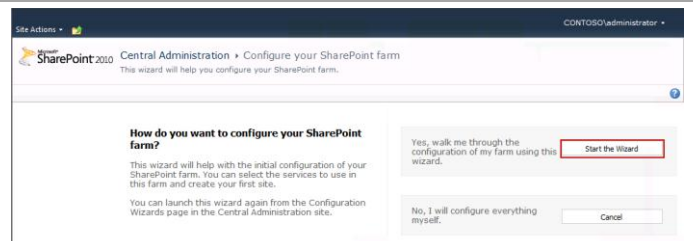
Once successful, the **Configuration Successful** dialog will appear. Click **Finish** to complete the configuration of SharePoint Foundation 2010 Service Pack 1.



When prompted in the **Help Make SharePoint Better** page, select the appropriate option based on your organization's policies and click **OK** to save this setting.



In the **Central Administration - Configure your SharePoint farm** page, click the **Start the Wizard** button to begin the SharePoint configuration.



In the **Service Account** section, select the **Use existing managed account** and select the Service Manager Service Account from the drop-down menu.

In the **Services** section, select the **Business Data Connectivity Services** and **Usage and Health data collection** check boxes.

Click **Next** to continue.

Initial Farm Configuration Wizard - Windows Internet Explorer

Site Actions • FLEXPOD\administrator •

SharePoint 2010 Central Administration • Configure your SharePoint farm

Select the services you want to run in your farm. The services you select below will run with default settings on all servers in your farm.

Service Account

Services require an account to operate. For security reasons, it is recommended that you use an account that's different from the farm admin account.

☒ Use existing managed account
FLEXPOD\VT-SQL-SVC

☐ Create new managed account
User name: _____
Password: _____

Services

Select the services you want to run in your farm. The services you select below will run with default settings on all servers in your farm.

☒ Business Data Connectivity Service
Enabling this service provides the SharePoint farm with the ability to upload BDC models that describe the interfaces of your enterprise's line of business systems and thereby access the data within these systems.

☒ Usage and Health data collection
This service collects farm wide usage and health data and provides the ability to view various usage and health reports.

Next Cancel

In the Web Site configuration page, click the **Skip** button to continue without configuring these settings.

Site Actions • CONTOSO\administrator •

SharePoint 2010 Central Administration • Configure your SharePoint farm

Use this page to create a new top-level Web site.

Skip OK Cancel

Title and Description

Type a title and description for your new site. The title will be displayed on each page in the site.

Title: _____
Description: _____

Web Site Address

Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

URL: http://scsm03/

To add a new URL Path go to the [Define Managed Paths](#) page.

The SharePoint farm configuration is now complete. Click the **Finish** button to exit.

Site Actions • CONTOSO\administrator •

SharePoint 2010 Central Administration • Configure your SharePoint farm

This completes the Farm Configuration Wizard.

Details of this SharePoint farm:

Site Title: N/A
Site URL: N/A

Service Applications:

- Security Token Service Application
- Application Discovery and Load Balancer Service Application
- Usage and Health Data Collection Service Application
- Business Data Connectivity Service Application

Click Finish to continue to the SharePoint Central Administration page where you can continue configuring other settings for your farm.

To return to this wizard, or access additionally installed wizards, click 'Configuration Wizards' in the left navigation pane.

Finish

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.

Home - Central Administration - Windows Internet Explorer

Site Actions • Browse Page Administrator •

SharePoint 2010 Central Administration

Central Administration

- Application Management
 - Manage web applications
 - Create site collections
 - Manage service applications
 - Manage content databases
- Monitoring
 - Review problems and solutions
 - Check job status
- Security
 - Manage the farm administrators group
 - Configure service accounts
- General Application Settings
 - Configure send to connections

System Settings

- Manage servers in this farm
- Manage services on server
- Manage farm features
- Configure alternate access mappings

Backup and Restore

- Perform a backup
- Restore from a backup
- Perform a site collection backup

Upgrade and Migration

- Check product and patch installation status
- Check upgrade status

Configuration Wizards

Resources

There are currently no favorite links to display. To add a new link, click "Add new link".

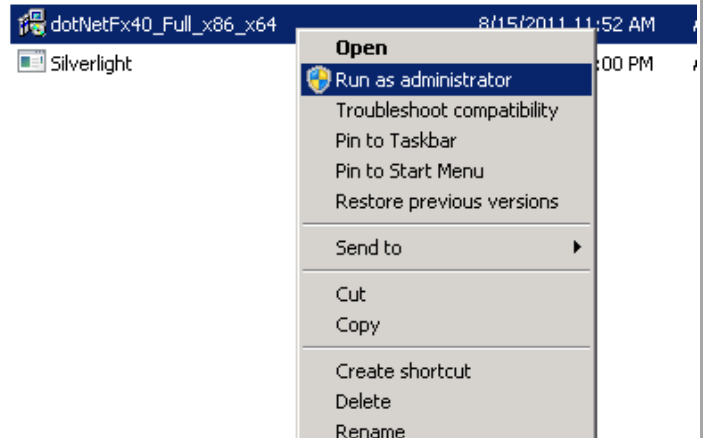
[Add new link](#)

Install .NET Framework 4 on the Self-Service Portal Server

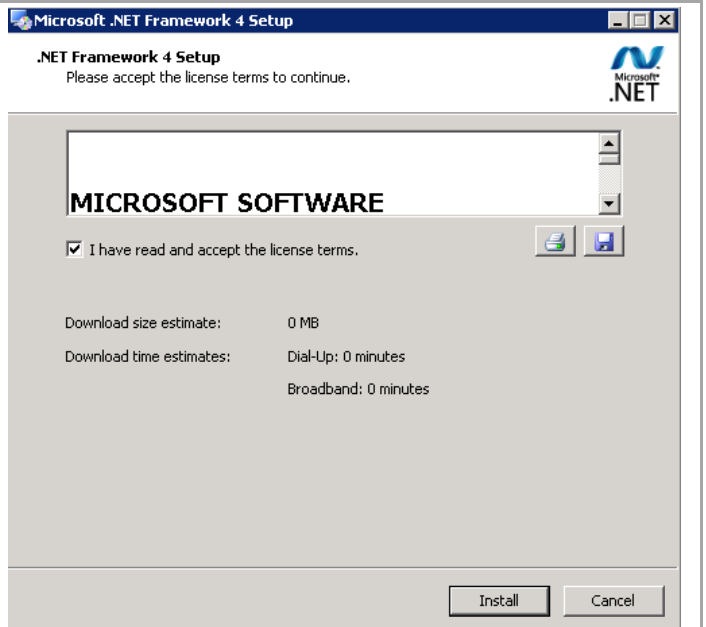
Additionally, the Service Manager self-service portal installation also requires the .NET Framework 4 package to be installed prior to installation. Follow these steps to install the .NET Framework 4 on the self-service portal.

► Perform the following steps on the **Service Manager self-service portal (SCSM03)** virtual machine.

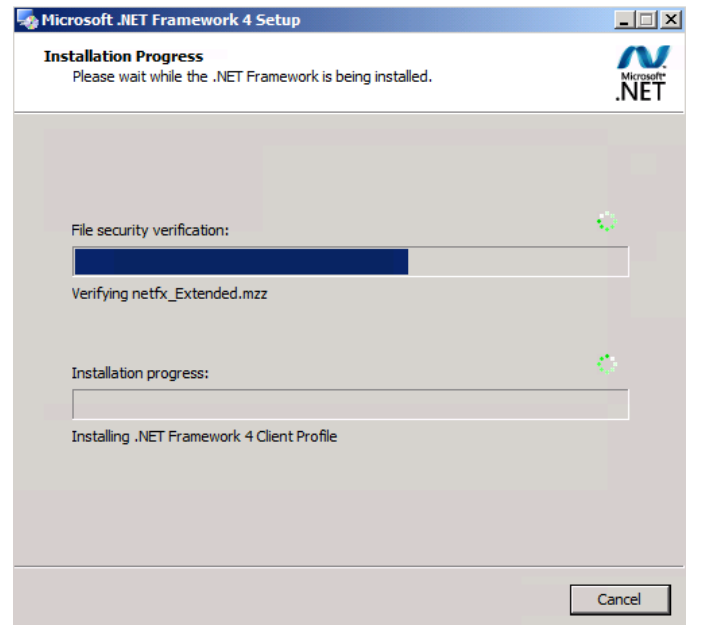
From the installation media source, right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** from the context menu to begin setup.



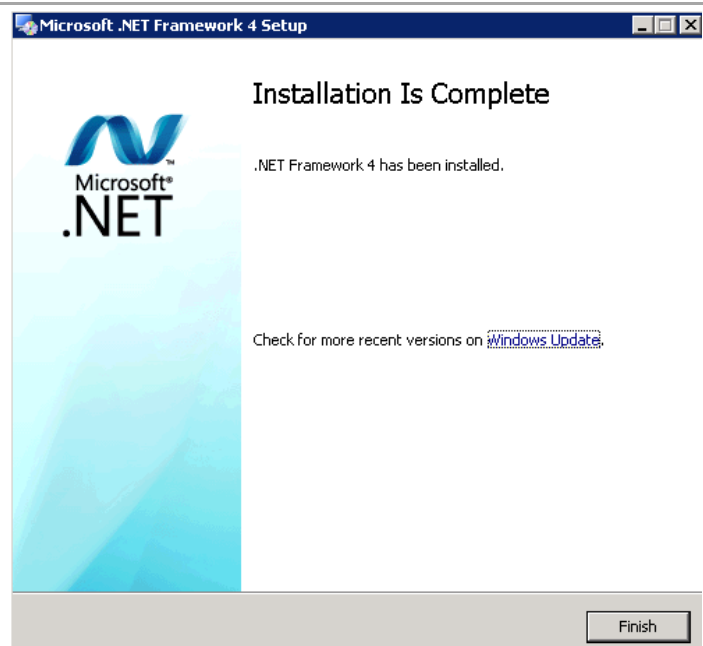
Within the **Microsoft .NET Framework 4 Setup** dialog, select the **I have read and accept the license terms** checkbox and click **Install** to begin the installation.



The installation progress will be displayed in the setup wizard.



Once completed, click **Finish** to exit the installation.



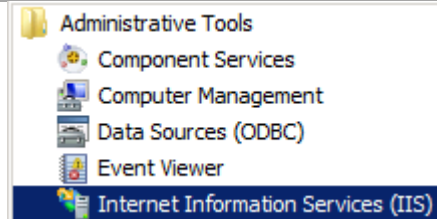
Request and Install an SSL Certificate on the Self-Service Portal Server

Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website.¹⁸ 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.

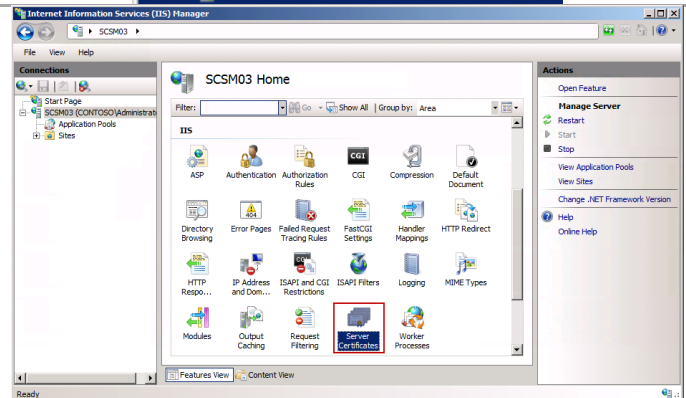
¹⁸ SSL Certificates for the self-service portal - <http://technet.microsoft.com/en-us/library/hh667343.aspx>.

► Perform the following steps on the **Service Manager self-service portal (SCSM03)** virtual machine.

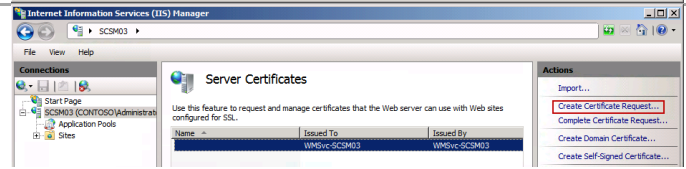
Log on to the Service Manager virtual machine with a user with local admin rights. From the Start Menu select **Administrative Tools** then select **Internet Information Services (IIS) Manager**.



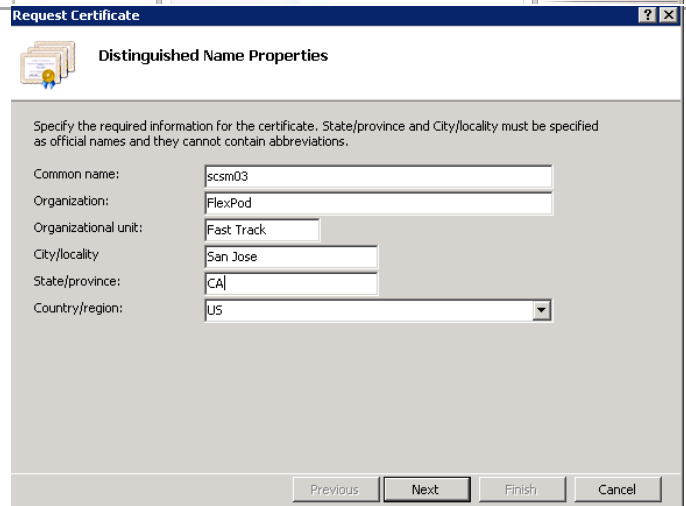
In the **Internet Information Services (IIS) Manager** console, select the server node and in the IIS section, double-click **Server Certificates**.



The **Server Certificates** pane will expand. Under actions, click **Create Certificate Request...**



The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name that the server will be accessed in the web browser. Click **Next** to continue.



In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing certification authority (CA). In most cases, selecting the default CSP and default bit length is satisfactory. Click **Next** to continue.

The screenshot shows the 'Request Certificate' wizard window with the title 'Cryptographic Service Provider Properties'. It contains instructions: 'Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' Below this, there are two dropdown menus: 'Cryptographic service provider:' set to 'Microsoft RSA SChannel Cryptographic Provider' and 'Bit length:' set to '1024'. At the bottom are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

Once completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.

The screenshot shows the 'Request Certificate' wizard window with the title 'File Name'. It contains the instruction: 'Specify the file name for the certificate request. This information can be sent to a certification authority for signing.' Below this, there is a text box labeled 'Specify a file name for the certificate request:' containing 'C:\scsm03.req' and a browse button (...). At the bottom are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

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 screenshot shows the 'Internet Information Services (IIS) Manager' console. The 'Server Certificates' feature is selected in the left-hand 'Connections' pane. The main area shows a table with columns 'Name', 'Issued To', and 'Issued By', containing one entry for 'WINGV-SCSM03'. On the right, the 'Actions' pane is visible, with 'Complete Certificate Request...' highlighted in red.

The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Click **OK** to complete the operation.

The screenshot shows the 'Complete Certificate Request' wizard window with the title 'Specify Certificate Authority Response'. It contains the instruction: 'Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.' Below this, there are two text boxes: 'File name containing the certification authority's response:' containing 'C:\SCSM03\Cert.cer' and a browse button (...), and 'Friendly name:' containing 'SCSM03'. At the bottom are two buttons: 'OK' and 'Cancel'.

In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.

Connections

Start Page

SCSM03 (FLEXPOD)administrator

Application Pools

Sites

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

No...	Issued To	Issued By	Expiration Date	Certificate Hash
	WM5vc-SCSM03	WM5vc-SCSM03	10/15/2023 11:11:...	0F5598387B062165E
SCSM03	scsm03	flexpod-SCINFRA-CA	10/18/2015 1:39:2...	EA086E07E52BA826C

Configuration of Service Manager Environmental Prerequisites

The following steps must to be completed in order to install the Service Manager roles correctly.

► Perform the following steps on **all Service Manager Servers** virtual machines.

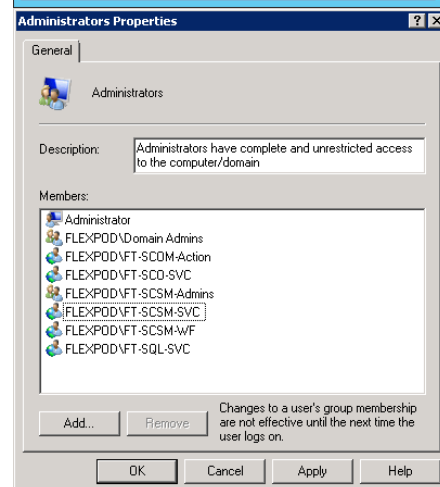
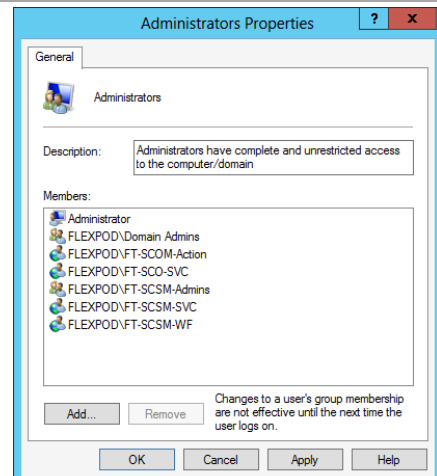
Log on to each Service Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on each Service Manager virtual machine:

- Operations Manager action account.
- Service Manager workflow account.
- Service Manager service account.
- Service Manager Admins group.
- Orchestrator service account.

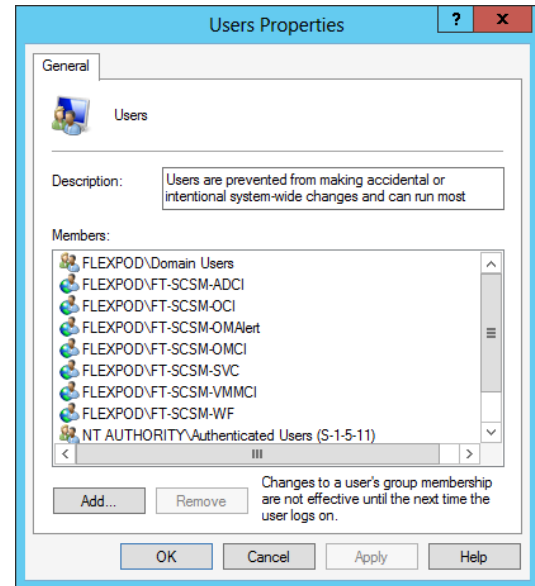
On the self-service portal server, also add the following accounts:

- SQL service account



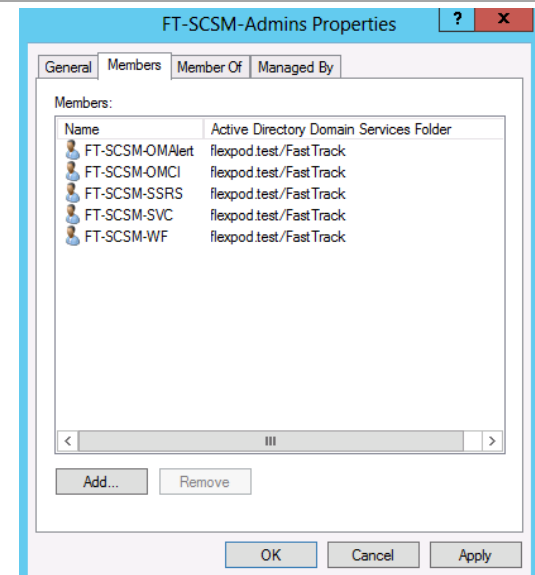
Verify that the following accounts and/or groups are members of the Local Users group on each Service Manager virtual machine:

- Service Manager Active Directory CI connection account.
- Service Manager Orchestrator CI connection account.
- Service Manager Operations Manager alert connection account.
- Service Manager Operations Manager CI connection account.
- Service Manager service account.
- Service Manager users group.
- Service Manager Virtual Machine Manager CI connection account.
- Service Manager workflow account.

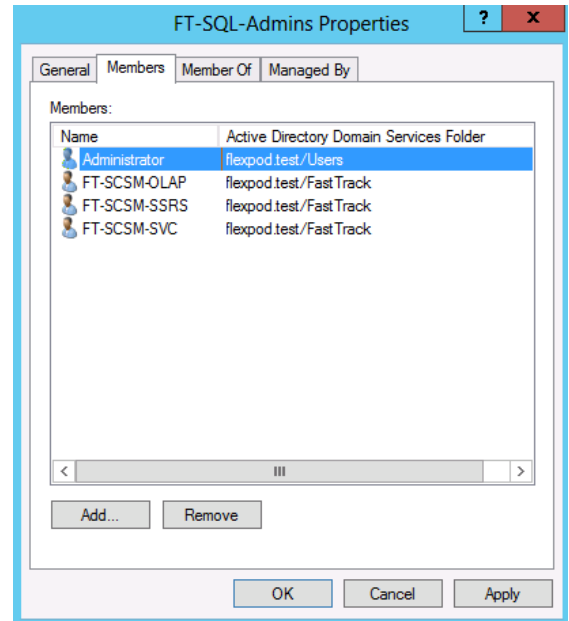


► Perform the following step on an **Active Directory Domain Controller** in the target environment.

In the domain where Service Manager will be installed, verify that the SM Operations Manager alert connectors and the Service Manager service accounts are members of the SM Admins group created earlier.

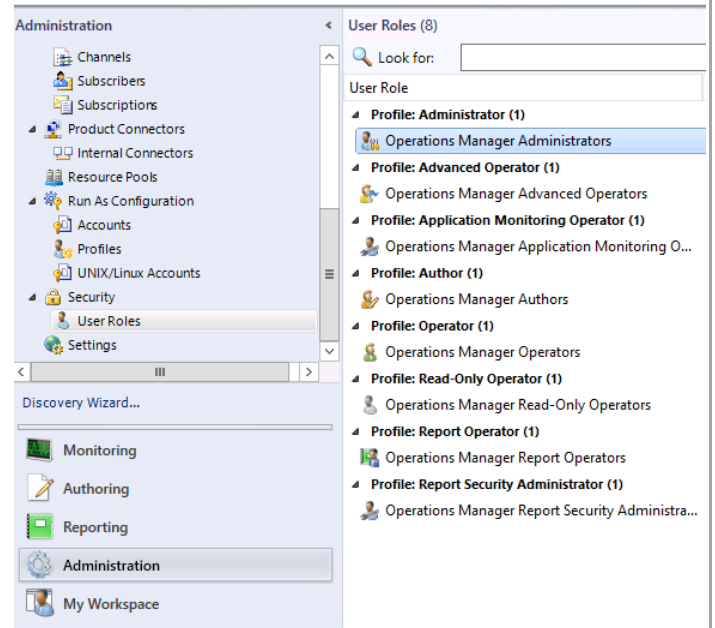


In the domain where Service Manager will be installed, verify that the SM OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group created earlier.



► Perform the following steps on the **Operations Manager** virtual machine.

Log on to the Operations Manager server as an Administrator. In the **Operations Manager console**, navigate to **Administration pane**. In the **Security** node under **User Roles** locate the **Operations Manager Administrators** role.



Click Properties and add the **SCSM Admins** group and **SCOM Admins** group to the role. Click **OK** to save the changes.

Operations Manager Administrators - User Role Properties

General Properties | Author Scope | Group Scope | Tasks | Dashboards and Views

General

User role name: Operations Manager Administrators

Description: The Operations Manager Administrators user role is created at setup time and cannot be deleted. This role must contain one or more global groups.

Profile: Administrator

Profile description: The Administrator profile includes full privileges to Operations Manager. No scoping of the Administrator profile is supported.

User role members:

+ Add... - Remove

Member Name	Domain
BUILTIN\Administrators	
FLEXPOT/FT-SCOM-Admins	
FLEXPOT/FT-SCSM-Admins	

OK Cancel Apply

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.

Operations Manager Operators - User Role Properties

General Properties | Group Scope | Tasks | Dashboards and Views

General

User role name: Operations Manager Operators

Description: The Operations Manager Operators user role is created at setup time, is globally scoped and cannot be deleted.

Profile: Operator

Profile description: The Operator profile includes a set of privileges designed for users that need access to Alerts, Views and Tasks. A role based on the Operators profile grants members the ability to interact with Alerts, execute Tasks and access Views according to their configured scope.

User role members:

+ Add... - Remove

Member Name	Domain
FLEXPOT/FT-SCSM-OMCI	

OK Cancel Apply

18.2 Installation

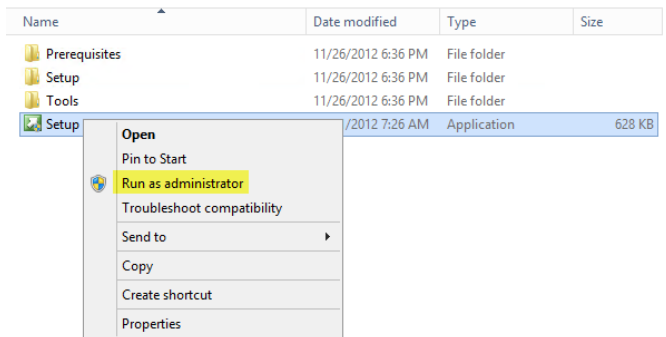
Install the Service Manager Management Server

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 or the self-service portal server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



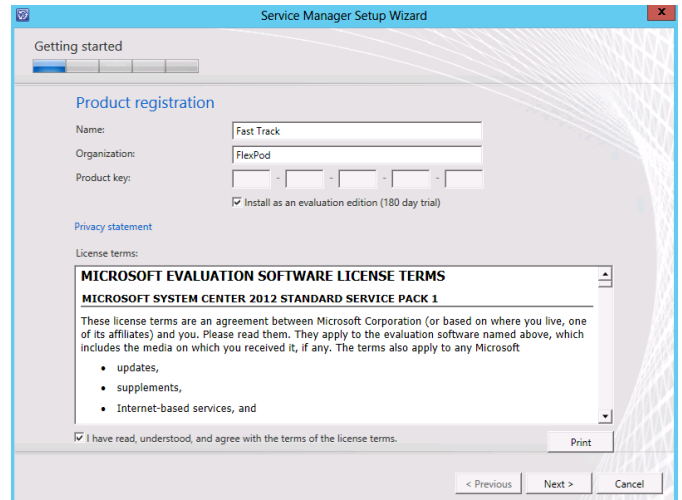
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager management server** to begin the Service Manager server installation.



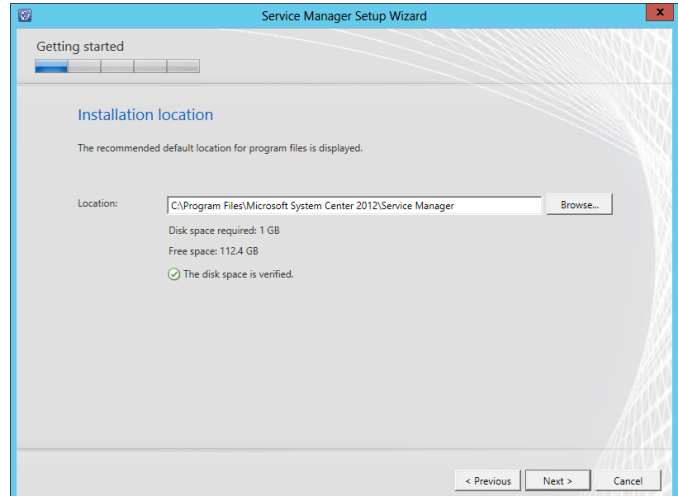
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name** – specify the name of the primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.
- **Product key** – provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.

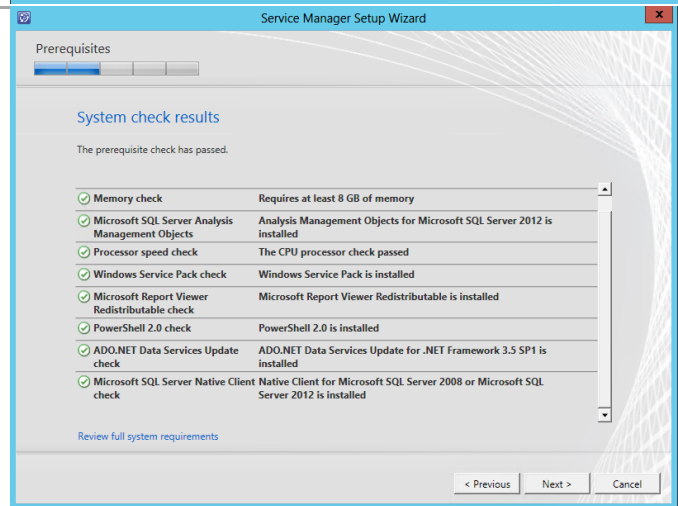
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. Once all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.



In the **Configure the Service Manager database** dialog, specify the following information in the provided text boxes:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation.*
- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation.*

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – *specify the name of the Service Manager database. In most cases the default value of ServiceManager should be used.*
- **Size (MB)** – *specify the initial database size¹⁹. 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 work sheet identified earlier.*
- **Log file folder** – *specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager database. This should be cross-checked with the work sheet identified earlier.*

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step titled 'Configure the Service Manager database'. The instructions state: 'First, specify the name of the server that hosts the instance of SQL Server 2008 that contains or will contain the Service Manager database. Then, select whether to create a new database or use an existing Service Manager database.' Below this, a note says 'Only supported instances are listed.' The 'Database server' field contains 'scsmdb' and the 'SQL Server instance' dropdown is set to 'SCSMDB'. Two radio buttons are present: 'Create a new database' (selected) and 'Use an existing database'. For the 'Create a new database' option, the 'Database name' is 'ServiceManager', the 'Size (MB)' is '2000', the 'Data file folder' is 'E:\MSSQL11.SCSMDB\MSSQL\DATA', and the 'Log file folder' is 'F:\MSSQL11.SCSMDB\MSSQL\DATA'. Both folder fields have 'Browse...' buttons. A blue information icon with a note states: 'Both folders are located on the scsmdb server.' At the bottom right are '< Previous', 'Next >', and 'Cancel' buttons.

¹⁹ 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.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure the Service Manager management group' step. The 'Management group name' text box contains 'FlexPod'. Below it, the 'Management group administrators' section shows a dropdown menu with 'FLEXPOD\FT-SCSM-Admins' selected. At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

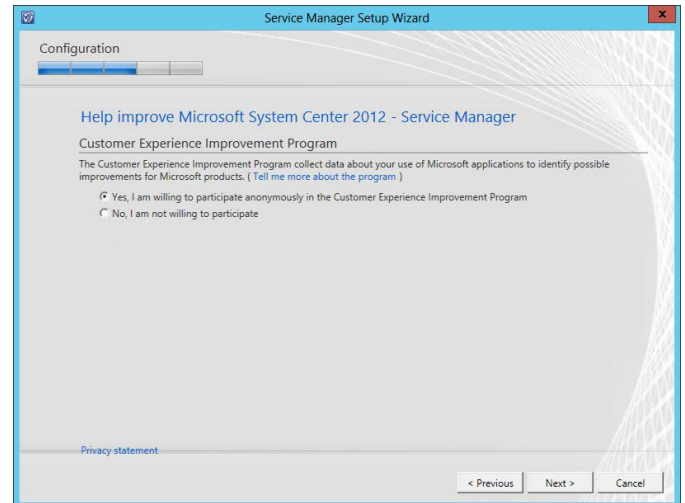
In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. Once successful, click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure the account for Service Manager services' step. The 'Domain account' radio button is selected. The 'User name' text box contains 'FT-SCSM-SVC', the 'Password' text box contains masked characters, and the 'Domain' dropdown menu shows 'FLEXPOD'. A 'Test Credentials' button is visible, and a green checkmark indicates 'The credentials were accepted.' At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

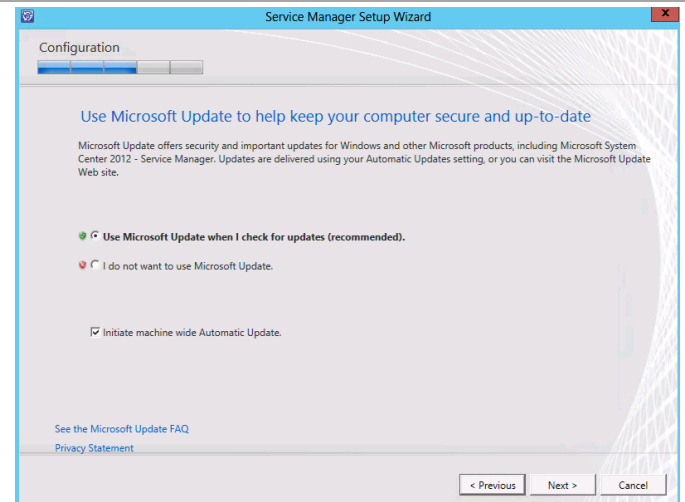
In the **Configure the account for Service Manager workflow account** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu. Before proceeding, click the **Test Credentials** button to verify the credentials provided. Once successful, click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure the Service Manager workflow account' step. The 'Domain account' radio button is selected. The 'User name' text box contains 'FT-SCSM-WF', the 'Password' text box contains masked characters, and the 'Domain' dropdown menu shows 'FLEXPOD'. A 'Test Credentials' button is visible, and a green checkmark indicates 'The credentials were accepted.' At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

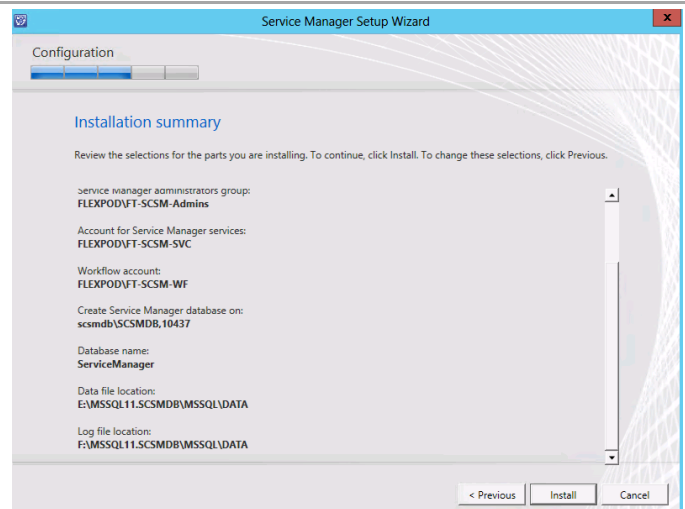
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



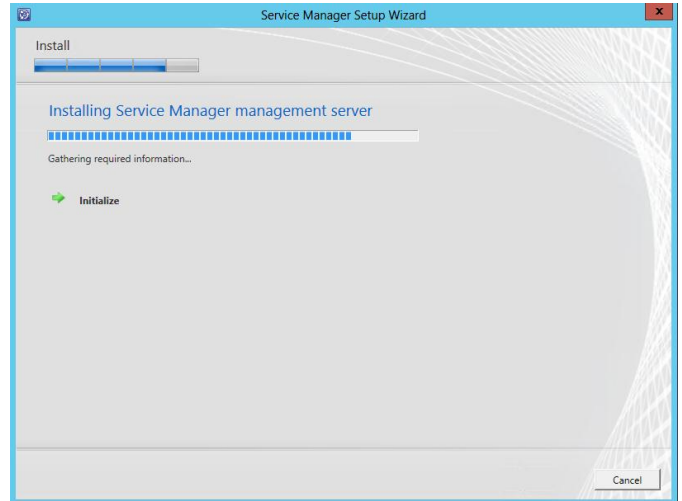
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine 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.



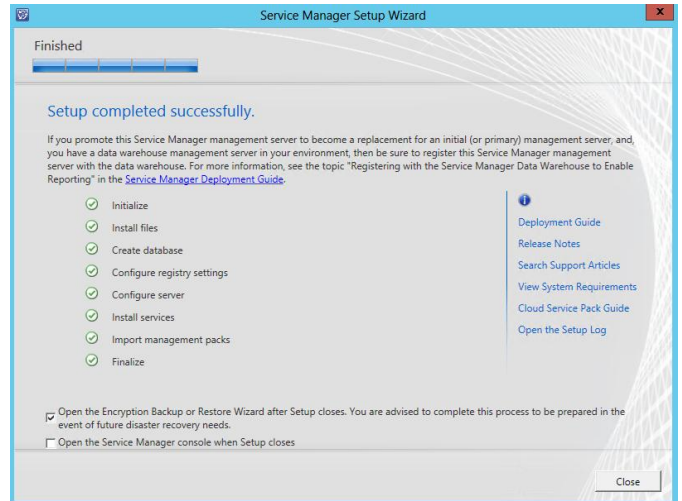
The wizard will display the progress while installing features.



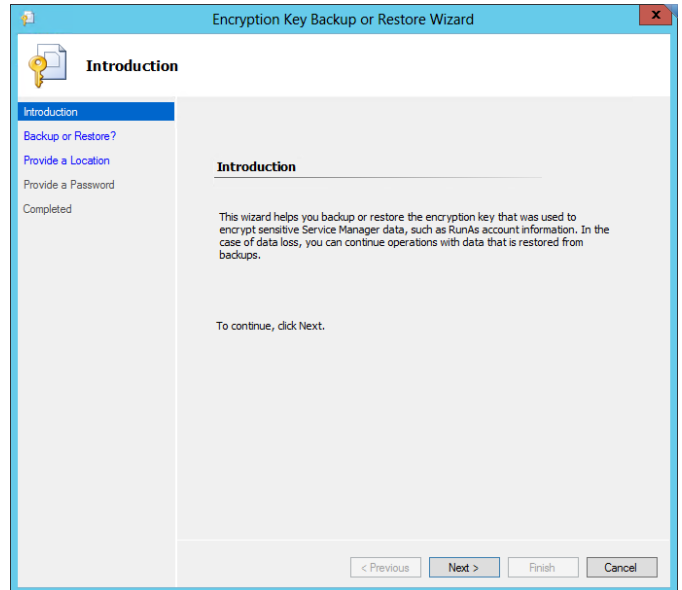
Once the installation completes, the wizard will display the **Setup completed successfully** dialog.

Once all steps show successful installation, ensure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to launch the wizard after setup.

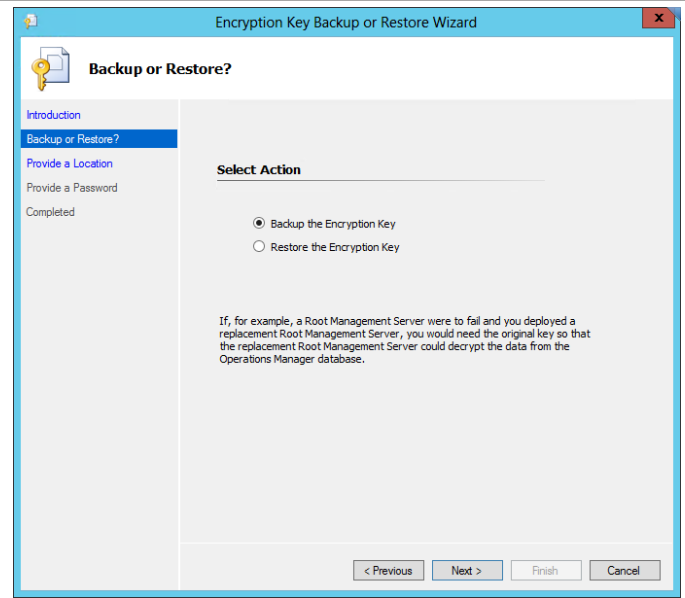
Click **Close** to complete the installation.



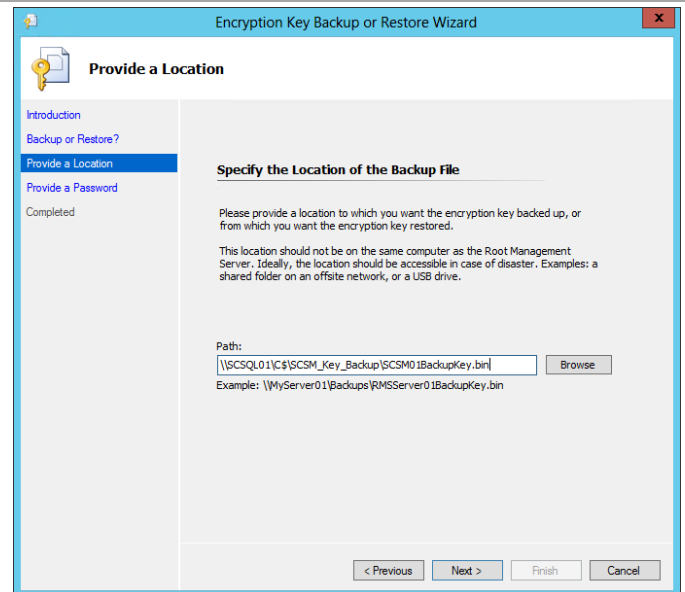
Once the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



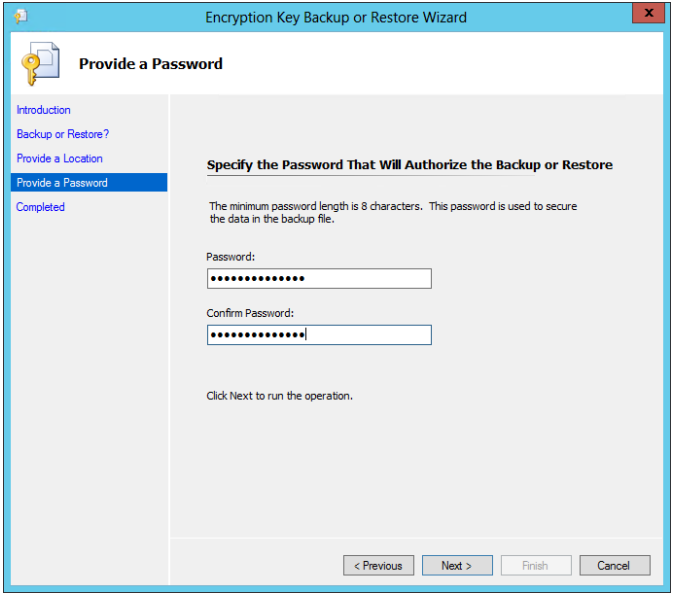
In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.



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.

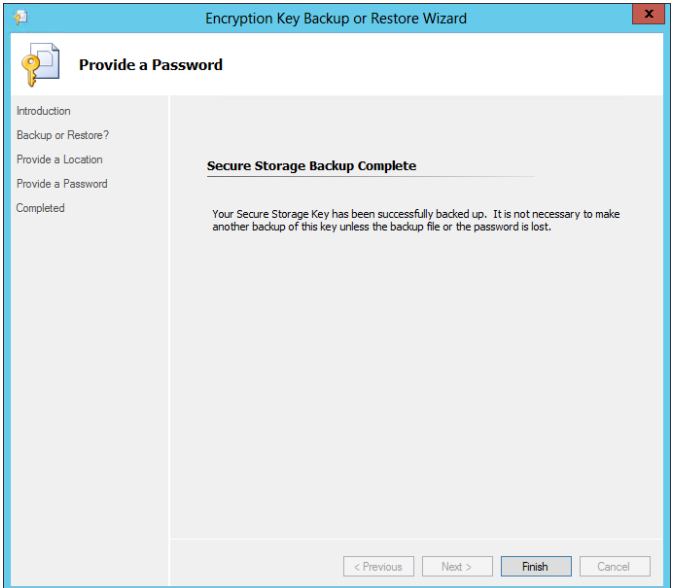


In the **Provide a Password** dialog, specify a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box and click **Next** to begin the backup process.



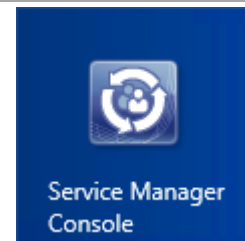
The screenshot shows the 'Provide a Password' step of the 'Encryption Key Backup or Restore Wizard'. The left sidebar contains a list of steps: Introduction, Backup or Restore?, Provide a Location, Provide a Password (highlighted), and Completed. The main area is titled 'Specify the Password That Will Authorize the Backup or Restore'. It includes a note: 'The minimum password length is 8 characters. This password is used to secure the data in the backup file.' Below this are two text boxes: 'Password:' and 'Confirm Password:', both filled with dots. A message at the bottom says 'Click Next to run the operation.' At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Once complete, click **Finish** to exit the wizard.

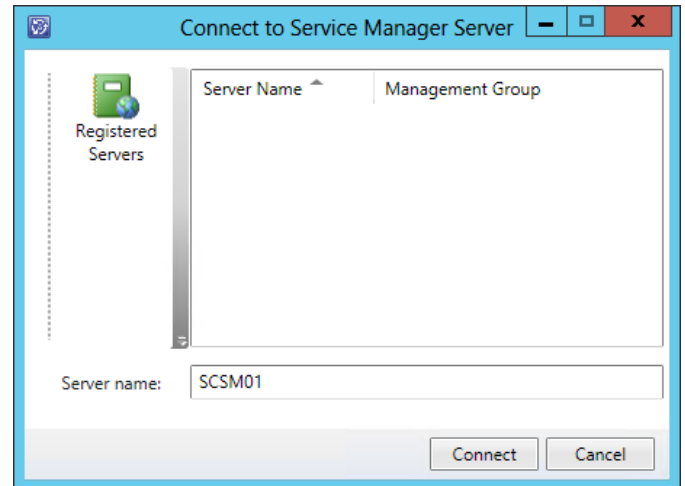


The screenshot shows the 'Secure Storage Backup Complete' step of the 'Encryption Key Backup or Restore Wizard'. The left sidebar shows the same list of steps as the previous screenshot, but 'Provide a Password' is no longer highlighted, and 'Completed' is now highlighted. The main area is titled 'Secure Storage Backup Complete' and contains a message: 'Your Secure Storage Key has been successfully backed up. It is not necessary to make another backup of this key unless the backup file or the password is lost.' At the bottom right are four buttons: '< Previous', 'Next >', 'Finish' (highlighted), and 'Cancel'.

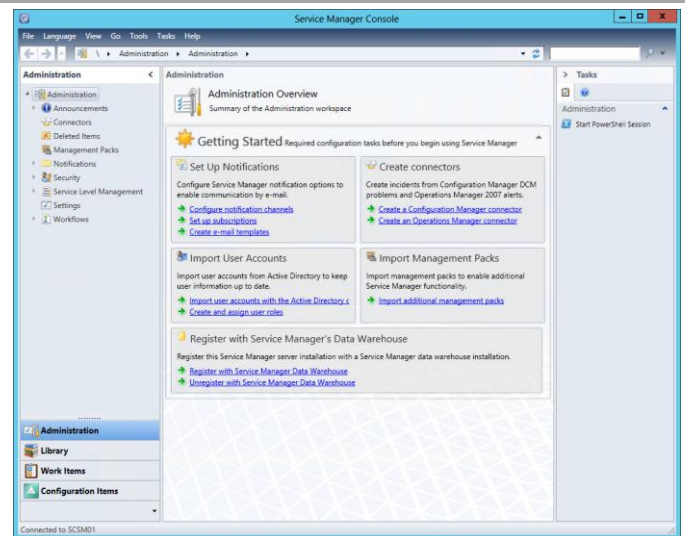
Once installed, verify that the Service Manager management server installed properly by opening the console. From the **Start** screen, click the **Service Manager Console** tile.



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.



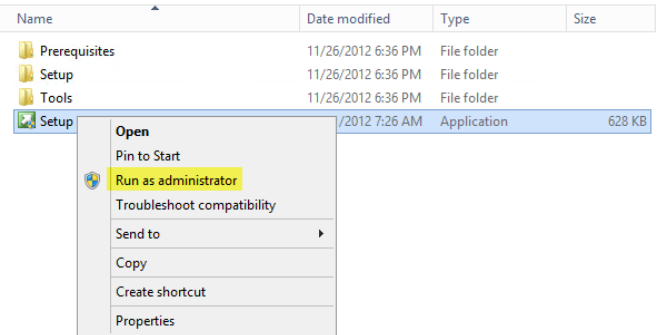
Install the Service Manager Data Warehouse Server

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.



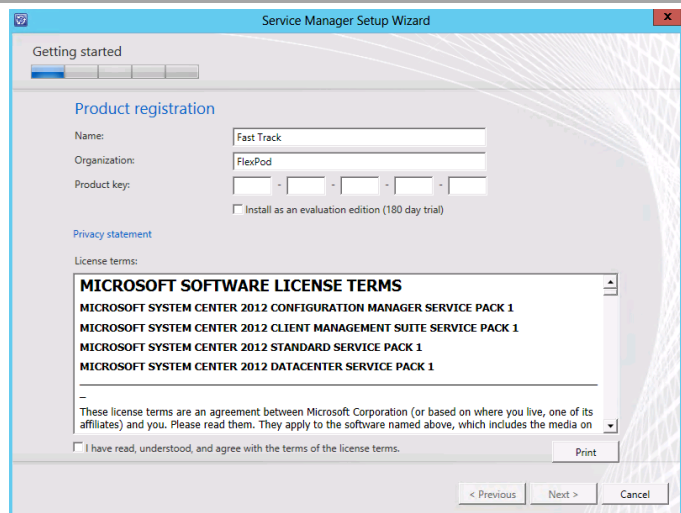
The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager data warehouse management server** to begin the Service Manager server installation.



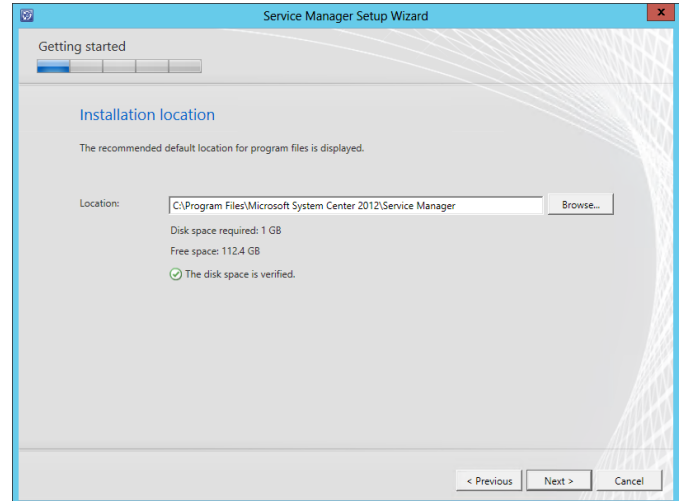
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **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.

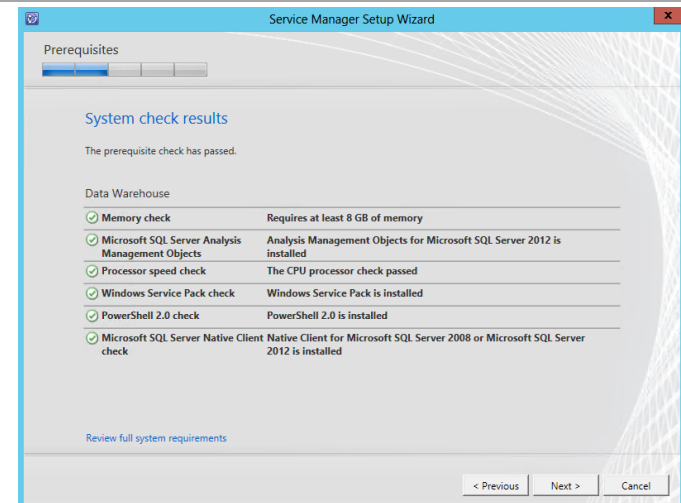
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. Once all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.

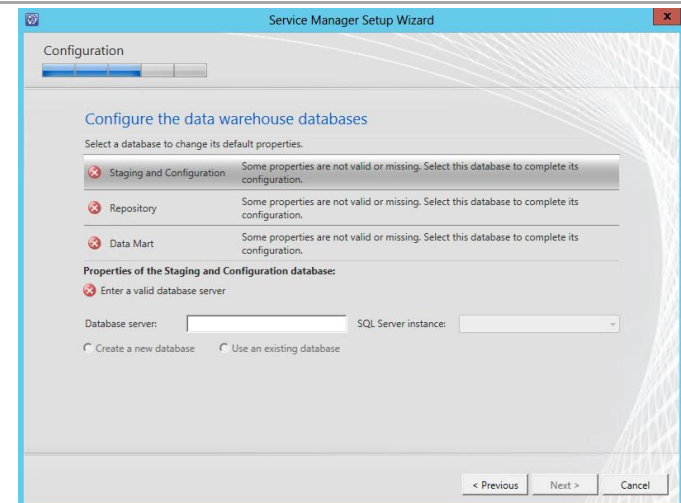


The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.



When the **Configure the data warehouse databases** dialog launches each subcategory will appear with an error message until each of the following sections are configured:

- **Staging and Configuration.**
- **Repository.**
- **Data Mart.**



In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse.

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the SM Data Warehouse database. In most cases the default value of *DWStagingAndConfig* should be used 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 work sheet identified earlier. Set the correct value on the Staging and Configuration section as well as the Repository section.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the work sheet identified earlier. Set the correct value on the Staging and Configuration section as well as the Repository section

Click **Data Mart** to continue.

Service Manager Setup Wizard

Configuration

Configure the data warehouse databases

Select a database to change its default properties.

Staging and Configuration A database named DWStagingAndConfig will be created on scsmdw\SCSMDW,10438.

Repository A database named DWRepository will be created on scsmdw\SCSMDW,10438.

Data Mart Some properties are not valid or missing. Select this database to complete its configuration.

Properties of the Staging and Configuration database:

Only supported instances are listed.

Database server: scsmdw SQL Server instance: SCSMDW

Create a new database Use an existing database

Database name: DWStagingAndConfig Size (MB): 2000

Data file folder: G:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Log file folder: H:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Both folders are located on the scsmdw server.

< Previous Next > Cancel

Service Manager Setup Wizard

Configuration

Configure the data warehouse databases

Select a database to change its default properties.

Staging and Configuration A database named DWStagingAndConfig will be created on scsmdw\SCSMDW,10438.

Repository A database named DWRepository will be created on scsmdw\SCSMDW,10438.

Data Mart Some properties are not valid or missing. Select this database to complete its configuration.

Properties of the Repository database:

Only supported instances are listed.

Database server: scsmdw SQL Server instance: SCSMDW

Create a new database Use an existing database

Database name: DWRepository Size (MB): 2000

Data file folder: G:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Log file folder: G:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Both folders are located on the scsmdw server.

< Previous Next > Cancel

In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (This should be the same as used for the Staging and Configuration and Repository above).

Select the **Create a new database** option and specify the following information in the provided text boxes:

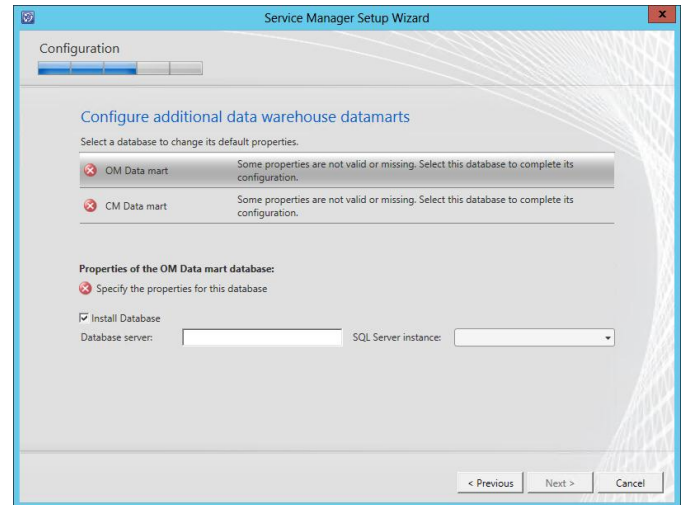
- **Database name** – specify the name of the Service Manager Data Warehouse database. In most cases the default value of DWDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)
- **Log file folder** – Specify the same drive letter associated above for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step titled 'Configure the data warehouse databases'. The wizard has three progress indicators at the top: 'Staging and Configuration', 'Repository', and 'Data Mart', all of which are marked with green checkmarks. Below these, a message states: 'Select a database to change its default properties.' The 'Data Mart' section is active, showing a summary: 'A database named DWDataMart will be created on scsmdw\SCSMDW,10438.' Below this, the 'Properties of the Data Mart database:' section is expanded, showing a warning icon and the text 'Only supported instances are listed.' The 'Database server:' field is set to 'scsmdw' and the 'SQL Server instance:' dropdown is set to 'SCSMDW'. The 'Create a new database' radio button is selected, while 'Use an existing database' is unselected. The 'Database name:' field contains 'DWDataMart' and the 'Size (MB):' field contains '2000'. The 'Data file folder:' field is 'G:\MSSQL11.SCSMDW\MSSQL\DATA' and the 'Log file folder:' field is 'H:\MSSQL11.SCSMDW\MSSQL\DATA'. Both fields have 'Browse...' buttons next to them. A blue information icon at the bottom of the folder fields indicates 'Both folders are located on the scsmdw server.' At the bottom right of the dialog are three buttons: '< Previous', 'Next >', and 'Cancel'.

When the **Configure additional data warehouse datamarts** dialog launches, each subcategory will appear with an error message until each of the following sections are configured:

- **OM Data mart.**
- **CM Data mart.**



In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **OM Data Mart** section:

- **Database server** – *specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*
- **SQL Server instance** – *specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse. (this should be the same as used for the Staging and Configuration and Repository above)*

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – *specify the name of the Service Manager OM Data mart database. In most cases the default value of OMDWDataMart should be used.*
- **Size (MB)** – *specify the initial database size. The default value can be used for Fast Track validation.*
- **Data file folder** – *specify the same drive letter associated above for the database data files for the Service Manager OM Data mart database. This should be cross-checked with the work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*
- **Log file folder** – *specify the same drive letter associated above for the database log files for the Service Manager OM Data mart database. This should be cross-checked with the work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)*

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' tab. The title bar reads 'Service Manager Setup Wizard'. Below the title bar, there's a progress indicator with three steps, the second of which is active. The main heading is 'Configure additional data warehouse datamarts'. Below this, a message says 'Select a database to change its default properties.' There are two entries: 'OM Data mart' with a green checkmark and a note 'A database named OMDWDataMart will be created on scsmdw\SCSMDW,10438.', and 'CM Data mart' with a red X and a note 'Some properties are not valid or missing. Select this database to complete its configuration.' Below this is a section titled 'Properties of the OM Data mart database:' with a sub-note 'Only supported instances are listed.' There's a checkbox 'Install Database' which is checked. Below it are four fields: 'Database server:' with 'scsmdw', 'SQL Server instance:' with a dropdown showing 'SCSMDW', 'Database name:' with 'OMDWDataMart', and 'Size (MB):' with '2000'. Below these are two 'Browse...' buttons for 'Data file folder:' (G:\MSSQL11.SCSMDW\MSSQL\DATA) and 'Log file folder:' (H:\MSSQL11.SCSMDW\MSSQL\DATA). A blue information icon at the bottom states 'Both folders are located on the scsmdw server.' At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

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 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 work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)
- **Log file folder** – specify the same drive letter associated above for the database log files for the Service Manager CM Data mart database. This should be cross-checked with the work sheet identified earlier. (this should be the same as used for the Staging and Configuration and Repository above)

Click **Next** to continue.

Service Manager Setup Wizard

Configuration

Configure additional data warehouse datamarts

Select a database to change its default properties.

OM Data mart A database named OMDWDataMart will be created on scsmdw\SCSMDW,10438.

CM Data mart A database named CMDWDataMart will be created on scsmdw\SCSMDW,10438.

Properties of the CM Data mart database:

Only supported instances are listed.

Install Database

Database server: scsmdw SQL Server instance: SCSMDW

Database name: CMDWDataMart Size (MB): 2000

Data file folder: G:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Log file folder: H:\MSSQL11.SCSMDW\MSSQL\DATA Browse...

Both folders are located on the scsmdw server.

< Previous Next > Cancel

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.

The screenshot shows the 'Configure the data warehouse management group' step of the Service Manager Setup Wizard. The 'Management group name' text box contains 'DW_SMMG01'. A warning icon and message state: 'You cannot use the same name as any other management group in Service Manager, including other Data Warehouse management groups.' The 'Management group administrators' section shows 'FLEXPOD\FT-SCSM-Admins' selected in the object picker, with a 'Browse...' button next to it. Navigation buttons at the bottom are '< Previous', 'Next >', and 'Cancel'.

In the **Configure the reporting server for the data warehouse** dialog, specify the Data Warehouse server in the **Report server** text box.

In the **Report server instance** drop-down menu, select **Default**.

In the **Web service URL** drop-down menu, select the default reporting server URL.

Click **Next** to continue.

The screenshot shows the 'Configure the reporting server for the data warehouse' step. The 'Report server' text box contains 'SCSM02'. The 'Report server instance' drop-down menu is set to 'Default'. The 'Web service URL' drop-down menu shows 'http://SCSM02:80/ReportServer'. A green checkmark and message confirm: 'The SSRS Web server URL is valid'. Navigation buttons at the bottom are '< Previous', 'Next >', and 'Cancel'.

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.

Once successful, click **Next** to continue.

The screenshot shows the 'Configure the account for Service Manager services' step. The 'Domain account' radio button is selected. The 'User name' text box contains 'FT-SCSM-SVC'. The 'Password' text box is masked with dots. The 'Domain' drop-down menu shows 'FLEXPOD'. A 'Test Credentials' button is visible. A green checkmark and message confirm: 'The credentials were accepted.' Navigation buttons at the bottom are '< Previous', 'Next >', and 'Cancel'.

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.

Once successful, click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure the reporting account' step. The window has a title bar with the text 'Service Manager Setup Wizard' and a close button. Below the title bar is a progress bar with four steps, the second of which is highlighted. The main content area has a blue header 'Configure the reporting account' and a sub-header 'This account is used to read the data warehouse reporting data sources and generate reports.' Below this, there are three text boxes: 'User name:' with the value 'FT-SCSM-SSRS', 'Password:' with masked characters, and 'Domain:' with a dropdown menu showing 'FLEXPOD'. A 'Test Credentials' button is located below these fields. To the right of the button, a green checkmark and the text 'The credentials were accepted.' are displayed. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

In the **Configure Analysis Services for OLAP cubes** dialog, select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server cluster CNO created for the Service Manager installation SQL Server Analysis Services.
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation SQL Server Analysis Services.
- **Database name** – specify the name of the SQL Server Analysis Services database. In most cases the default value of *DWASDataBase* should be used.

Confirm that the **Change database storage directory** check box is clear and click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure Analysis Services for OLAP cubes' step. The window has a title bar with the text 'Service Manager Setup Wizard' and a close button. Below the title bar is a progress bar with four steps, the third of which is highlighted. The main content area has a blue header 'Configure Analysis Services for OLAP cubes' and a sub-header 'Install Analysis Services Online Analytical Processing (OLAP) cubes. In order to do that you need to have SQL Server Analysis Services installed in either the same or different servers than the data warehouse databases.' Below this, there is a section 'Analysis Services server database information:' with two radio buttons: 'Create a new database' (selected) and 'Use an existing database'. Below the radio buttons, there are two text boxes: 'Database server:' with the value 'SCSM02' and 'SQL Server instance:' with a dropdown menu showing 'SCSM02'. At the bottom of the main content area, there is a red error icon and the text 'Microsoft SQL Server 2008 Analysis Services is not installed on SCSM02.' At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configure Analysis Services for OLAP cubes' step. The window has a title bar with the text 'Service Manager Setup Wizard' and a close button. Below the title bar is a progress bar with four steps, the third of which is highlighted. The main content area has a blue header 'Configure Analysis Services for OLAP cubes' and a sub-header 'Install Analysis Services Online Analytical Processing (OLAP) cubes. In order to do that you need to have SQL Server Analysis Services installed in either the same or different servers than the data warehouse databases.' Below this, there is a section 'Analysis Services server database information:' with two radio buttons: 'Create a new database' (selected) and 'Use an existing database'. Below the radio buttons, there are three text boxes: 'Database server:' with the value 'scsmas', 'SQL Server instance:' with a dropdown menu showing 'SCSMAS', and 'Database name:' with the value 'DWASDataBase'. Below these text boxes, there is a checkbox 'Change database storage directory:' which is unchecked. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

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.

Once successful, click **Next** to continue.

The screenshot shows the 'Configure Analysis Services credential' step of the Service Manager Setup Wizard. The 'User name' field contains 'FT-SCSM-OLAP', the 'Password' field is masked with dots, and the 'Domain' dropdown menu is set to 'FLEXPOD'. A 'Test Credentials' button is visible, and a green checkmark indicates 'The credentials were accepted.' Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

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.

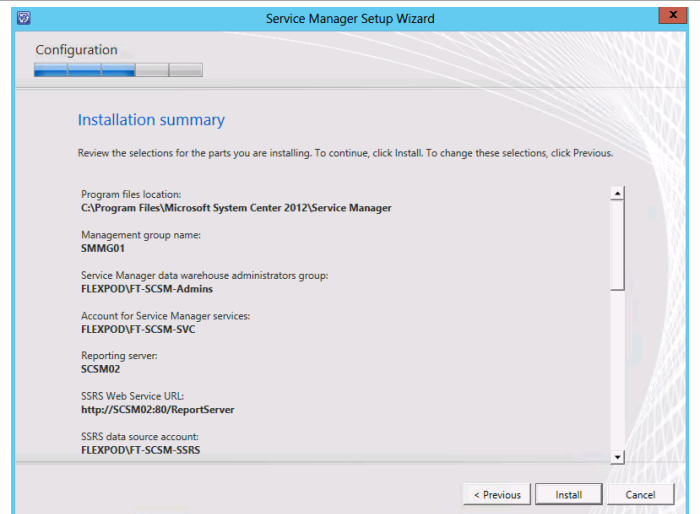
The screenshot shows the 'Help improve Microsoft System Center 2012 - Service Manager' step. It describes the Customer Experience Improvement Program (CEIP) and provides two radio button options: 'Yes, I am willing to participate anonymously in the Customer Experience Improvement Program' (which is selected) and 'No, I am not willing to participate'. A 'Privacy statement' link is at the bottom. Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

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 screenshot shows the 'Use Microsoft Update to help keep your computer secure and up-to-date' step. It explains that Microsoft Update offers security and important updates. There are two radio button options: 'Use Microsoft Update when I check for updates (recommended)' (which is selected) and 'I do not want to use Microsoft Update.' Below these, there is a checked checkbox for 'Initiate machine wide Automatic Update.' Links for 'See the Microsoft Update FAQ' and 'Privacy Statement' are at the bottom. Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

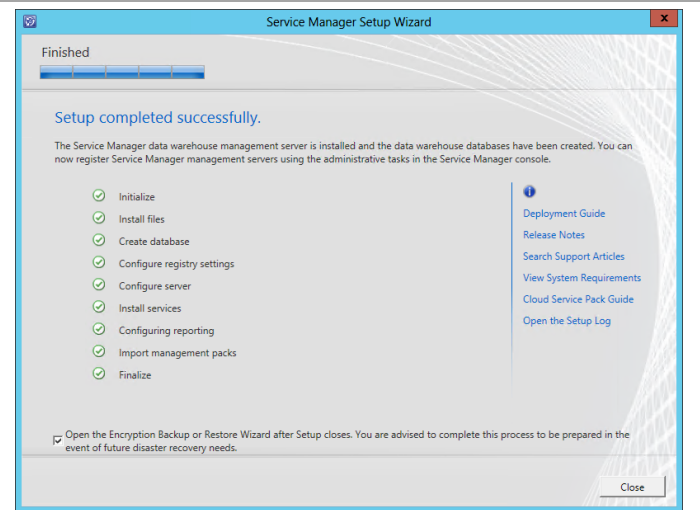
The wizard will display the progress while installing features.



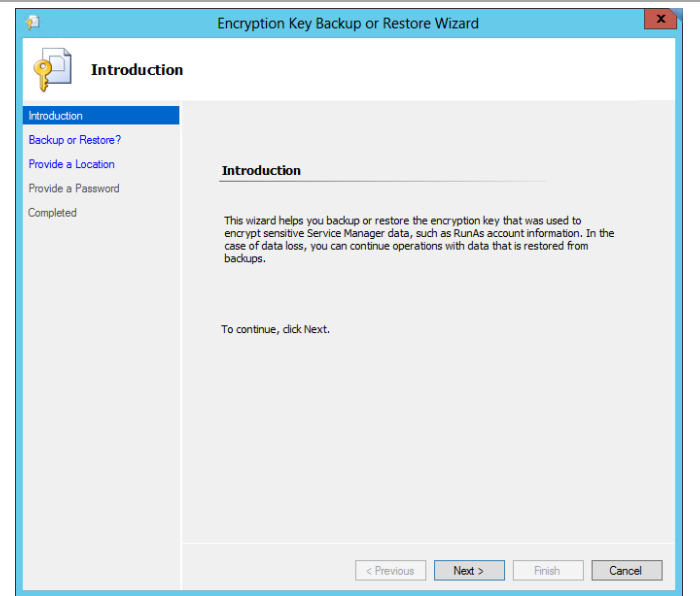
Once the installation completes, the wizard will display the **Setup completed successfully** dialog.

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.



Once the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



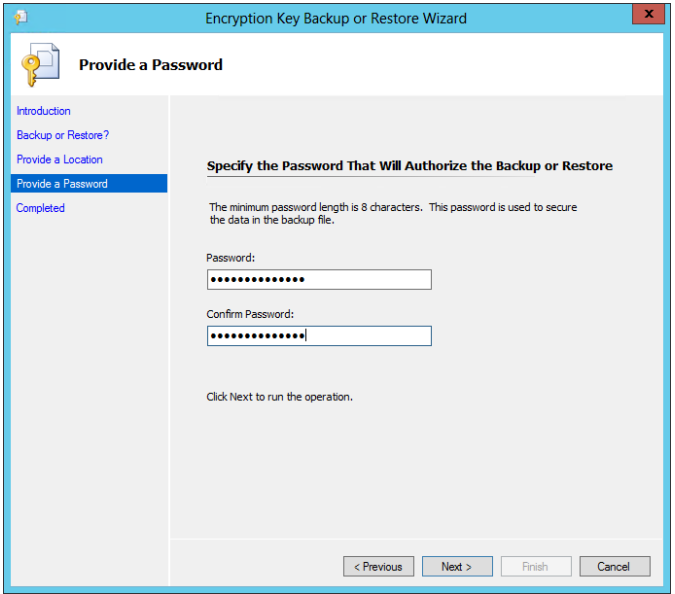
In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.

The screenshot shows the 'Encryption Key Backup or Restore Wizard' dialog box. The title bar reads 'Encryption Key Backup or Restore Wizard'. The main window has a blue header with a key icon and the text 'Backup or Restore?'. On the left, a vertical pane lists the steps: 'Introduction', 'Backup or Restore?' (highlighted), 'Provide a Location', 'Provide a Password', and 'Completed'. The main area is titled 'Select Action' and contains two radio buttons: 'Backup the Encryption Key' (selected) and 'Restore the Encryption Key'. Below the radio buttons, there is a paragraph of text: 'If, for example, a Root Management Server were to fail and you deployed a replacement Root Management Server, you would need the original key so that the replacement Root Management Server could decrypt the data from the Operations Manager database.' At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.

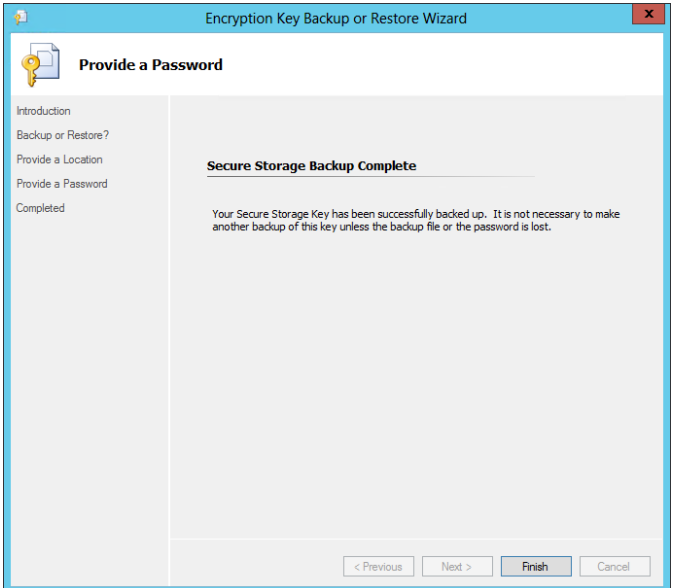
The screenshot shows the 'Encryption Key Backup or Restore Wizard' dialog box, specifically the 'Provide a Location' step. The title bar reads 'Encryption Key Backup or Restore Wizard'. The main window has a blue header with a key icon and the text 'Provide a Location'. On the left, a vertical pane lists the steps: 'Introduction', 'Backup or Restore?', 'Provide a Location' (highlighted), 'Provide a Password', and 'Completed'. The main area is titled 'Specify the Location of the Backup File'. It contains a paragraph of text: 'Please provide a location to which you want the encryption key backed up, or from which you want the encryption key restored.' Below this, another paragraph states: 'This location should not be on the same computer as the Root Management Server. Ideally, the location should be accessible in case of disaster. Examples: a shared folder on an offsite network, or a USB drive.' There is a 'Path:' label followed by a text box containing the path '\\csqr01\\c:\\SCSM_Key_Backup\\SCSM02BackupKey.bin' and a 'Browse' button. Below the text box, an example path is shown: 'Example: \\MyServer01\\Backups\\RMSServer01BackupKey.bin'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.



The screenshot shows the 'Provide a Password' step of the 'Encryption Key Backup or Restore Wizard'. The left sidebar contains a list of steps: Introduction, Backup or Restore?, Provide a Location, Provide a Password (highlighted), and Completed. The main area is titled 'Specify the Password That Will Authorize the Backup or Restore'. It includes a note: 'The minimum password length is 8 characters. This password is used to secure the data in the backup file.' Below this are two text boxes labeled 'Password:' and 'Confirm Password:', both filled with dots. A message at the bottom says 'Click Next to run the operation.' At the bottom right are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

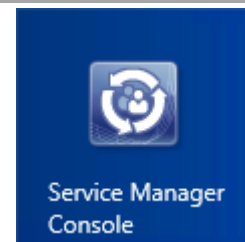
Once complete, click **Finish** to exit the wizard.



The screenshot shows the 'Secure Storage Backup Complete' step of the 'Encryption Key Backup or Restore Wizard'. The left sidebar shows the same list of steps as the previous screenshot, but 'Provide a Password' is no longer highlighted, and 'Completed' is now highlighted. The main area is titled 'Secure Storage Backup Complete' and contains a message: 'Your Secure Storage Key has been successfully backed up. It is not necessary to make another backup of this key unless the backup file or the password is lost.' At the bottom right are buttons for '< Previous', 'Next >', 'Finish' (highlighted), and 'Cancel'.

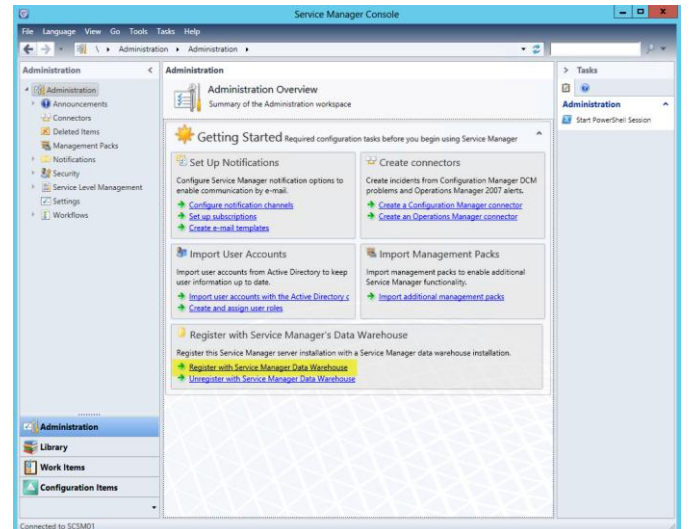
- Perform the following steps on the **Service Manager management server (scsm01)** virtual machine to register the Service Manager Data Warehouse and enable reporting in the Service Manager instance.

Logon to the Service Manager management server using an account with administrator permissions. From the Windows **Start** screen, select the **Service Manager Console** tile.

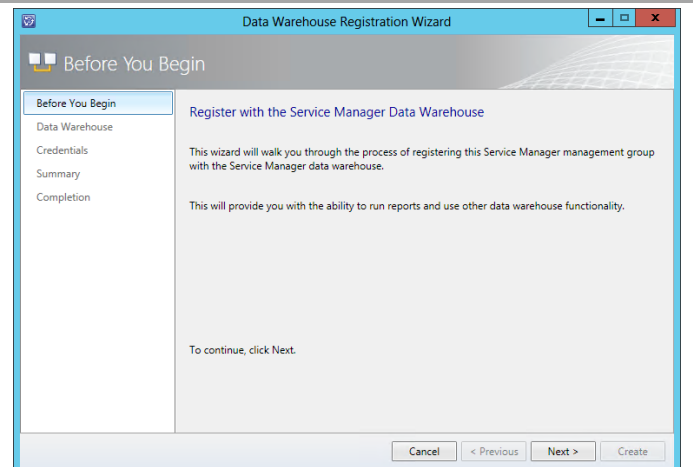


Within the **Service Manager Console**, select the **Administration** node and navigate to the **Register with Service Manager's Data Warehouse** section. Click the **Register with Service manager Data Warehouse** link to enable reporting.

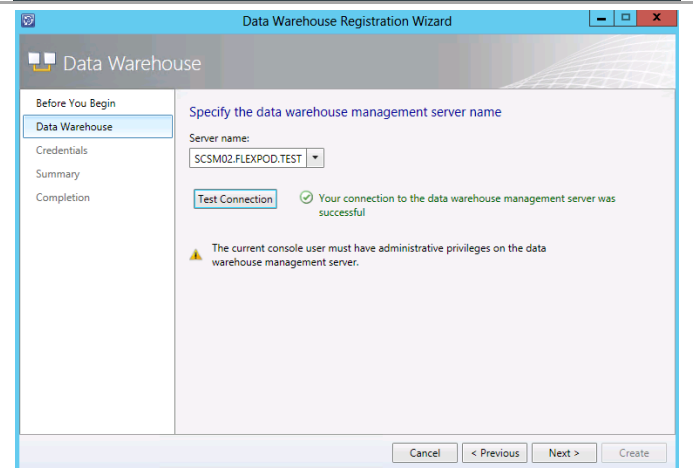
***Note:** if the console was open from the previous installation, close it and re-open the console.*



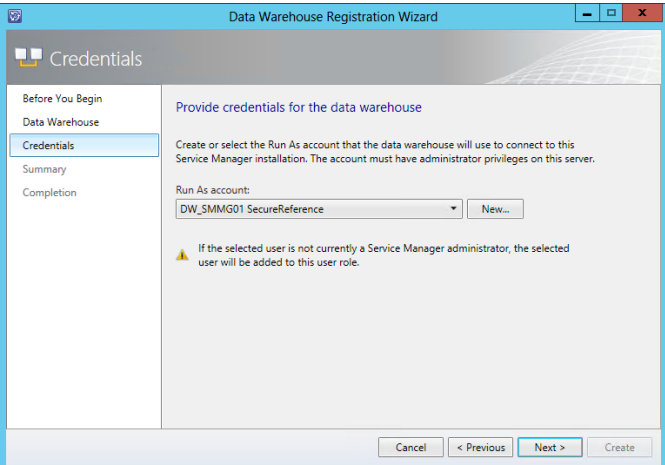
The **Data Warehouse Registration Wizard** will launch. Click **Next** to begin registration.



In the **Specify the data warehouse management server name** dialog, specify the Service Manager Data Warehouse server FQDN in the **Server name** drop-down menu. Once selected, click the **Test Connection** button to validate connectivity between the Service Manager management and Data Warehouse servers. Click **Next** to continue.

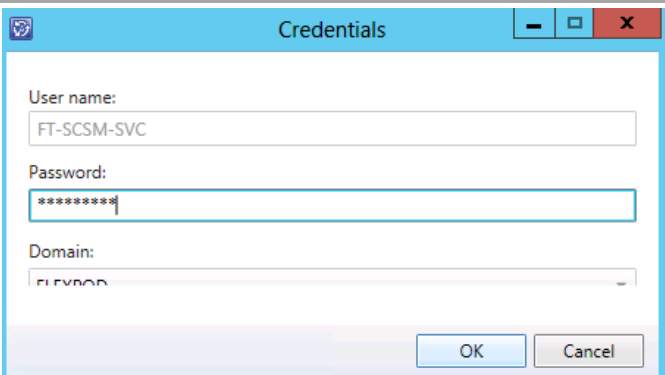


In the **Provide credentials for the data warehouse** dialog. Click **Next** to use the current SM and DW service account as the **Run As account** for the Data Warehouse connection.



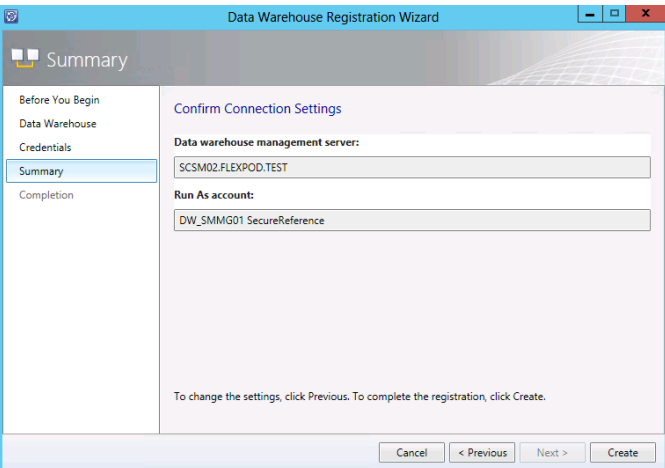
The screenshot shows the 'Data Warehouse Registration Wizard' window, specifically the 'Credentials' step. On the left, a sidebar lists the steps: 'Before You Begin', 'Data Warehouse', 'Credentials' (which is selected and highlighted in blue), 'Summary', and 'Completion'. The main area is titled 'Provide credentials for the data warehouse'. It contains a text box for 'Run As account:' with the value 'DW_SMMG01 SecureReference' and a 'New...' button. Below this, a warning icon and text state: 'If the selected user is not currently a Service Manager administrator, the selected user will be added to this user role.' At the bottom right, there are four buttons: 'Cancel', '< Previous', 'Next >', and 'Create'.

A **Credentials** dialog will appear and prompt you for the password for the SM service account. Once provided, click **OK** to continue.



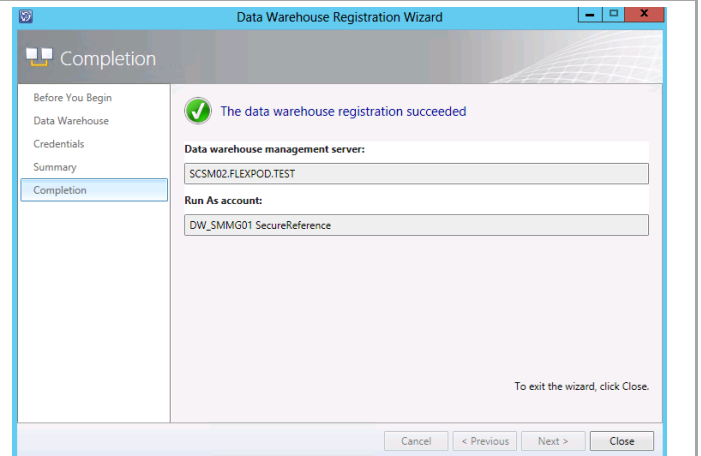
The screenshot shows a 'Credentials' dialog box. It has three input fields: 'User name:' with the text 'FT-SCSM-SVC', 'Password:' with masked characters '*****', and 'Domain:' with the text 'FLEXPOD'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

The **Summary** dialog will appear. Review the information that was provided earlier and click **Create** to begin the registration process.

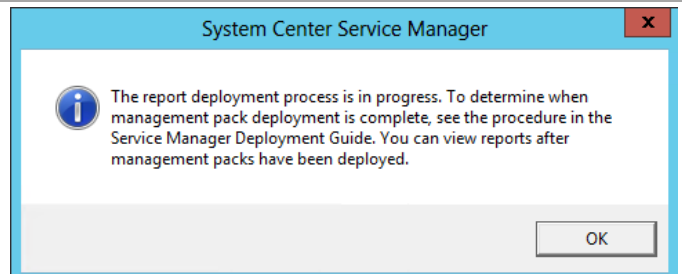


The screenshot shows the 'Data Warehouse Registration Wizard' window, specifically the 'Summary' step. The sidebar on the left is the same as in the first screenshot, with 'Summary' now selected and highlighted in blue. The main area is titled 'Confirm Connection Settings'. It contains two text boxes: 'Data warehouse management server:' with the value 'SCSM02.FLEXPOD.TEST' and 'Run As account:' with the value 'DW_SMMG01 SecureReference'. At the bottom, a message reads: 'To change the settings, click Previous. To complete the registration, click Create.' At the bottom right, there are four buttons: 'Cancel', '< Previous', 'Next >', and 'Create'.

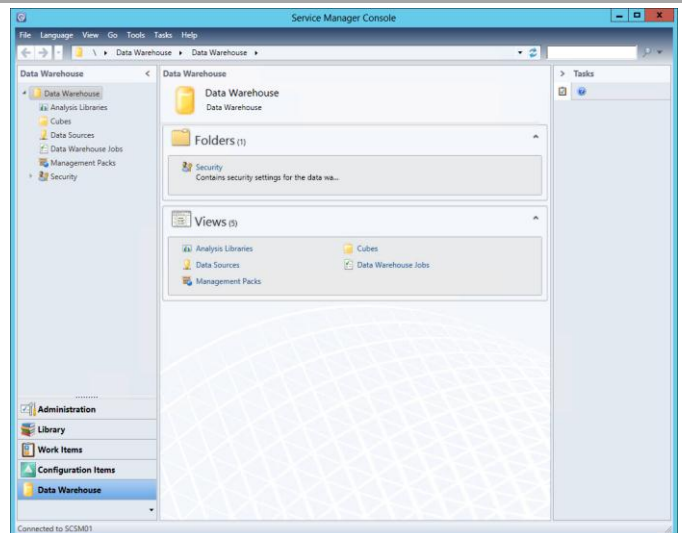
The **Completion** dialog will show the successful registration of the Data Warehouse. Click **Close** to exit the wizard.



Note: The Data Warehouse registration process can take several hours for the registration process to complete. During this time several management packs are imported into the Data Warehouse server and several Data Warehouse jobs run.



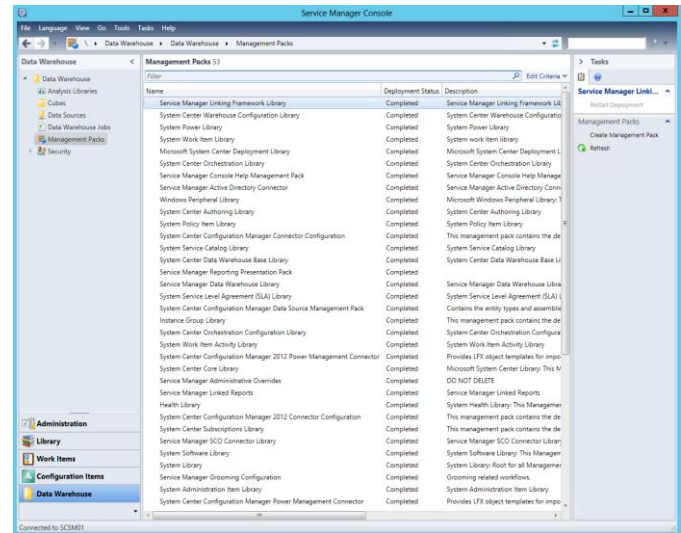
After a few minutes the **Data Warehouse** button will be added to the **Service Manager Console**.



Note: this deployment and association process can take up to two hours to complete.

The status of the management pack imports can be checked by selecting **Management Packs** in the **Data Warehouse** pane.

Deployment is complete when all listed management packs show a deployment status of **Completed**.



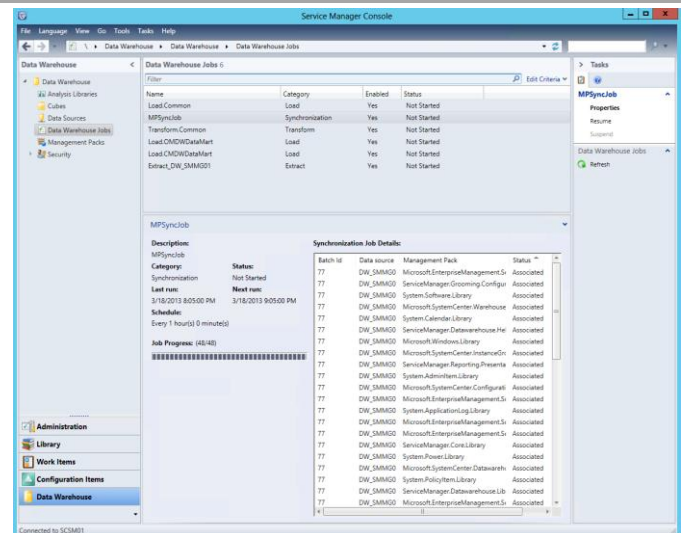
Note: this deployment and association process can take up to two hours to complete.

In the **Data Warehouse** pane, select **Data Warehouse Jobs**.

In the **Data Warehouse Jobs** pane, click **MPSyncJob**.

In the **MPSyncJob** details pane, in the **Synchronization Job Details** list, scroll to the right to view the **Status** column, and then click **Status** to alphabetically sort the status column.

Scroll through the **Status** list. The management pack deployment process is complete when the status for all of the management packs is **Associated** or **Imported**. Confirm that there is no status of either **Pending Association** or **Failed** in the status list. In the **Data Warehouse Jobs** pane, the status of the **MPSyncJob** will have changed from **Running** to **Not Started** when the registration process is complete.



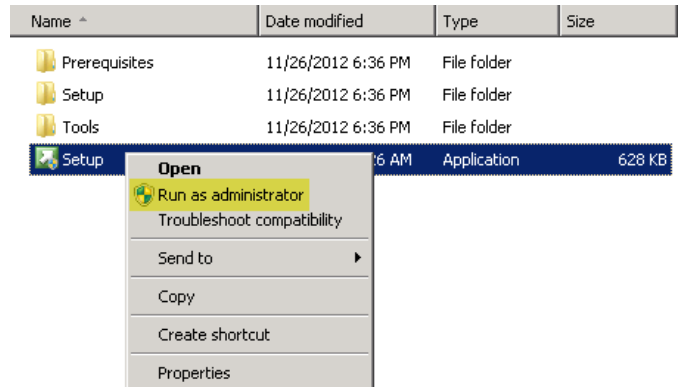
Install the Service Manager Self-Service Portal Server

The following steps must be completed in order to install the Service Manager self-service portal server role.

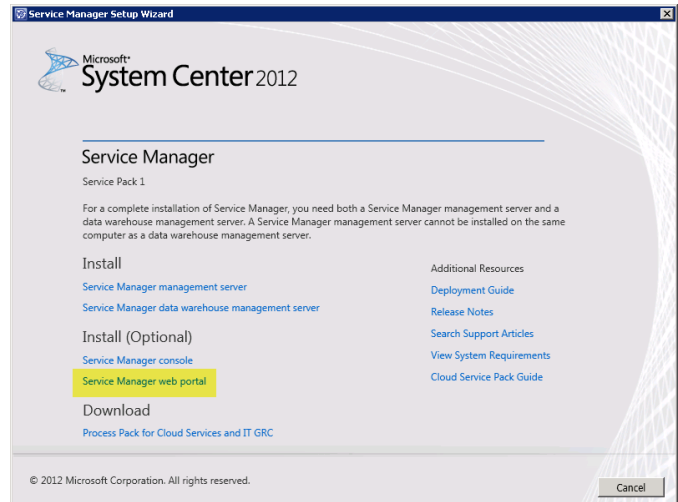
- Perform the following steps on the **System Center Service Manager self-service portal (SCSM03)** virtual machine.

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.

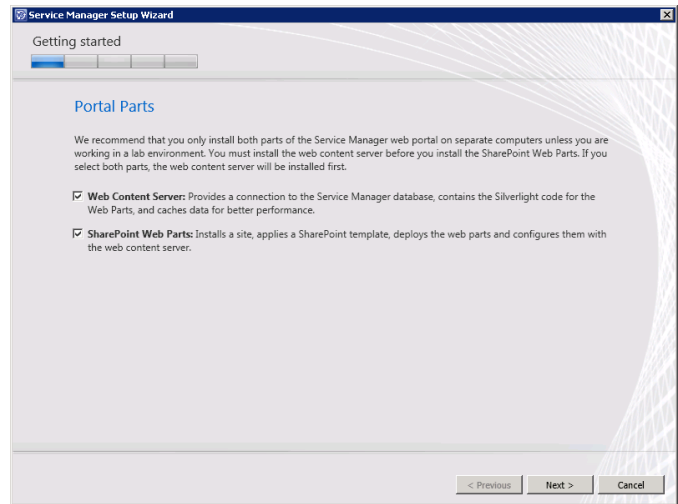


The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager web portal** to begin the Service Manager self-service portal server installation.



The **Service Manager Setup Wizard** will open. In the **Portal Parts** dialog, select the **Web Content Server** and **SharePoint Web Parts** checkboxes 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. Once all selections are confirmed, click **Next** to continue.

The screenshot shows the 'Product registration' step of the Service Manager Setup Wizard. It includes fields for 'Name' (containing 'Fast Track') and 'Organization' (containing 'FlexPod'). Below these is a 'License terms' section with a list of Microsoft software licenses and a checkbox labeled 'I have read, understood, and agree with the terms of the license terms.' which is checked. Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

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 screenshot shows the 'Installation location' step. It displays the recommended default location: 'C:\inetpub\wwwroot\System Center Service Manager Portal'. Below this, it shows 'Disk space required: 1 GB' and 'Free space: 108.8 GB', with a green checkmark indicating 'The disk space is verified.' Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.

The screenshot shows the 'System check results' step. It states 'The prerequisite check has passed.' and lists several checks under 'Service Manager Self-Service Portal', all of which are marked with green checkmarks: 'Memory check' (Requires at least 8 GB of memory), 'Processor speed check' (The CPU processor check passed), 'IIS check' (IIS 7.0 is installed), 'ASP.NET check' (ASP.NET is installed), 'Basic Authentication check' (Basic Authentication is enabled), 'Windows Authentication check' (Windows Authentication is enabled), 'Microsoft .NET Framework 4 check' (Microsoft .NET Framework 4 is installed), 'Windows Service Pack check' (Windows Service Pack is installed), and 'SharePoint Server 2010 check' (SharePoint Server 2010 is installed). A link 'Review full system requirements' is at the bottom. Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

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 SCSSMWebContentServer 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' window, specifically the 'Configuration' tab. The title bar reads 'Service Manager Setup Wizard'. Below the title bar, there's a progress indicator with three steps, the second of which is highlighted. The main heading is 'Configure the Service Manager Self-Service Portal name and port'. Below this, a sub-heading says 'Specify a name for your Self-Service Portal and the port that this website will use.' There are two input fields: 'Website name' with the value 'SCSSMWebContentServer' and 'Port' with the value '443'. Below these, there's a checkbox labeled 'Enable SSL encryption (recommended)' which is checked. A note below the checkbox states: 'To more securely transfer data between the browser and the Self-Service Portal, you must configure the Self-Service Portal to use Secure Sockets Layer (SSL) encryption.' At the bottom, there's an 'SSL certificate' dropdown menu showing 'scsm03, OU=Fast Track, O=FlexPod, L=San Jose, S=CA, '. 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 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' window, specifically the 'Configuration' tab. The title bar reads 'Service Manager Setup Wizard'. Below the title bar, there's a progress indicator with three steps, the second of which is highlighted. The main heading is 'Select the Service Manager database'. Below this, a sub-heading says 'Specify the name of the server that hosts the instance of SQL Server 2008 that contains the Service Manager database, and then select the Service Manager database.' There's an information icon followed by the text: 'Service Manager Self-Service Portal will use the existing 'ServiceManager' database'. There are two input fields: 'Database server' with the value 'scsmdb' and 'SQL Server instance' with the value 'SCSMD8'. Below these, there's a 'Database' dropdown menu showing 'ServiceManager'. At the bottom right, there's a warning icon 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.

Once successful, click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step. The title bar reads 'Service Manager Setup Wizard'. Below the title bar is a progress bar with four steps, the second of which is highlighted. The main heading is 'Configure the account for the Self-Service Portal'. A note states: 'The Self-Service Portal can access the Service Manager database under the Local System account, if installed on the same computer, or under a domain user or service account. Setup will add the domain account to the Service Manager Administrators user role.' There are two radio button options: 'Local System account' (unselected) and 'Domain account' (selected). Under 'Domain account', there are three input fields: 'User name' with the text 'FT-SCSM-SVC', 'Password' with masked characters '*****', and 'Domain' with a dropdown menu showing 'FLEXPOD'. A 'Test Credentials' button is located below these fields. To the right of the button is a green checkmark icon and the text 'The credentials were accepted.' At the bottom of the window are three buttons: '< Previous', 'Next >', and 'Cancel'.

In the **Configure the Service Manager SharePoint Web site** dialog, provide the following information:

- In the **SharePoint site** section, specify the following information in the provided text boxes:
 - **Website name** – specify the name of the website used for the self-service portal. In most cases, the default name of Service Manager Portal should be used.
 - **Port** – specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases the default value of **443** should be kept.
- Select the appropriate server authentication certificate from the **SSL certificate** drop-down menu. This will be the same certificate used for the content server in the previous step.
- In the SharePoint database section, specify the following information in the provided text boxes:
 - **Database server** – specify the name of the SQL Server cluster network name created for the Service Manager installation SharePoint Farm (SCDB).
 - **SQL Server instance** – specify the SQL Server database instance created for the Service Manager installation SharePoint Farm (SCDB).
 - **Database server** – specify the database name for the portal. In most cases, the default value of *SharePoint_SMPortalContent* will be used.

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' tab. The title bar reads 'Service Manager Setup Wizard'. Below the title bar, there's a progress indicator with three steps, the second of which is highlighted. The main heading is 'Configure the Service Manager SharePoint Web site'. Below this, a small instruction text says: 'Specify the name and port number for the SharePoint Web site. Specify the server and database that will be used to store content for this SharePoint Web site, and then specify the URL for the web content server.'

The configuration fields are as follows:

- SharePoint site:**
 - Website name:
 - Port:
- ☒ **Enable SSL encryption (recommended)**
- SSL certificate:
- SharePoint database:**
 - Database server:
 - SQL Server instance:
 - Database name:
- Web content server:**
 - URL:

At the bottom right, there are three buttons: '< Previous', 'Next >', and '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. Once successful, click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step. The title is 'Configure the account for Service Manager SharePoint application pool'. Below the title, it says 'The Service Manager SharePoint application pool can run under a domain user or service account.' There are three input fields: 'User name:' with the value 'FT-SCSM-SVC', 'Password:' with masked characters, and 'Domain:' with a dropdown menu showing 'FLEXPOD'. A 'Test Credentials' button is located below these fields. To the right of the button, a green checkmark icon and the text 'The credentials were accepted.' are displayed. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

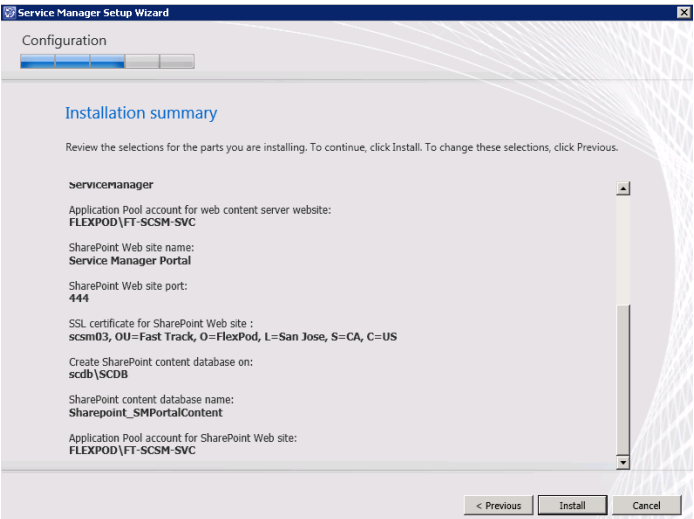
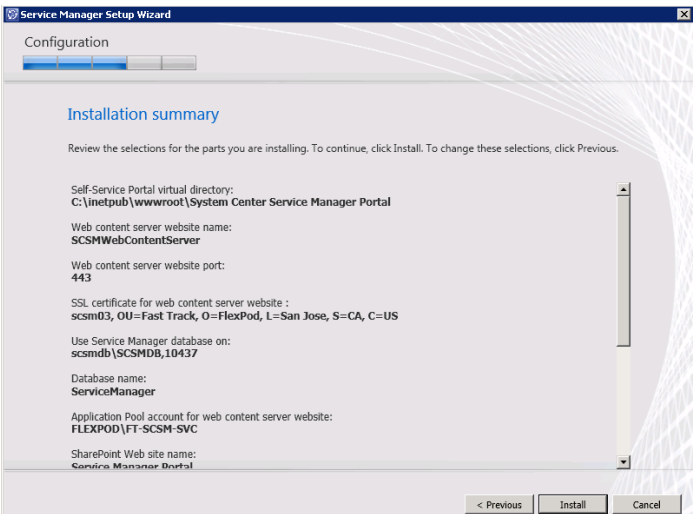
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step. The title is 'Help improve Microsoft System Center 2012 - Service Manager'. Below the title, it says 'Customer Experience Improvement Program'. A paragraph explains that the program collects data to identify possible improvements. There are two radio button options: 'Yes, I am willing to participate anonymously in the Customer Experience Improvement Program' (which is selected) and 'No, I am not willing to participate'. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'. A link for 'Privacy statement' is also visible at the bottom left.

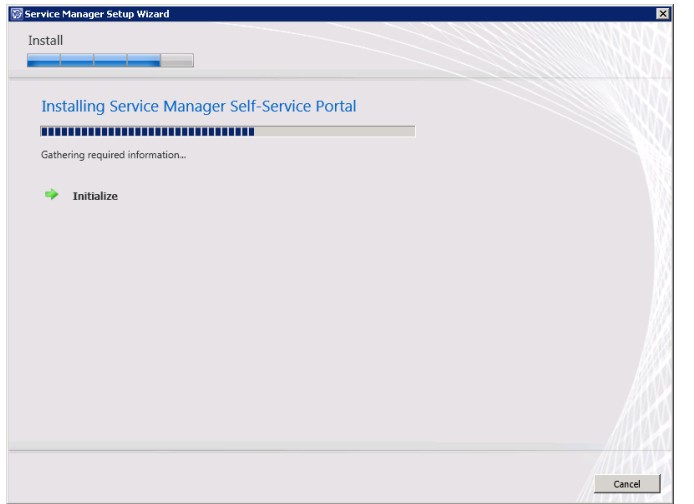
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog may appear. Select the appropriate option to either participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step. The title is 'Use Microsoft Update to help keep your computer secure and up-to-date'. Below the title, it says 'Microsoft Update offers security and important updates for Windows and other Microsoft products, including Microsoft System Center 2012 - Service Manager. Updates are delivered using your Automatic Updates setting, or you can visit the Microsoft Update Web site.' There are two radio button options: 'Use Microsoft Update when I check for updates (recommended)' (which is selected) and 'I do not want to use Microsoft Update.' Below these, there is a checkbox labeled 'Initiate machine wide Automatic Update.' which is checked. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'. Links for 'See the Microsoft Update FAQ' and 'Privacy Statement' are also visible at the bottom left.

The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

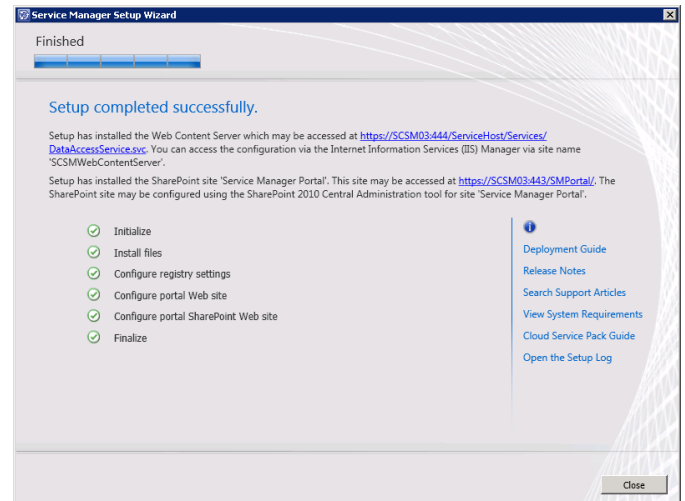


The wizard will display the progress while installing features.



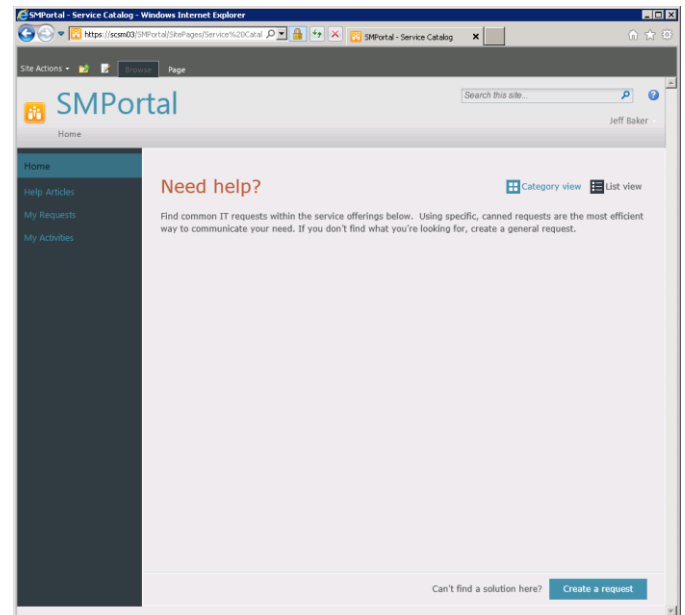
Once completed, the **Service Manger Setup Wizard** will display the **Setup completed successfully** dialog. Click **Close** to finish the installation.

Note the SMPortal link provided in the dialog.



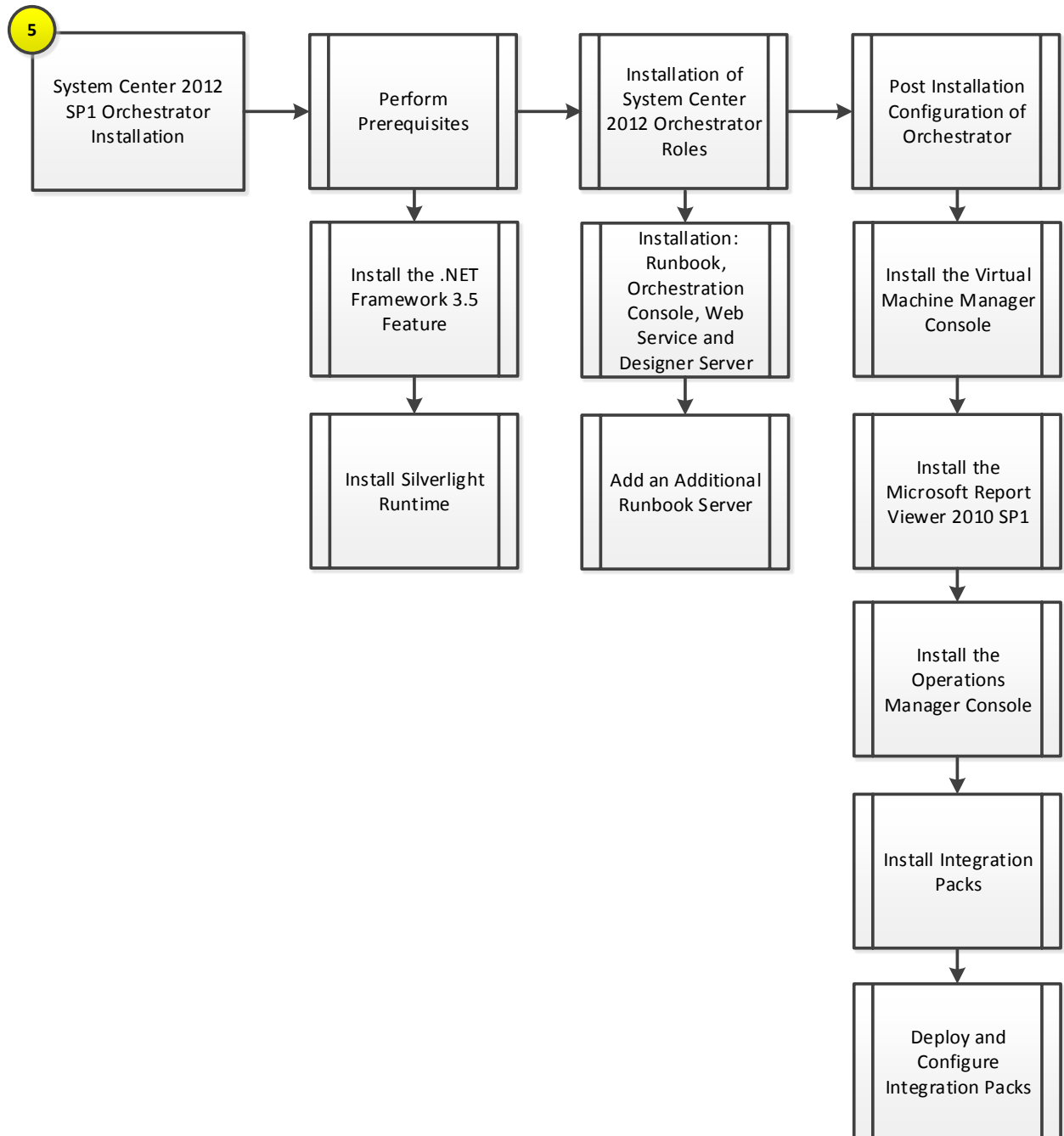
From Microsoft Internet Explorer®, open the Service Manager self-service portal at <https://<servername>/SMPortal>.

Verify that the page loads completely and that all sections display as expected.



19 Orchestrator

The Orchestrator installation process includes the following high-level steps:



19.1 Overview

This section provides the setup procedure for Orchestrator into the Fast Track fabric management architecture. The following assumptions are made:

- Base virtual machines running Windows Server 2012 have been provisioned.
- A multi-node, SQL Server 2012 cluster with dedicated instance has been established in previous steps for Orchestrator.
- The .NET Framework 3.5 Feature is installed.

19.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security accounts have been created:

User name	Purpose	Permissions
<DOMAIN>\FT-SCO-SVC	Orchestrator service account	<p>This account will need:</p> <ul style="list-style-type: none"> • Full admin permissions on all target systems to be managed • Log on As a Service rights (User Rights) • <i>Sysadmin</i> on the SQL Server, or <i>dbo</i> rights to the Orchestrator database after its created <p>This account will need to be a member in the following groups:</p> <ul style="list-style-type: none"> • FT-VMM-Admins

Groups

Verify that the following security groups have been created:

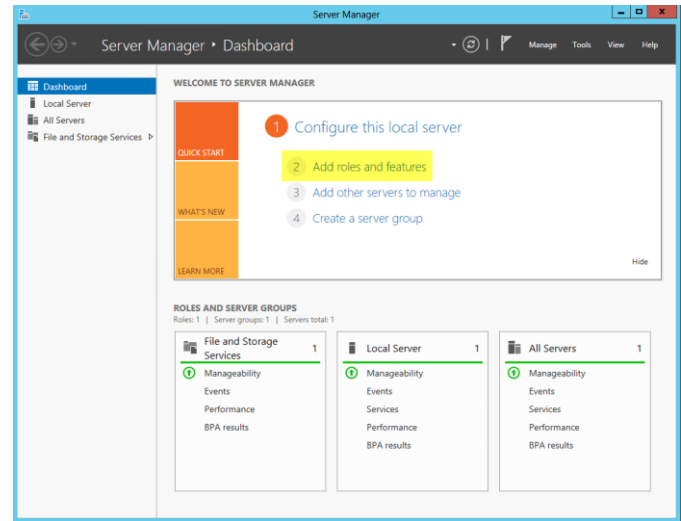
Security group name	Group scope	Members	Member of
<DOMAIN>\FT-SCO-Operators	Global		
<DOMAIN>\FT-SCO-Admins	Global	<DOMAIN>\FT-SCO-SVC	<p>Local Administrators</p> <p>Target Active Directory domain</p> <p>BUILTIN\Distributed COM Users</p>

Add the .NET Framework 3.5 Feature

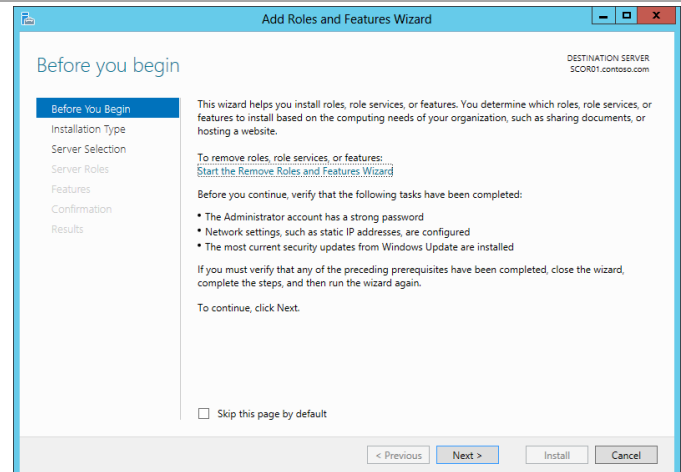
The Orchestrator installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5 Feature.

- Perform the following steps on all **Operations Manager** virtual machines.

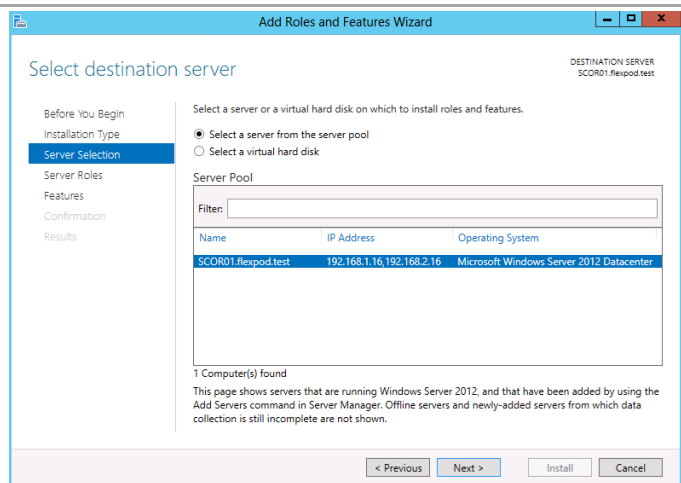
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



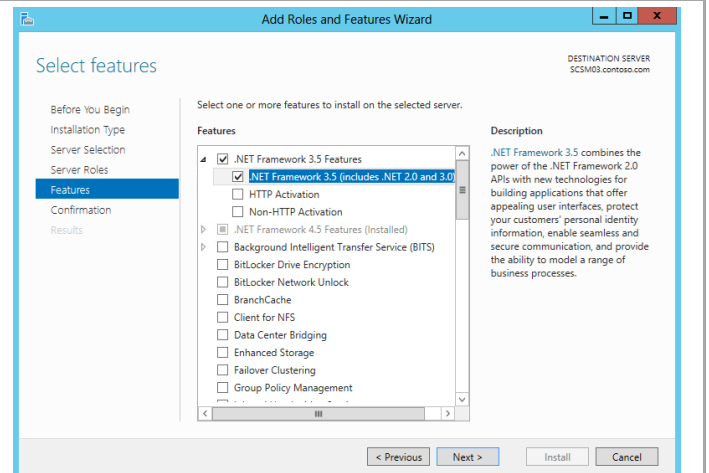
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



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.



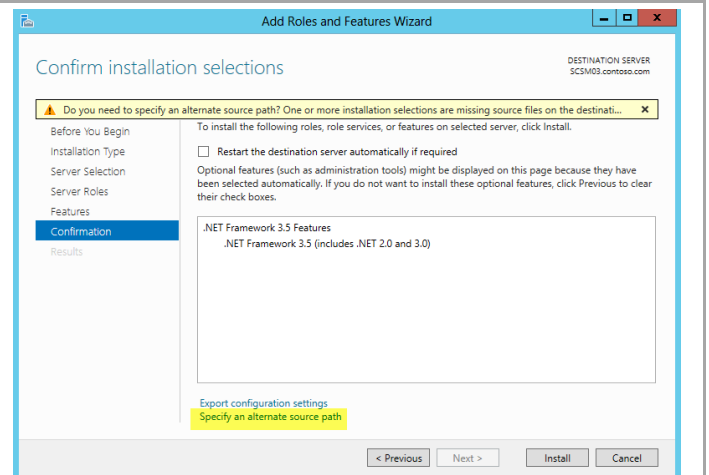
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



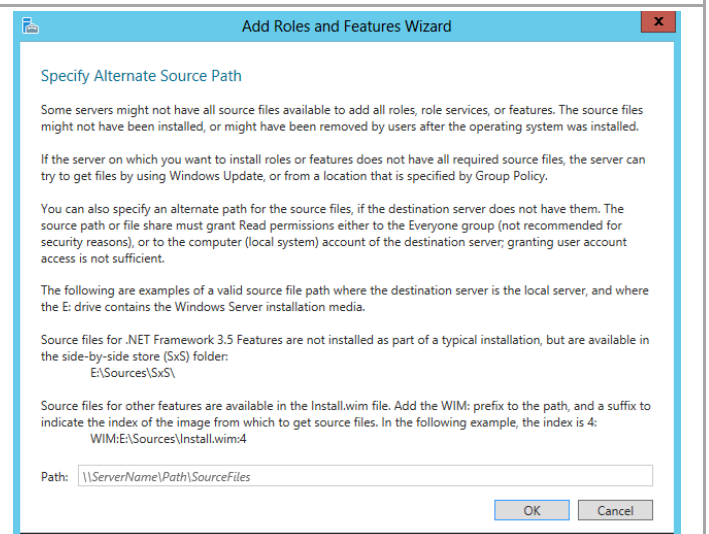
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

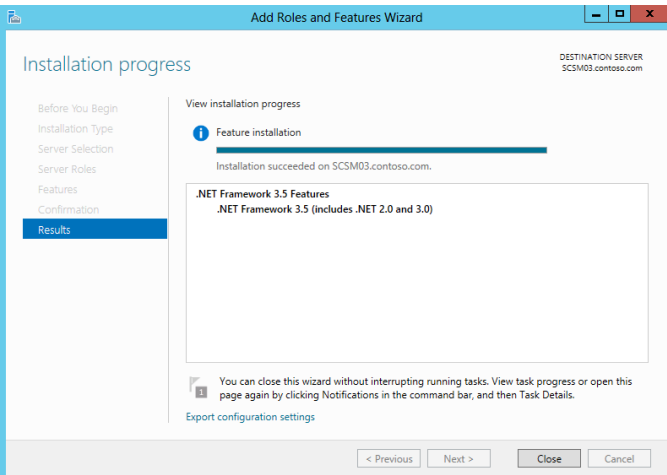
*Also, If the server does not have internet access an alternate source path can be specified by clicking the **Specify and alternate source patch link**.*



For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location be specified for the installation.



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



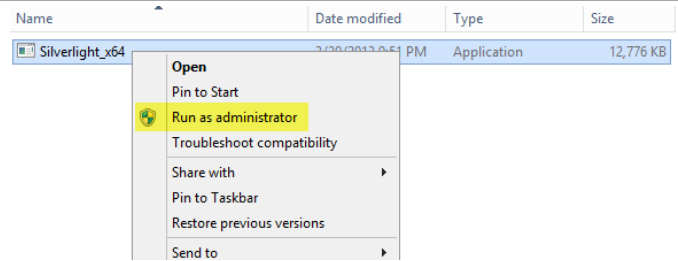
Note that while the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.



Install the Silverlight Runtime

► Perform the following steps on the **Orchestrator** virtual machine.

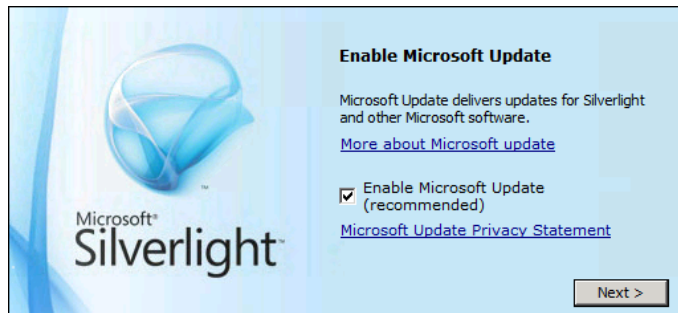
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.



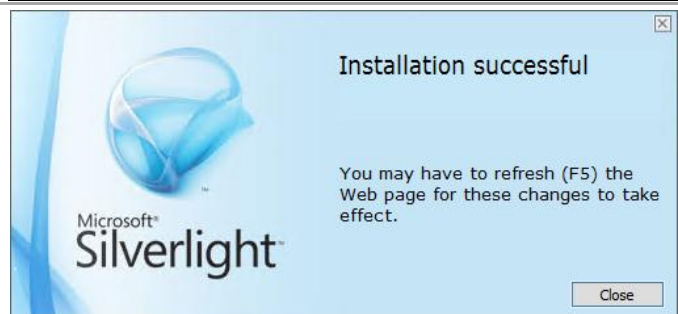
In the **Install Silverlight** dialog, click **Install now**.



In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** checkbox based on organizational preferences and click **Next** to continue.



In the **Installation Successful** dialog, click **Close** to exit the installation.



19.3 Installation

Install the Orchestrator Runbook, Web Service and Designer Server

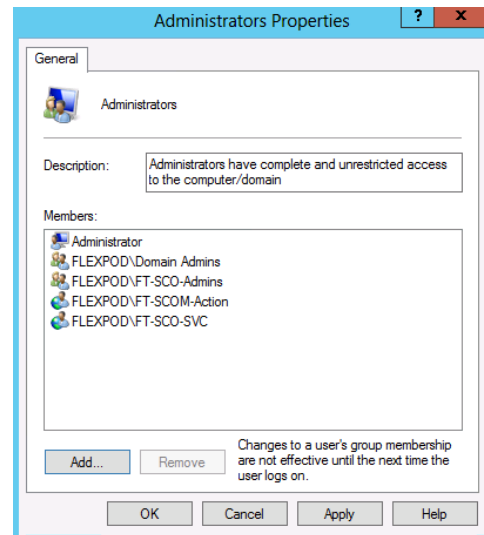
The following steps need to be completed in order to install the Orchestrator Runbook Server component.

► Perform the following steps on the **Orchestrator** virtual machine.

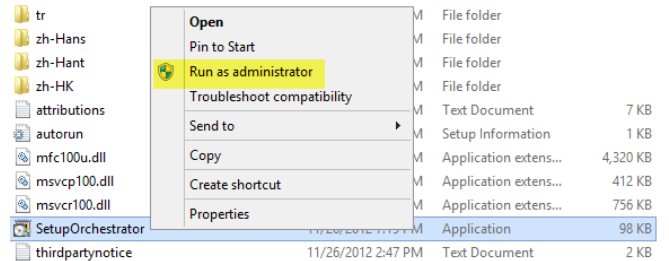
Log on to the Orchestrator virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:

- Orchestrator service account.
- Orchestrator Admins group.
- Operations Manager Action account.



Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** from the context menu to begin setup.



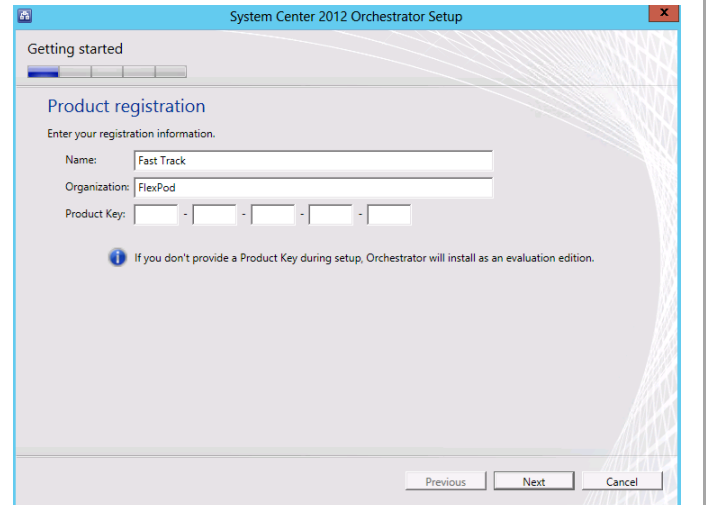
The Orchestrator installation wizard will begin. At the splash page, click **Install** to begin the Orchestrator server installation.



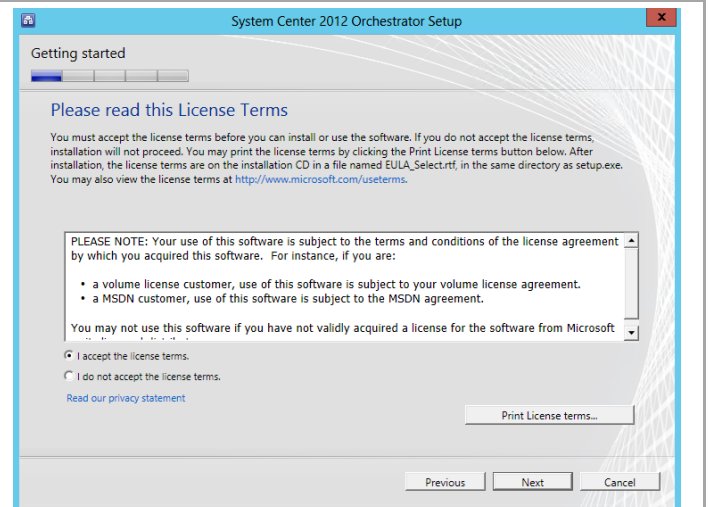
In the **Product registration information** dialog, provide the following information in the provided text boxes:

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

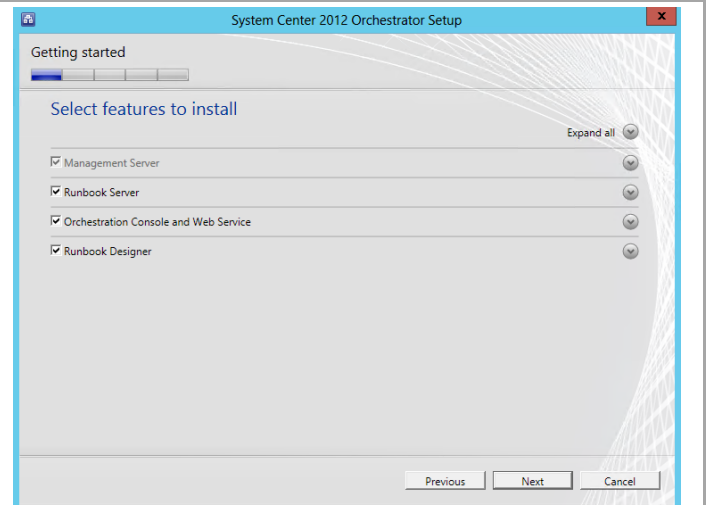
Click **Next** to continue.



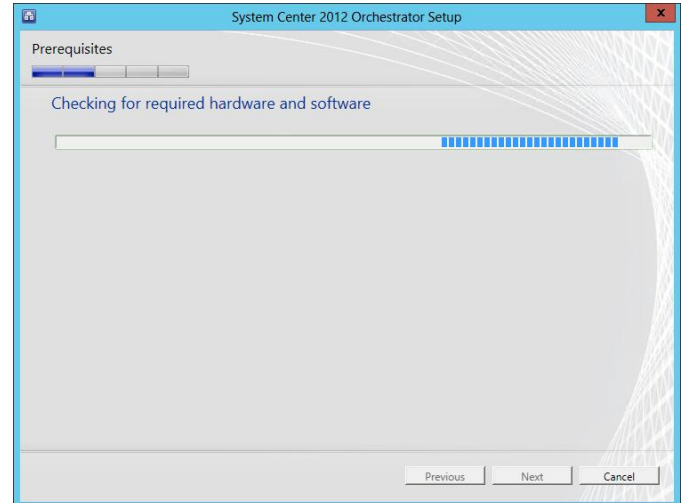
In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option checkbox is selected and click **Next** to continue.



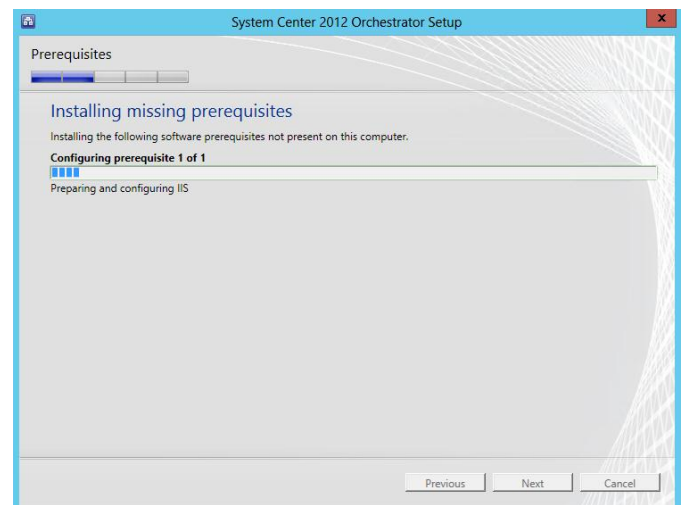
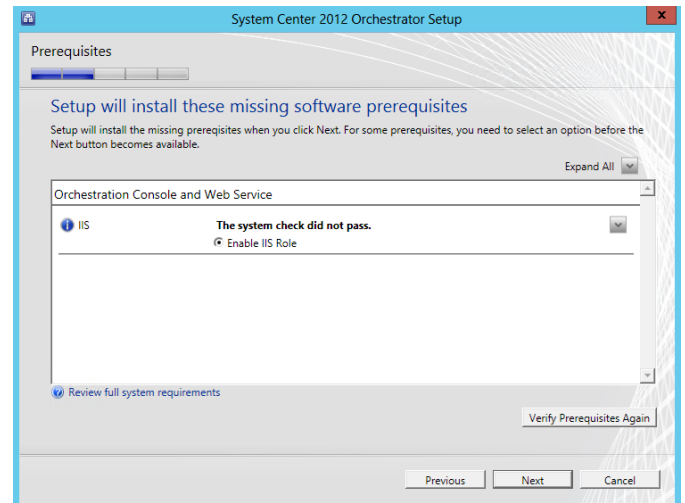
In the **Select Features to install** dialog, select the **Management Server** (default selected), **Runbook server**, **Orchestration console and web service**, **Runbook Designer** check boxes and click **Next** to continue.



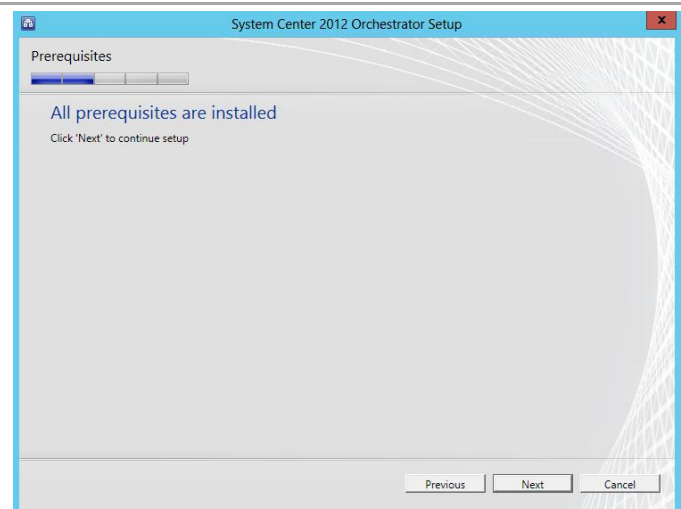
The **Checking for required hardware and software** dialog will appear to verify the installation prerequisites. Once validation completes, click **Next** to continue.



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. Once completed, click **Next** to continue.

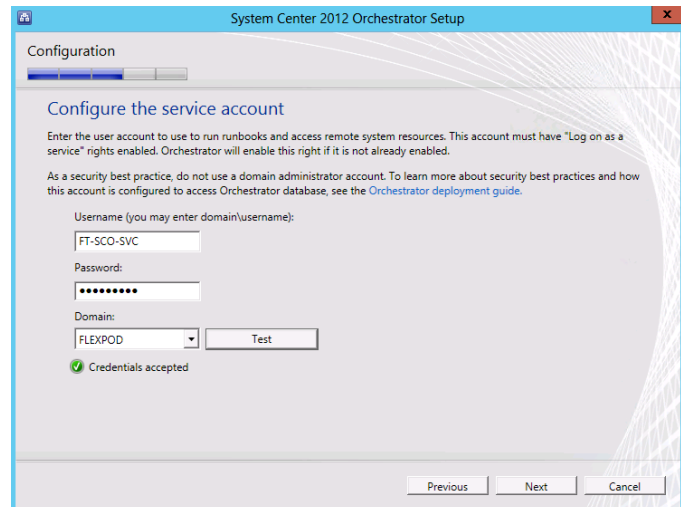


Once the installation of the missing prerequisites is completed, click **Next** to continue.



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.

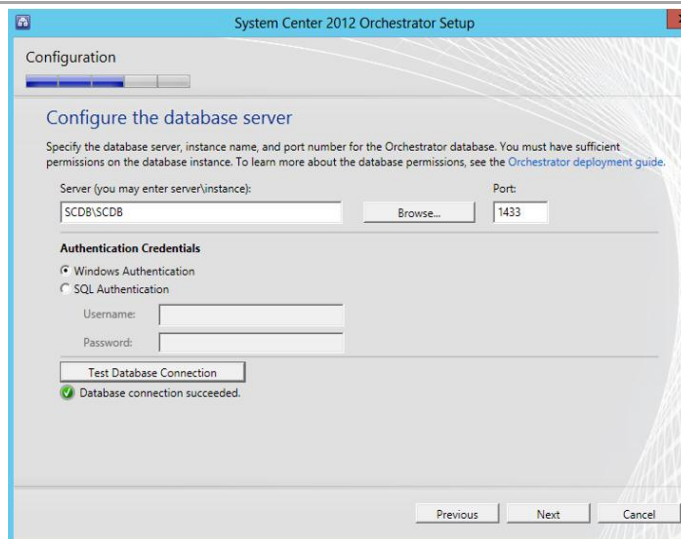
Before proceeding, click the **Test** button to verify the credentials provided.
Once successful, click **Next** to continue.



In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
- **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*

In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.
Once successful, click **Next** to continue.



In the **Configure the database** dialog in the **Database** section, select the **New Database** option. Specify the default database name of *Orchestrator*.

Click **Next** to continue.

The screenshot shows the 'Configure the database' step in the 'System Center 2012 Orchestrator Setup' wizard. The 'Database' section has two options: 'New database' (selected) and 'Existing database'. The 'New database' option has a text box containing 'Orchestrator'. The 'Existing database' option has a dropdown menu. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

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.

The screenshot shows the 'Configure Orchestrator users group' step in the 'System Center 2012 Orchestrator Setup' wizard. The 'Orchestrator users group' section has a text box containing 'FLEXPOD/FT-SCO-Operators' and a 'Browse...' button. Below this, there is a checkbox labeled 'Grant remote access to the Runbook Designer' which is checked. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

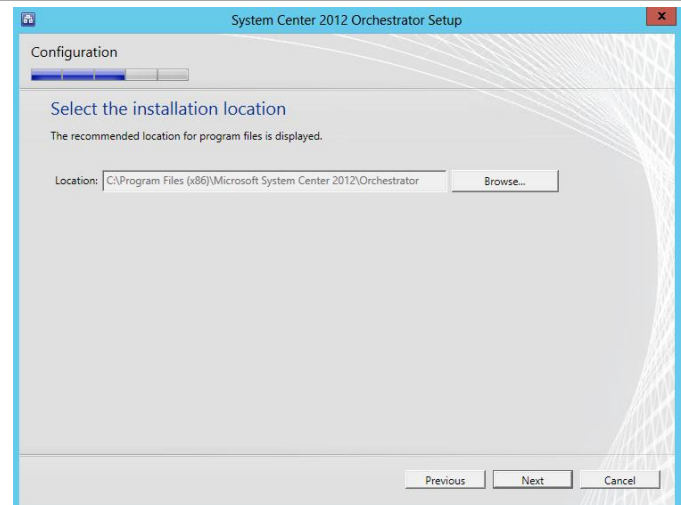
In the **Configure the ports for the web services** dialog, provide the following information in the provided text boxes:

- **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.*

Once successful, click **Next** to continue.

The screenshot shows the 'Configure the ports for the web services' step in the 'System Center 2012 Orchestrator Setup' wizard. The 'Web service port' section has a text box containing '81'. The 'Orchestration console port' section has a text box containing '82'. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

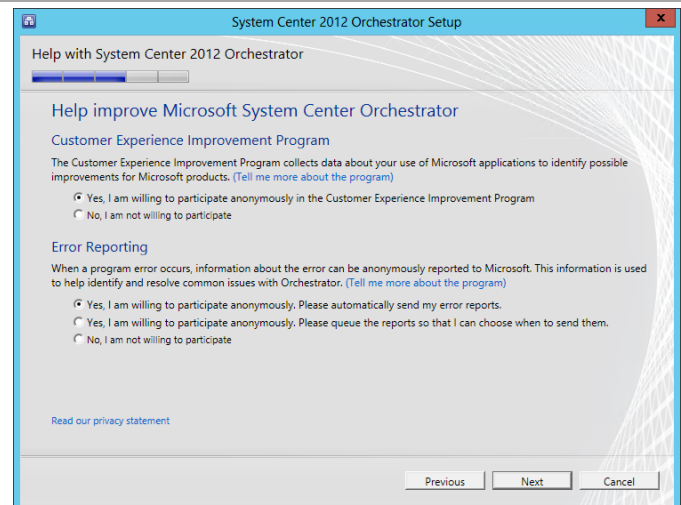
In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.



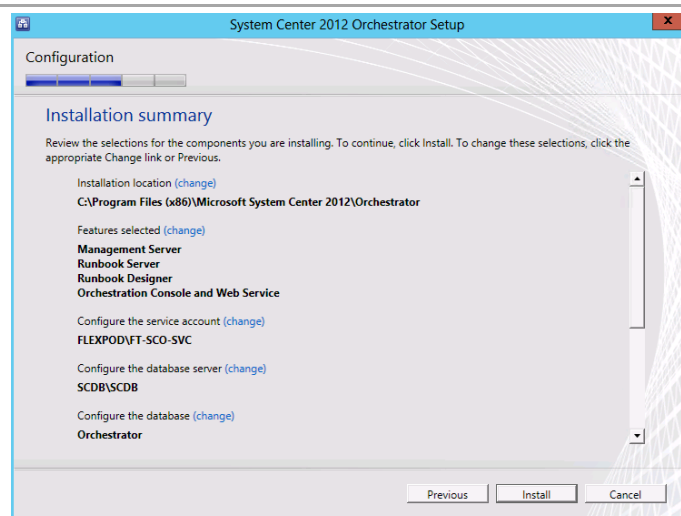
The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

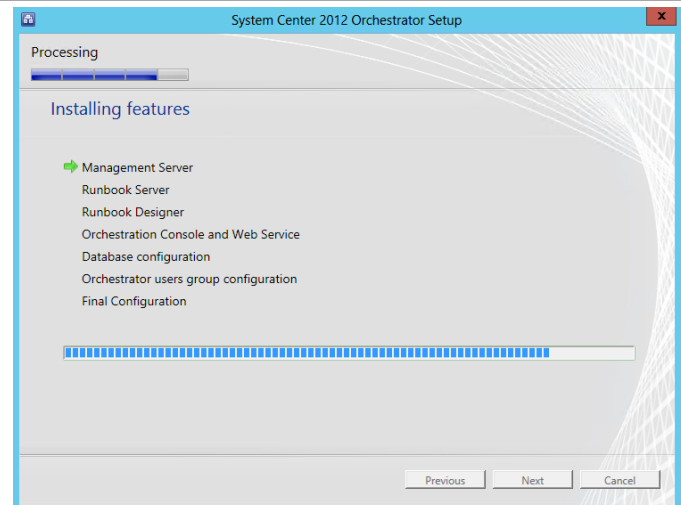
Select the appropriate option based on your organization's policies and click **Next** to continue.



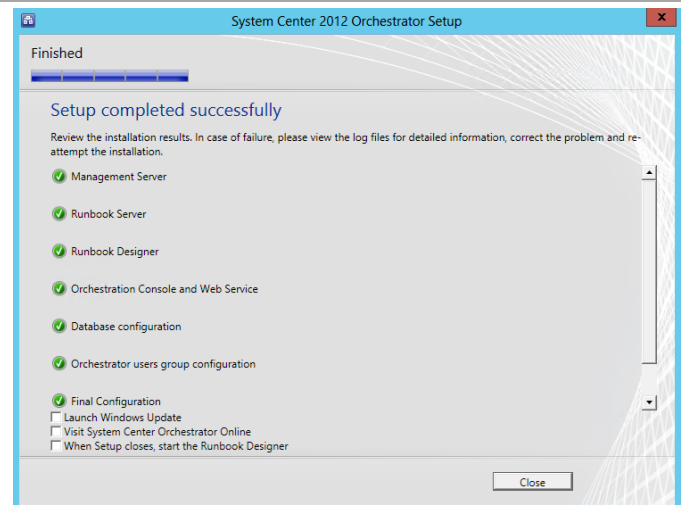
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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.

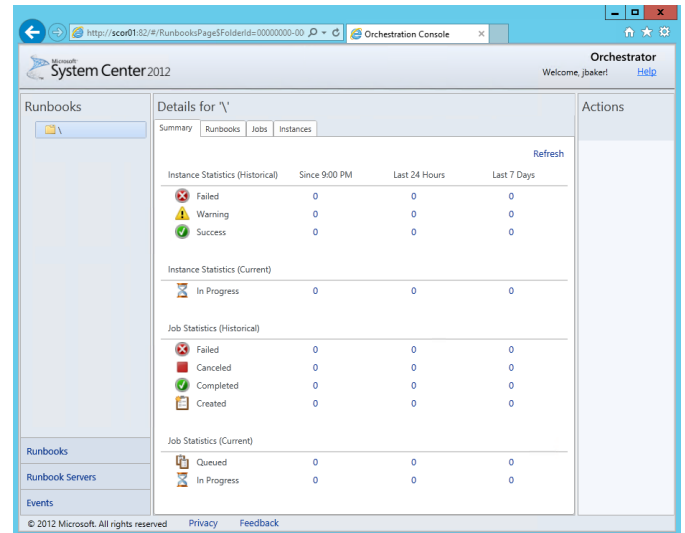


Once installed, verify that the Orchestrator roles installed properly by opening the consoles. From the **Start** screen, then select the **Orchestration Console** tile.

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.



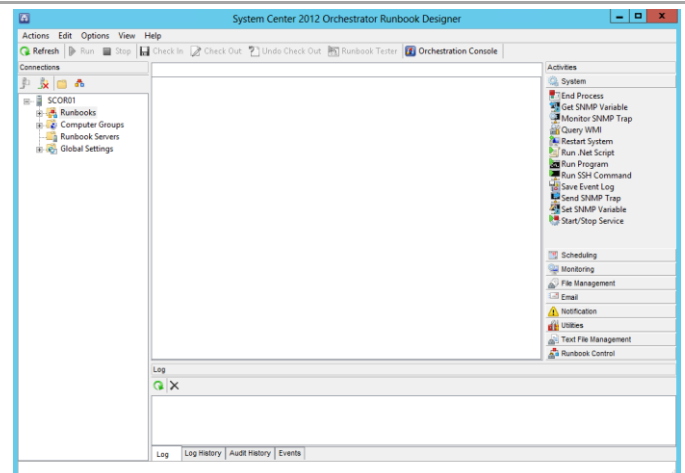
Validate that the **Orchestration console** performs properly in Internet Explorer.



From the **Start Menu**, then select the **Runbook Designer** tile.



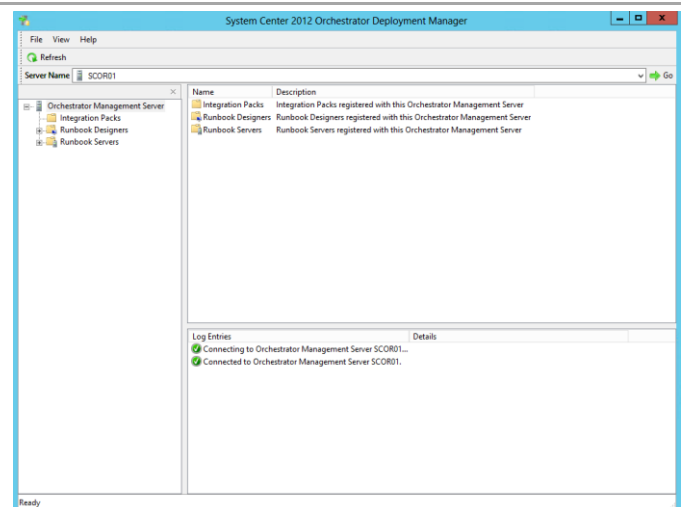
Launch the **Runbook Designer** console and verify that it performs properly.



From the **Start Menu**, then select the **Deployment Manager** tile.



Launch the **DeploymentManager** console and verify that it performs properly.

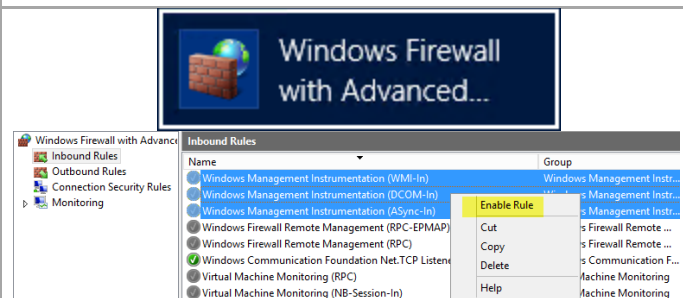


From the Start Screen, click on the Windows Firewall tile. Configure Windows Firewall for the first Orchestrator Runbook Server.²⁰

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)"
```

```
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
PS C:\Windows\system32>
```

²⁰ 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>.

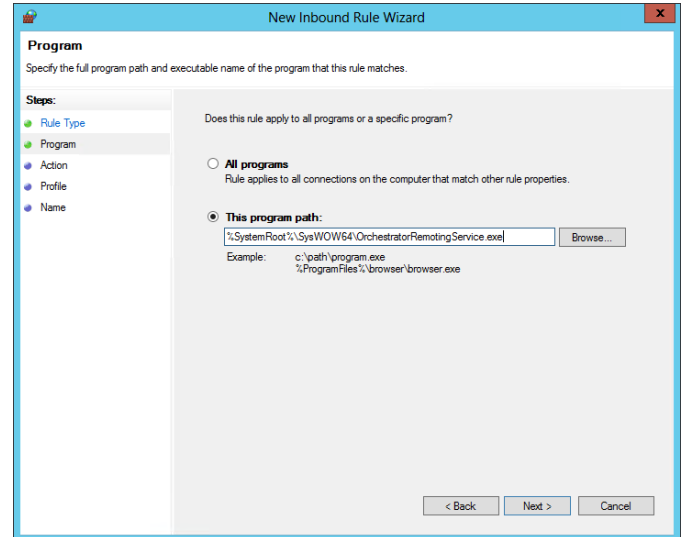
In Windows Firewall create a new Program rule using the following program path:

- %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 Discove...	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

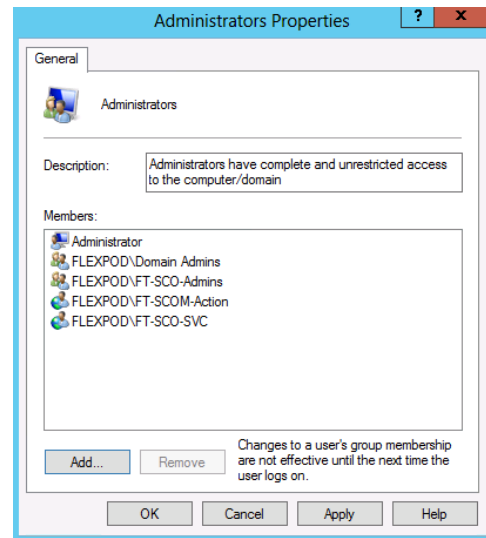
The following steps need to be completed in order to install an additional Orchestrator Runbook Server.

► Perform the following steps on the **second Orchestrator Runbook Server** virtual machine.

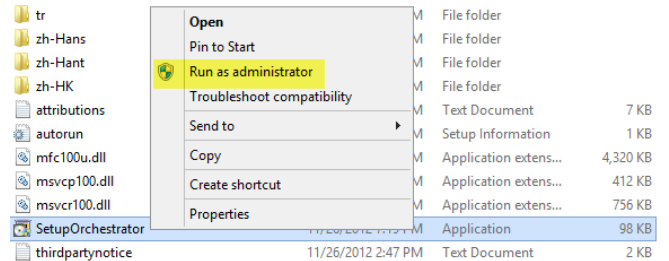
Log on to the Orchestrator virtual machine with a user with local admin rights.

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.



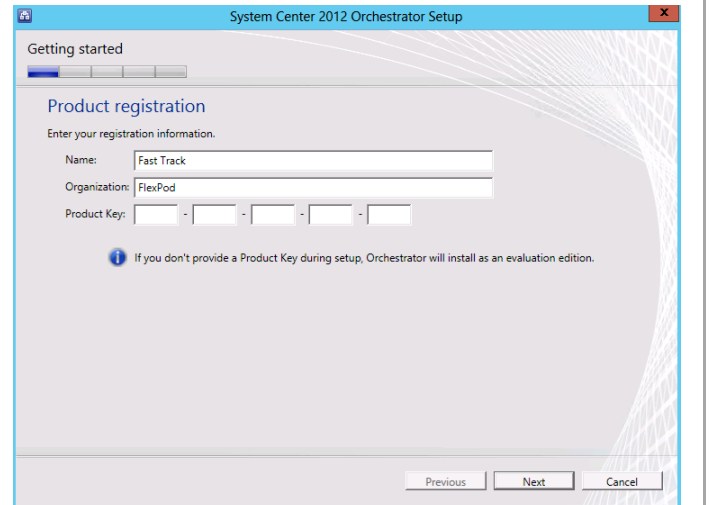
The Orchestrator installation wizard will begin. At the splash page, click **Install** begin the Orchestrator server installation.



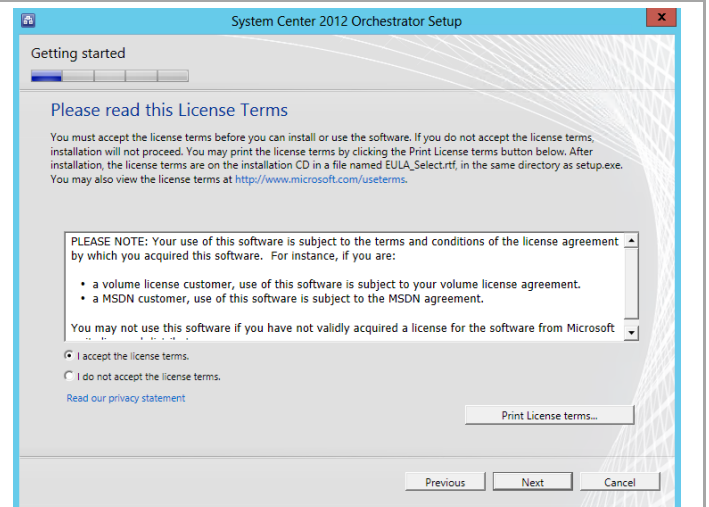
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **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.*

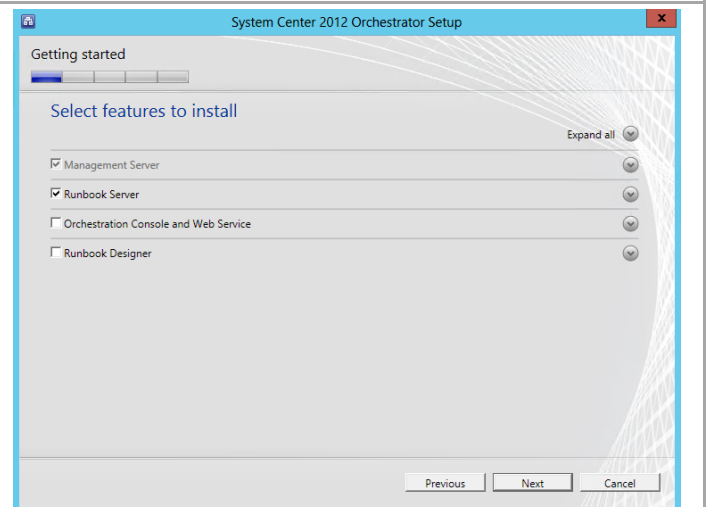
Click **Next** to continue.



In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option checkbox 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.
Once successful, click **Next** to continue.

The screenshot shows the 'Configure the service account' dialog box. It has a title bar 'System Center 2012 Orchestrator Setup' and a subtitle 'Configuration'. The main heading is 'Configure the service account'. Below it, there is explanatory text: '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.' and a security best practice note. The form includes fields for 'Username (you may enter domain\username):' with the value 'FT-SCO-SVC', 'Password:' with masked characters, and 'Domain:' with a dropdown menu showing 'FLEXPOD'. A 'Test' button is next to the domain field. A green checkmark and the text 'Credentials accepted' are displayed below the fields. At the bottom are 'Previous', 'Next', and 'Cancel' buttons.

In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – *specify the SQL Server cluster name and instance name created in the steps above.*
- **Port** – *specify the TCP port used for the SQL Server if not the default. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack will be used.*

In the **Authentication Credentials** section, select the **Windows Authentication** option and click the **Test Database Connection** button.

Once successful, click **Next** to continue.

The screenshot shows the 'Configure the database server' dialog box. It has a title bar 'System Center 2012 Orchestrator Setup' and a subtitle 'Configuration'. The main heading is 'Configure the database server'. Below it, there is explanatory text: '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.' The form includes a 'Server (you may enter server/instance):' field with the value 'SCDB\SCDB' and a 'Browse...' button, and a 'Port:' field with the value '1433'. Under the 'Authentication Credentials' section, the 'Windows Authentication' radio button is selected. There are fields for 'Username:' and 'Password:'. A 'Test Database Connection' button is present. A green checkmark and the text 'Database connection succeeded.' are displayed below the fields. At the bottom are 'Previous', 'Next', and 'Cancel' buttons.

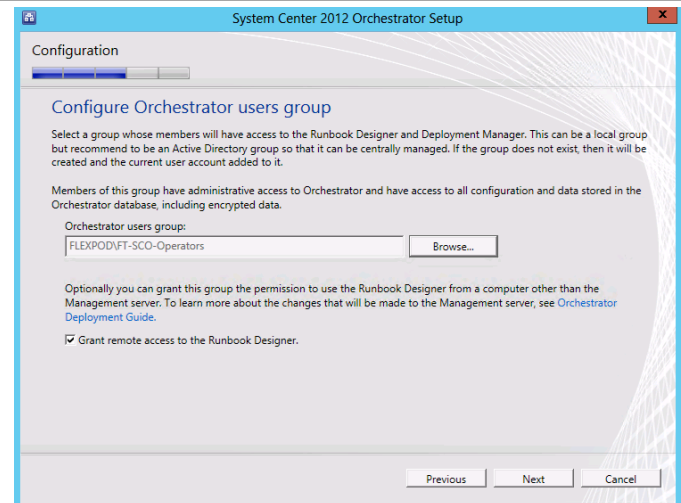
In the **Configure the database** dialog in the **Database** section, select the **Existing Database** option. Select the default database name of *Orchestrator* from the drop-down menu.

Click **Next** to continue.

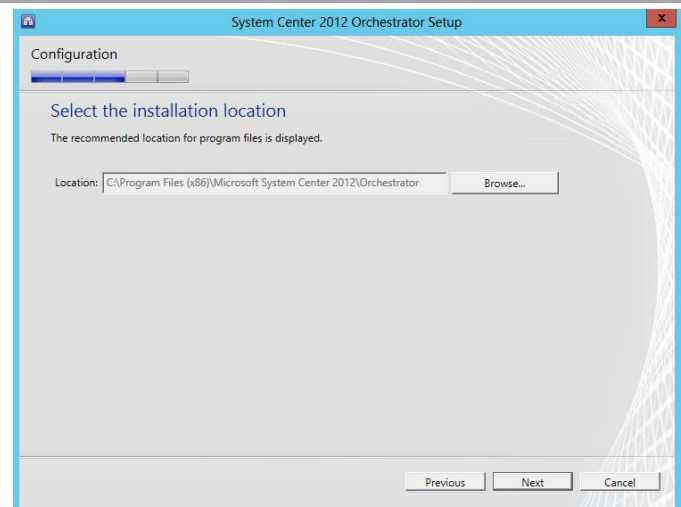
The screenshot shows the 'Configure the database' dialog box. It has a title bar 'System Center 2012 Orchestrator Setup' and a subtitle 'Configuration'. The main heading is 'Configure the database'. Below it, there is explanatory text: 'Specify a new or existing database. You must have sufficient permissions on the database instance.' and a note about the 'Existing Database' option. The form includes a 'Database' section with 'Specify a database.' and two options: 'New database:' with a text field containing 'Orchestrator', and 'Existing database:' with a dropdown menu also showing 'Orchestrator'. At the bottom are 'Previous', 'Next', and 'Cancel' buttons.

In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse...** and selecting the associated group. For Fast Track, this is the Orchestrator operators group.

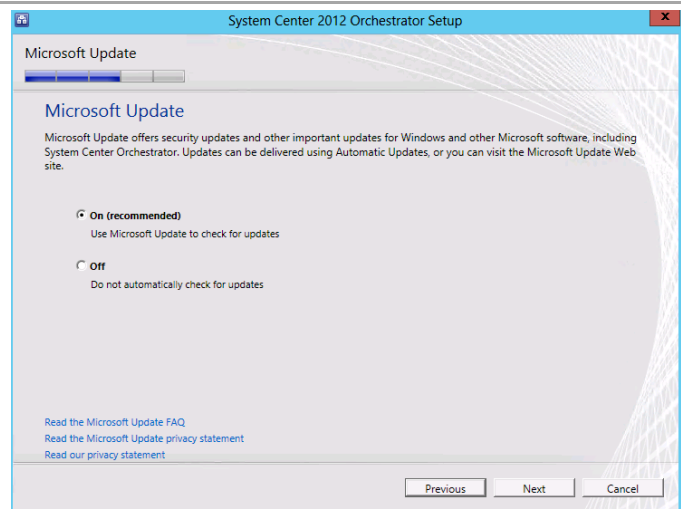
Verify that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



In the **Select the installation location** dialog, specify a location or accept the default location of *%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator* for the installation. Click **Next** to continue.



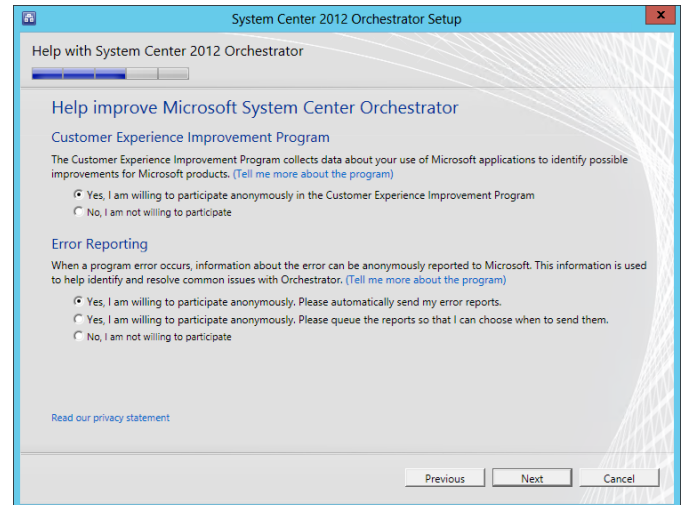
Depending on the current configuration of the server the Microsoft Updates Dialog may appear. The **Microsoft Update** dialog provides options for participating in automatic updates for Orchestrator. Select the appropriate option based on your organization's policies and click **Next** to continue.



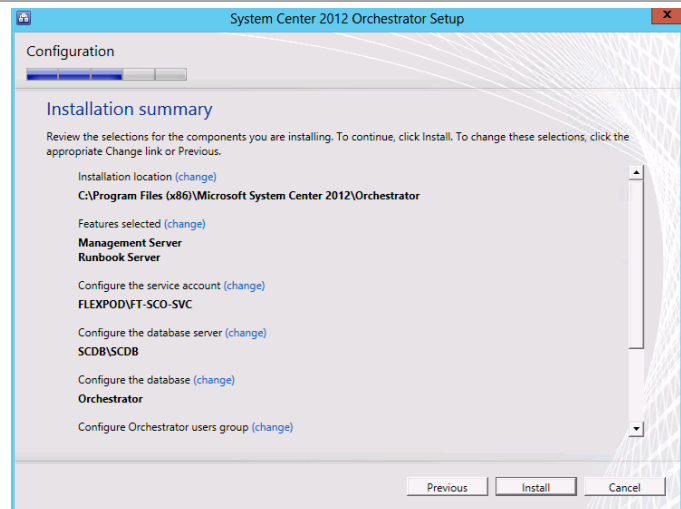
The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. This includes:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

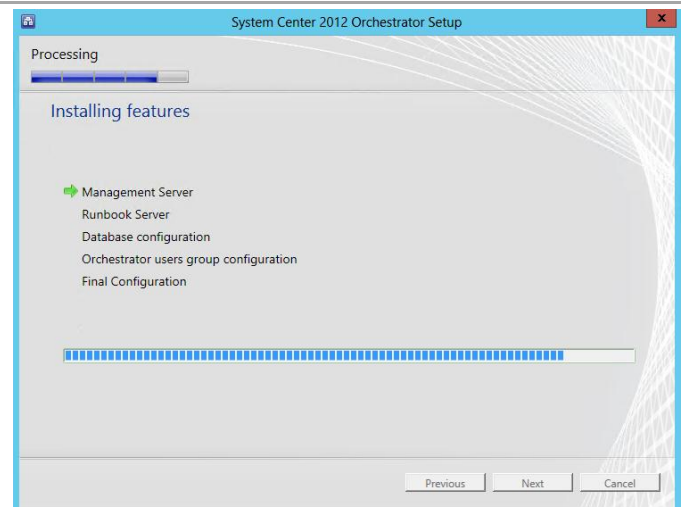
Select the appropriate option based on your organization's policies and click **Next** to continue.



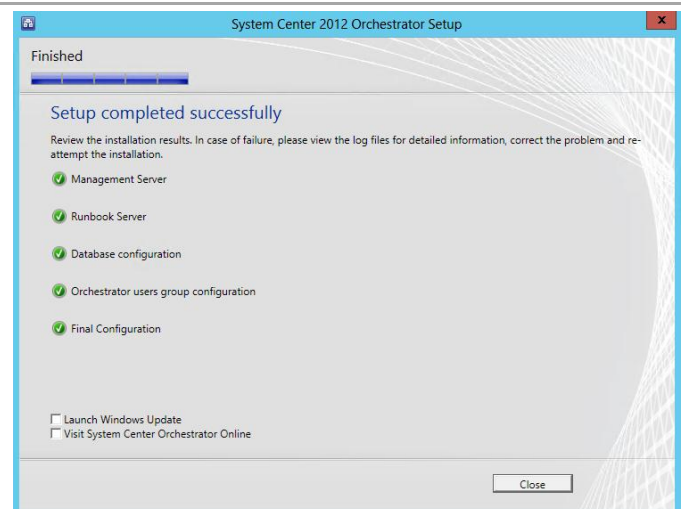
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



In the **Installing features** dialog, the installation will proceed and show progress.



The **Setup completed successfully** dialog will appear once all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.



Configure Windows Firewall for the second Orchestrator Runbook Server.²¹

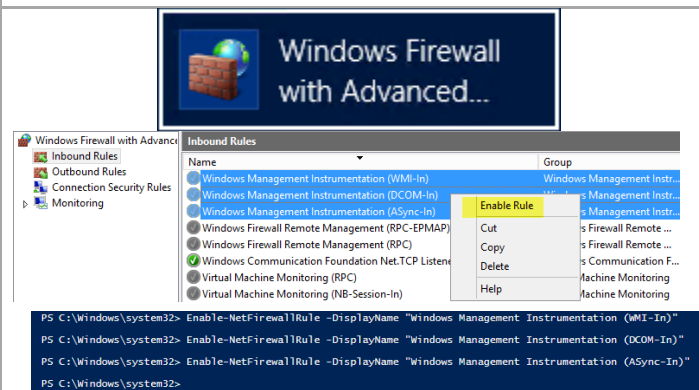
If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:

- 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)"
```



²¹ 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:

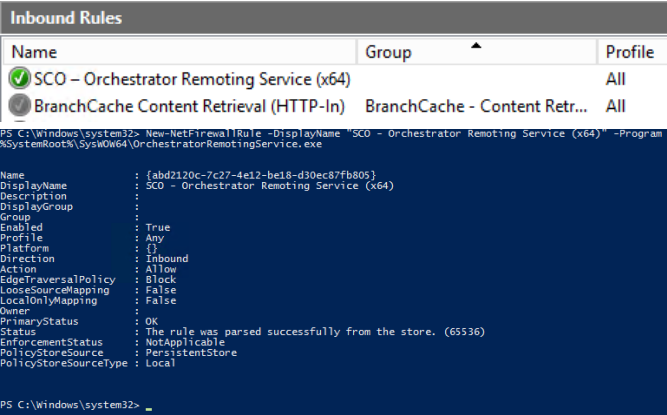
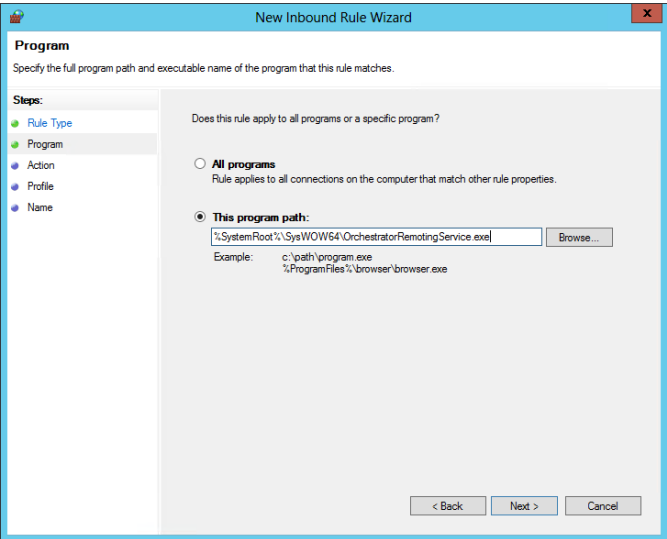
- %SystemRoot%\SysWOW64\orchestratorRemotingService.exe

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\OrchestratorRemoting  
Service.exe
```

Restart the Orchestrator server.



19.4 Install Cisco UCS Integration Pack

The following steps need to be completed in order to install the Cisco UCS Integration Pack. Download the integration pack from <http://developer.cisco.com/web/unifiedcomputing/systemcenter>

► Perform the following steps on the **Orchestrator** virtual machines.

19.5 Post-Installation Tasks

When the installation is complete, install and configure Orchestrator Integration Packs on the target Runbook Servers.

Install the Virtual Machine Manager Console

► Perform the following steps on the **Orchestrator** virtual machines.

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.

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

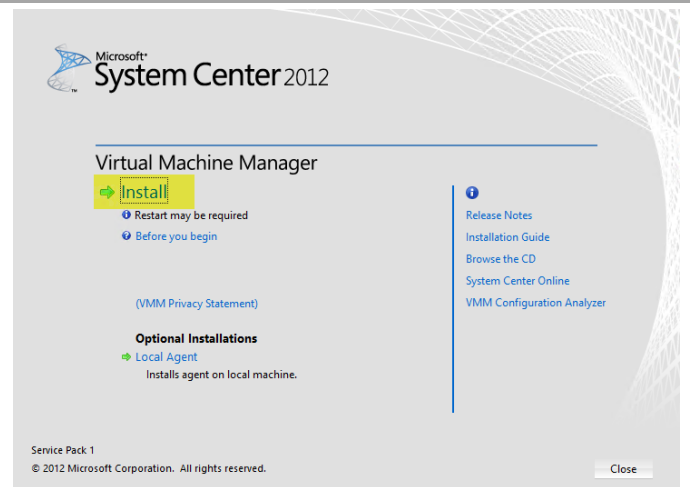
Open

Pin to Start

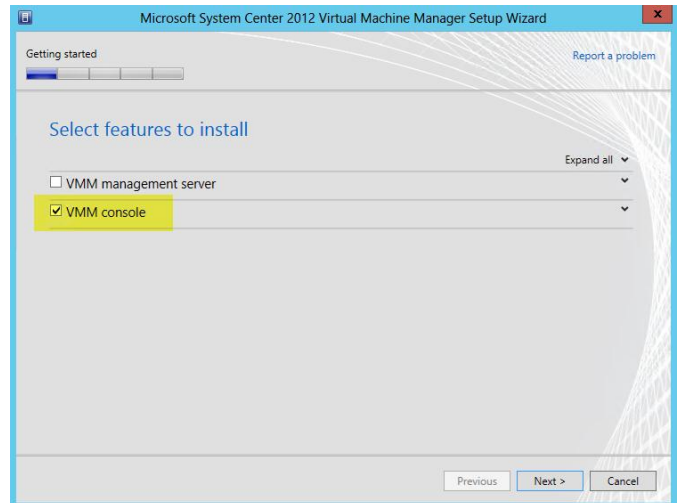
Run as administrator

Troubleshoot compatibility

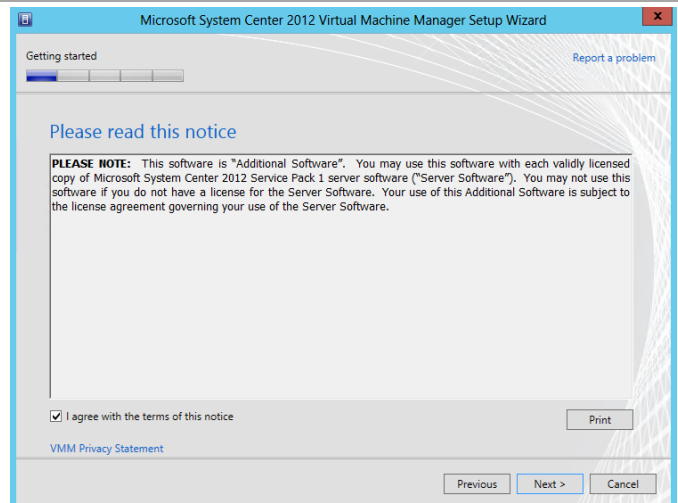
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



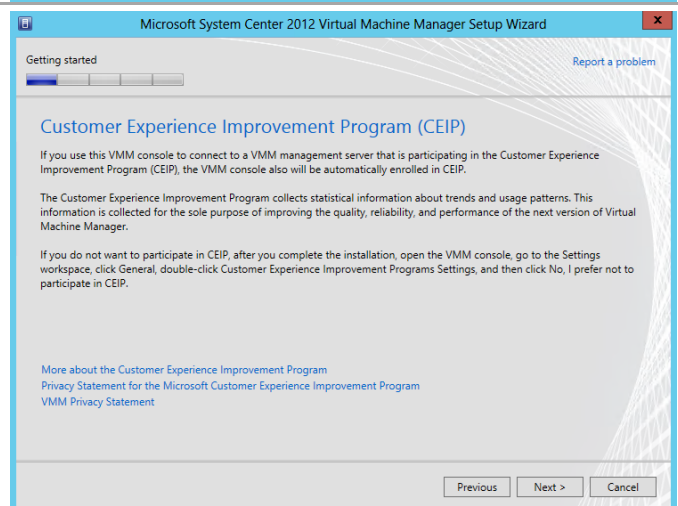
In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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.



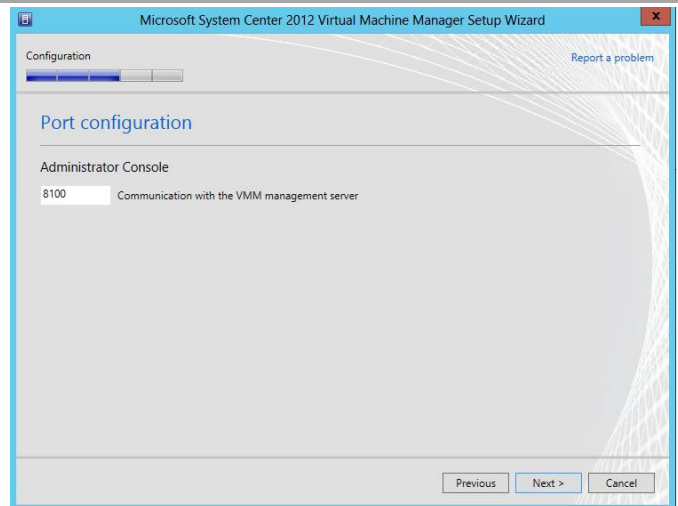
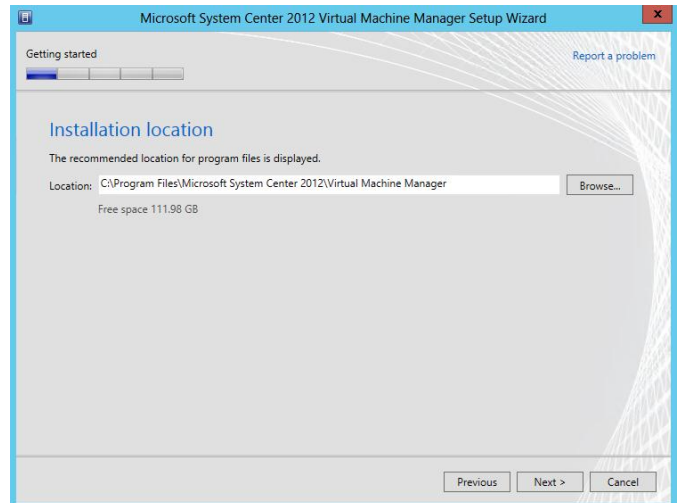
In the **Customer Experience Improvement Program** dialog, click **Next** to continue.



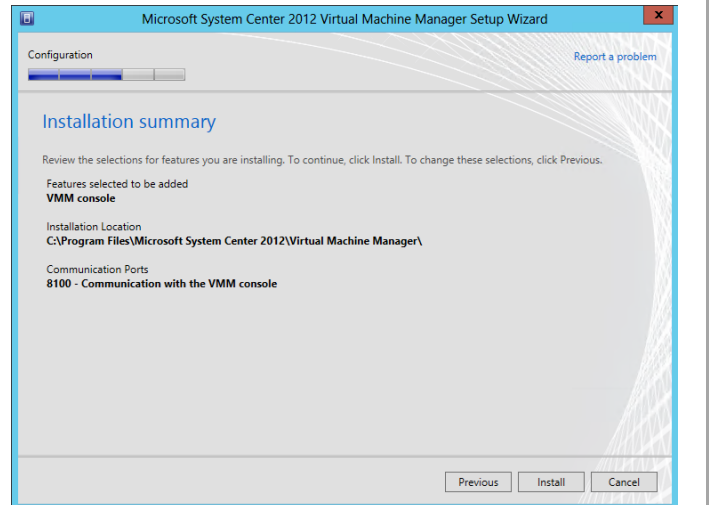
Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. 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.

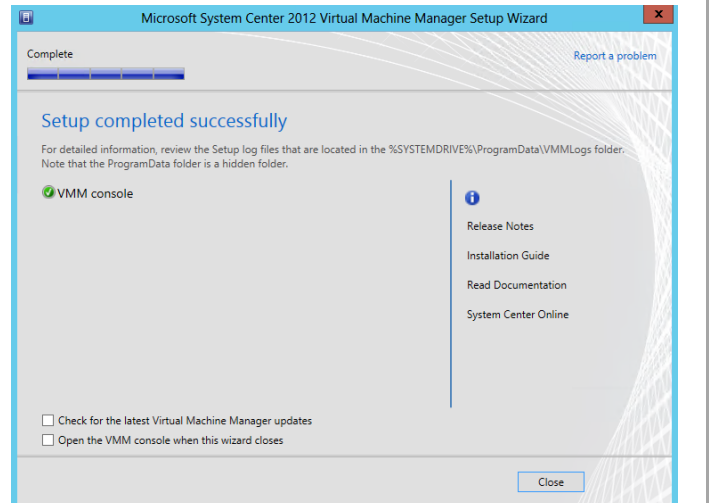
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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

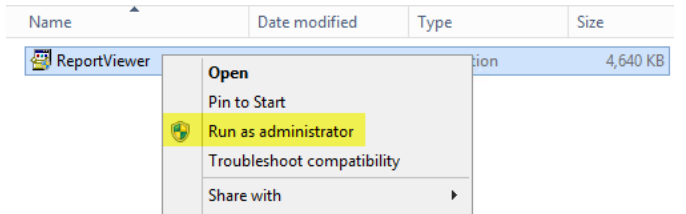


Install the Microsoft Report Viewer 2010 SP1

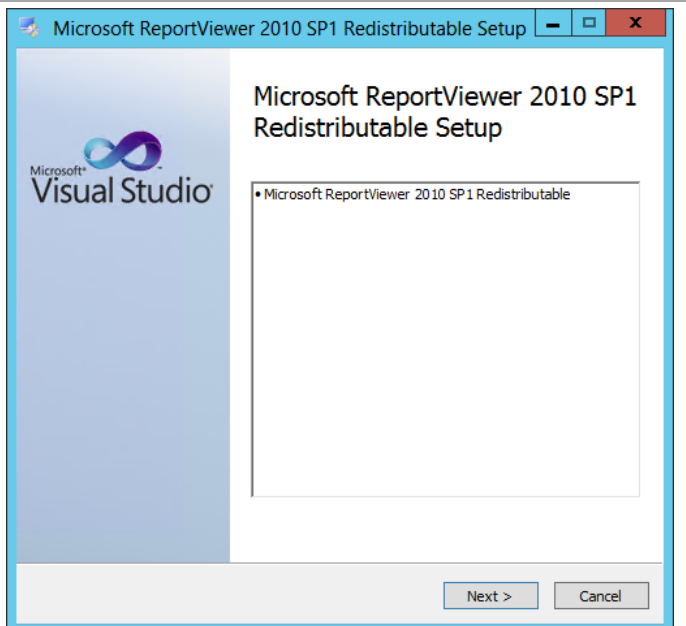
Additionally, inside Orchestrator the Operations Manager console is required, but this also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.²² Follow the provided steps to install the SP1 package.

► Perform the following steps on both **Orchestrator** virtual machines.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.

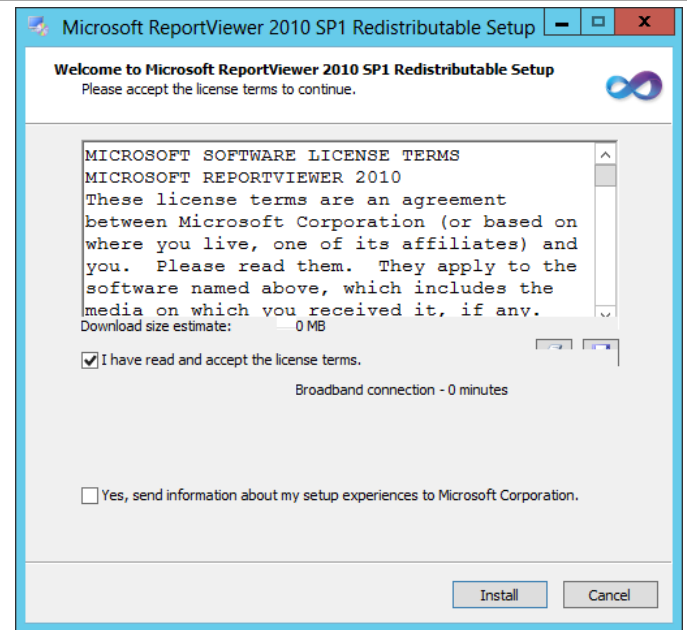


Within the **Microsoft ReportViewer 2010 SP1 Redistributable Setup** dialog, select **Next** to begin the installation.

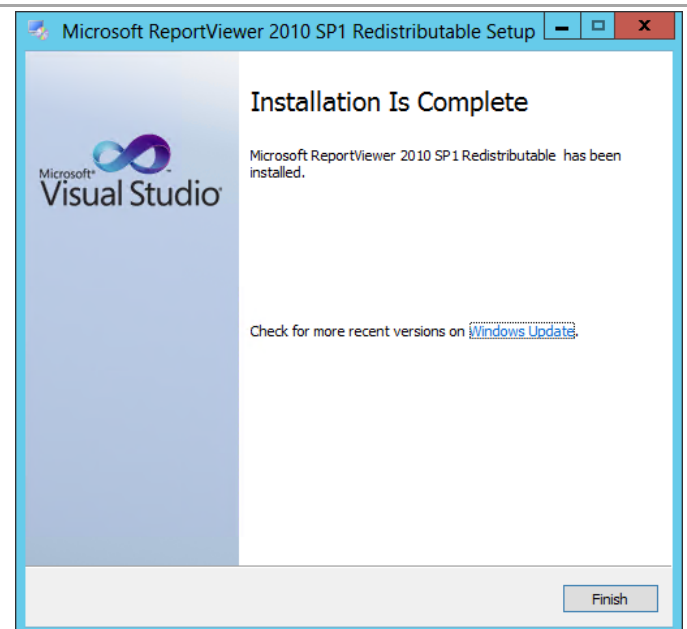


²² Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en>.

Select the **I have read and accept the license terms** check box and click **Install**.



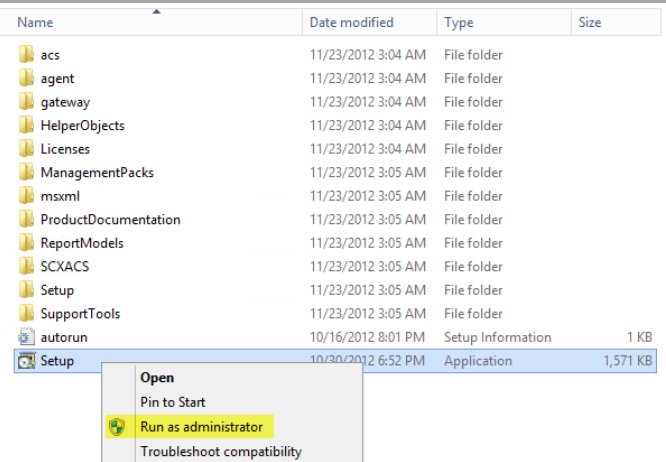
The installation progress will be displayed in the setup wizard. Once completed, click **Finish** to exit the installation.



Install the Operations Manager Console

► Perform the following steps on both of the **Orchestrator** virtual machines.

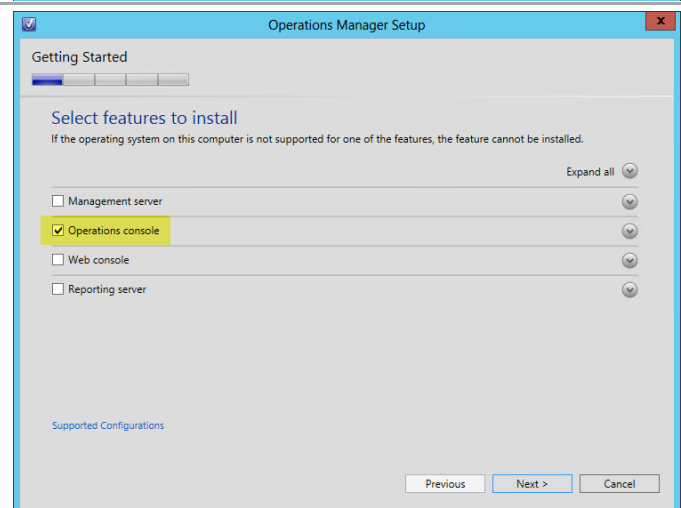
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



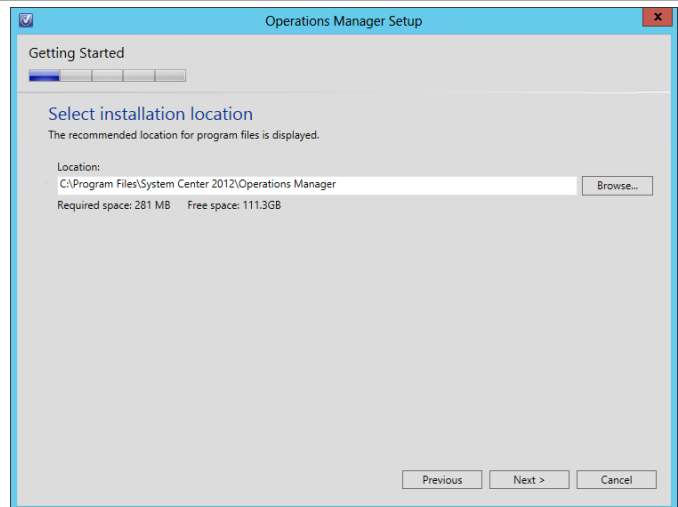
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



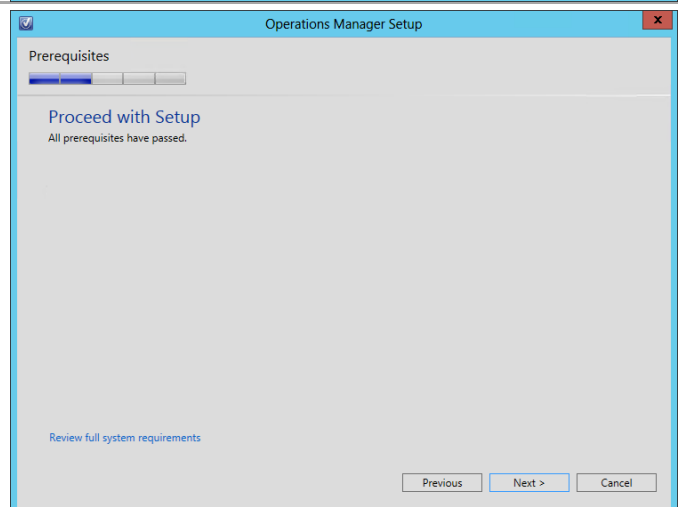
In the **Select features to install** dialog, verify that the **Operations console** checkbox is selected. Click **Next** to continue.



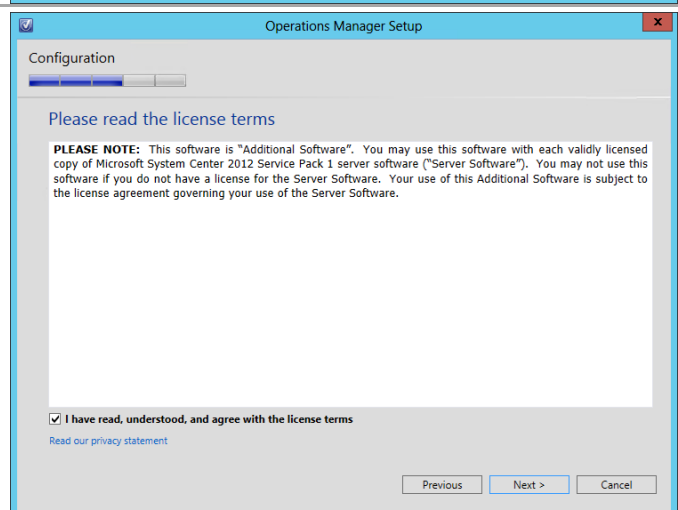
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.



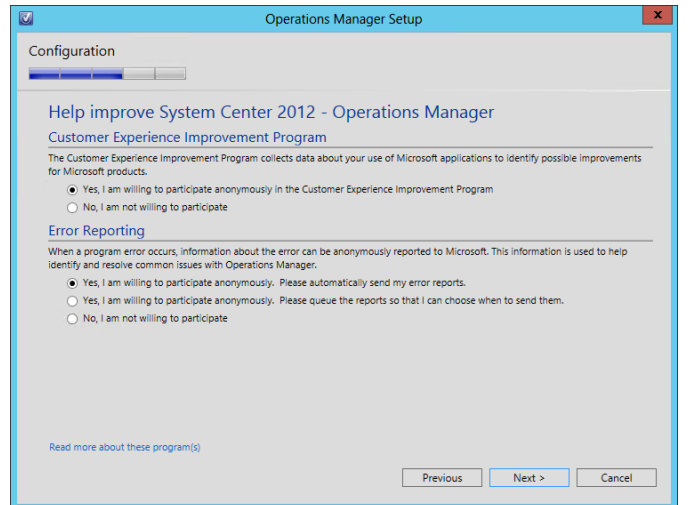
In the **Please read the license terms** dialog, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected and click **Next** to continue.



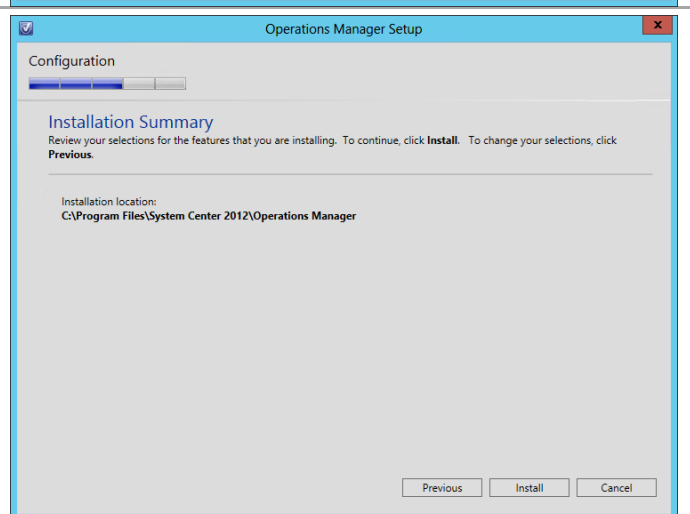
The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

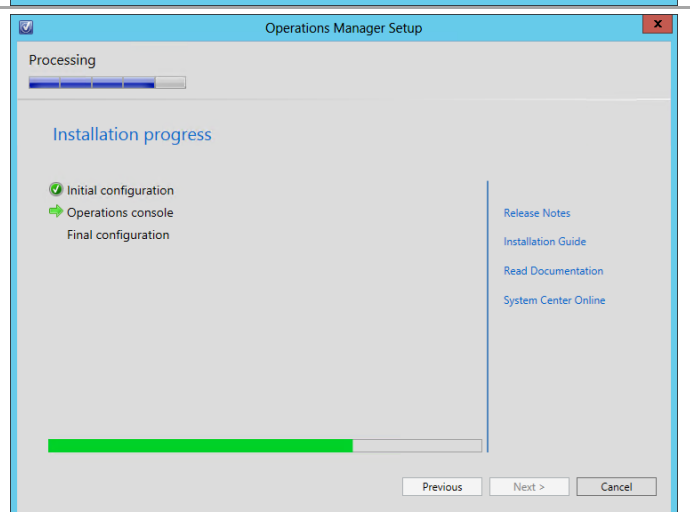
Select the appropriate option based on your organization's policies and click **Next** to continue.



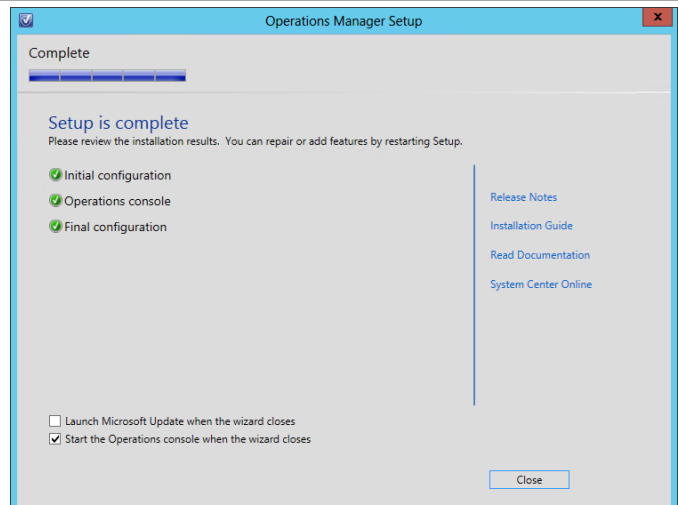
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



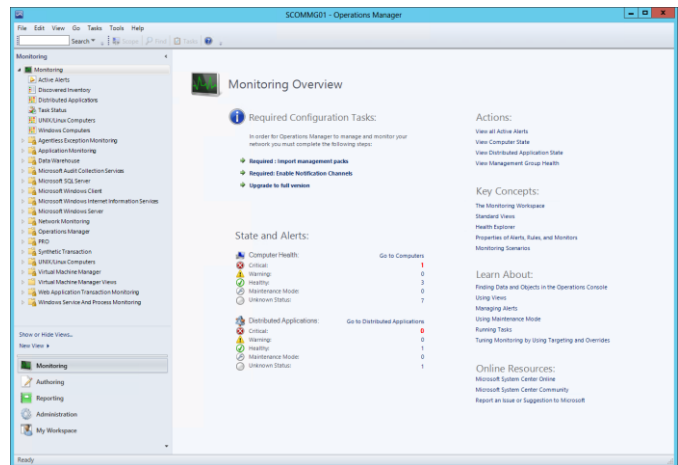
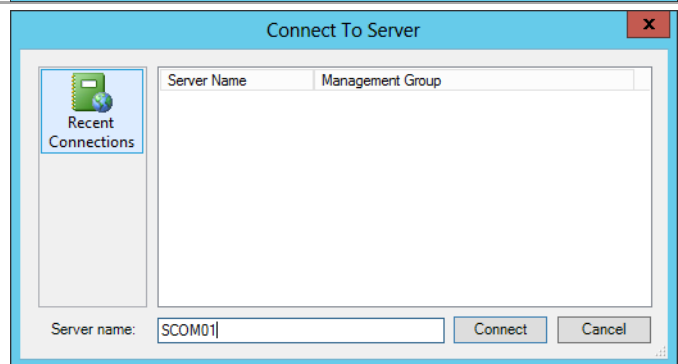
The installation progress will be displayed during the installation.



Once 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.



Once completed, the Operations Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



Install System Center 2012 SP1 and Cisco UCS Integration Packs

The following steps need to be completed in order to install the Orchestrator Integration Packs.

► Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

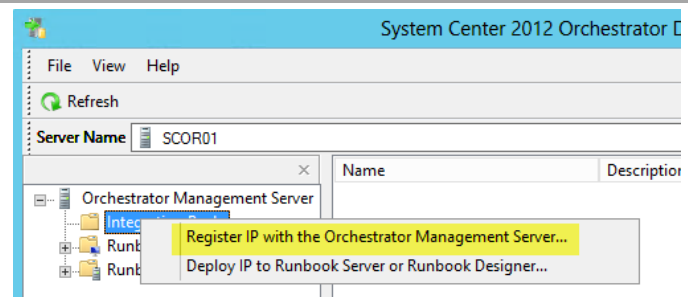
Download the System Center 2012 SP1 Integration Packs from <http://www.microsoft.com/en-us/download/details.aspx?id=34611> and expand them to a single location so the Orchestrator Integration Pack files are expanded.

Name	Date modified
attributions	3/14/2012 4:23 PM
Configuration_Manager_2007_Integration_Pack.oip	3/14/2012 5:11 PM
Data_Protection_Manager_2010_Integration_Pack.oip	3/14/2012 5:11 PM
Operations_Manager_2007_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Configuration_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Data_Protection_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Operations_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Service_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Virtual_Machine_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
Service_Manager_2010_Integration_Pack.oip	3/14/2012 5:11 PM
Virtual_Machine_Manager_2008_Integration_Pack.oip	3/14/2012 5:11 PM

From the **Start** screen, click the **Deployment Manager** tile.



In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Register IP with the Orchestrator Management Server...** option from the context menu.

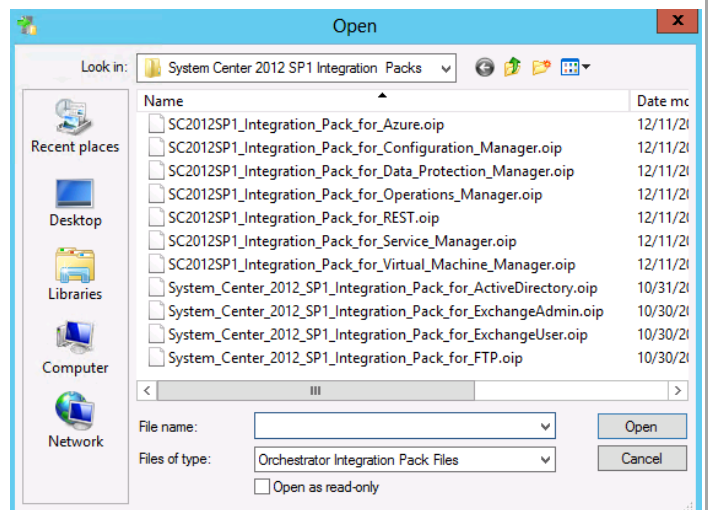
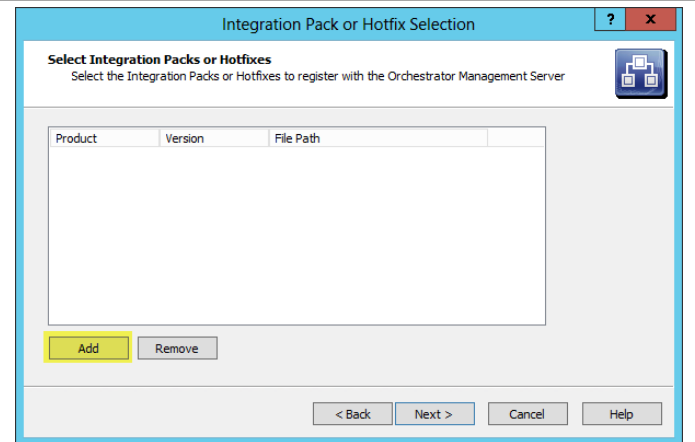


The **Integration Pack Registration Wizard** will appear. Click **Next** to continue.



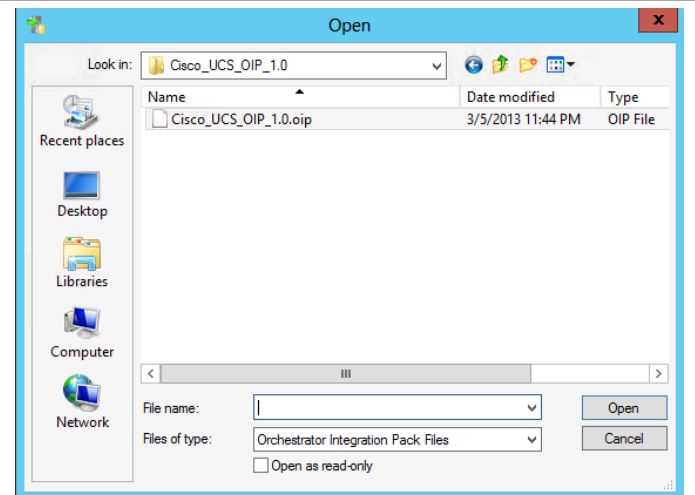
In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the expanded integration packs folder created earlier and select the following integration packs and click **Open**:

- System Center 2012 SP1 Configuration Manager.
- System Center 2012 SP1 Operations Manager.
- System Center 2012 SP1 Service Manager.
- System Center 2012 SP1 Virtual Machine Manager.

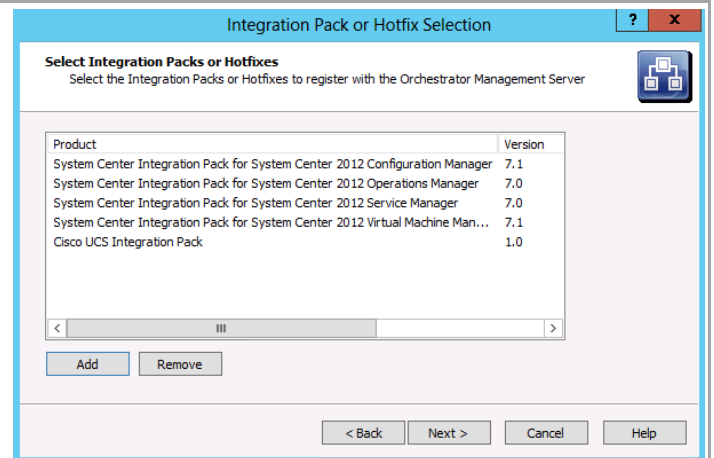


In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the location where the Cisco UCS OIP was extracted and select the following integration packs and click **Open**.

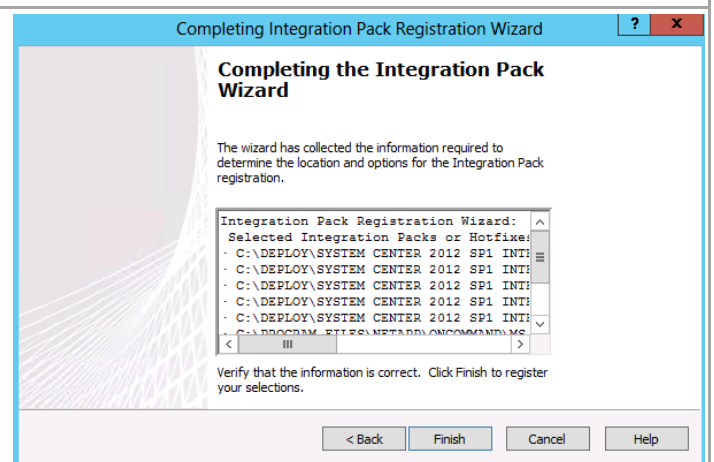
Cisco UCS OIP 1.0



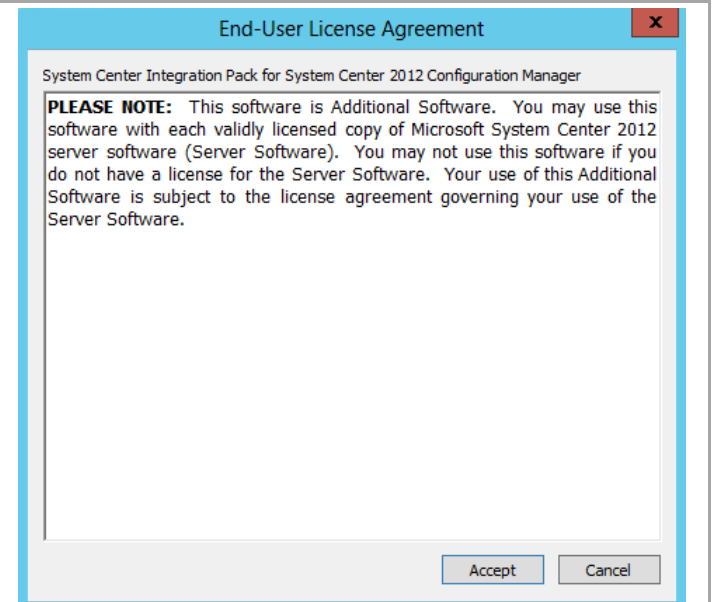
- Once all integration packs are selected, click **Next** to continue.



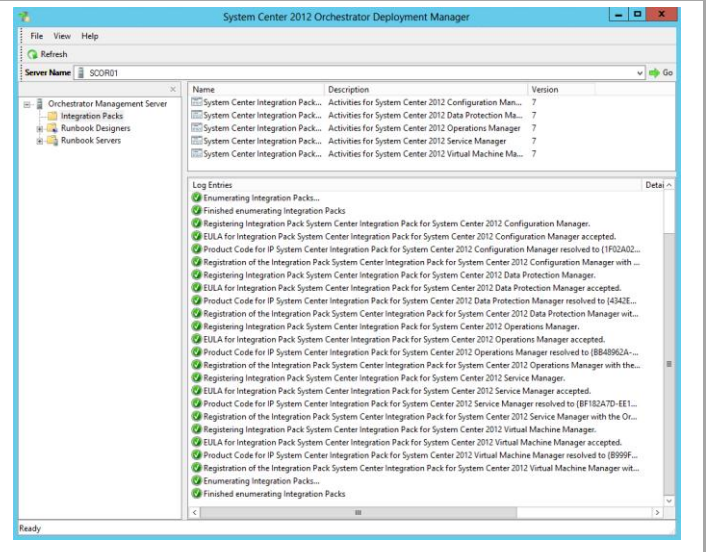
The **Completing the Integration Pack Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.



Once complete, each integration pack will be displayed in the Deployment Manager interface.



Deploy Integration Packs

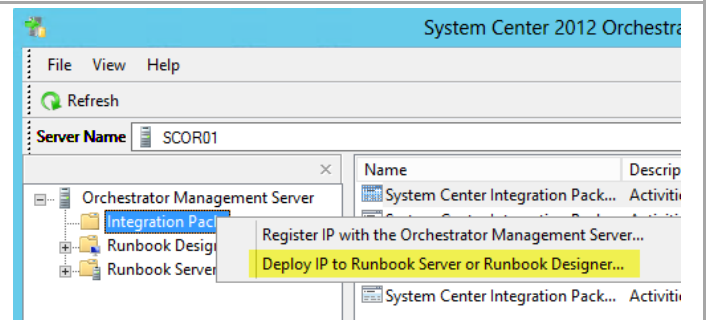
The following steps need to be completed in order to install the Orchestrator Integration Packs.²³

► Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

From the **Start** screen, click the **Deployment Manager** tile.

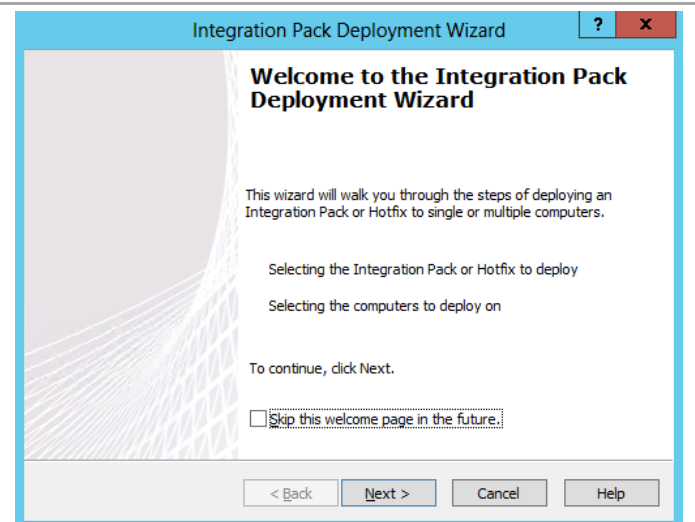


In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer...** option from the context menu.



²³ System Center 2012 SP1 – Orchestrator Component Add-ons and Extensions - <http://www.microsoft.com/en-us/download/details.aspx?id=34606>

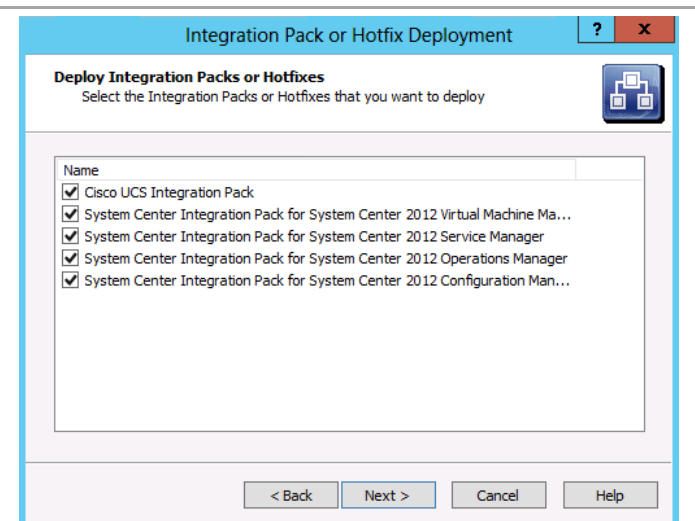
The **Integration Pack Deployment Wizard** will appear. Click **Next** to continue.



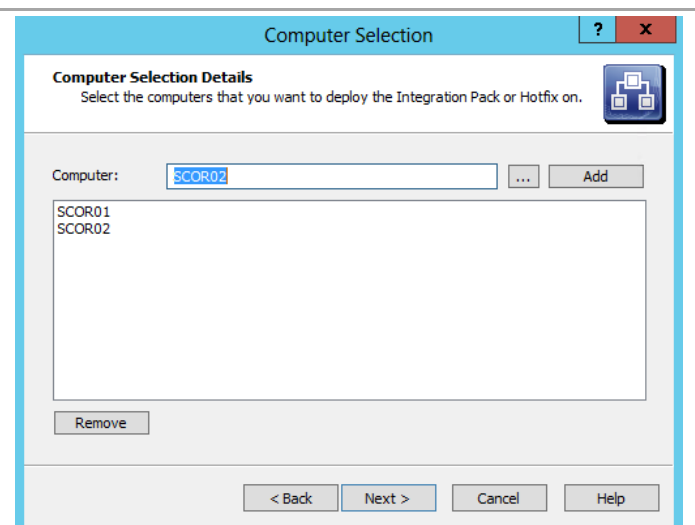
In the **Deploy Integration Packs or Hotfixes** dialog, select the check boxes integration packs folder created earlier and select the following integration packs:

- System Center 2012 Configuration Manager.
- System Center 2012 Operations Manager.
- System Center 2012 Service Manager.
- System Center 2012 Virtual Machine Manager.
- Cisco UCS Integration Pack

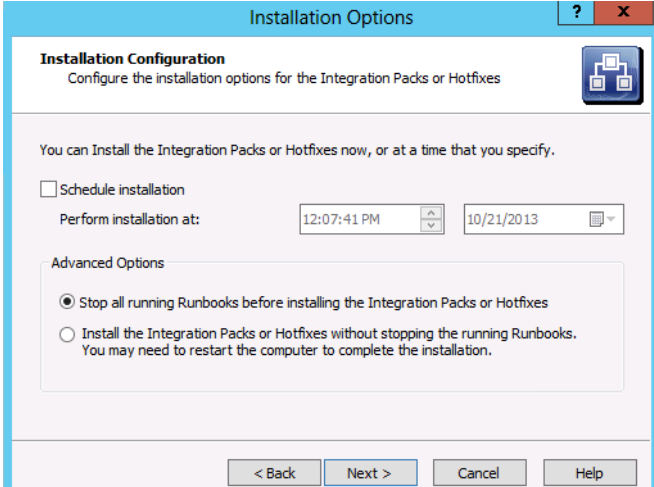
Once complete, click **Next** to continue.



In the **Computer Selection Details**, type the name of the Orchestrator management server and click **Add**. Once added, click **Next** to continue.

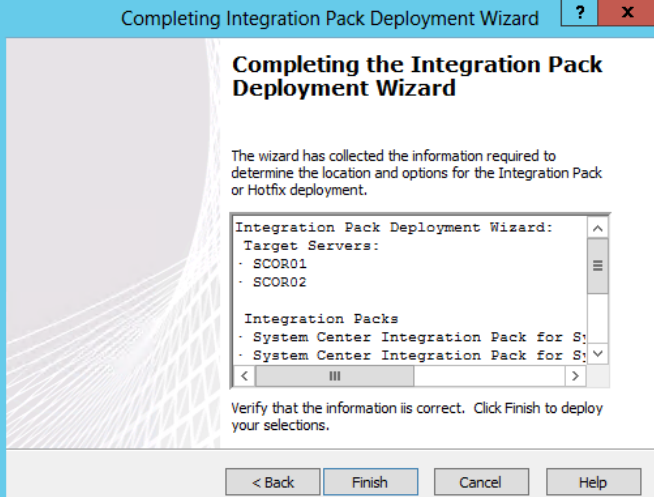


In the **Installation Configuration** dialog, in the **Advanced Options** pane select **Stop all running Runbooks before installing the Integration Packs or Hotfixes** option. Click **Next** to continue.



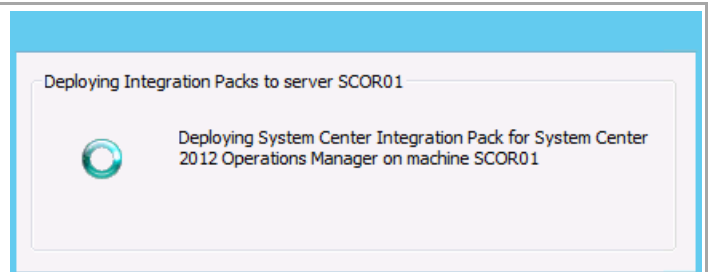
The **Installation Options** dialog box is shown. It has a title bar with a question mark and a close button. The main content area is titled **Installation Configuration** with the subtitle "Configure the installation options for the Integration Packs or Hotfixes". Below this, it says "You can install the Integration Packs or Hotfixes now, or at a time that you specify." There is a checkbox for "Schedule installation". If checked, there are fields for "Perform installation at:" with a time picker set to "12:07:41 PM" and a date picker set to "10/21/2013". Below this is the "Advanced Options" section with two radio buttons. The first radio button, "Stop all running Runbooks before installing the Integration Packs or Hotfixes", is selected. The second radio button is "Install the Integration Packs or Hotfixes without stopping the running Runbooks. You may need to restart the computer to complete the installation." At the bottom are buttons for "< Back", "Next >", "Cancel", and "Help".

The **Completing the Integration Pack Deployment Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



The **Completing Integration Pack Deployment Wizard** dialog box is shown. It has a title bar with a question mark and a close button. The main content area is titled **Completing the Integration Pack Deployment Wizard**. Below this, it says "The wizard has collected the information required to determine the location and options for the Integration Pack or Hotfix deployment." There is a summary box with the following content: "Integration Pack Deployment Wizard:", "Target Servers:", "· SCOR01", "· SCOR02", "Integration Packs", "· System Center Integration Pack for S", "· System Center Integration Pack for S". Below the summary box, it says "Verify that the information is correct. Click Finish to deploy your selections." At the bottom are buttons for "< Back", "Finish", "Cancel", and "Help".

During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.



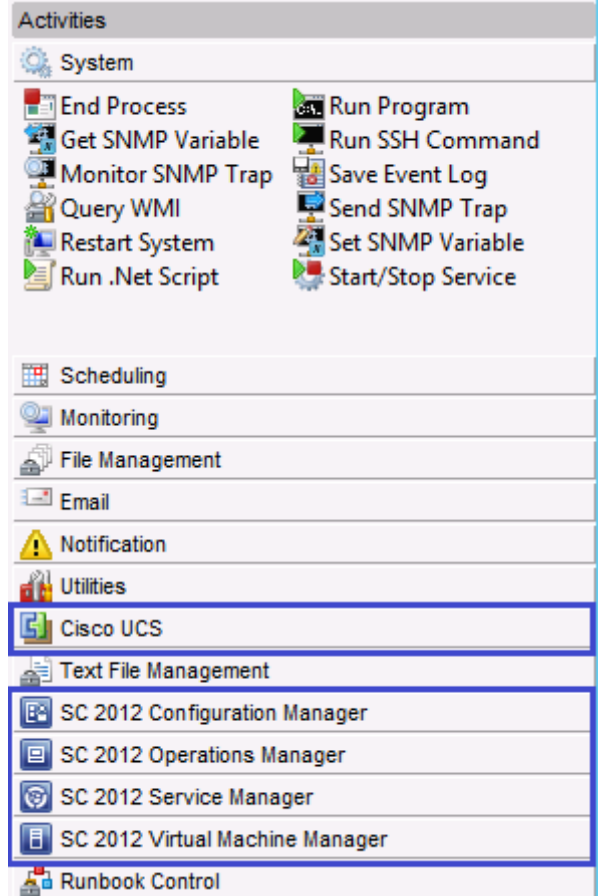
Log Entries

- ✓ Enumerating Integration Packs...
- ✓ Finished enumerating Integration Packs
- ✓ Deploying Integration Packs to server SCOR01
- ✓ Deploying System Center Integration Pack for System Center 2012 Data Protection Manager on machine SCOR01
- ✓ Deployment of System Center Integration Pack for System Center 2012 Data Protection Manager to machine SCOR01 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Virtual Machine Manager on machine SCOR01
- ✓ Deployment of System Center Integration Pack for System Center 2012 Virtual Machine Manager to machine SCOR01 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Service Manager on machine SCOR01
- ✓ Deployment of System Center Integration Pack for System Center 2012 Service Manager to machine SCOR01 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Operations Manager on machine SCOR01
- ✓ Deployment of System Center Integration Pack for System Center 2012 Operations Manager to machine SCOR01 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Configuration Manager on machine SCOR01
- ✓ Deployment of System Center Integration Pack for System Center 2012 Configuration Manager to machine SCOR01 succeeded
- ✓ Deploying Integration Packs to server SCOR02
- ✓ Deploying System Center Integration Pack for System Center 2012 Data Protection Manager on machine SCOR02
- ✓ Deployment of System Center Integration Pack for System Center 2012 Data Protection Manager to machine SCOR02 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Virtual Machine Manager on machine SCOR02
- ✓ Deployment of System Center Integration Pack for System Center 2012 Virtual Machine Manager to machine SCOR02 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Service Manager on machine SCOR02
- ✓ Deployment of System Center Integration Pack for System Center 2012 Service Manager to machine SCOR02 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Operations Manager on machine SCOR02
- ✓ Deployment of System Center Integration Pack for System Center 2012 Operations Manager to machine SCOR02 succeeded
- ✓ Deploying System Center Integration Pack for System Center 2012 Configuration Manager on machine SCOR02
- ✓ Deployment of System Center Integration Pack for System Center 2012 Configuration Manager to machine SCOR02 succeeded
- ✓ Enumerating Integration Packs...
- ✓ Finished enumerating Integration Packs

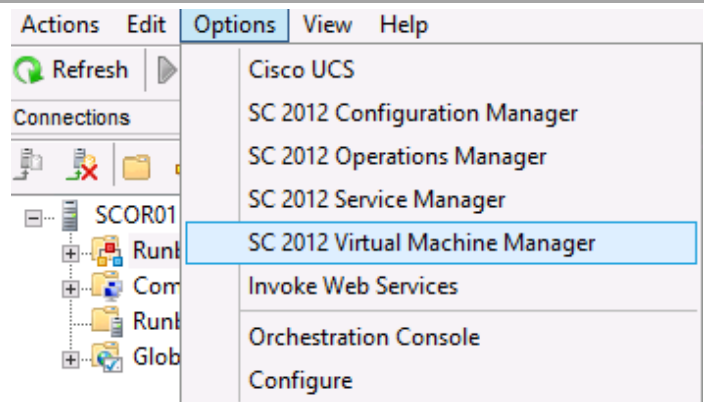
From the **Start** screen, click the **Runbook Designer** tile.



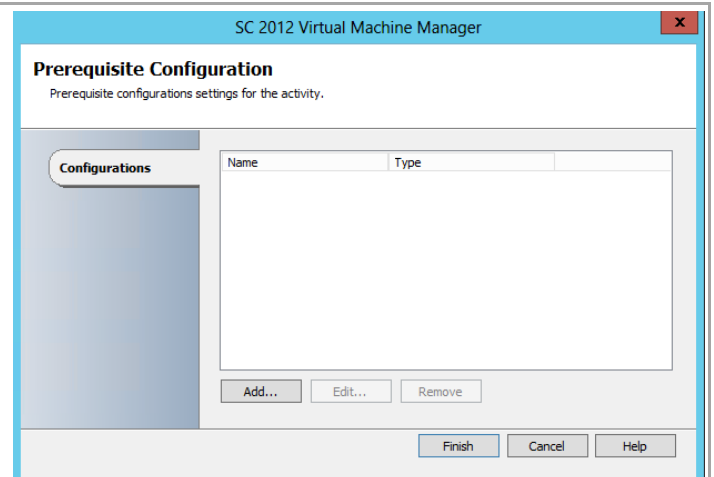
Once complete, each integration pack will be displayed in the Runbook Designer interface.



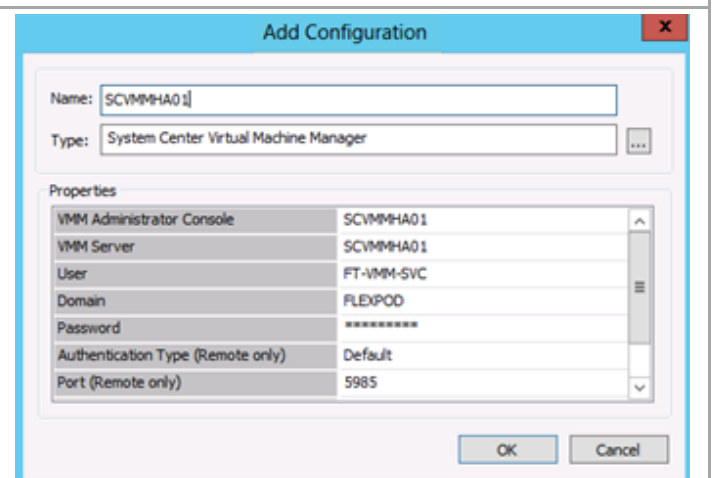
To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Virtual Machine Manager** option.



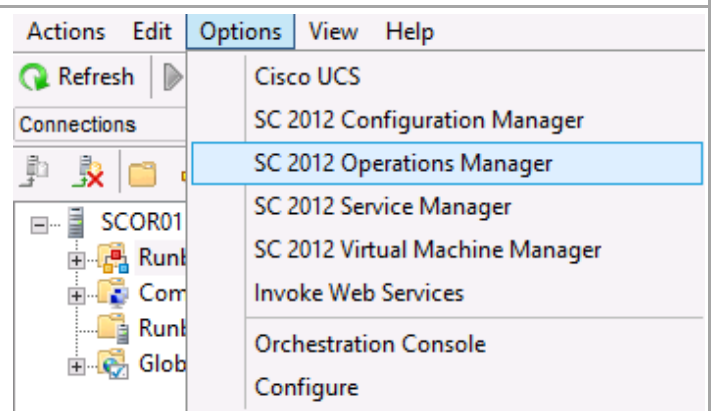
In the Prerequisite Configuration dialog, click **Add**.



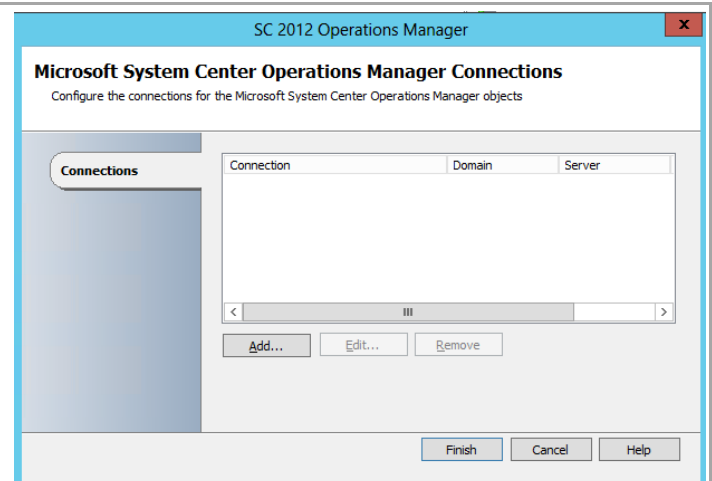
In the **Add Configuration** dialog, fill in the required information for the Virtual Machine Manager server as shown and click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.



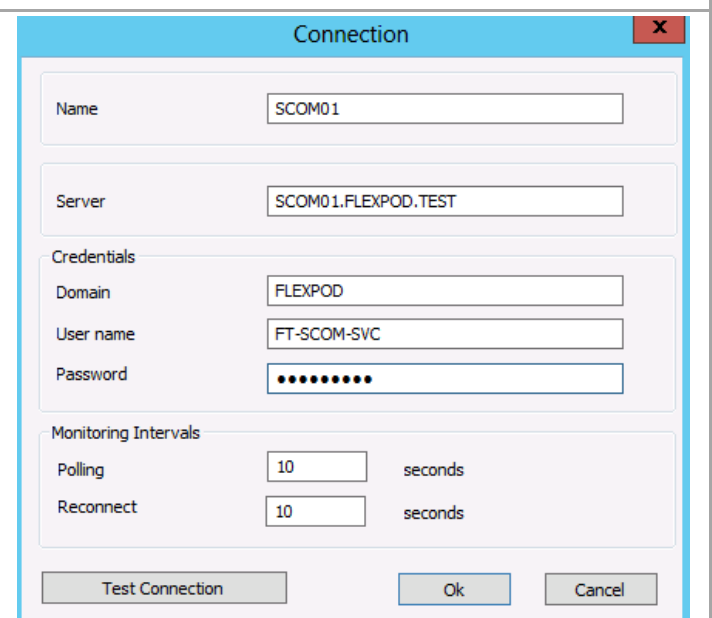
While still in the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Operations Manager** option.



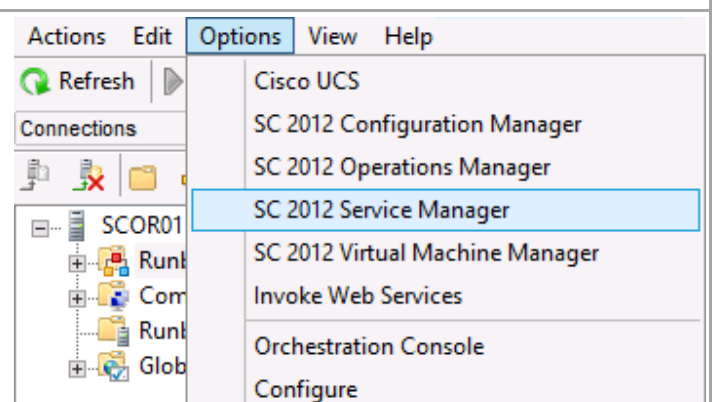
In the **Microsoft System Center Operations Manager Connections** dialog, click **Add**.



In the **MS System Center Operations Manager Connection Settings** dialog, fill in the required information for the Operations Manager management server and click **Test Connection**²⁴. Once connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

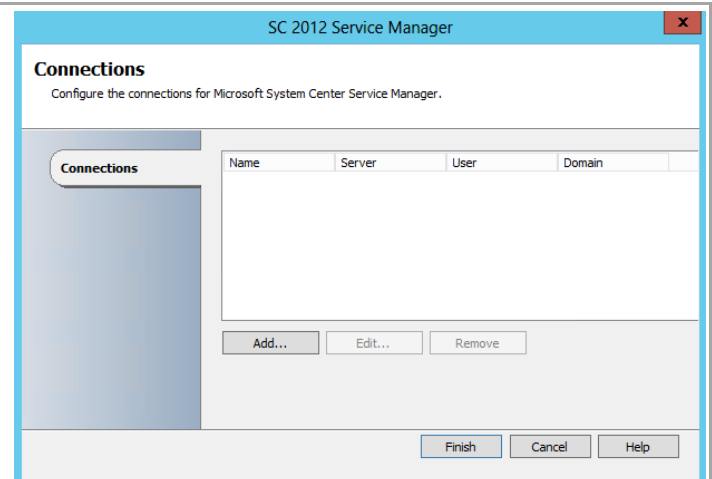


In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **SC 2012 Service Manager** option.

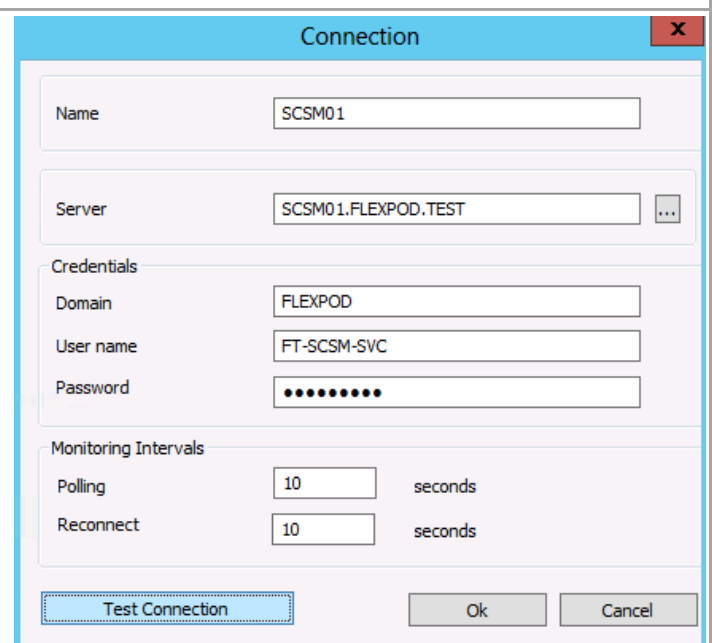


²⁴ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

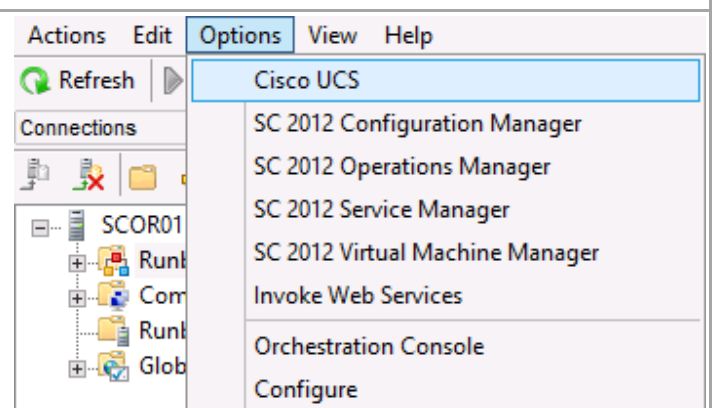
In the **Connections** dialog, click **Add**.



In the **Connection** dialog, fill in the required information for the Operations Manager management server²⁵ and click **Test Connection**. Once connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

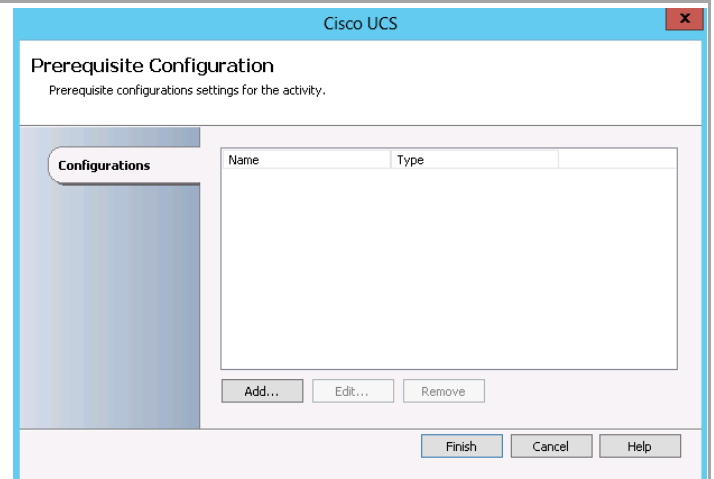


In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **Cisco UCS** option.

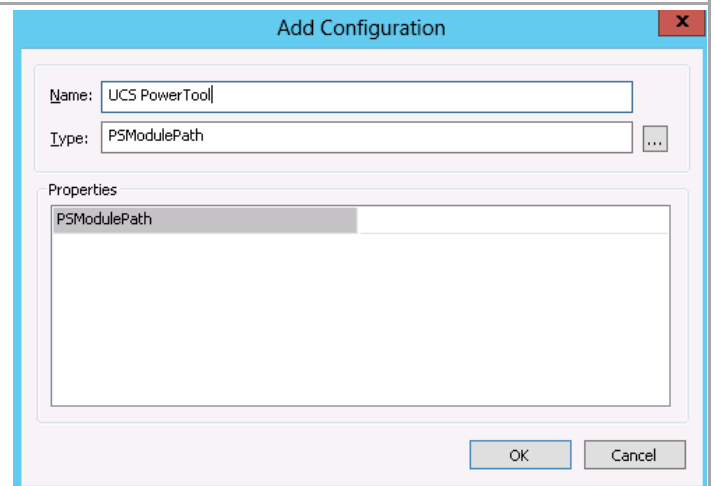


²⁵ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

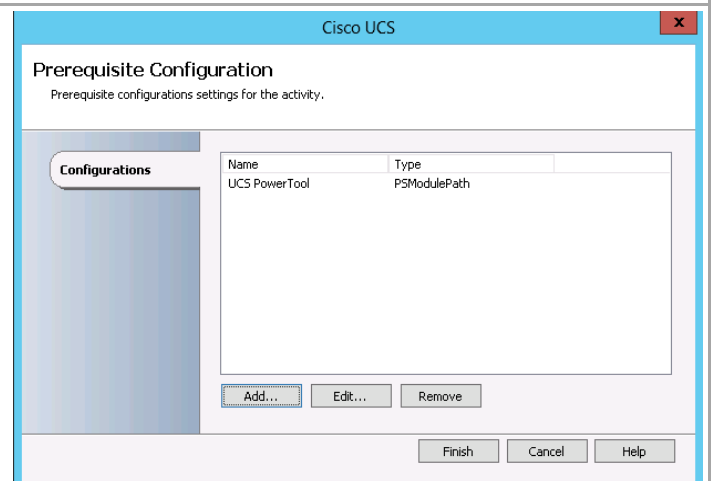
The Cisco UCS **Prerequisite Configuration** window opens. Click the **Add** button.



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.

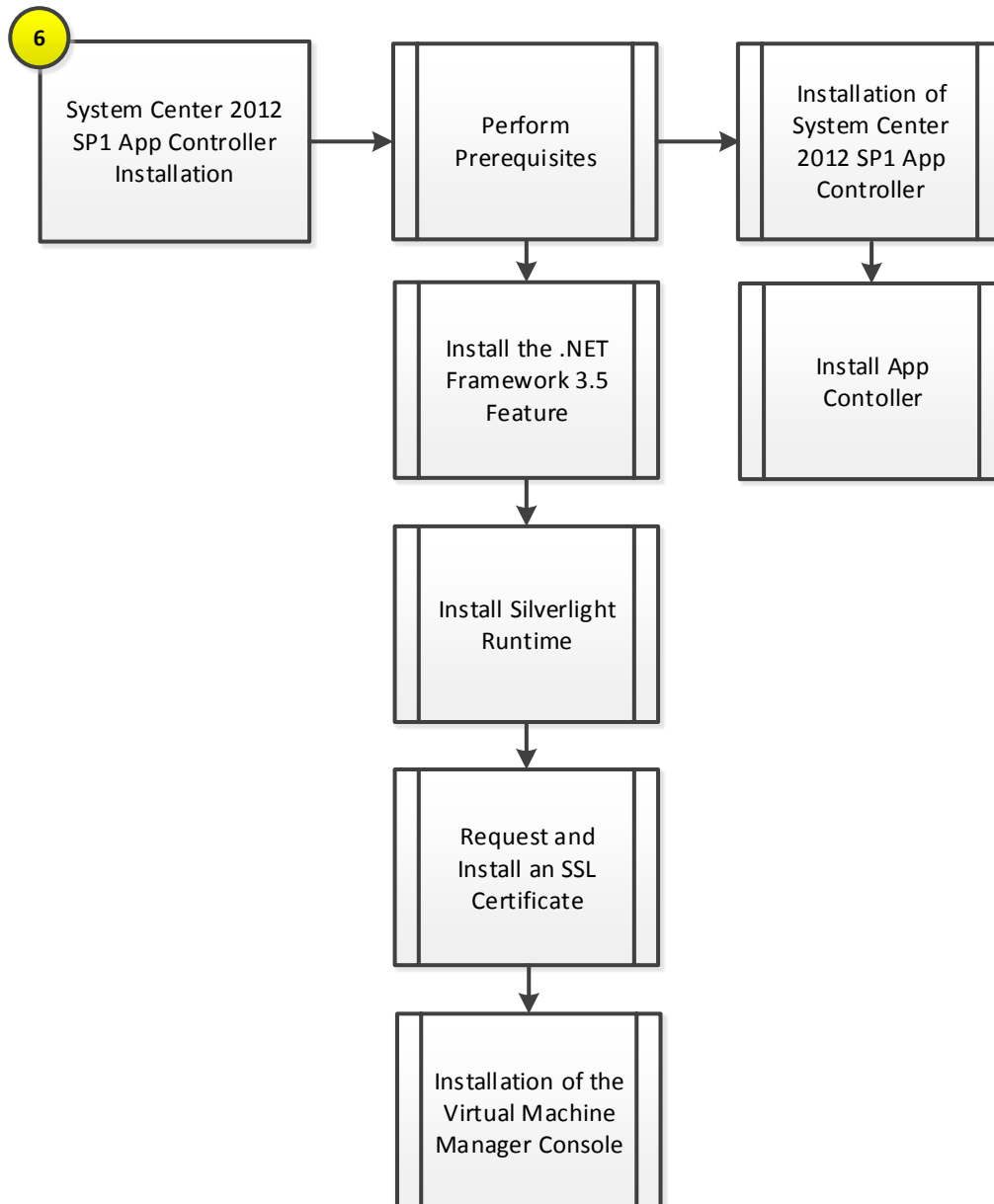


Click **Finish** to save the setting and close the window.



20 App Controller

The App Controller installation process includes the following high-level steps:



20.1 Overview

This section provides high-level walkthrough on how to setup App Controller. The following assumptions are made:

- A base virtual machine running Windows Server 2012 has been provisioned for App Controller.
- A SQL Server 2012 cluster with dedicated instance that has been established in previous steps for App Controller.
- The System Center Virtual Machine Manager console is installed
- The .NET Framework 3.5 Feature is installed.
- Microsoft Silverlight® Runtime is installed.
- A Trusted Server Authentication (SSL) Certificate (the CN field of the certificate must match server name) is installed.

20.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User name	Purpose	Permissions
<DOMAIN>\FT-SCAC-SVC	App controller service account	This account will need to be a member in the following groups: <ul style="list-style-type: none">• FT-SCAC-Admins• FT-VMM-Admins

Groups

Verify that the following security groups have been created:

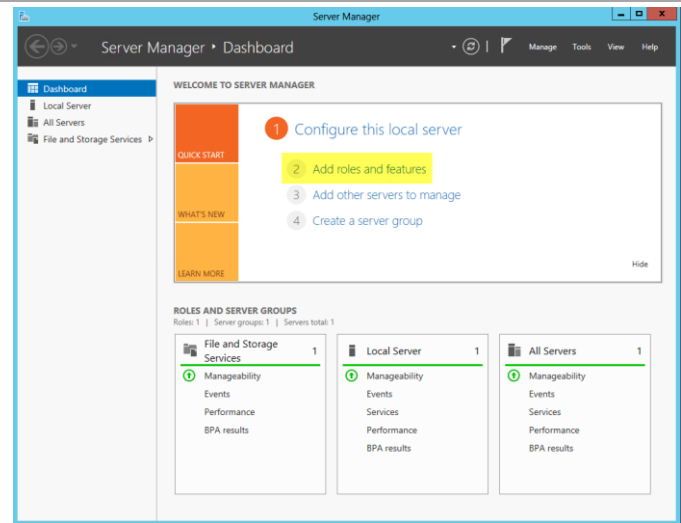
Group name	Purpose	Members
<DOMAIN>\FT-SCAC-Admins	App Controller Admin group	<DOMAIN>\FT-SCAC-SVC <DOMAIN>\FT-VMM-Admins

Install the .NET Framework 3.5 Feature

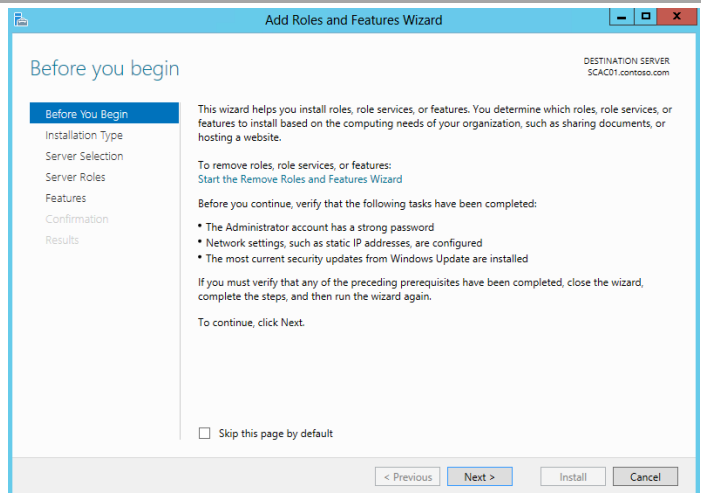
The App Controller installation requires the .NET Framework 3.5 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5 Feature.

► Perform the following steps on the **App Controller** virtual machine.

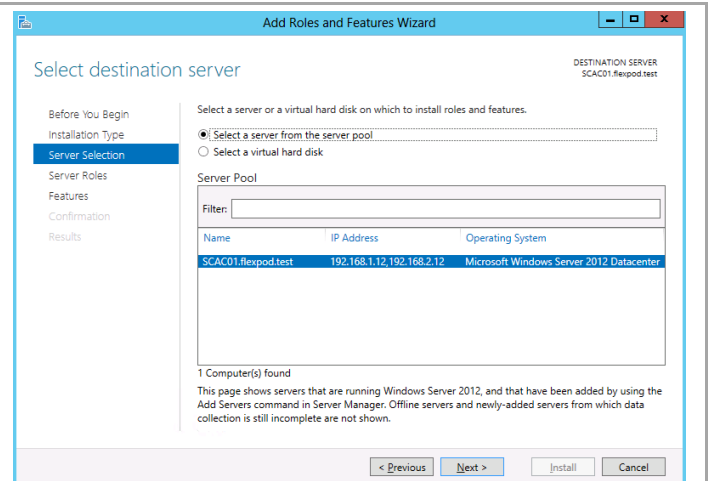
Launch **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features** from the available options.



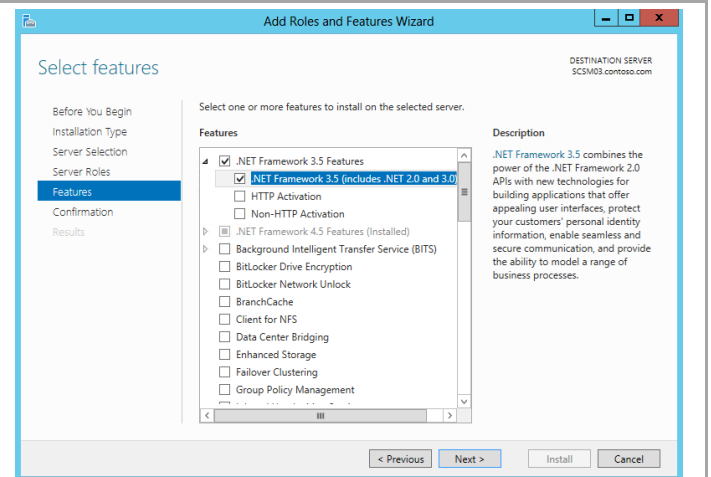
The **Add Roles and Features Wizard** will appear. In the **Before You Begin** dialog, do not click **Next** - for this installation, click the **Server Selection** menu option to continue.



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.



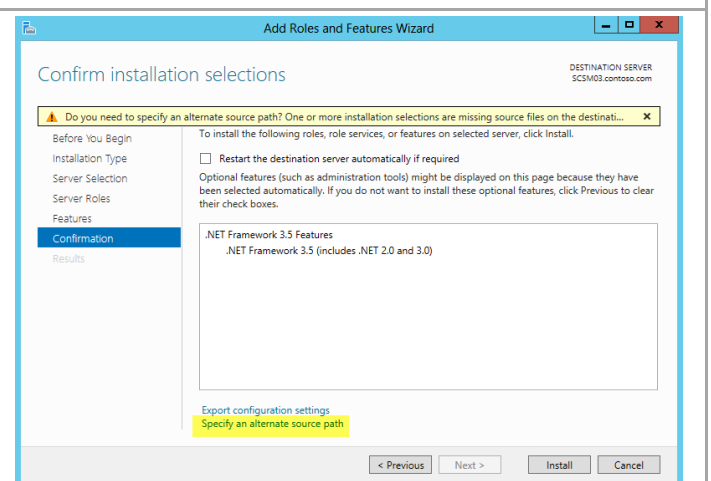
To add the .NET Framework 3.5 Feature, in the **Select Features** dialog in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



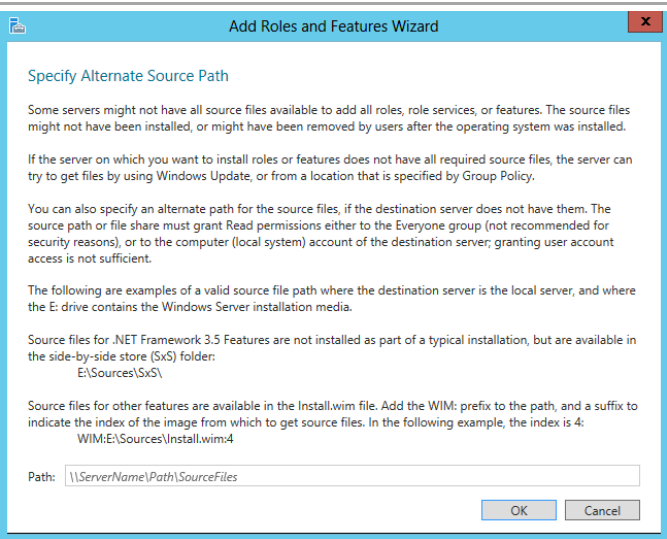
In the **Confirm installation selections** dialog, verify that the .NET Framework 3.5 features are selected. Ensure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

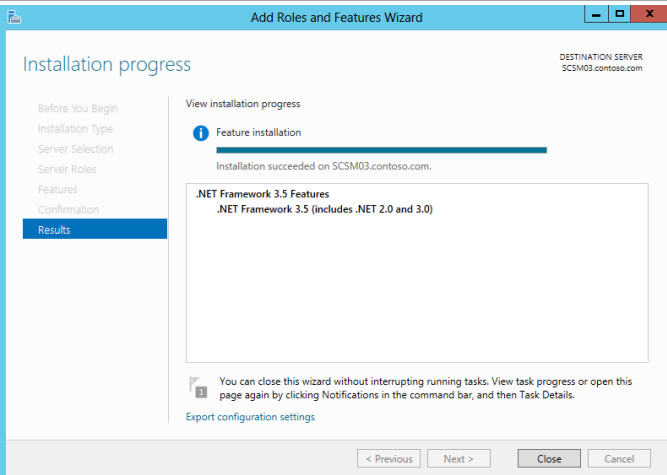
*Also, If the server does not have internet access an alternate source path can be specified by clicking the **Specify** and **alternate source patch** link.*



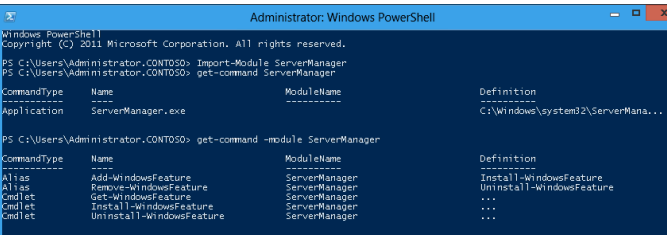
For servers without Internet access or if the .NET Source files already exist on the network, an alternate source location be specified for the installation.



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



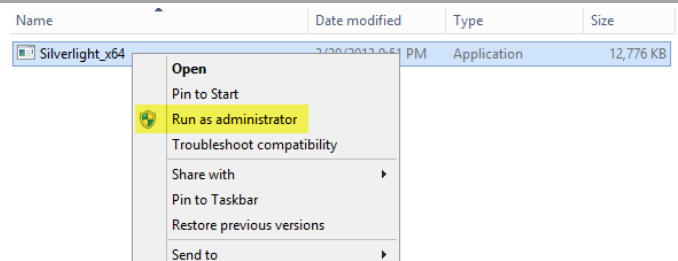
Note that while the following installation was performed interactively, the installation of roles and features can be automated using the Server Manager PowerShell module.



Install Silverlight Runtime

► Perform the following steps on the **App Controller** virtual machine.

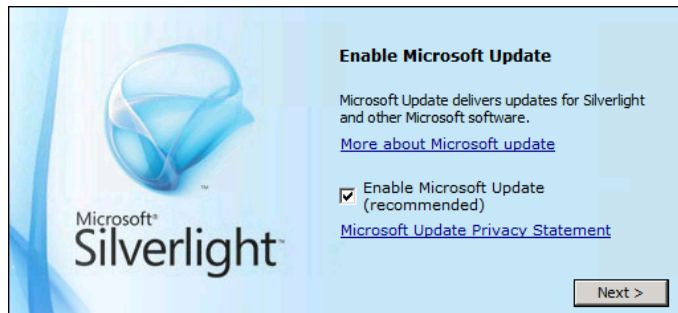
From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.



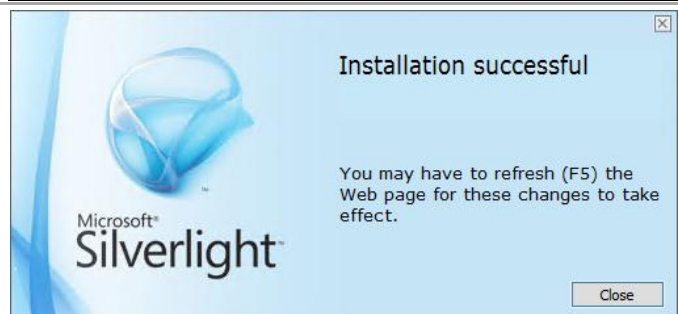
In the **Install Silverlight** dialog, click **Install now**.



In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** checkbox based on organizational preferences and click **Next** to continue.



In the **Installation Successful** dialog, click **Close** to exit the installation.

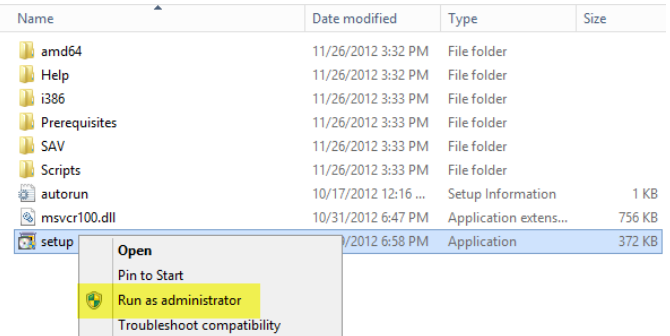


Install the Virtual Machine Manager Console

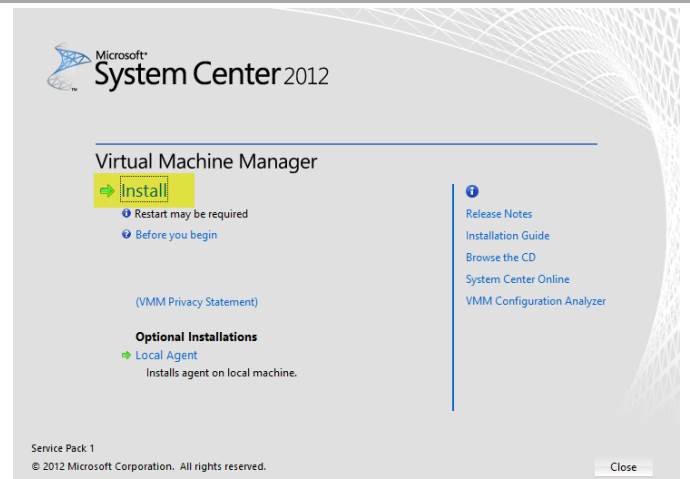
The following steps need to be completed in order to install the Virtual Machine Manager console on the target App Controller virtual machine.

► Perform the following steps on the **App Controller** virtual machines.

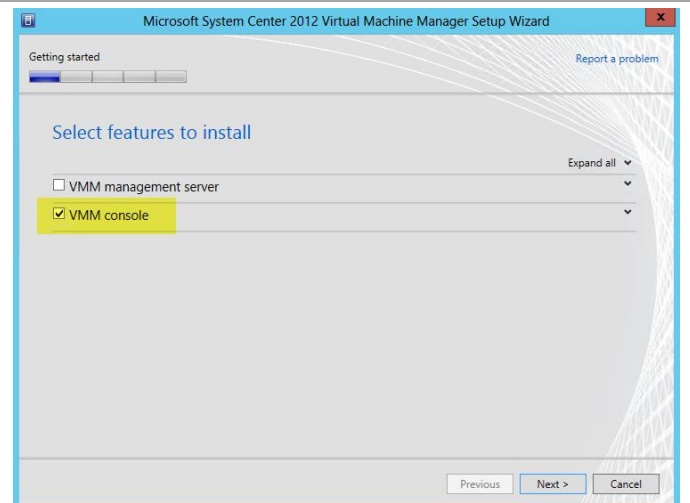
Log on to the App Controller server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



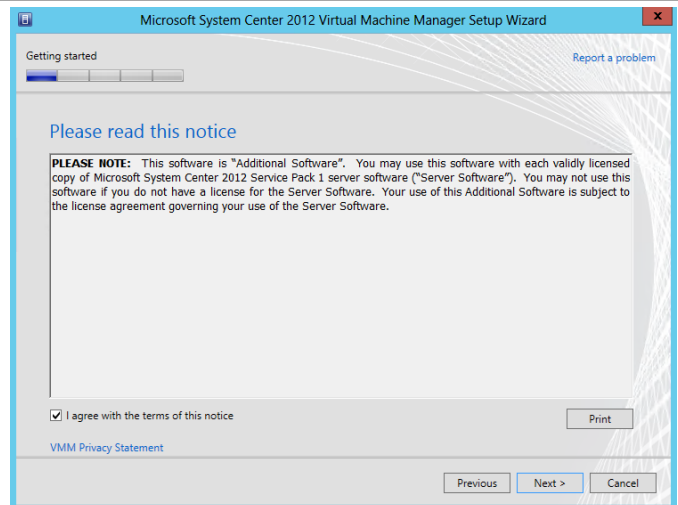
The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



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 checkbox is selected and click **Next** to continue.

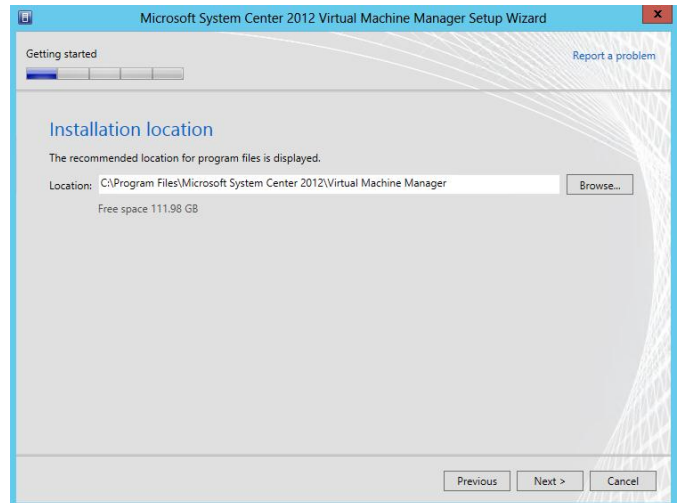


In the **Customer Experience Improvement Program** dialog, click **Next** to continue.

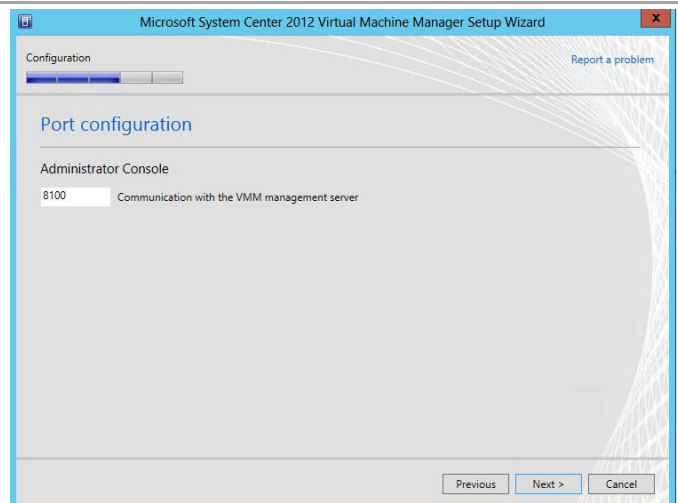


Depending on the current configuration of the server, the Microsoft Update dialog may appear. In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.

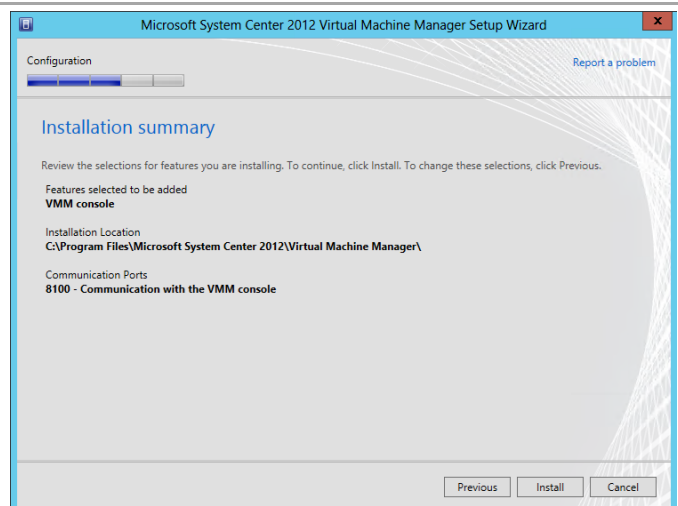
In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.



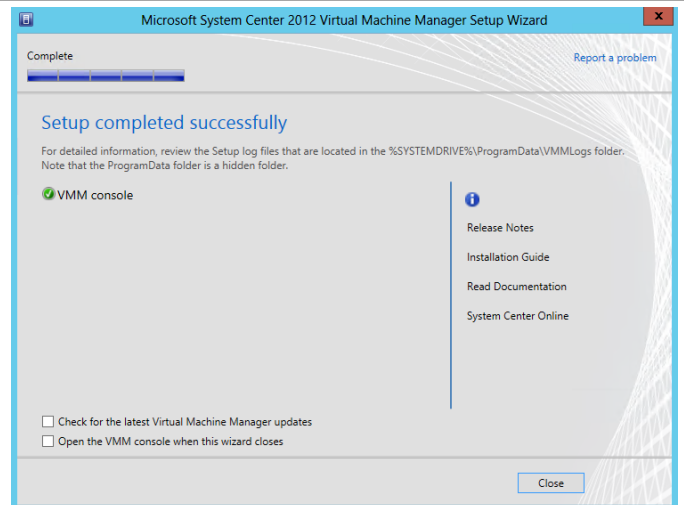
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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

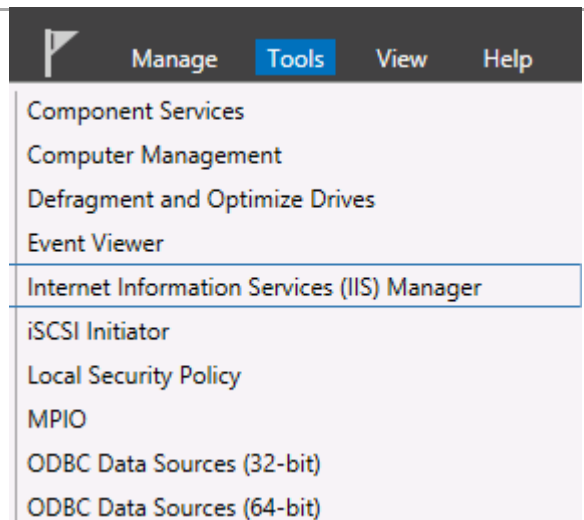


Request and Install an SSL Certificate on the AppController Server

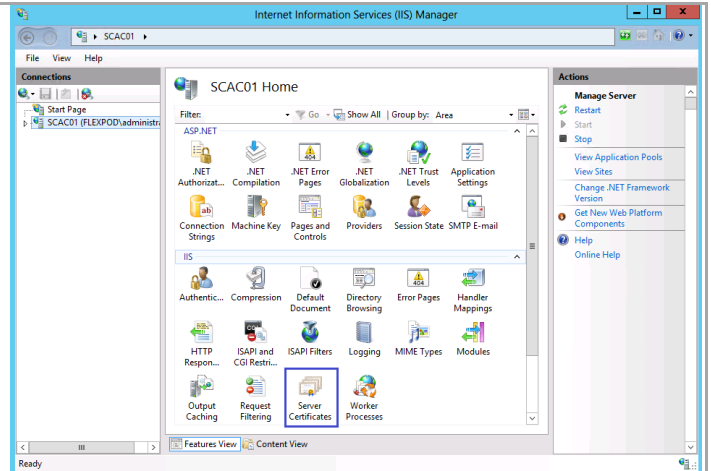
Additionally, the App Controller installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website. If the App Controller is to be installed without SSL this section can be skipped. There are several ways to request an SSL Certificate. One method, through the IIS Manager console, is outlined below.

► Perform the following steps on the **App Controller** (SCAC01) virtual machine.

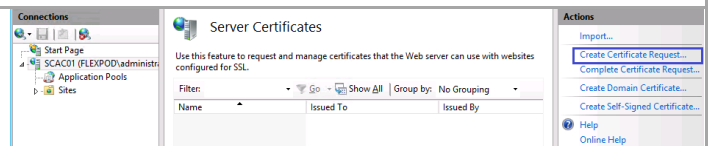
Log on to the App Controller virtual machine with a user with local admin rights. From **Server Manager** select **Tools** and **Internet Information Services (IIS) Manager**.



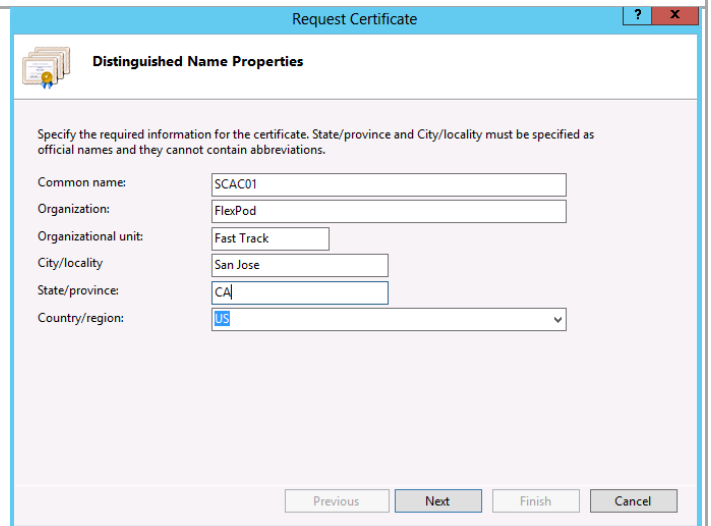
In the **Internet Information Services (IIS) Manager** console, select the server node and in the IIS section, double-click **Server Certificates**.



The **Server Certificates** pane will expand. Under actions, click **Create Certificate Request...**



The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name that the server will be accessed in the web browser. Click **Next** to continue.



In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing certification authority (CA). In most cases, selecting the default CSP and default bit length is satisfactory. Click **Next** to continue.

The screenshot shows the 'Request Certificate' wizard window. The title bar says 'Request Certificate'. The main window has a blue header with the title 'Cryptographic Service Provider Properties'. Below the header, there is a text box explaining that the bit length of the encryption key determines the certificate's encryption strength. There are two dropdown menus: 'Cryptographic service provider:' set to 'Microsoft RSA SChannel Cryptographic Provider' and 'Bit length:' set to '1024'. At the bottom, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

Once completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.

The screenshot shows the 'Request Certificate' wizard window, specifically the 'File Name' step. The title bar says 'Request Certificate'. The main window has a blue header with the title 'File Name'. Below the header, there is a text box explaining that the file name can be sent to a certification authority for signing. There is a text input field labeled 'Specify a file name for the certificate request:' with the value 'C:\CSAC01.req' and a browse button (...). At the bottom, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

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 screenshot shows the IIS Manager console. The left pane shows the 'Connections' tree with 'Start Page', 'SCAC01 (FLEXPOD/administr...', 'Application Pools', and 'Sites'. The main pane shows the 'Server Certificates' feature. Below the title bar, there is a text box explaining that this feature is used to request and manage certificates for websites configured for SSL. There is a 'Filter:' section with 'Name', 'Issued To', and 'Issued By' options. At the bottom, there is an 'Actions' pane with several options: 'Import...', 'Create Certificate Request...', 'Complete Certificate Request...' (highlighted with a blue border), 'Create Domain Certificate...', 'Create Self-Signed Certificate...', 'Help', and 'Online Help'.

The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Click **OK** to complete the operation.

Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\SCAC01Cert.cer

Friendly name:

SCAC01 Certificate

Select a certificate store for the new certificate:

Web Hosting

OK

Cancel

In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.

Connections

Start Page

SCAC01 (FLEXPOD)administr

Application Pools

Sites

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter:

Go

Show All

Group by: No Grouping

Name	Issued To	Issued By	Expiration I
SCAC01 Certificate	SCAC01	flexpod-SCINFRA-CA	10/21/2015

20.3 Installation

Install the App Controller Portal Server

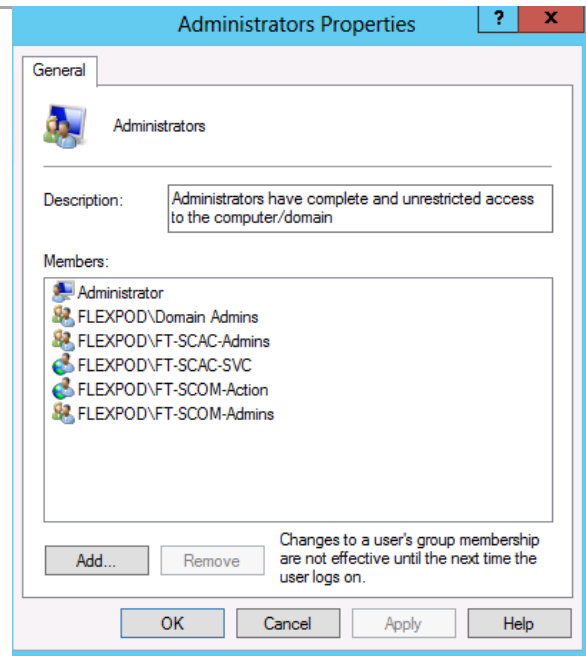
The following steps need to be completed in order to install App Controller.

► Perform the following steps on the **App Controller** virtual machine.

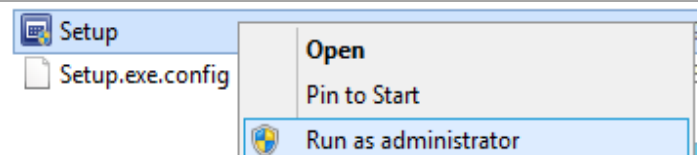
Log on to the App Controller virtual machine with a user with local admin rights.

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 Operations Manager Admins group.
- Fast Track App Controller service account.
- Fast Track App Controller Admins group.



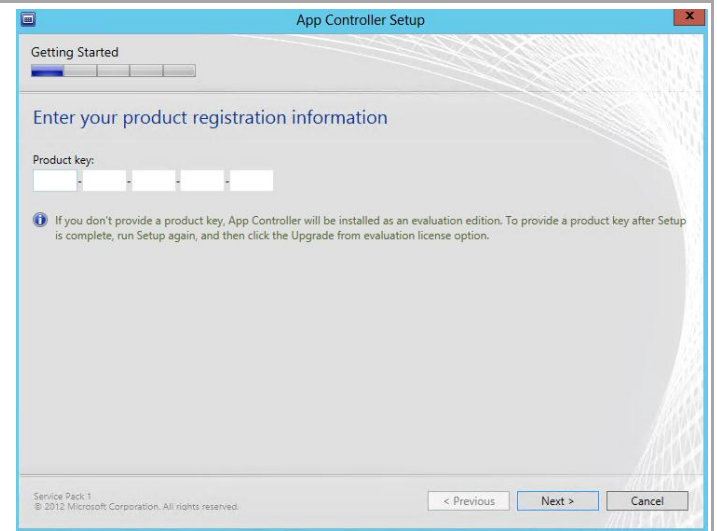
Log on to System Center App controller server. From the **System Center App Controller** installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



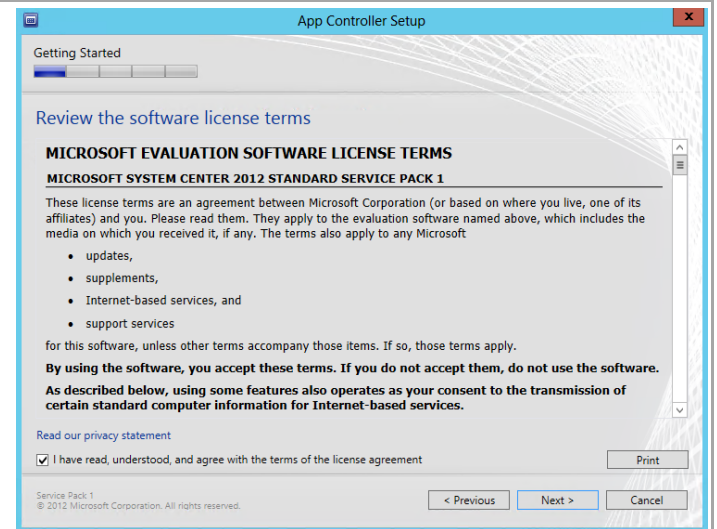
The **App Controller Setup** wizard will begin. At the splash page, click **Install** begin the App Controller server installation.



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.



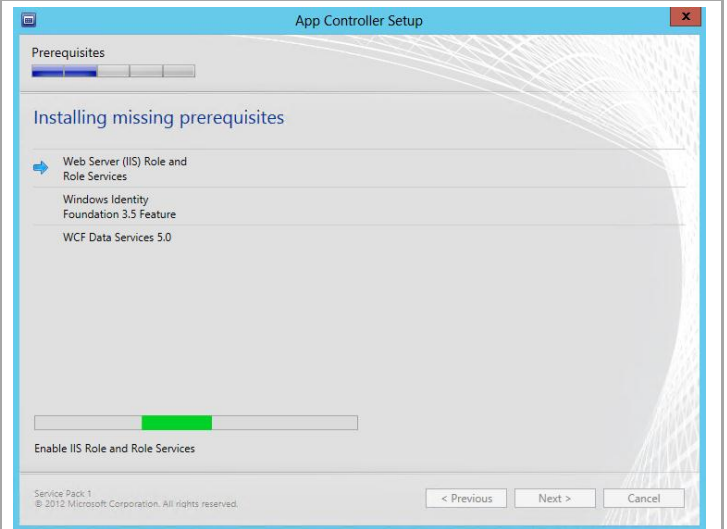
In the **Review the software license terms** dialog, verify that the **I have read, understood and agree with the terms of this license agreement** installation option checkbox is selected and click **Next** to continue.



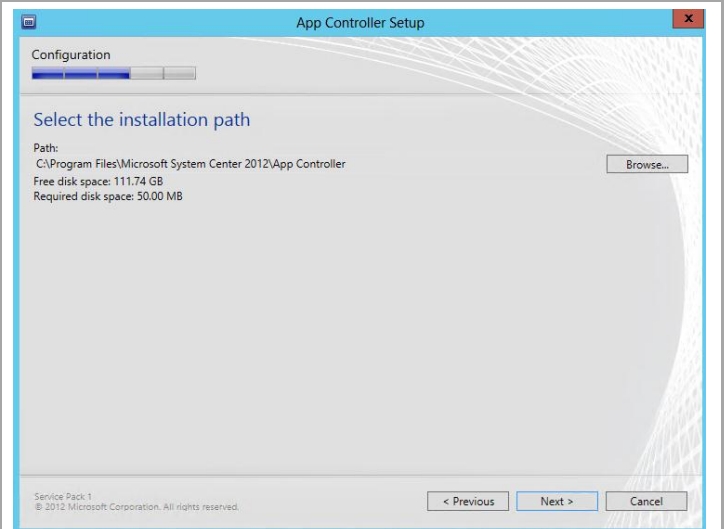
In the **Install missing software** dialog, the wizard will detect missing roles and software and attempt installation of missing prerequisites. Click **Install** to enable missing roles and features.



The wizard will detect missing roles and software and attempt installation of missing prerequisites. Please be patient during this process.

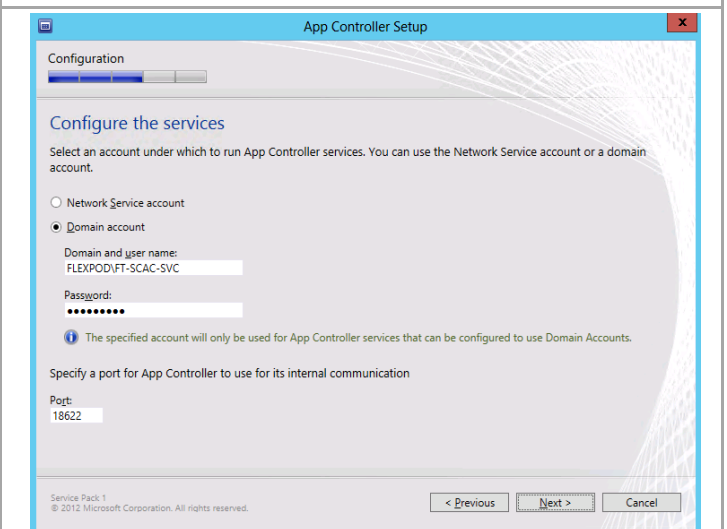


In the **Select the installation path** dialog, accept the default installation location of *%ProgramFiles%\Microsoft System Center 2012\App Controller* or specify a different location by hitting the **Browse** button. After making a selection hit **Next** to continue.



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. Once complete, click **Next** to continue.



In the **Configure the website** dialog, provide the following information:

- Under Website, in **Type: HTTPS**, set the **IP address** drop-down menu to **All unassigned**. Set the **Port** value to **443**.
- Verify that the **Use existing certificate** option is selected and select the proper Server Authentication certificate that installed within the virtual machine from the drop-down menu.

Once 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.

The screenshot shows the 'Configure the website' dialog box within the 'App Controller Setup' window. The dialog has a progress bar at the top. The title is 'Configure the website'. Below the title, it says 'Specify the binding settings you want to use for the App Controller website.' There are two radio buttons: 'Generate self-signed certificate' (unselected) and 'Use existing certificate' (selected). Under 'Use existing certificate', there is a dropdown menu showing 'SCAC01.flexpod.test' and two buttons: 'View...' and 'Refresh'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The footer text reads 'Service Pack 1 © 2012 Microsoft Corporation. All rights reserved.'

In the **Configure the SQL Server database** dialog, make the following selections install the App Controller database in the SCO instance (refer to the worksheet created earlier):

- **Server Name** – *specify the cluster network name of the SQL Server failover cluster hosting the instance.*
- **Port** – *specify the TCP port used for SQL Server connectivity. Note that the SCDB instance must use port 1433 if Cloud Services Process Pack is deployed.*
- **Instance name** - *specify the instance name where the AppController database will be installed to (the SCDB instance).*
- **Database name** – *specify the name of the App Controller database. In most cases the default value of AppController should be used.*

Click **Next** to continue.

The screenshot shows the 'Configure the SQL Server database' dialog box within the 'App Controller Setup' window. The dialog has a progress bar at the top. The title is 'Configure the SQL Server database'. Below the title, there are four fields: 'Server name:' with the value 'SCDB', 'Port:' with the value '1433', 'Instance name:' with a dropdown menu showing 'SCDB', and 'Database name:' with the value 'AppController'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The footer text reads 'Service Pack 1 © 2012 Microsoft Corporation. All rights reserved.'

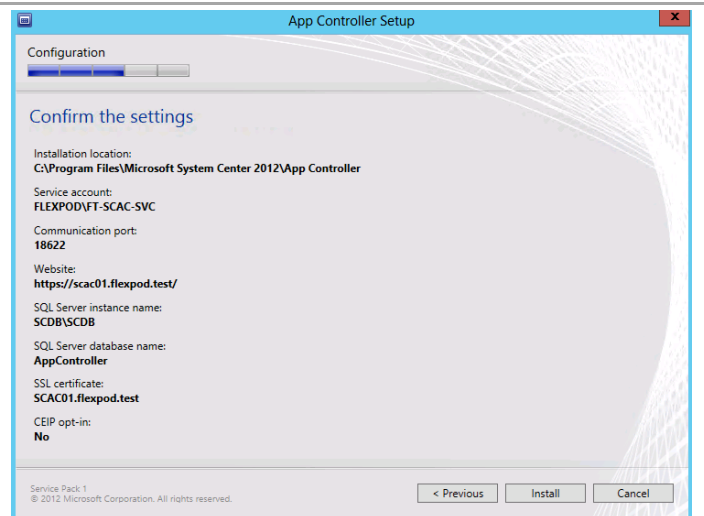
The **Help Improve App Controller for System Center 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Microsoft Update**

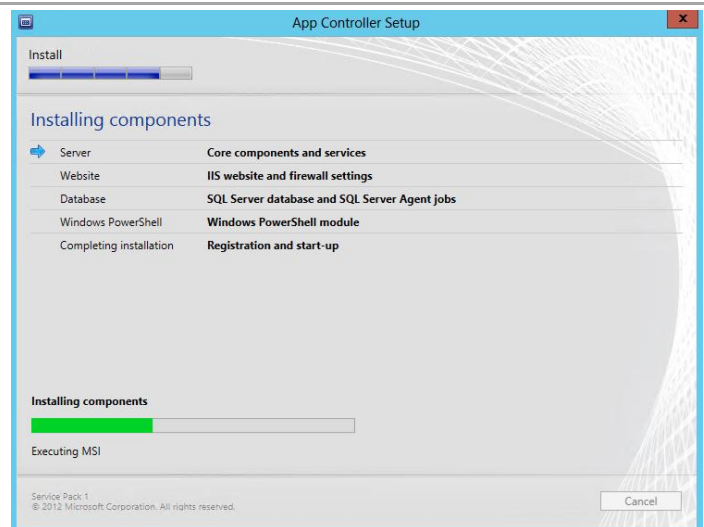
Select the appropriate option based on your organization's policies and click **Install** to continue.



In the **Confirm the settings** dialog, verify the settings provided during the installation wizard and click **Install** to begin the installation.

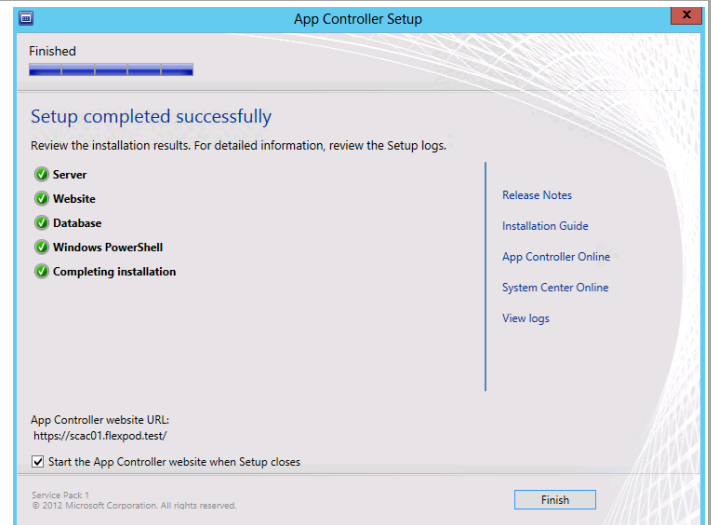


The required components will install and progress of the installation will be provided in the wizard.

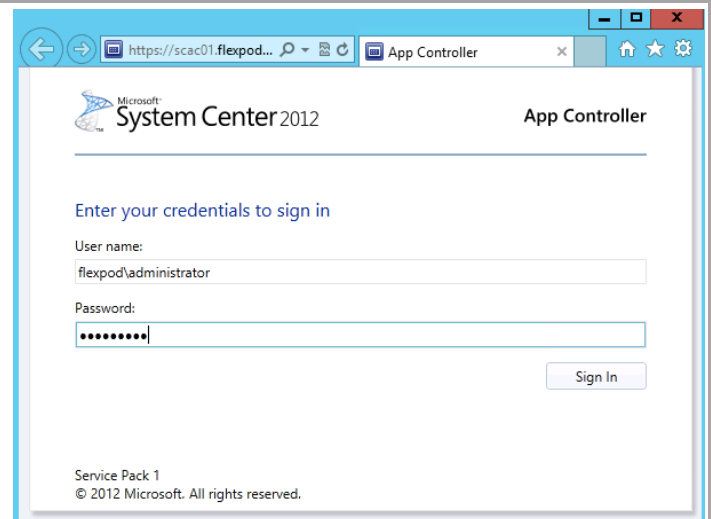


Once complete, the **Setup completed successfully** dialog will appear with progress of each component. Verify that each component successfully. Note the App Controller website in the provided text box.

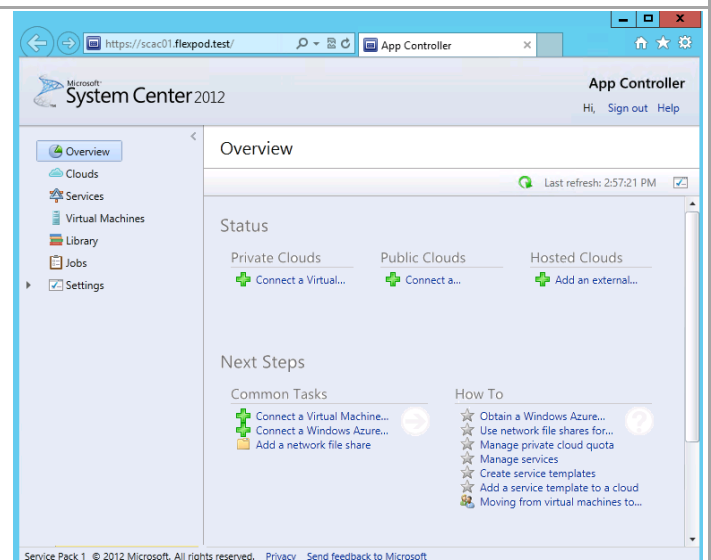
Verify that the **Start the App Controller website when Setup closes** check box is selected and click **Finish**.



The **System Center 2012 App Controller website** will launch. Because no users have been created in SCVMM, enter in the administrative account used to install Virtual Machine Manager (which has been assigned an admin role in SCVMM). Once complete, click **Sign in**.

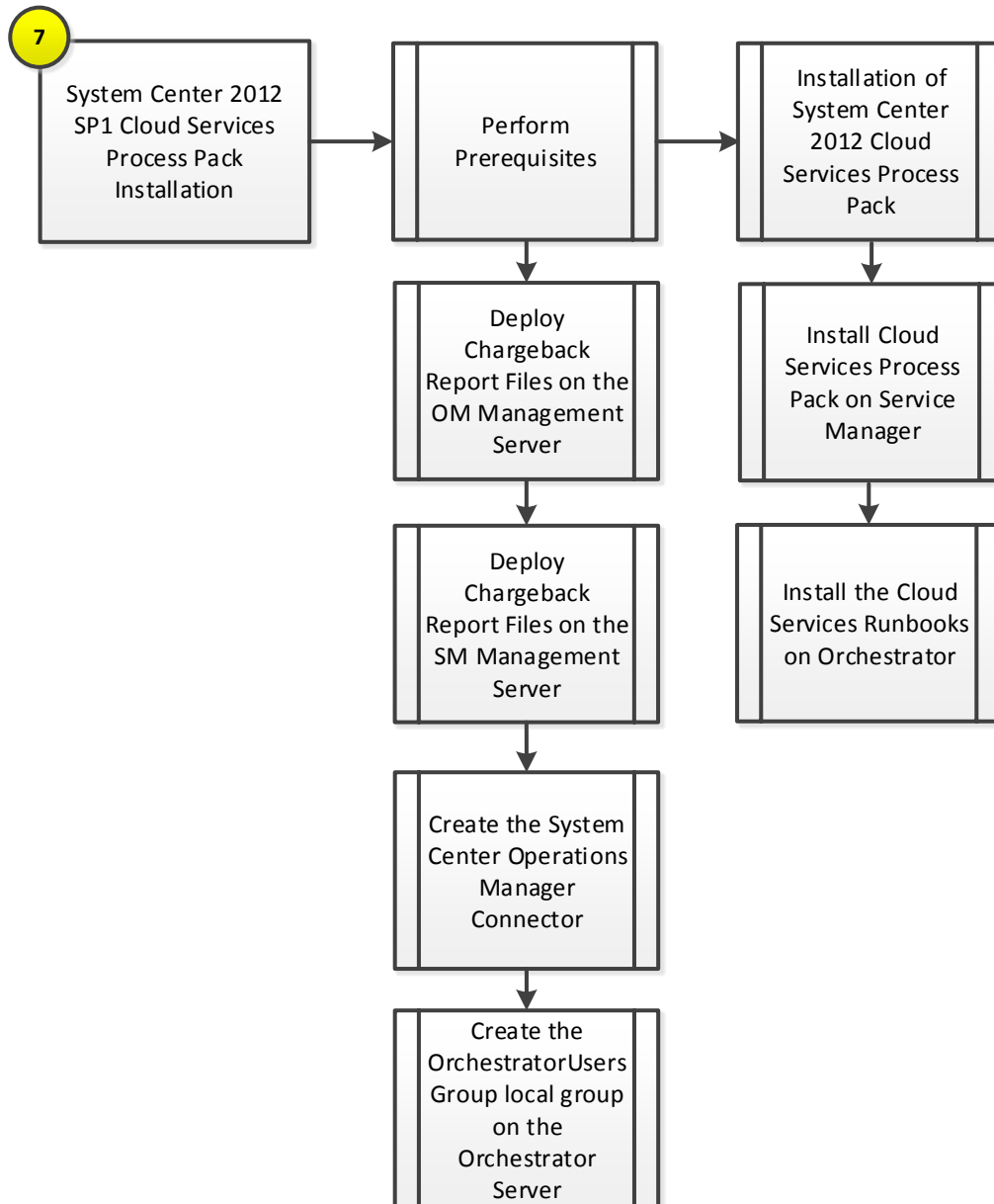


The App Controller portal will appear. After validating functionality, the App Controller installation is considered complete.



21 System Center Cloud Services Process Pack

The Cloud Services Process Pack installation process includes the following high-level steps:



21.1 Overview

This section provides the setup procedure for the Cloud Services Process Pack into the Fast Track fabric management architecture. The following assumptions are made:

- The system center integration pack for System Center 2012 – Service Manager needs to be imported into Orchestrator per previous steps.
- Operations Manager integration with Virtual Machine Manager should already be complete per previous steps.

System Center Cloud Services Process Pack is available at <http://www.microsoft.com/en-us/download/details.aspx?id=36497>. IT organizations considering IaaS will need to examine and adapt their existing tools, processes, workflows, and automation to meet the requirements of an effective cloud services implementation. While it is critical that the underlying components (such as self-service portal, ticketing infrastructure, notifications, workflows, and automation) integrate well with each other and account for industry-wide recommended practices, the work involved to implement an effective cloud service can be daunting and time consuming.

System Center Cloud Services Process Pack addresses these concerns by enabling IaaS while incorporating domain expertise and recommended practices from enterprises that have successfully deployed IaaS. These recommended practices are made available out-of-the box and are evident in all aspects of the Solution.

The potential benefits offered by System Center Cloud Services Process Pack for the enterprise include:

- Deep customization and extension of the cloud services experience that is natively supported by the System Center suite of products.
- Reduced cost, effort, and time to deploy cloud services to organizations that already utilizes the System Center platform.

The potential benefits offered by System Center Cloud Services Process Pack for consumers of IT within the enterprise include:

- Standardized and well-defined processes for requesting and managing cloud services, including the ability to define projects, capacity pools, and virtual machines.
- Natively supported request, approval, and notification to help enable businesses to effectively manage their own allocated infrastructure capacity pools.

The System Center Cloud Services Process Pack offers a self-service experience to facilitate private cloud capacity requests from your business unit IT application owners and end users, including the flexibility to request additional capacity as business demands increase.

21.2 Pre-Requisites

The following environment prerequisites must be met before proceeding.

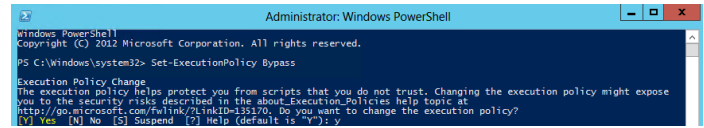
Deploy Chargeback Report Files on the Operations Manager Management Server

► Perform the following steps on the **Operations Manager management server** virtual machine.

From an elevated PowerShell prompt, configure the execution policy to Bypass.

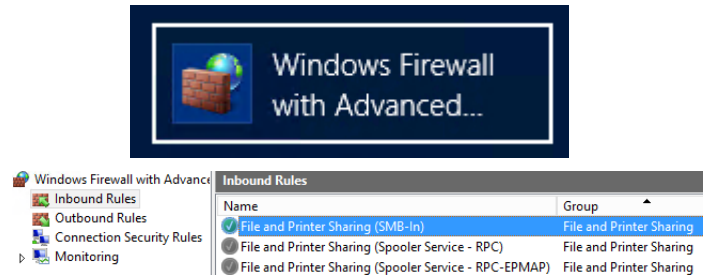
`Set-ExecutionPolicy Bypass`

Note, once installation is complete, execution policy should be configured to a more secure level within the organization.

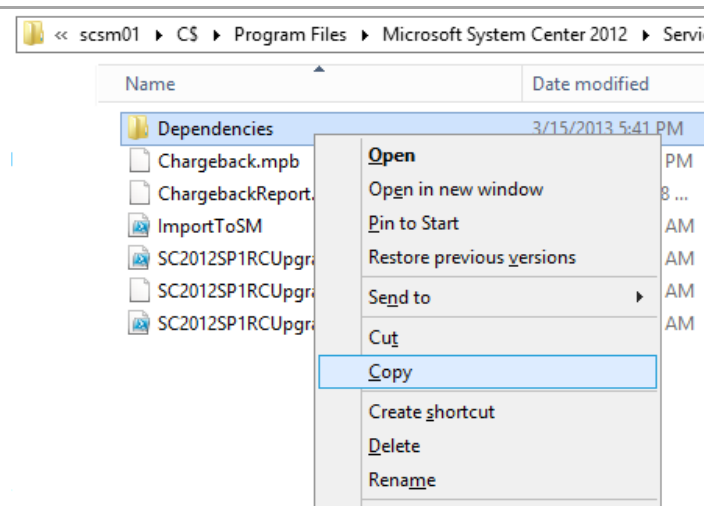


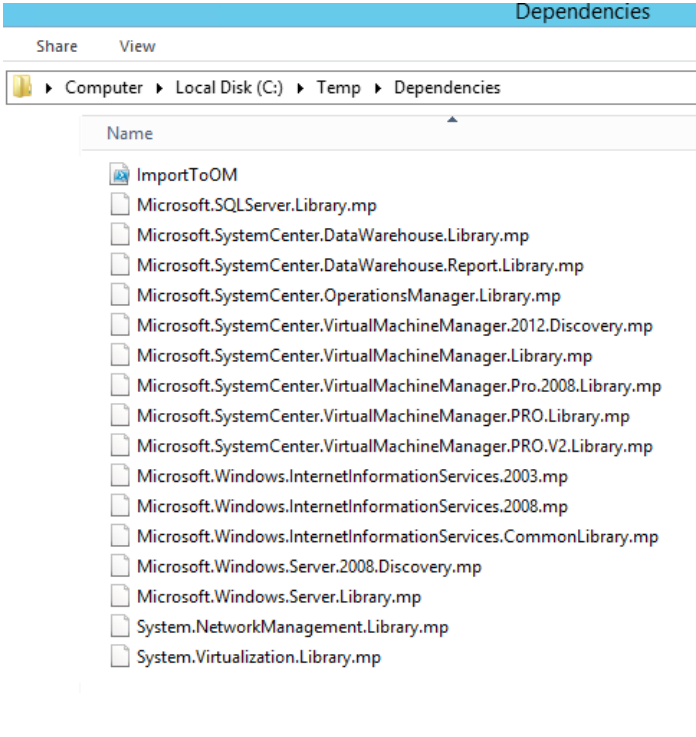
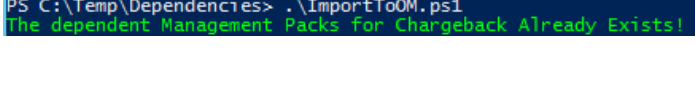
Open the **Windows Firewall with Advanced Security** MMC console.

Within the **Windows Firewall with Advanced Security** MMC console, select the **Inbound Rules** node and enable the **File and Printer Sharing (SMB-In)** rule from the action pane.



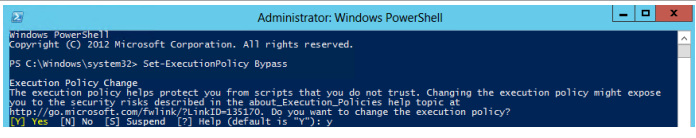
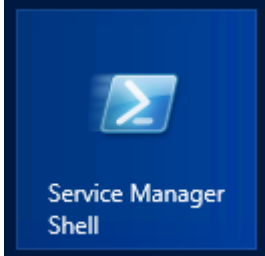
Connect to the administrative share where %ProgramFiles% resides on the Service Manager management server. Copy the **Dependencies** folder from the %ProgramFiles%\Microsoft System Center 2012\Service Manager\Chargeback installation folder on the remote Service Manager management server.



<p>Copy the Dependencies folder to a temporary directory on the Operations Manager management server.</p>	
<p>From the same elevated PowerShell session, navigate to the Dependencies folder which was copied locally and execute the ImportToOM.ps1 PowerShell script. In some cases the dependent management packs will already be deployed.</p>	

Deploy Chargeback Report Files on the Service Manager Management Server

► Perform the following steps on the **Service Manager management server** virtual machine.

<p>From an elevated PowerShell prompt, configure the execution policy to Bypass.</p> <p>Set-ExecutionPolicy Bypass</p> <p><i>Note, once installation is complete, execution policy should be configured to a more secure level within the organization.</i></p>	
<p>From the Start screen, select the Service Manager Shell tile and run this as an administrator.</p>	

In the elevated **Service Manager Shell** dialog, navigate to %ProgramFiles%\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies and execute the **ImportToSM.ps1** script. Once completed, close the console.

Note: ImportToSM.ps1 is in the %ProgramFiles%\Microsoft System Center 2012\Service Manager\Chargeback directory.

```
Administrator: Service Manager Shell
PS C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback> .\ImportToSM.ps1
There are 16 Management Packs to import.
Following Management Packs will be imported:
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.Windows.InternetInformationServices.CommonLibrary.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.Windows.Server.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SqlServer.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.DataWarehouse.Report.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\System.Virtualization.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.DataWarehouse.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.OperationsManager.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\System.NetworkManagement.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.Windows.Server.2008.Discovery.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.Windows.InternetInformationServices.2003.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.Windows.InternetInformationServices.2008.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.VirtualMachineManager.Pro.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.VirtualMachineManager.Pro.U2.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.VirtualMachineManager.2012.Discovery.mp
C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback\Dependencies\Microsoft.SystemCenter.VirtualMachineManager.Library.mp
Importing Dependent Management Packs...
All the Dependent Management Packs were imported!
Importing Chargeback Management Pack Bundle...
The Chargeback Management Packs Imported successfully!
```

Within the **Service Manager console**, navigate to the **Data Warehouse Jobs** node and select the **MPSyncJob** data warehouse job. In the **Tasks** pane, select **Resume** to begin the synchronization task.

The screenshot shows the Service Manager console interface. The left pane displays the 'Data Warehouse' tree with 'Data Warehouse Jobs' selected. The right pane shows 'Data Warehouse Jobs 13' with a list of jobs including 'Extract_SMMG01', 'Load.Common', and 'MPSyncJob'. Below this, the 'Tasks' pane for 'MPSyncJob' is visible, showing options for 'Properties', 'Resume', and 'Suspend'. At the bottom, a table lists the job details.

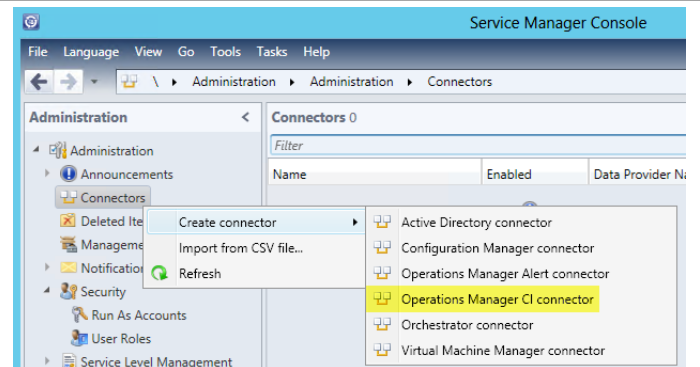
Name	Category	Enabled	Status
MPSyncJob	Synchronization	Yes	Running

Create the System Center Operations Manager Connector

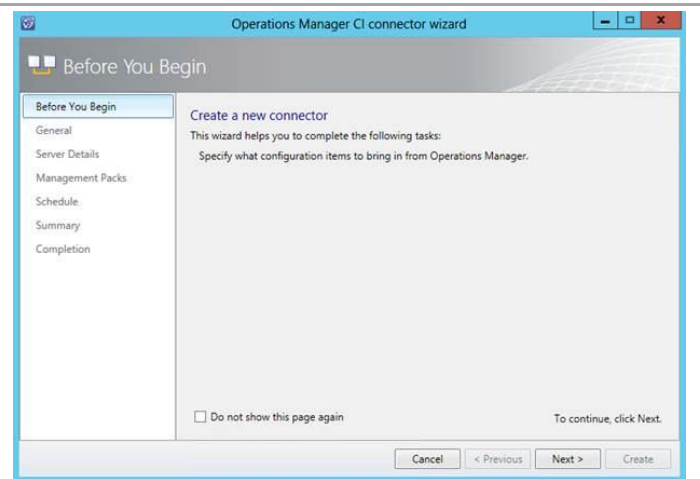
► Perform the following steps on the **Service Manager management server** virtual machine.

Open the **Service Manager Console**, select **Administration** from the navigation tree and navigate to the **Cloud Services** node.

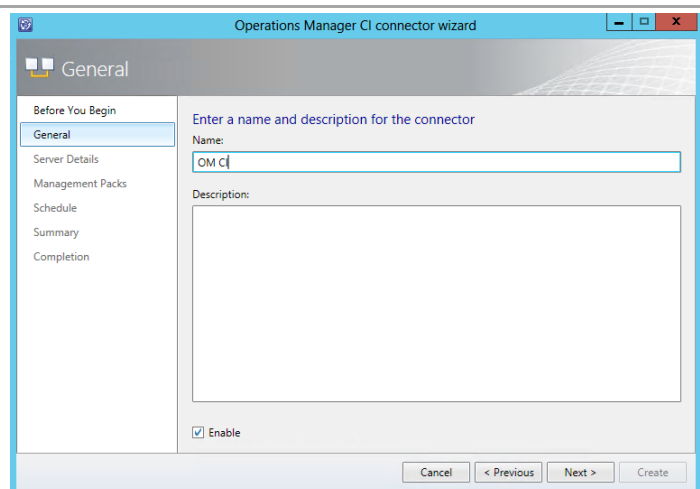
In the Getting Started pane, click **Create an Operations Manager Connector**.



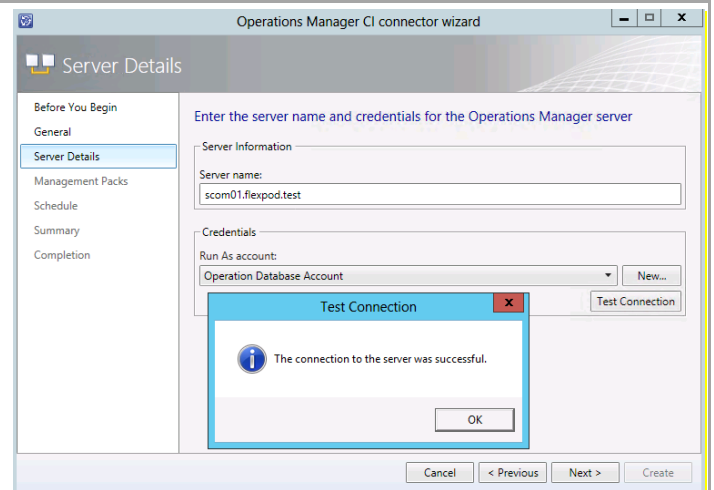
In the **Before you Begin** dialog, click **Next** to continue.



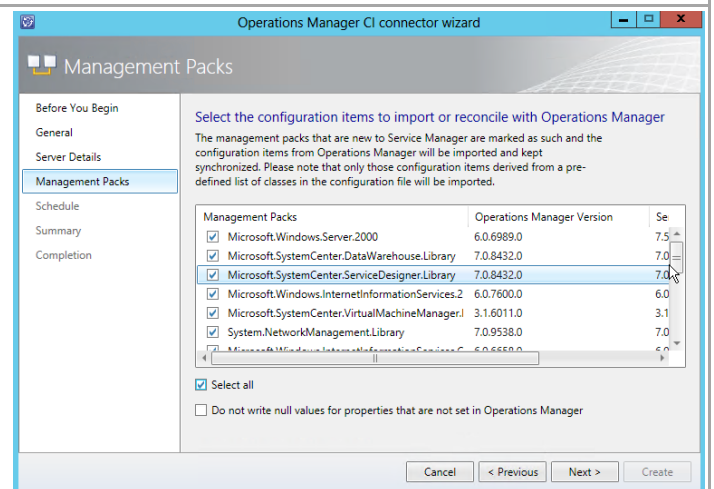
The **Operations Manager CI connector** wizard will appear. In the **General** dialog, type a descriptive name for the connector in the **Name** textbox. Verify the **Enable** checkbox is selected. Click **Next** to continue.



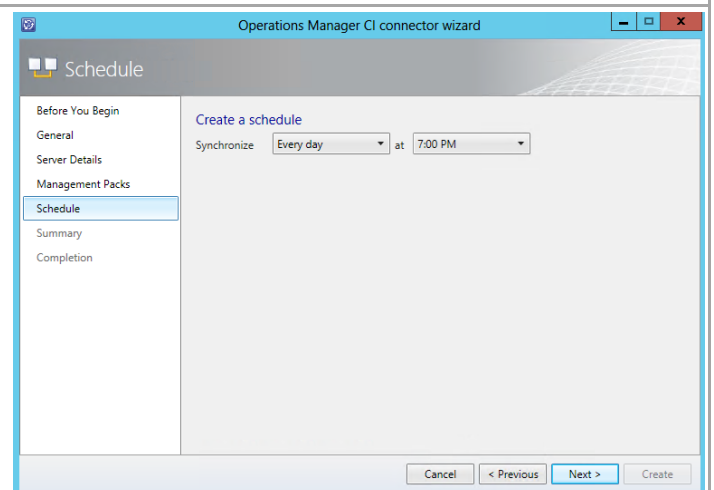
In the **Server Details** dialog, type the FQDN of the Operations Manager server in the **Server Name** textbox. In the **Credentials** section, click the **New...** button and create a Run As account using the **FT-SCOM-SVC** account. Click **Test Connection** to verify the account. Click **Next** to continue



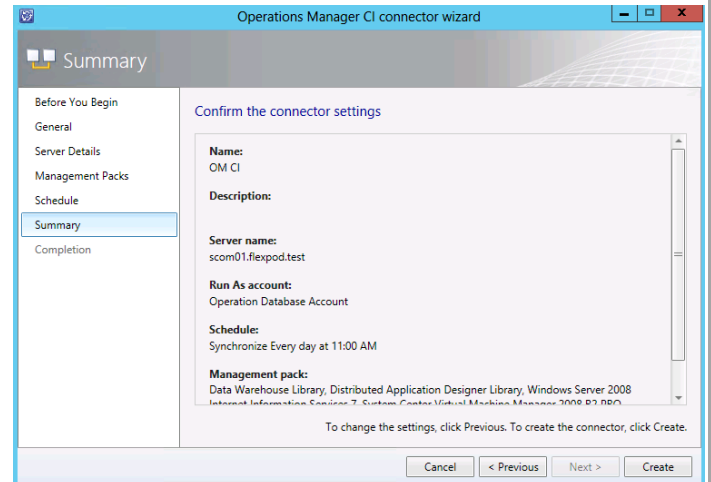
In the **Management Packs** dialog, select the **Select All** checkbox. Click **Next** to continue.



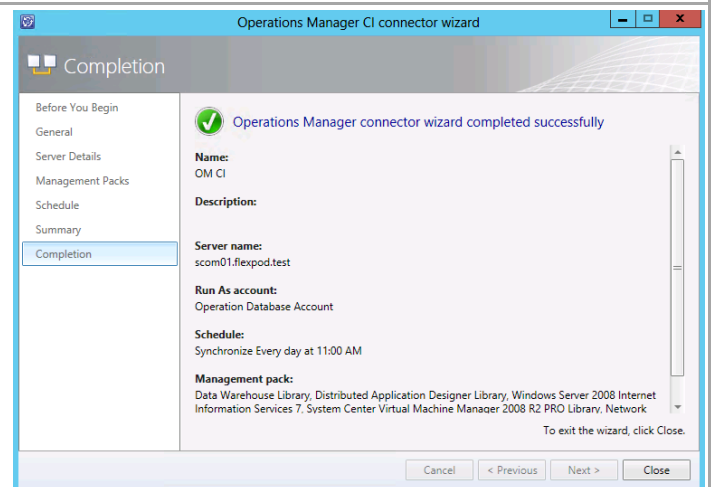
In the **Schedule** dialog, create a schedule for the connector or leave the defaults. Click **Next** to continue.



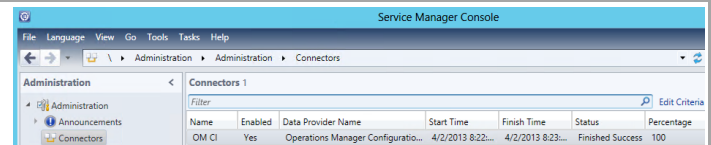
In the **Summary** dialog, verify the selections made and click **Create** to create the connector.



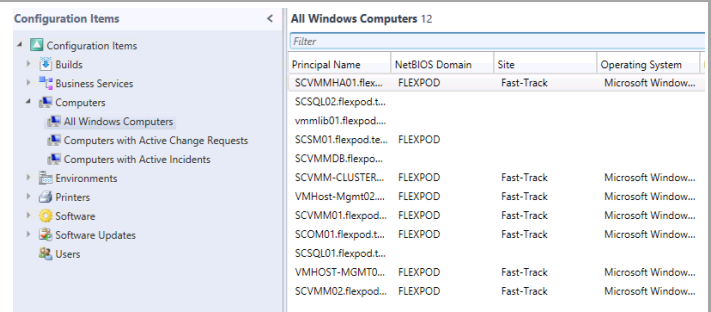
In the **Completion** dialog, verify the process completes successfully and click **Close**.



Once created, verify the Connector has a successful run by checking that there is a time listed in the **Finish Time** column.



In the **Service Manager console**, select the **Configuration Items** pane and navigate to the **All Windows Computers** node. Ensure that the configuration items have synchronized from the Operations Manager connector.



Create the OrchestratorUsersGroup local group on the Orchestrator Server

Perform the following steps to avoid issues related to CSPP setup on Orchestrator.

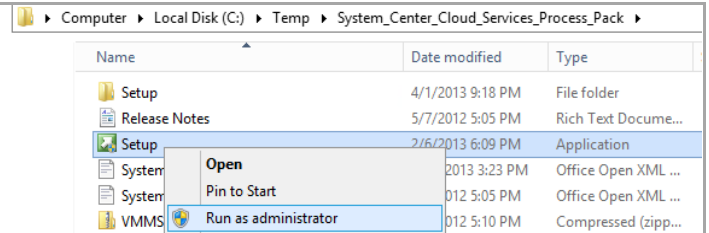
- Perform the following steps on both **Orchestrator** virtual machines.

Log on to both Orchstraotr virtual machines with a user with local admin rights.

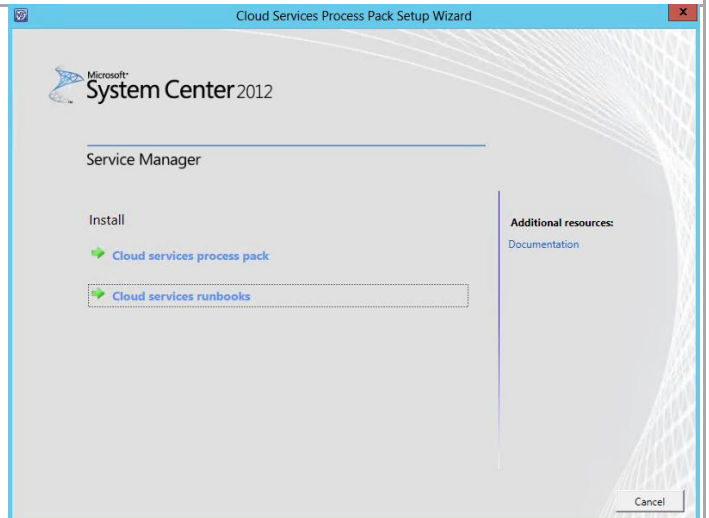
Verify the account has the following rights:

- An Orchstrator administrator.
- An administrator on the server that is running Orchestrator.

After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and run **Setup.exe** as an Administrator.



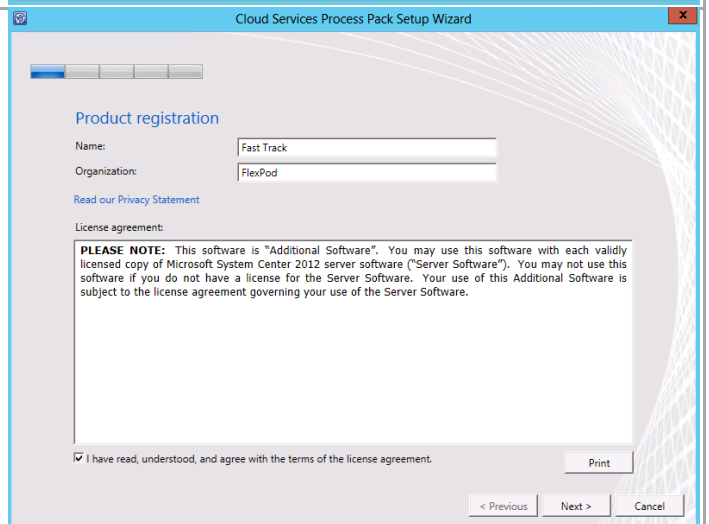
The **Cloud Services Process Pack Setup Wizard** will appear. In the Install section, select **Cloud services process pack**.



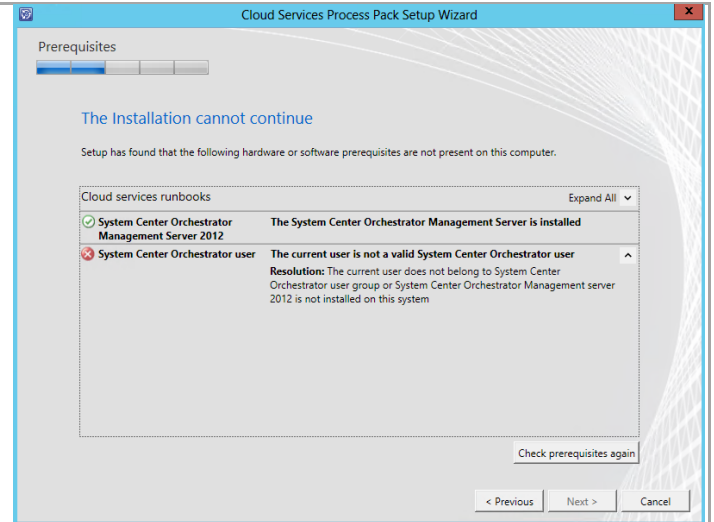
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization.*
- **Organization** - *specify the name of the licensed organization.*

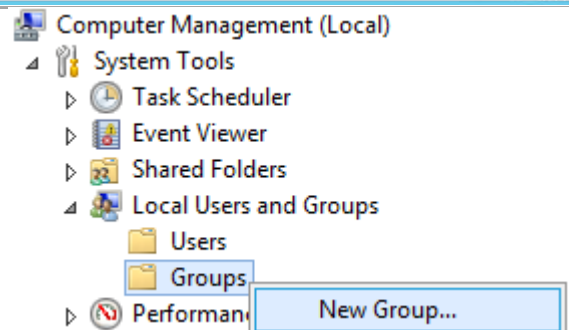
Click **Next** to continue.



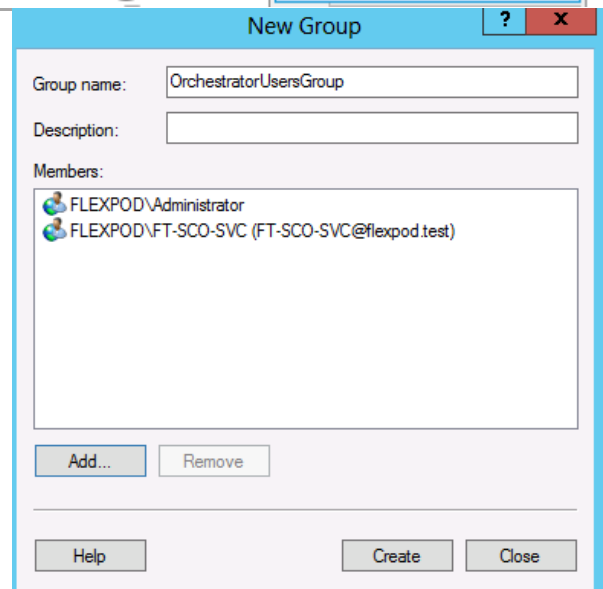
The pre-requisite checker in CSPP validates settings in Orchestrator, but during its process it verifies if the logged in user is directly a member of a local security group called “**OrchestratorUsersGroup**”, regardless of how security for Orchestrator is configured. Per the recommended configuration this group was changed to a domain group, however a local group must be created with membership granted to the installation account to complete setup²⁶.



To satisfy this requirement, a local group must be created on the Orchestrator servers where the runbooks will be installed. In Server Manager, navigate to the **Local Users and Groups** node, right-click **Groups** and select **New Group...** from the context menu.



In the **New Group** dialog, provide the **Group name** of **OrchestratorUsersGroup** and ensure that the membership contains the account you are using to perform this installation. Click **Create** to complete the creation of the local group.



²⁶ <http://blogs.technet.com/b/orchestrator/archive/2012/05/10/faq-cloud-service-mp-pre-reg-error-the-current-user-is-not-a-valid-system-center-orchestrator-user.aspx>

21.3 Installation

Install the Cloud Services Process Pack

The following steps need to be completed in order to install the Cloud Services Process Pack.

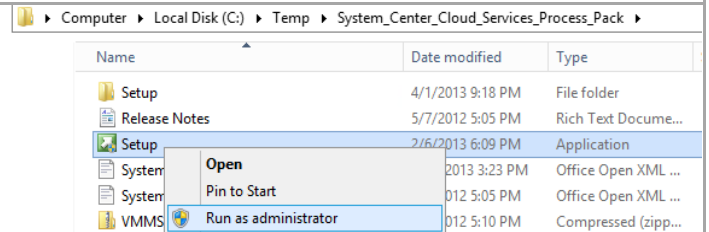
► Perform the following steps on the **Service Manager management server** virtual machine.

Log on to the Service Manager management server virtual machine with a user with local admin rights.

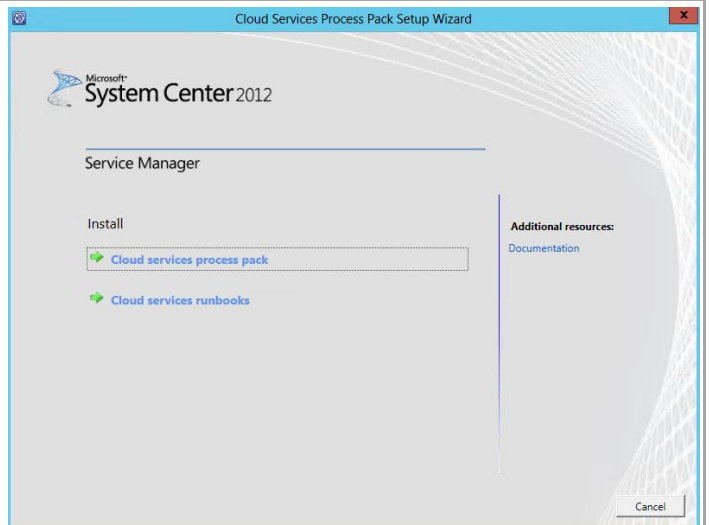
Verify the account has the following rights:

- A Service Manager administrator.
- An administrator on the server that is running Service Manager.

After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and run **Setup.exe** as an Administrator.



The **Cloud Services Process Pack Setup Wizard** will appear. In the Install section, select **Cloud services process pack**.



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

- **Name** – *specify the name of the primary user or responsible party within your organization.*
- **Organization** - *specify the name of the licensed organization.*

Click **Next** to continue.

The screenshot shows the 'Product registration' step of the 'Cloud Services Process Pack Setup Wizard'. It includes a progress bar at the top with four steps, the first of which is active. The 'Name' field contains 'Fast Track' and the 'Organization' field contains 'FlexPod'. Below these fields is a link to 'Read our Privacy Statement'. A 'License agreement' section contains a 'PLEASE NOTE' text block. At the bottom, there is a checkbox labeled 'I have read, understood, and agree with the terms of the license agreement.' which is checked, and a 'Print' button. Navigation buttons at the bottom right are '< Previous', 'Next >', and 'Cancel'.

Cloud Services Process Pack Setup Wizard

Product registration

Name: Fast Track

Organization: FlexPod

[Read our Privacy Statement](#)

License agreement:

PLEASE NOTE: This software is "Additional Software". You may use this software with each validly licensed copy of Microsoft System Center 2012 server software ("Server Software"). You may not use this software if you do not have a license for the Server Software. Your use of this Additional Software is subject to the license agreement governing your use of the Server Software.

☒ I have read, understood, and agree with the terms of the license agreement.

Print

< Previous Next > Cancel

The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.

The screenshot shows the 'System check results' step of the 'Cloud Services Process Pack Setup Wizard'. It includes a progress bar at the top with four steps, the second of which is active. The title is 'System check results'. Below the title, it states 'The prerequisite check has passed'. A section titled 'Cloud services process pack' contains a table of checks.

Cloud Services Process Pack Setup Wizard

Prerequisites

System check results

The prerequisite check has passed

Cloud services process pack

<input checked="" type="checkbox"/> System Center Service Manager 2012	The System Center Service Manager 2012 is installed
<input checked="" type="checkbox"/> Administrator on System Center Service Manager 2012	The current user is Administrator on System Center Service Manager 2012
<input checked="" type="checkbox"/> VMM Discovery Management Pack	VMM Discovery Management Pack has been found in System Center Service Manager 2012
<input checked="" type="checkbox"/> Drive Space Check	We require at least 0.1 GB of free space on the system drive

< Previous Next > Cancel

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 screenshot shows the 'Installation summary' step of the 'Cloud Services Process Pack Setup Wizard'. It includes a progress bar at the top with four steps, the third of which is active. The title is 'Installation summary'. Below the title, it says 'Review the selections for the components you are installing. To continue, click Install. To change these selections, click Previous.' A section titled 'Installing Component:' shows 'Cloud services process pack'. Below this, it lists the 'Program files location', 'Service Manager server name', 'Service Manager Administrator account', and 'Install log file path'.

Cloud Services Process Pack Setup Wizard

Installation summary

Review the selections for the components you are installing. To continue, click Install. To change these selections, click Previous.

Installing Component:
Cloud services process pack

Program files location:
C:\Program Files\Microsoft System Center 2012\Service Manager\Cloud services process pack

Service Manager server name:
SCSM01

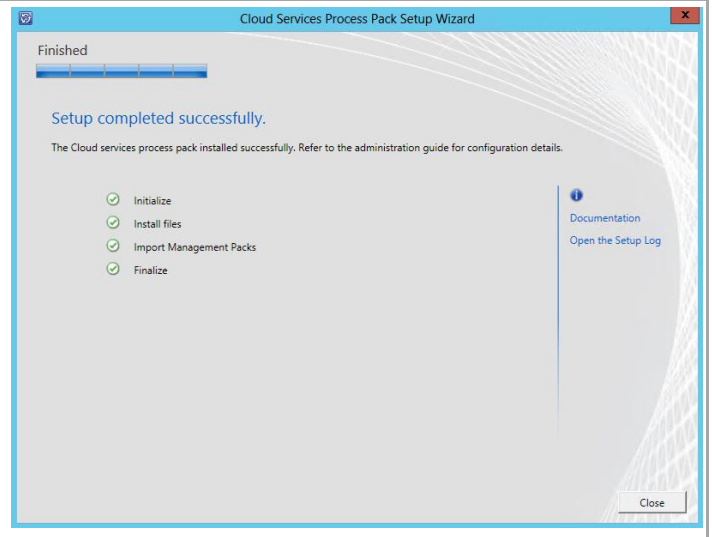
Service Manager Administrator account:
FLEXPOD\Administrator

Install log file path:
C:\Users\Administrator\FLEXPOD\AppData\Local\SCCloudServices\LOGS\SCCloudservicesprocesspackInstall02.log

< Previous Install Cancel

Once the installation completes, the wizard will display the **Setup completed successfully** dialog.

Click **Close** to complete the installation.



Install the Cloud Services Process Pack Runbooks

The following steps need to be completed in order to install the Cloud Services Process Pack Orchestrator runbooks.

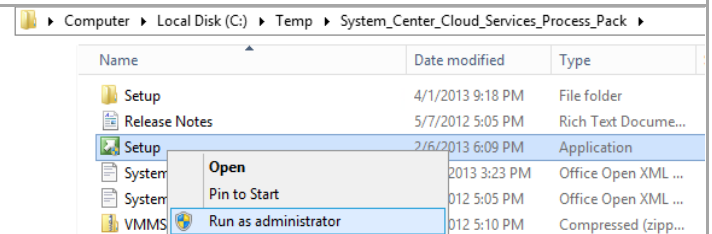
► Perform the following steps on the **Orchestrator** virtual machine.

Log on to the Orchestrator management server virtual machine with a user with local admin rights.

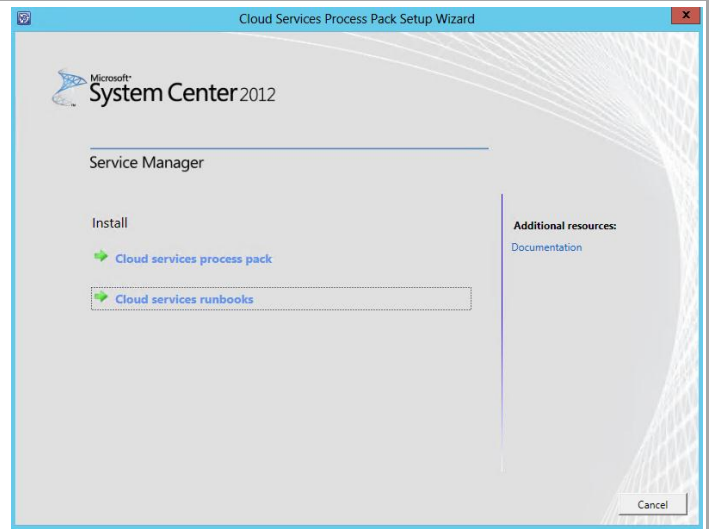
Verify the account has the following rights:

- An administrator on the machine on which the program is installed as well as an Orchestrator administrator.
- An administrator in the Orchestrator database.
- An administrator on each SQL Server cluster node.
- An administrator on VMM.
- A member of the local OrchestratorUsersGroup created in earlier steps.

After verification, navigate to the folder where the Cloud Services Process Pack (CSPP) was extracted and click **Setup.exe** as an Administrator.



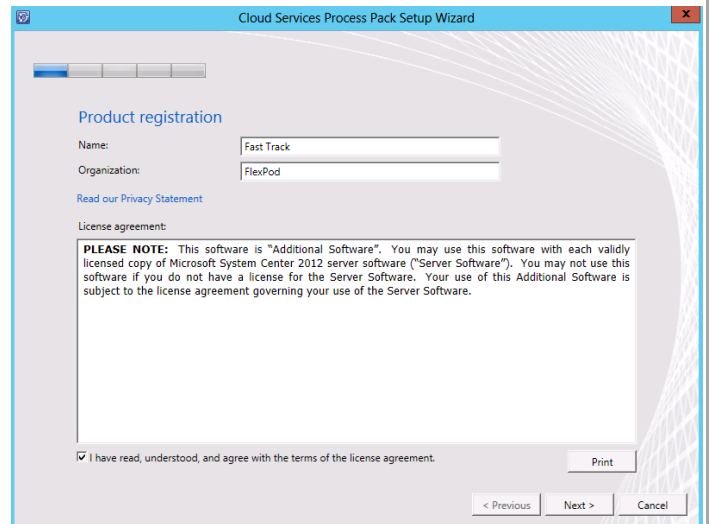
The **Cloud Services Process Pack Setup Wizard** will appear. In the **Install** section, select **Cloud services process pack**.



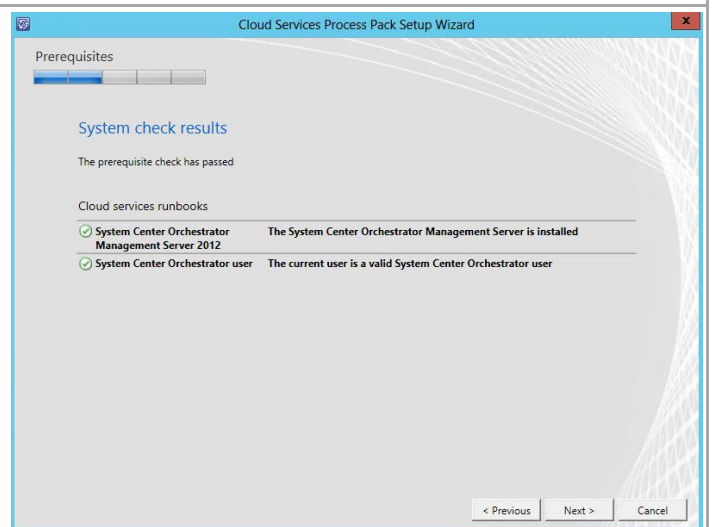
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – *specify the name of the primary user or responsible party within your organization.*
- **Organization** - *specify the name of the licensed organization.*

Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. Once verified, click **Next** to continue.



In the **Configure System Center Orchestrator account and Database** dialog, specify the Orchestrator service account in the dialog and click **Test Credentials**. Specify the Orchestrator database server name, the instance and database. Once selected, click **Next** to continue.

The screenshot shows the 'Cloud Services Process Pack Setup Wizard' window, specifically the 'Configure System Center Orchestrator account and Database' step. The dialog has a title bar with a close button. Below the title bar is a progress bar with four steps, the second of which is highlighted. The main content area has a blue header with the title 'Configure System Center Orchestrator account and Database'. Below this is a descriptive text: 'Specify a domain account that is a member of Orchestrator users group. This account will be used to import the Runbooks and will remain securely encrypted. Specify the Orchestrator Database Server, instance and Database name details.' There are two main sections: 'System Center Orchestrator user account:' and 'System Center Orchestrator Database Server:'. The first section has fields for 'User name:' (FT-SCO-SVC), 'Password:' (masked with dots), and 'Domain:' (FLEXPOD), with a 'Test Credentials' button below. The second section has fields for 'SQL Server instance:' (SCDB) and 'Orchestrator Database:' (Orchestrator). At the bottom, there is a green checkmark icon and the text 'The credentials were accepted.' and navigation buttons: '< Previous', 'Next >', and 'Cancel'.

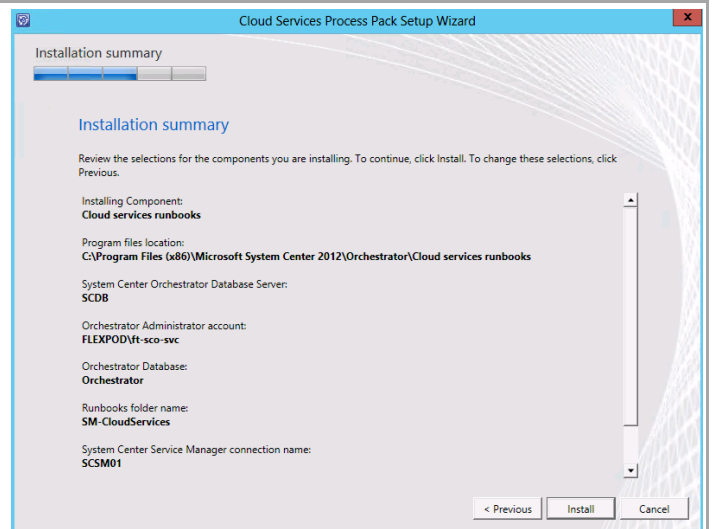
NOTE: If the SCDB instance is not configured to use port 1433, the following error will appear when attempting to enumerate the Orchestrator database from the SQL named instance. Setup will not continue if this is the case.

The screenshot shows a 'Database error' dialog box with a red 'X' icon in the top right corner. The main text area contains a red circular icon with a white 'X' and the following text: 'A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)'. At the bottom right is an 'OK' button.

In the **Configure the System Center Orchestrator connections** dialog, specify the name of the Service Manager Orchestrator connector name created in the Orchestrator post-installation steps earlier. Click **Next** to continue.

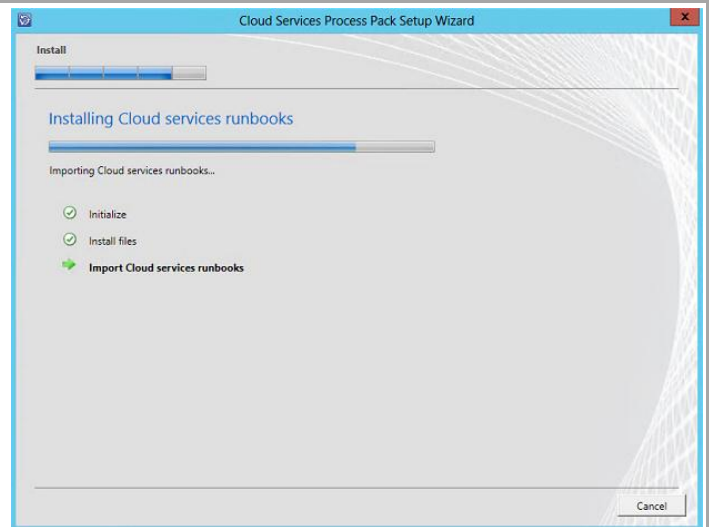
The screenshot shows the 'Cloud Services Process Pack Setup Wizard' window, specifically the 'Configure the System Center Orchestrator connections' step. The dialog has a title bar with a close button. Below the title bar is a progress bar with four steps, the third of which is highlighted. The main content area has a blue header with the title 'Configure the System Center Orchestrator connections'. Below this is a descriptive text: 'Specify the System Center Service Manager connection name that is configured in the System Center Orchestrator server.' There are two main sections: 'Runbooks folder name:' and 'System Center Service Manager connection name:'. The first section has a text box with 'SM-CloudServices'. The second section has a text box with 'SCSM01'. At the bottom right are navigation buttons: '< Previous', 'Next >', and 'Cancel'.

The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



Once the installation completes, the wizard will display the **Setup completed successfully** dialog.

Click **Close** to complete the installation

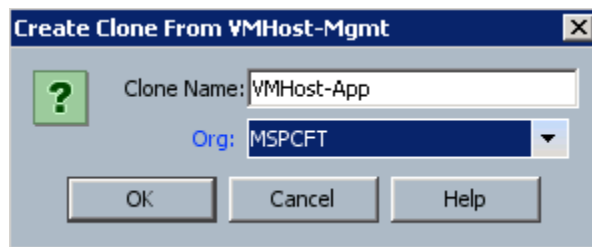


22 Deploy App Cluster from Gold Master

22.1 Create Service Profile Template

These steps provide details for creating a service profile template from by cloning and the previously created service profile template and then modifying it.

1. In Cisco UCS Manager, Select the Servers tab at the top left of the window.
2. Select Service Profile Templates VMHost-Mgmt in the sub-organization.
3. Right-click and select Create a Clone.
4. Enter VMHost-App for the Clone Name.
5. Select the Organization.
6. Click OK to create the new service profile template.



7. Expand the new service profile template and select vNICs.
8. Right-Click the VM-Database vNIC and click Delete.
9. Right-Click the MF-Public vNIC and click Delete.
10. Right-Click vNICs and click Create vNIC.
11. The Create vNIC window displays. Name the vNIC VM-AF-Public.
12. Check the Use LAN Connectivity Template checkbox.
13. Select VM-AF-Public for the vNIC Template field.
14. Select Windows in the Adapter Policy field.
15. 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](#)

16. Click **Modify vNIC/vHBA Placement**.
17. Select **vCon1** in the **Virtual Network Interface Policy**
18. Select the **VM-AF Public vNIC** and click **assign**.
19. Place the **VM-AF Public vNIC** after the **CSV vNIC** and click **OK**.

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: [+ 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

vNICs

vHBAs

Name

>> assign >>

<< remove <<

Virtual Network Interfaces Policy (read only)

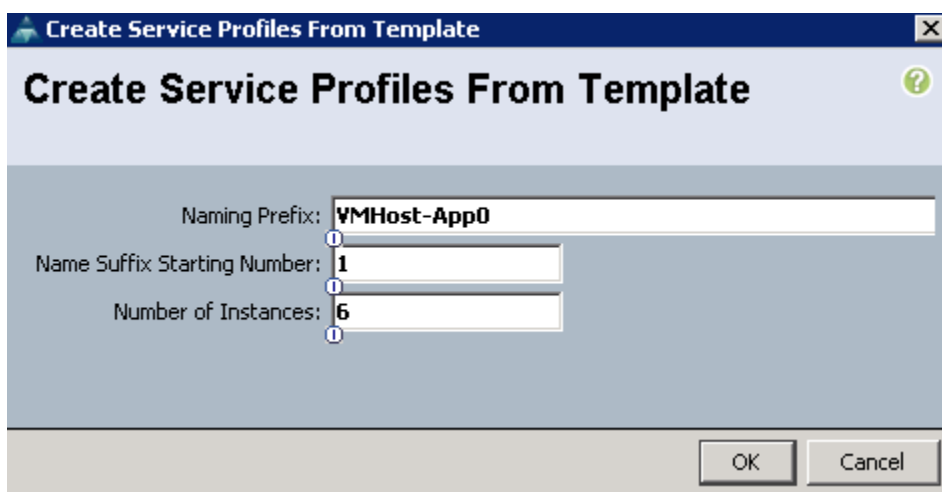
Name	Order	Selection Preference
vCon 1		Assigned Only
vNIC Mgmt	1	
vNIC SMB	4	
vNIC LiveMigration	8	
vNIC CSV	12	
vNIC VM-AF-Public	15	
vNIC App-Cluster-Comm	16	
vHBA Fabric-A-1	17	

Move Up Move Down

22.2 Create Service Profiles

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

1. In Cisco UCS Manager, Select the **Servers** tab at the top left of the window.
2. Select **Service Profile Templates VMHost-App** in the sub-organization.
3. Right-click and select **Create Service Profile From Template**.
4. Enter **VMHost-App0** for the service profile prefix.
5. Enter **1** for the Name Suffix Starting Number.
6. Enter **6** for the number of service profile instances to create.
7. Click **OK** to create the service profile.



8. Click **OK** in the message box.

22.3 Gather Necessary Information

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

Table 24) 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		
VMHost-App05		
VMHost-App06		

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.

22.4 Create Device Aliases

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

Nexus 5548 A

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

```
device-alias database
  device-alias name VMHost-App01-A-1_A pwnn <Fabric-A WWPN>
  device-alias name VMHost-App02-A-1_A pwnn <Fabric-A WWPN>
  device-alias name VMHost-App03-A-1_A pwnn <Fabric-A WWPN>
  device-alias name VMHost-App04-A-1_A pwnn <Fabric-A WWPN>
  device-alias name VMHost-App05-A-1_A pwnn <Fabric-A WWPN>
  device-alias name VMHost-App06-A-1_A pwnn <Fabric-A WWPN>
exit
device-alias commit
copy running-config startup-config
```

Nexus 5548 B

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

```
device-alias database.
  device-alias name VMHost-App01-B-1_B pwnn <Fabric-B WWPN>
  device-alias name VMHost-App02-B-1_B pwnn <Fabric-B WWPN>
  device-alias name VMHost-App03-B-1_B pwnn <Fabric-B WWPN>
  device-alias name VMHost-App04-B-1_B pwnn <Fabric-B WWPN>
  device-alias name VMHost-App05-B-1_B pwnn <Fabric-B WWPN>
  device-alias name VMHost-App06-B-1_B pwnn <Fabric-B WWPN>
exit
device-alias commit
copy running-config startup-config
```

22.5 Create Zones for Each Service Profile

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

Nexus 5548 A

1. Create the Zones and Add Members

```
zone name VMHost-App01_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App01-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name VMHost-App02_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App02-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
```

```

exit
zone name VMHost-App03_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App03-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name VMHost-App04_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App04-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name VMHost-App05_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App05-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit
zone name VMHost-App06_A vsan <Fabric A VSAN ID>
  member device-alias VMHost-App06-A-1_A
  member device-alias Infra_vs1_lif01a
  member device-alias Infra_vs1_lif02a
exit

```

2. Create the Zoneset and Add the Necessary Members

```

zoneset name FlexPod vsan <Fabric A VSAN ID>
  member VMHost-App01_A
  member VMHost-App02_A
  member VMHost-App03_A
  member VMHost-App04_A
  member VMHost-App05_A
  member VMHost-App06_A
exit

```

3. Activate the Zoneset

```

zoneset activate name flexpod vsan < Fabric A VSAN ID>
exit
copy running-config startup-config

```

Nexus 5548 B

1. Create the Zones and Add Members

```

zone name VMHost-App01_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App01-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
zone name VMHost-App02_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App02-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
zone name VMHost-App03_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App03-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit

```

```

zone name VMHost-App04_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App04-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
zone name VMHost-App05_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App05-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit
zone name VMHost-App06_B vsan <Fabric B VSAN ID>
  member device-alias VMHost-App06-B-1_B
  member device-alias Infra_vs1_lif01b
  member device-alias Infra_vs1_lif02b
exit

```

2. Create the Zoneset and Add the Necessary Members

```

zoneset name FlexPod vsan <Fabric B VSAN ID>
  member VMHost-App01_B
  member VMHost-App02_B
  member VMHost-App03_B
  member
  member VMHost-App04_B
  member VMHost-App05_B
  member VMHost-App06_B
exit

```

3. Activate the Zoneset

```

zoneset activate name FlexPod vsan < Fabric B VSAN ID>
exit
copy running-config startup-config

```

22.6 FlexClone Boot LUN

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

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

```
Import-Module DataONTAP
```

2. Connect to the NetApp controller

```
Connect-NcController <<var_vserver_mgmt_ip>> -credential vsadmin
```

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

```

New-NcQtree -Volume ucs_boot -Qtree VMHost-App01
New-NcQtree -Volume ucs_boot -Qtree VMHost-App02
New-NcQtree -Volume ucs_boot -Qtree VMHost-App03
New-NcQtree -Volume ucs_boot -Qtree VMHost-App04
New-NcQtree -Volume ucs_boot -Qtree VMHost-App05
New-NcQtree -Volume ucs_boot -Qtree VMHost-App06

```

4. Using the information in Table 21, Create igroups

```

New-NcIgroup -Name VMHost-App01 -Protocol fcp -Type windows |
  Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
  Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-App02 -Protocol fcp -Type windows |
  Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
  Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-App03 -Protocol fcp -Type windows |

```

```

Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-App04 -Protocol fcp -Type windows |
Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-App05 -Protocol fcp -Type windows |
Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>
New-NcIgroup -Name VMHost-App06 -Protocol fcp -Type windows |
Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> |
Add-NcIgroupInitiator -Initiator <vHBA_B WWPN>

```

5. Add-NcIgroupInitiator -Initiator <vHBA_A WWPN> | Add-NcIgroupInitiator -Initiator <vHBA_B WWPN> Clone the boot LUN from the goldmaster boot LUN.

```

New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App01/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App02/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App03/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App04/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App05/boot.lun
New-NcClone -Volume ucs_boot -SourcePath /goldmaster/boot.lun `
-destinationPath /VMHost-App06/boot.lun

```

6. Map the boot LUN to the new iGroup.

```

Add-NcLunMap -Path /vol/ucs_boot/VMHost-App01/boot.lun -InitiatorGroup VMHost-App01
Add-NcLunMap -Path /vol/ucs_boot/VMHost-App02/boot.lun -InitiatorGroup VMHost-App02
Add-NcLunMap -Path /vol/ucs_boot/VMHost-App03/boot.lun -InitiatorGroup VMHost-App03
Add-NcLunMap -Path /vol/ucs_boot/VMHost-App04/boot.lun -InitiatorGroup VMHost-App04
Add-NcLunMap -Path /vol/ucs_boot/VMHost-App05/boot.lun -InitiatorGroup VMHost-App05
Add-NcLunMap -Path /vol/ucs_boot/VMHost-App06/boot.lun -InitiatorGroup VMHost-App06

```

22.7 Boot Service Profiles

Complete the following steps to boot each new service profile.

All Hosts

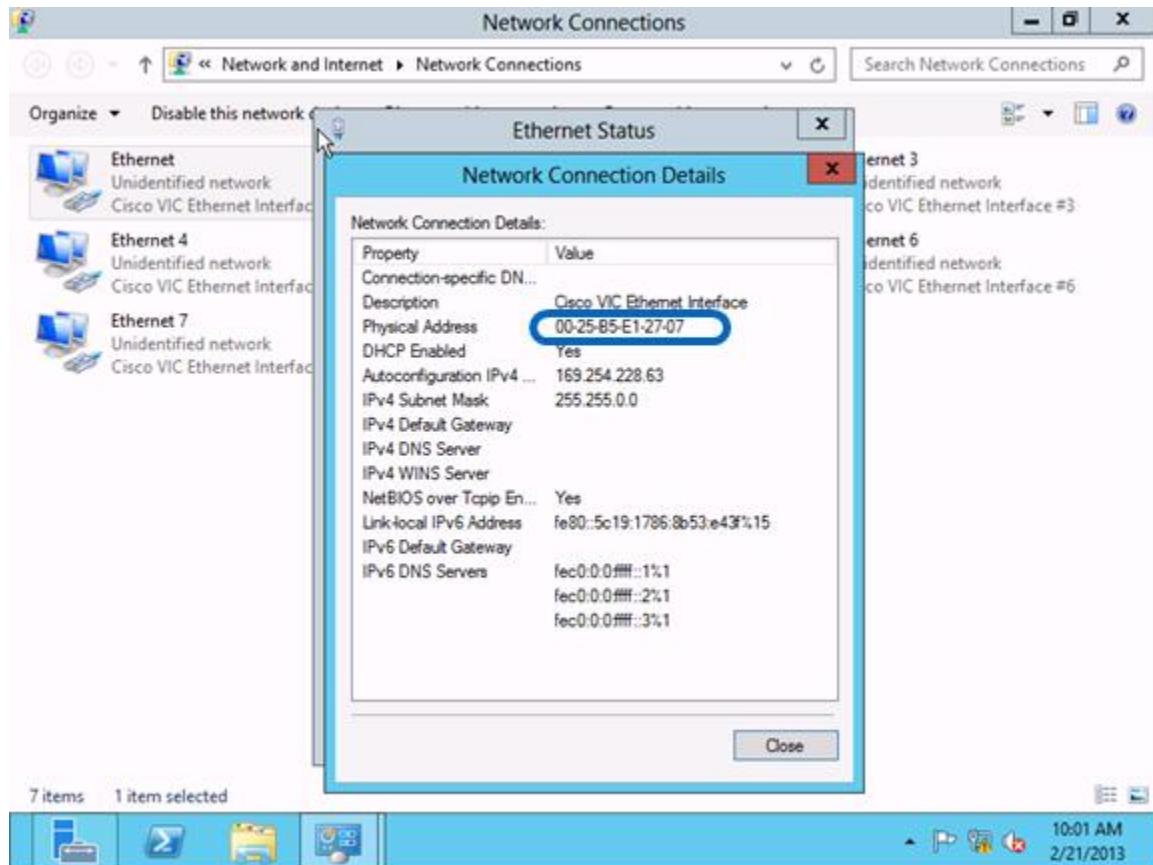
1. Back in USCM right-click on Service profile and select Associate with Server Pool.
2. From the Pool Assignment box, select the App_Pool and click OK, and OK again to acknowledge.
3. Right-click the <Hyper-V hostname> and select KVM Console.
4. Click Boot Server, the service profile will then pull a server from the VMHost-Infra pool, 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 App_Pool, and configure the hardware per the service profile.
7. Once 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.

22.8 Configure Windows Networking for FlexPod

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

All Hosts

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



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

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

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

vNICs		
Filter Export Print		
Name	MAC Address	Actual Order ▲
vNIC Mgmt	00:25:B5:E1:26:BE	1
vNIC SMB	00:25:B5:E1:27:0E	2
vNIC LiveMigration	00:25:B5:E1:26:FE	3
vNIC CSV	00:25:B5:E1:26:CE	4
vNIC VM-Database	00:25:B5:E1:26:EE	5
vNIC VM-MF-Public	00:25:B5:E1:26:DE	6

6. Identify the vNIC with the MAC Address noted in step 3.
 7. Back in windows rename the LAN adapter to reflect the network it is associated with.
 8. Set the appropriate IP settings for that adapter.
- Note:** Assign IP Addresses to the LiveMigration, CSV, and Mgmt adapters.
9. Repeat for each eNIC in windows.
 10. In the Network Connections Control Panel. Press the Alt key to drop down the extended menu, and select Advanced -> Advanced Settings
 11. Select the adapter and use the arrows to move it up or down in binding order.
 12. The recommended binding order is:
 - Mgmt
 - SMB
 - LiveMigration
 - CSV
 - VM-Database
 - VM-MF-Public

22.9 Create Hyper-V Virtual Network Switches

The VM Cluster Communication virtual network switch is provide in the case a Windows cluster needs to be deployed in virtual machines on the Application Cluster. A public communications switch will be added as part of the Nexus 1000V configuration.

All Hosts

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

Virtual Network Name	Connection Type	Enable SR-IOV	Interface Name	Share Network with Management Host
VM-Cluster-Comm	External	No	VM-Cluster-Comm	No

3. Create virtual switch VM-Cluster-Comm.

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

22.10 Create Virtual Fibre Channel Switches

Create Hyper-V virtual fibre channel switches and mind them to two unused HBAs on the host. These virtual fibre channel switches will be used by the virtual fibre channel adapter in the Failover Cluster virtual machines.

1. Obtain the PWWN for the second pair of HBAs on the Hyper-V hosts.

(Table 23) vHBA WWPNS for Fabric A and Fabric B.

Cisco UCS Service Profile Name	WWNN	Fabric-A-2 WWPN	Fabric-B-2 WWPN
VMHost-App01			
VMHost-App02			
VMHost-App03			
VMHost-App04			
VMHost-App05			
VMHost-App06			

All Hosts

1. Create two virtual fibre channel switches.

```
New-VMSan -Name vFabric-A -WorldWideNodeName <vHBA_A WWN> `
    -WorldWidePortName <vHBA_A WWPN>

New-VMSan -Name vFabric-B -WorldWideNodeName <vHBA_B WWN> `
    -WorldWidePortName <vHBA_B WWPN>
```

22.11 Prepare nodes for Clustering

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

All Hosts

1. Install windows feature

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

2. Rename the Host.

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

3. Add the host to Active Directory.

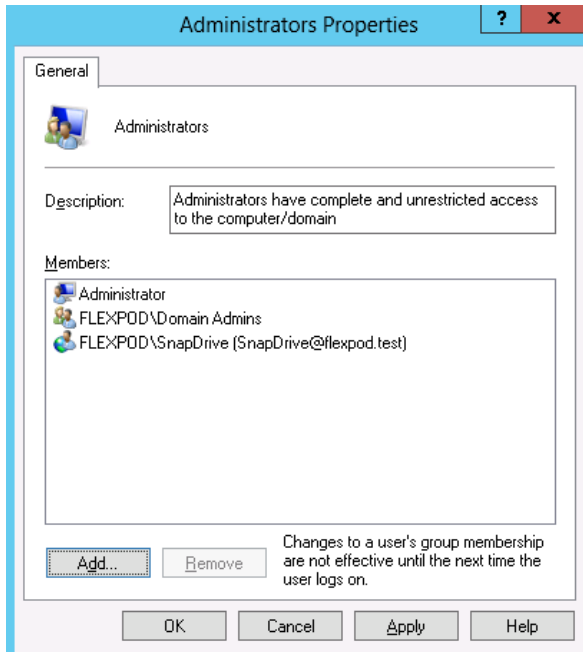
```
Add-Computer -DomainName <domain_name> -Restart
```

22.12 Install NetApp SnapDrive

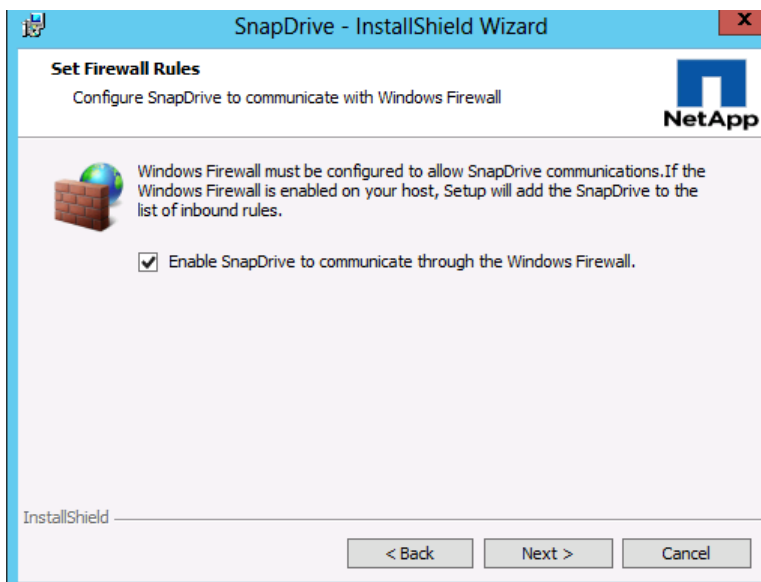
The following section describes how to installation of the NetApp SnapDrive Windows. For detailed information regarding the installation see the Administration and Installation Guide.

All App Fabric Hosts

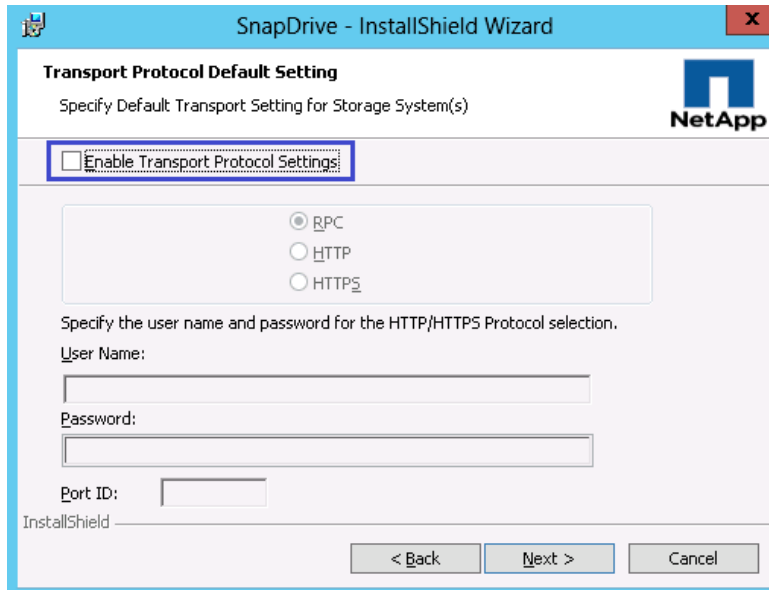
1. Add the SnapDrive service account to the local Administrators group in Windows.



2. Download SnapDrive installer
http://support.netapp.com/NOW/download/software/snapdrive_win/7.0/SnapDrive7.0_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 Protection Manger 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.

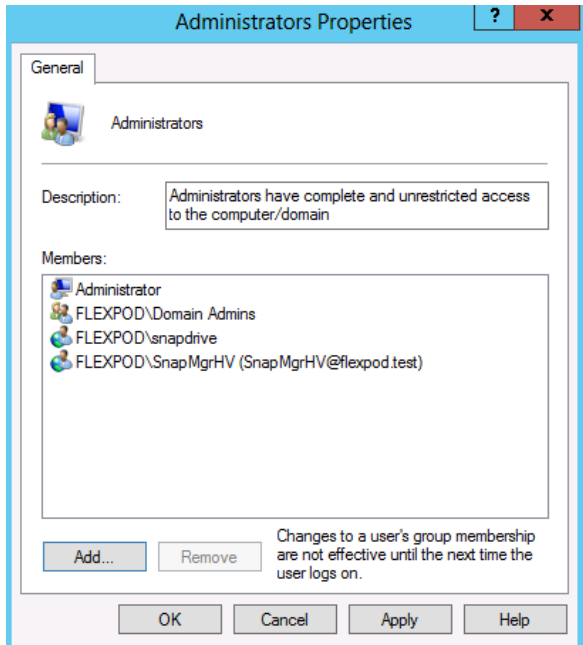
```
Set-SdStorageConnectionSetting -StorageSystem <<var_vserver_mgmt>> -protocol https -credential vsadmin
```

22.13 Install NetApp SnapManager for Hyper-V

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

All App Fabric Hosts

1. Add the SMHV service account to the local Administrators group in Windows.



All App Fabric Hosts

1. Download the SnapManger for Hyper-V installer from 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. Enter your User Name, and Organization information, and click Next.
5. Validate the installation path and click Next.
6. Enter the Account information for the SMHV service account, Click Next.
7. Click Next, through the SMHV Web Service EndPoint configuration.
8. Click Install.

22.14 Create a Cluster

One Server Only

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

```
New-Cluster -Name <cluster_name> -Node <Node1>, <Node2>, <node3>, <node4>, <node5>, <node6> -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'}
```

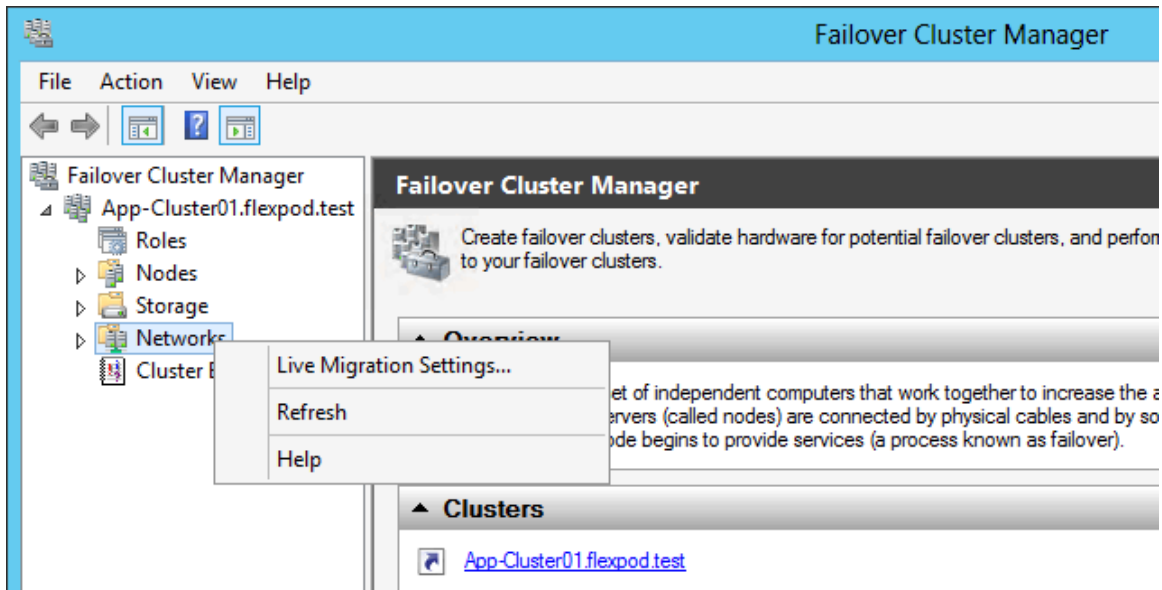
4. Designate the CSV network.

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

22.15 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.

22.16 Configure Quorum LUN

The following section will describe now to create the quorum disk, and configure the cluster to use the quorum witness.

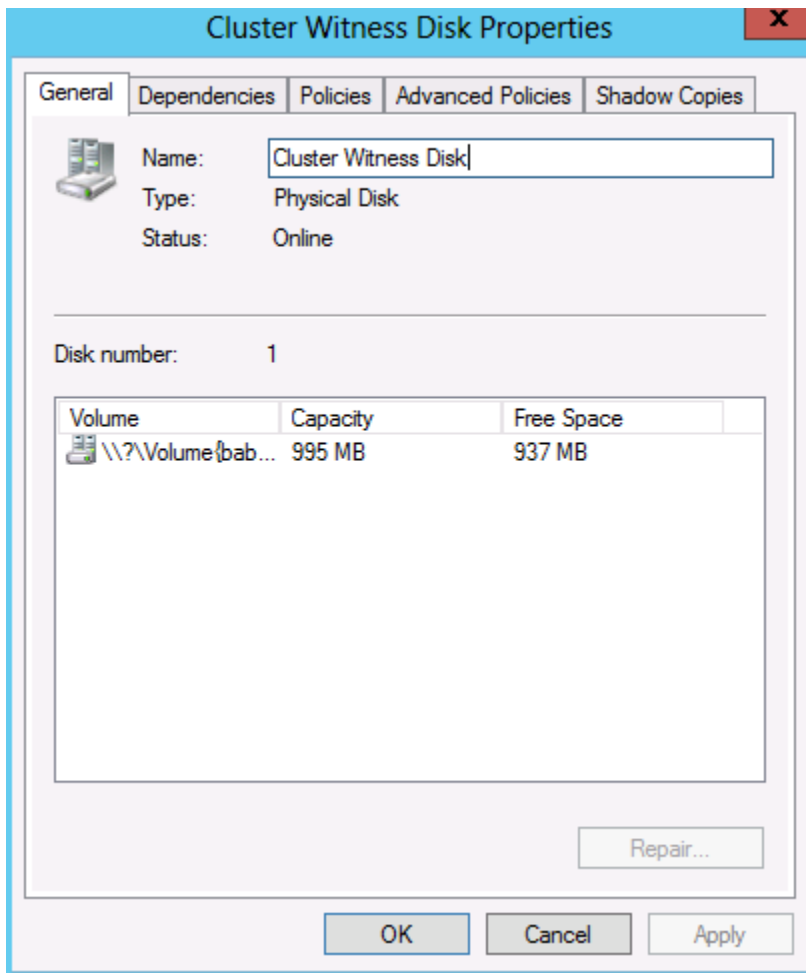
One Server Only

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

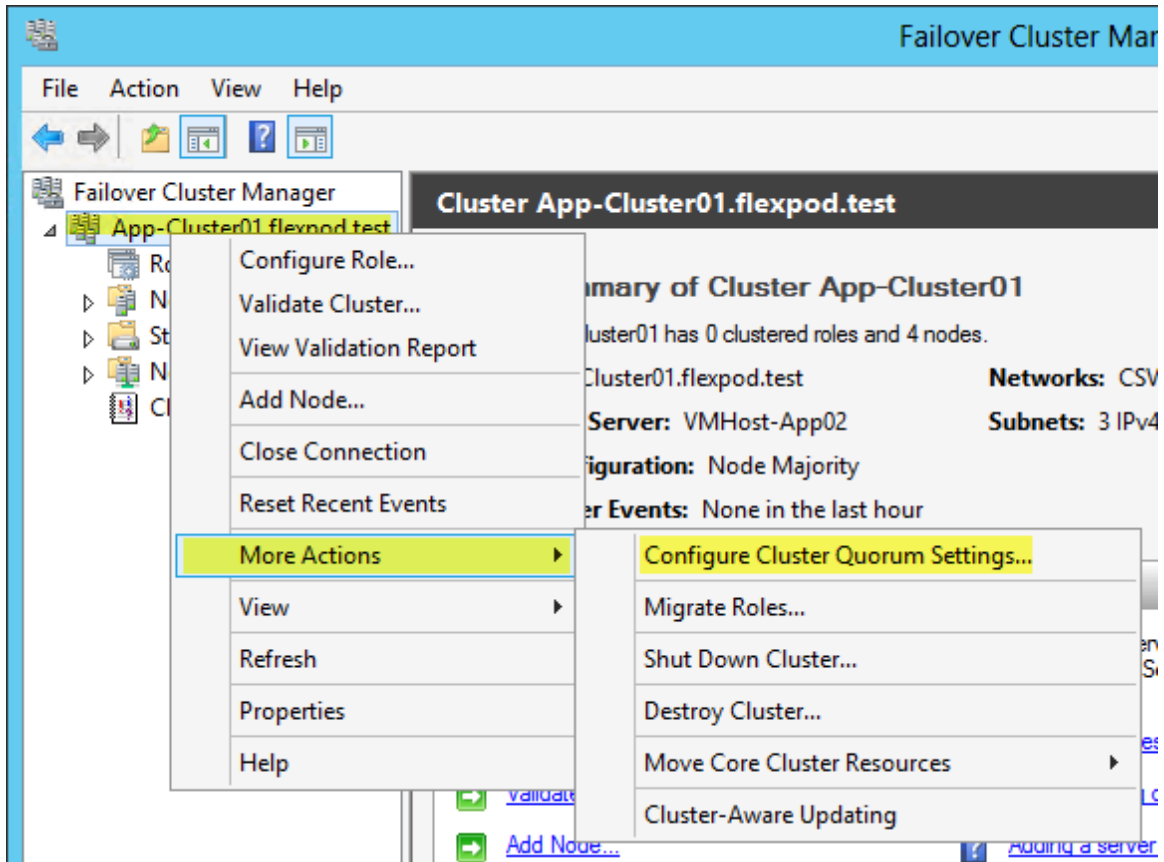
```
Move-ClusterGroup "Available Storage" -Node $env:COMPUTERNAME | Start-ClusterGroup
```

2. Open SnapDrive from the start screen to configure cluster storage.
3. From SnapDrive, Open the Server name, then Open the Disks Icon.
4. Right-click the Disks Icon and choose to **Create Disk**.
5. Type in the IP Address of the controller that contains the quorum Volume.
6. Once 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. Select **Select the cluster group Availavle 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. Select **Add or Change the Quorum Witness**, and click **Next**.
21. Select **Configure a disk witness**, and click **Next**.

Configure Cluster Quorum Wizard

Configure Storage Witness

Before You Begin

Select Quorum Configuration Option

Select Quorum Witness

Configure Storage Witness

Confirmation

Configure Cluster Quorum Settings

Summary

Select the storage volume that you want to assign as the disk witness.

Name	Status	Node	Location
<input checked="" type="checkbox"/> Cluster Witness Disk Volume: (\?\Volume... File System: NTFS	Online	VMHost-App01	Available Storage
		937 MB free of 995 MB	

< Previous Next > Cancel

22. Select **Cluster Witness Disk**, and click **Next**.

23. Click **Next**.

24. Click **Finish**.

Configure Cluster Quorum Wizard

Summary

Before You Begin

Select Quorum Configuration Option

Select Quorum Witness

Configure Storage Witness

Confirmation

Configure Cluster Quorum Settings

Summary

You have successfully configured the quorum settings for the cluster.

Configure Cluster Quorum Settings

Quorum Configuration: Node and Disk Majority

Storage: Cluster Witness Disk

Cluster Managed Voting: Enabled

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

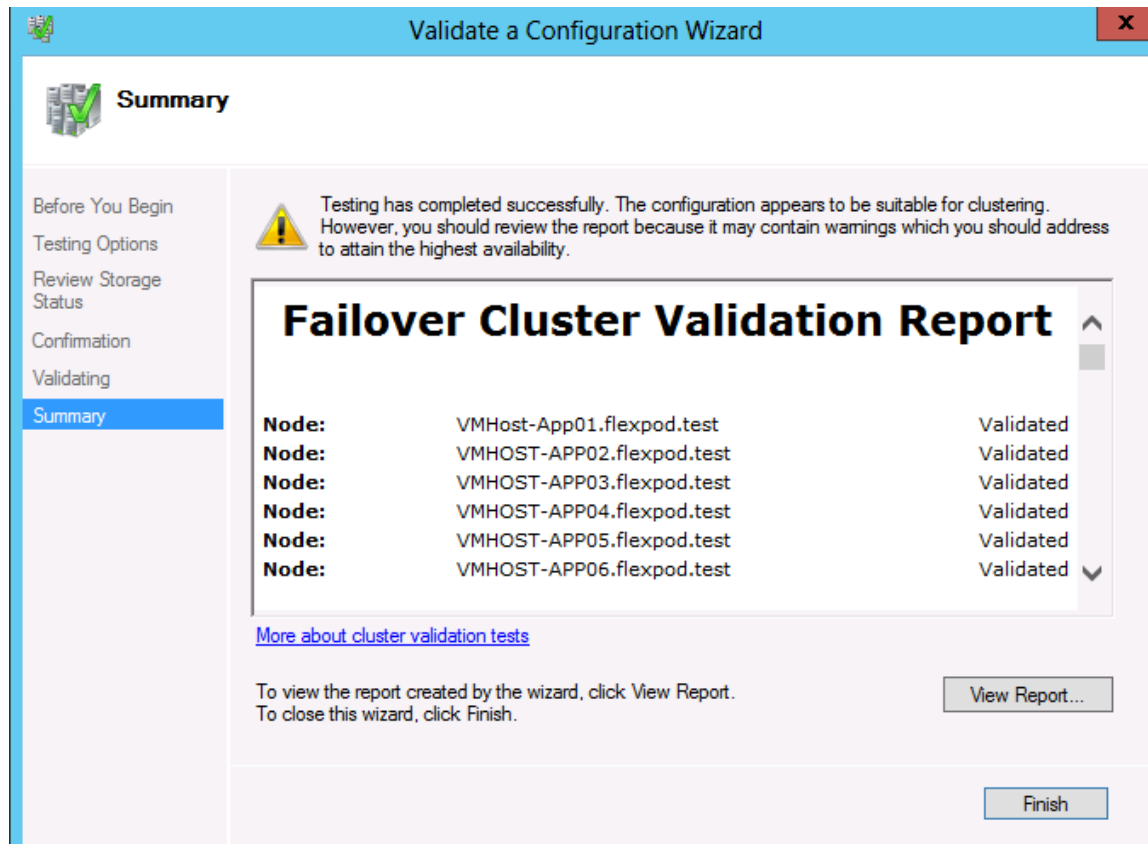
View Report...

Finish

22.17 Validated the Cluster

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

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



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

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

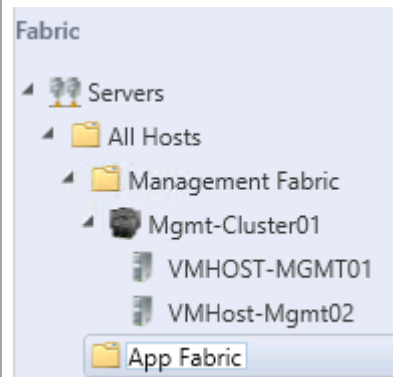
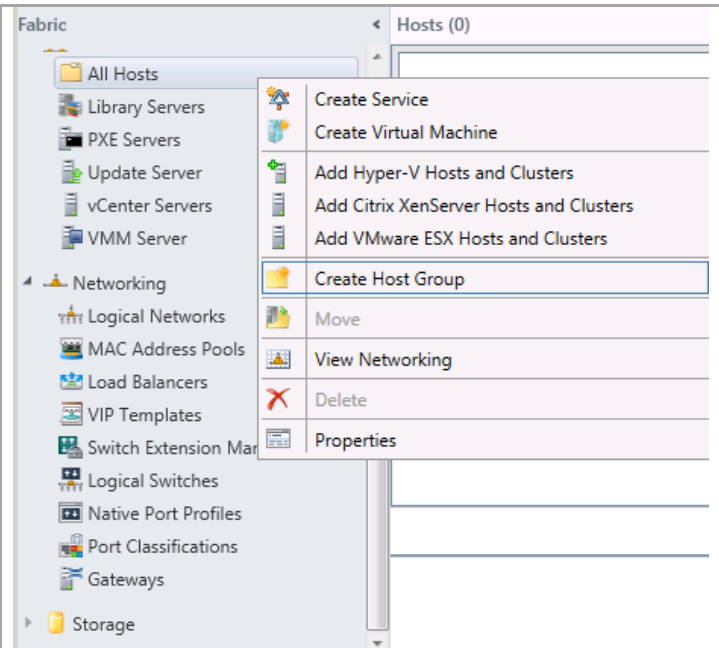
Successfully issued call to Persistent Reservation REGISTER using Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for Test Disk 0 from node VMHost-Mgmt01.flexpod.test.

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

22.18 Add the Cluster to SCVMM

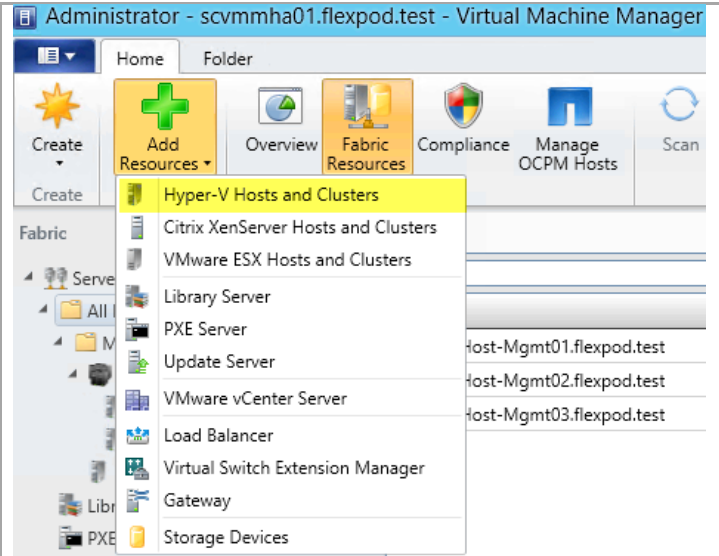
Perform the following steps on the SCVMM server.

Click **Fabric** in the left tree view and right click **All Hosts**. Select **Create Host Group**. Name the new Host Group.

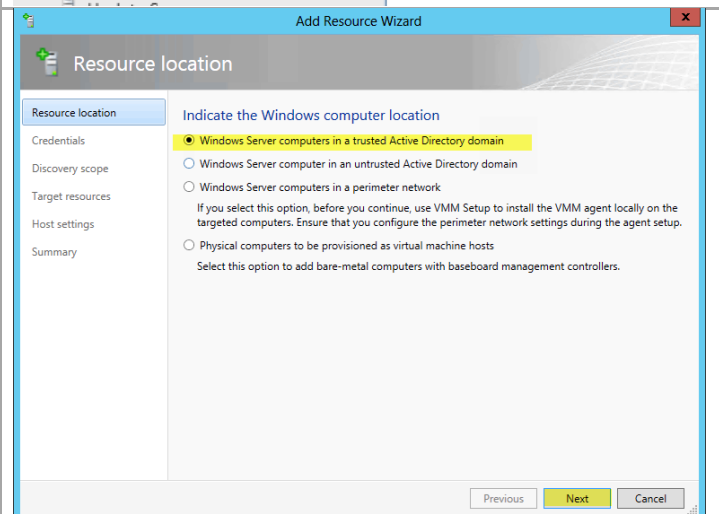


In the **Virtual Machine Manger** console, navigate to the **Fabric** pane.

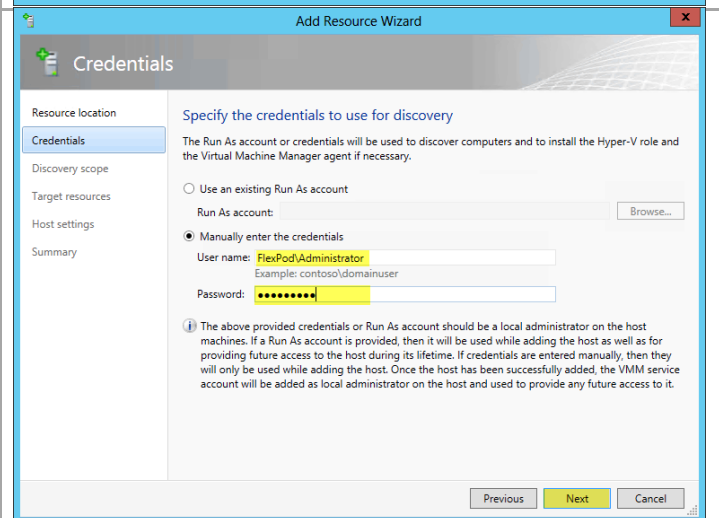
Select Add Resources, Hyper-V Hosts and Clusters.



Select Windows Server Computers in a trusted Active Directory domain, and click Next.



Enter an account that has permission on the cluster and click **Next**.



Enter the cluster name and click **Next**.

The screenshot shows the 'Add Resource Wizard' window, specifically the 'Discovery scope' step. The left sidebar contains a list of steps: Resource location, Credentials, Discovery scope (selected), Target resources, Host settings, and Summary. The main area is titled 'Specify the search scope for virtual machine host candidates'. It provides instructions on how to search for computers and offers two radio button options: 'Specify Windows Server computers by names' (selected) and 'Specify an Active Directory query to search for Windows Server computers'. Below these options is a text box labeled 'Computer names:' containing the text 'App-Cluster01'. There is also a checkbox for 'Skip AD verification' and a section for 'Examples' showing various server names and IP addresses. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

Select the cluster object and click **Next**.

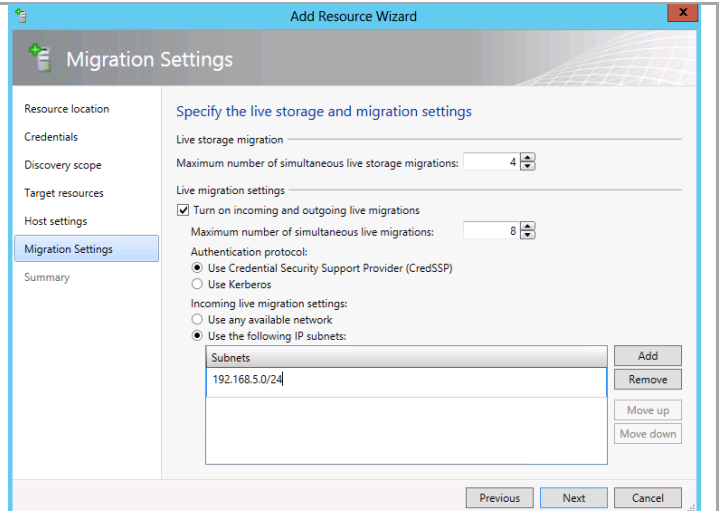
The screenshot shows the 'Add Resource Wizard' window, specifically the 'Target resources' step. The left sidebar shows the same list of steps as the previous screenshot, with 'Target resources' now selected. The main area is titled 'Select the computers that you want to add as hosts'. It displays a table of 'Discovered computers' with columns for 'Computer Name', 'Operating System', and 'Hypervisor'. The first row, 'app-cluster01.flexpod.test', is selected with a checkmark. Below the table are 'Select all', 'Refresh', and 'Stop' buttons. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

Computer Name	Operating System	Hypervisor
app-cluster01.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-APP04.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-APP02.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-APP05.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-APP03.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHOST-APP06.flexpod.test	Windows Server 2012 Datacenter	Hyper-V
VMHost-App01.flexpod.test	Windows Server 2012 Datacenter	Hyper-V

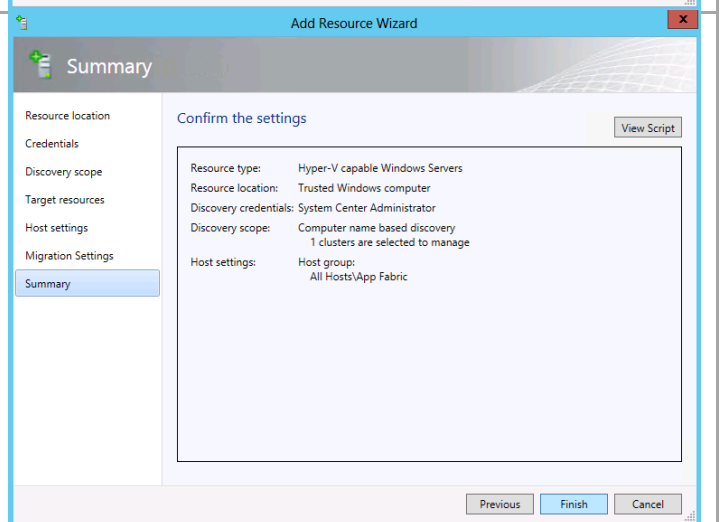
Select the Host group **App Fabric** from the dropdown menu and click **Next**.

The screenshot shows the 'Add Resource Wizard' window, specifically the 'Host settings' step. The left sidebar shows the same list of steps, with 'Host settings' now selected. The main area is titled 'Specify a host group and virtual machine placement path settings for hosts'. It instructs the user to 'Assign the selected computers to the following host group:' and shows a dropdown menu with 'App Fabric' selected. Below this, there is a checkbox for 'Reassociate this host with this VMM environment' which is currently unchecked. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

Set live migration settings. Default is 2 for each. Check the box **Turn on incoming and outgoing live migrations**. Set the IP subnet for live migration network. Click **Next**.



Click **Finish**.

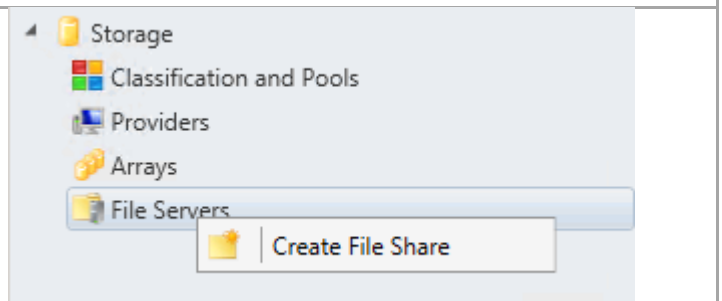


22.19 Provision the File Share to the Application Cluster

Complete the following steps to Add the Fabric Management Hyper-V hosts to VMM.

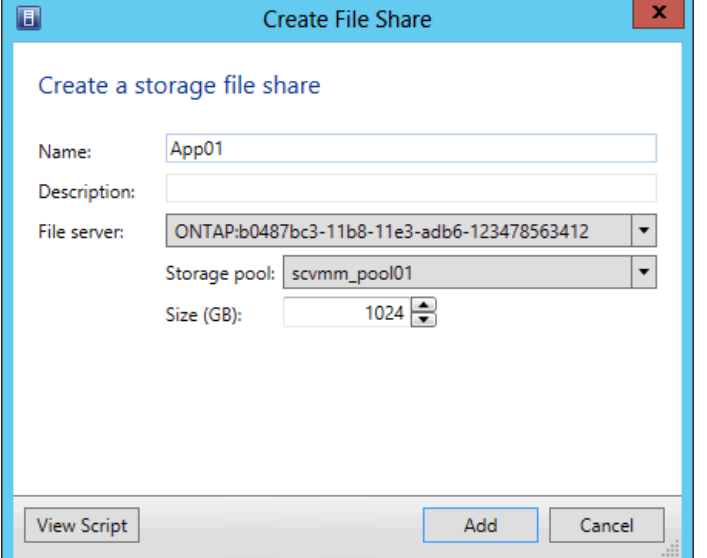
► Perform the following steps on the **Virtual Machine Manager** virtual machine.

Click **Fabric** in the left tree view. Expand **Storage**, and right click on **File Servers**, and select **Create File Share**.



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**.

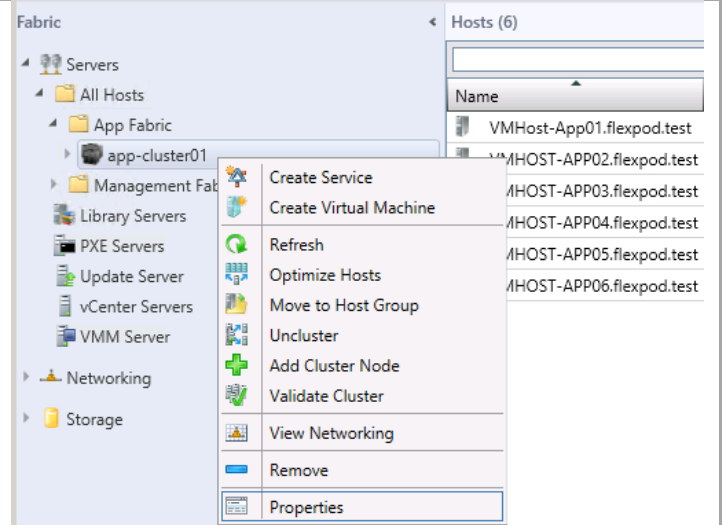


The 'Create File Share' dialog box is shown. It has a title bar with a close button. The main area is titled 'Create a storage file share'. It contains the following fields:

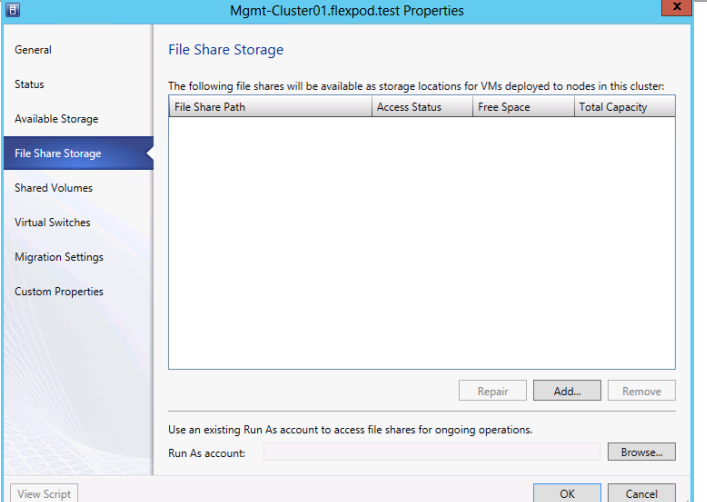
- Name: App01
- Description: (empty)
- File server: ONTAP:b0487bc3-11b8-11e3-adb6-123478563412
- Storage pool: scvmm_pool01
- Size (GB): 1024

At the bottom, there are three buttons: 'View Script', 'Add', and 'Cancel'.

Click **Fabric** in the left tree view. Expand **Servers**, **All Hosts**, and **App Fabric**. Right click the **App Cluster** and select **Properties**.

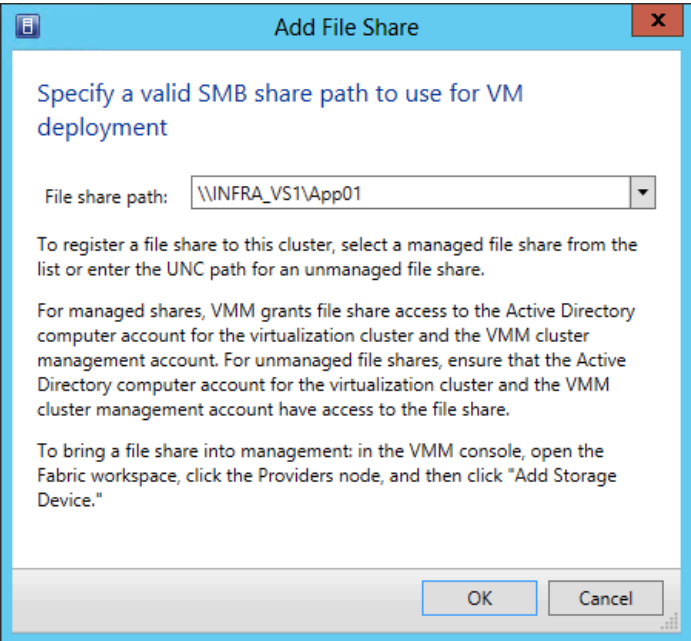


Select **File Share Storage** and click **Add**.

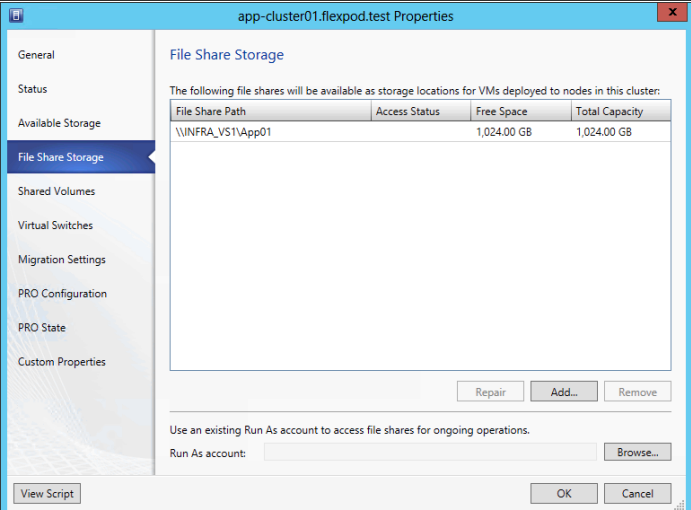


The 'Mgmt-Cluster01.flexpod.test Properties' dialog box is shown, with the 'File Share Storage' tab selected. The left pane shows a list of tabs: General, Status, Available Storage, File Share Storage (selected), Shared Volumes, Virtual Switches, Migration Settings, and Custom Properties. The main area is titled 'File Share Storage' and contains the text: 'The following file shares will be available as storage locations for VMs deployed to nodes in this cluster:'. Below this is a table with the following columns: File Share Path, Access Status, Free Space, and Total Capacity. The table is currently empty. At the bottom of the table area are three buttons: 'Repair', 'Add...', and 'Remove'. Below the table area is a section titled 'Use an existing Run As account to access file shares for ongoing operations.' with a 'Run As account:' label and a 'Browse...' button. At the very bottom of the dialog are two buttons: 'View Script' and 'OK', and a 'Cancel' button on the right.

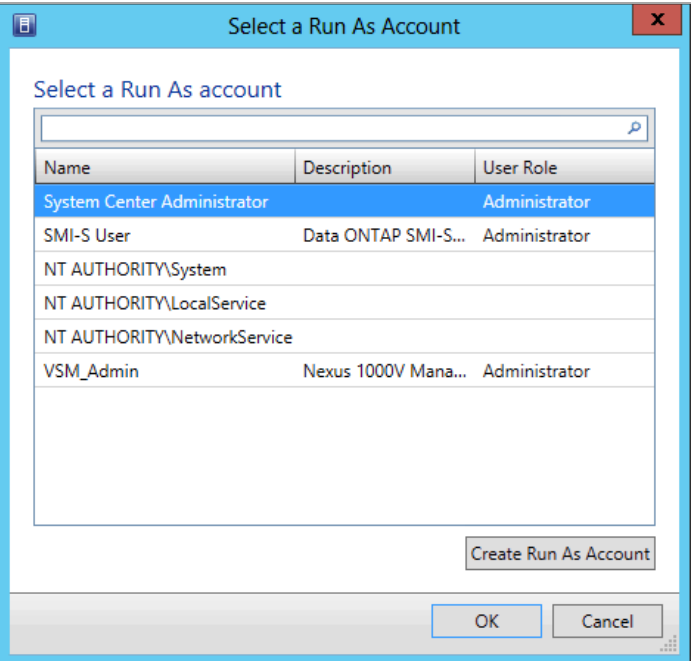
Select the **File Share Path** previously provisionined from the drop down and click **OK**.



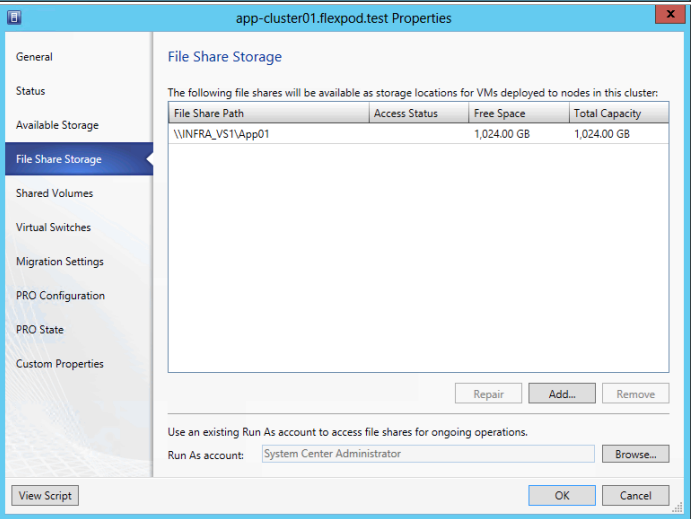
Click **Browse** to add a **Run As** account.



Select the Run As account and click **OK**.



Click **OK** to register the file share.



22.1 Configure App Fabric Network Segement in the 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

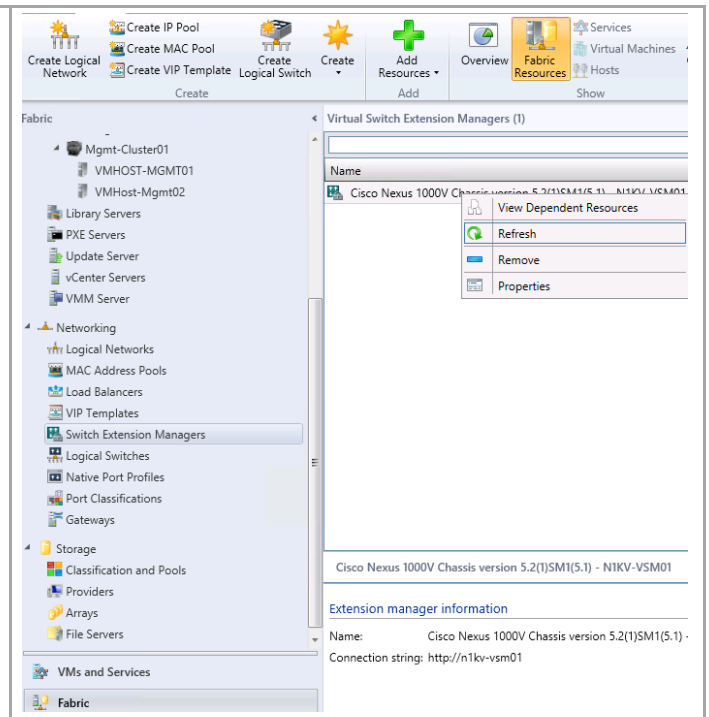
nsm network segment N1KV-AF-Public
member-of network segment pool App-Fabric
switchport access vlan 1007
ip pool import template N1KV-AF-Public-IP-Pool
publish network segment
exit

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

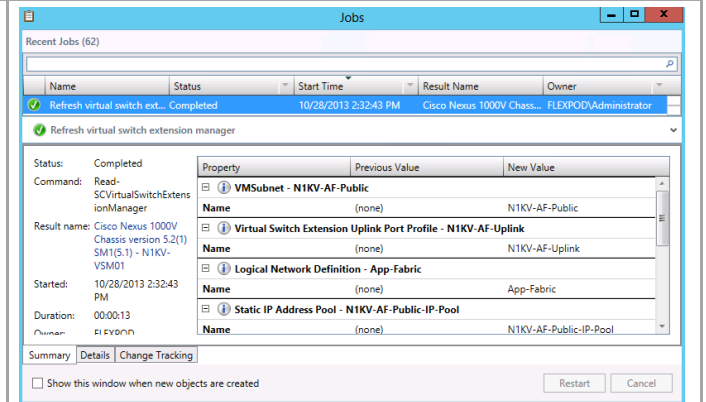
copy running-config startup-config
```

22.2 Configure a Logical Switch In Virtual Machine Manager

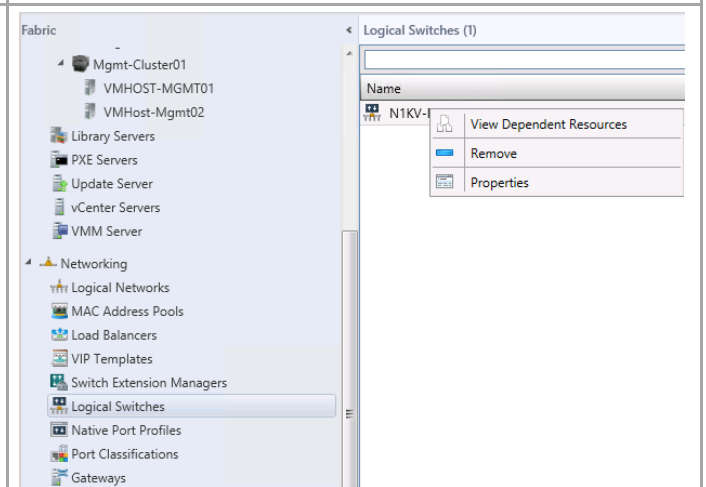
Open the Virtual Machine Manager Console. In the lower left pane select **Fabric** and select **Switch Extension Manager**. Select **Cisco Nexus 1000V** switch extension in the right pane and right click **Refresh**.



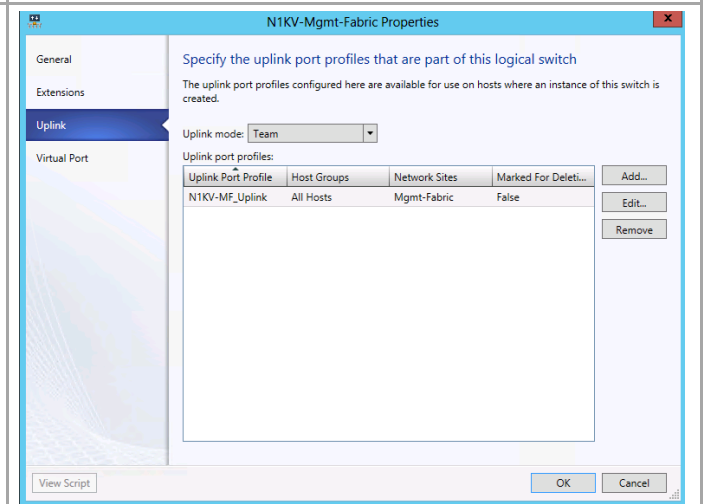
Click Jobs and verify the the refresh operation completed successfully.



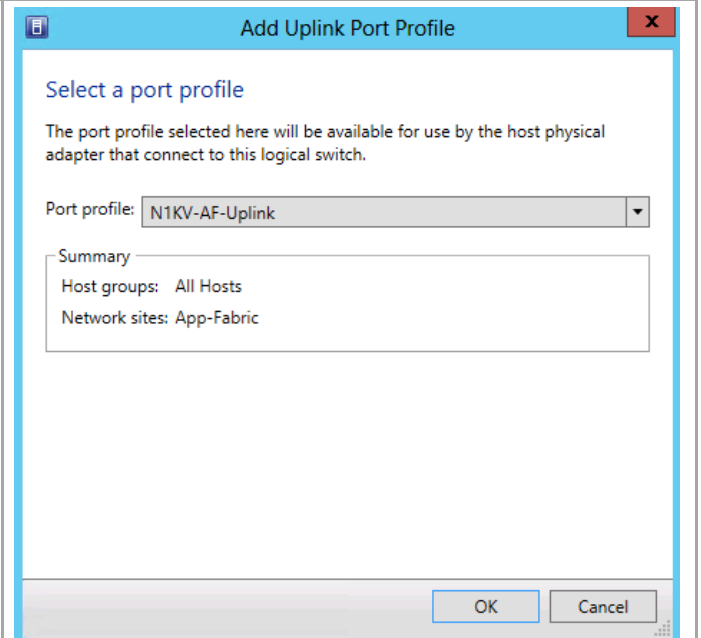
In the left pane of Virtual Machine Manager select **Fabric**. Expand **Networking** and select **Logical Switches**. Right click the previously created Nexus 1000V logical switch and click **Properties**.



Click **Uplink** in the left pane and click **Add**.



In the pull down menu, select **N1KV-AF-Uplink** port profile. Click **OK**.



Add Uplink Port Profile

Select a port profile

The port profile selected here will be available for use by the host physical adapter that connect to this logical switch.

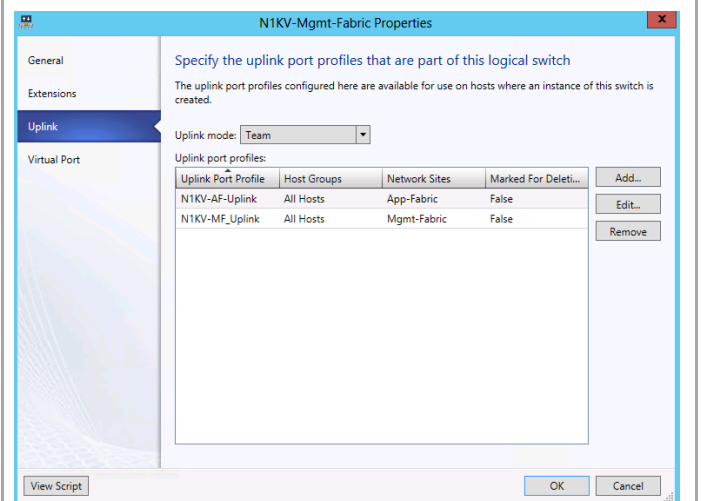
Port profile: **N1KV-AF-Uplink**

Summary

Host groups: All Hosts

Network sites: App-Fabric

OK Cancel



N1KV-Mgmt-Fabric Properties

General

Extensions

Uplink

Virtual Port

Specify the uplink port profiles that are part of this logical switch

The uplink port profiles configured here are available for use on hosts where an instance of this switch is created.

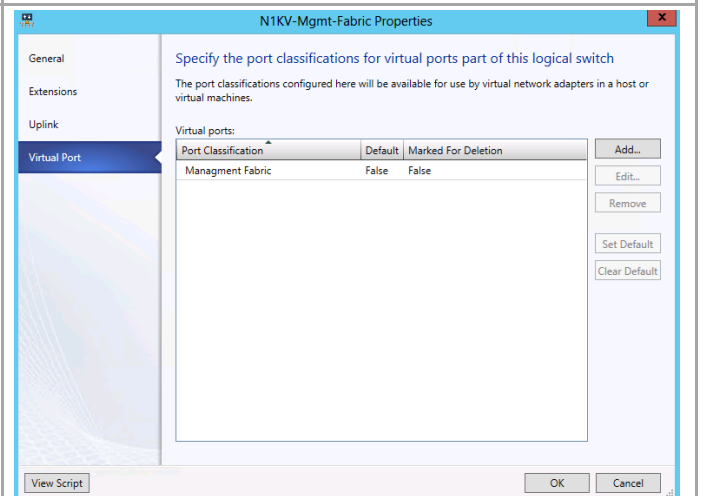
Uplink mode: **Team**

Uplink port profiles:

Uplink Port Profile	Host Groups	Network Sites	Marked For Deletion	
N1KV-AF-Uplink	All Hosts	App-Fabric	False	Add...
N1KV-MF-Uplink	All Hosts	Mgmt-Fabric	False	Edit...
				Remove

View Script OK Cancel

Click **Virtual Port** in the left pane and click **Add**.



N1KV-Mgmt-Fabric Properties

General

Extensions

Uplink

Virtual Port

Specify the port classifications for virtual ports part of this logical switch

The port classifications configured here will be available for use by virtual network adapters in a host or virtual machines.

Virtual ports:

Port Classification	Default	Marked For Deletion	
Management Fabric	False	False	Add...
			Edit...
			Remove
			Set Default
			Clear Default

View Script OK Cancel

Click **Browes** and **Create Port Classification**.

Add Virtual Port

Configure the virtual port

Specify the port classification for the virtual port. For each switch extension associated to the logical switch, one port profile may be selected. Additionally, a native virtual network adapter port profile may be associated to the virtual port.

Port classification:

Browse...

☐ N1KV-VSM01

Use this port profile:

☐ Include a virtual network adapter port profile in this virtual port

Native virtual network adapter port profile:

OK

Cancel

Select a Port Profile Classification

Select a Port Profile Classification

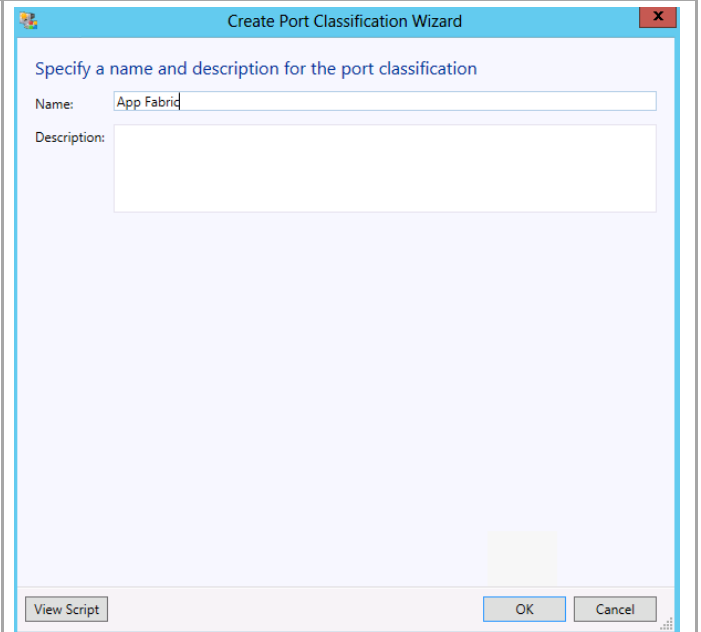
Name	Description
SR-IOV	Port classification to be used for virtual machines t...
Host management	Port classification to be used for host managemen...
Network load balancing	Port classification to be used for virtual machines t...
Live migration workload	Port classification to be used for host live migratio...
Medium bandwidth	Port classification to be used for virtual machines t...
Host Cluster Workload	Port classification for host cluster workloads.
Low bandwidth	Port classification to be used for virtual machines t...
High bandwidth	Port classification to be used for virtual machines t...
iSCSI workload	Port classification for host iSCSI workloads.

Create Port Classification...

OK

Cancel

Enter the **Port Classification Name** and click **OK**.



The 'Create Port Classification Wizard' dialog box is shown. It has a title bar with a close button. The main area is titled 'Specify a name and description for the port classification'. It contains a 'Name:' label with a text box containing 'App Fabric' and a 'Description:' label with a larger text box. At the bottom, there are three buttons: 'View Script', 'OK', and 'Cancel'.

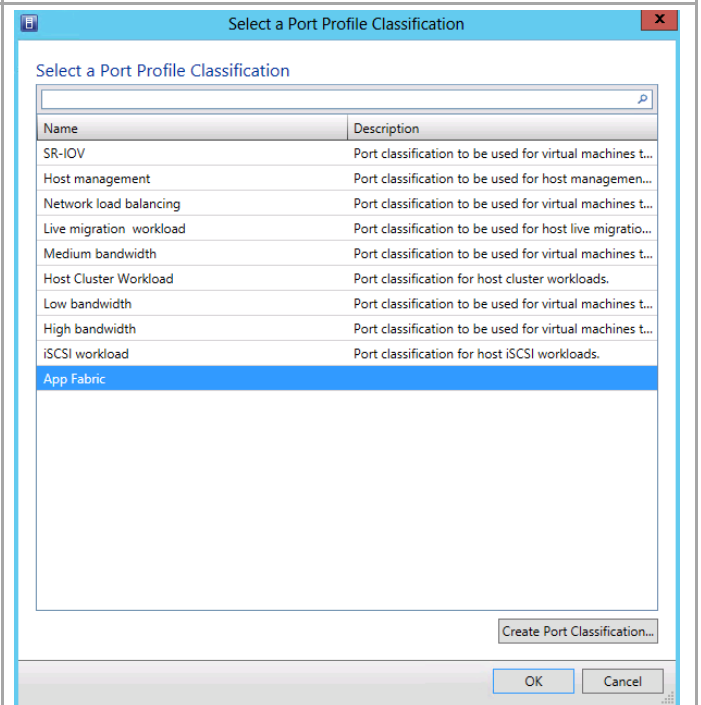
Specify a name and description for the port classification

Name: App Fabric

Description:

View Script OK Cancel

Select the Port Classification and click **OK**.



The 'Select a Port Profile Classification' dialog box is shown. It has a title bar with a close button. The main area is titled 'Select a Port Profile Classification'. It contains a search box at the top. Below it is a table with two columns: 'Name' and 'Description'. The table lists several port classifications, with 'App Fabric' highlighted in blue. At the bottom right, there is a 'Create Port Classification...' button. At the very bottom, there are 'OK' and 'Cancel' buttons.

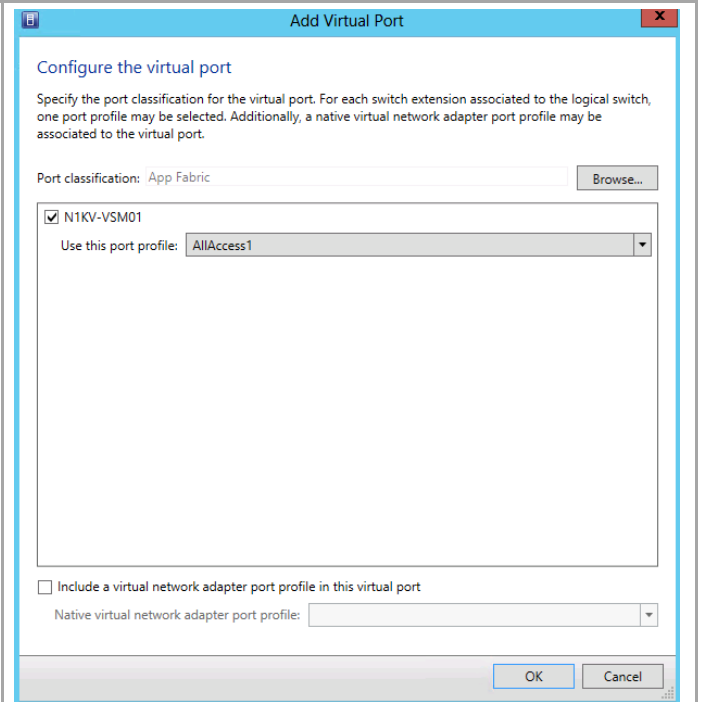
Select a Port Profile Classification

Name	Description
SR-IOV	Port classification to be used for virtual machines t...
Host management	Port classification to be used for host managemen...
Network load balancing	Port classification to be used for virtual machines t...
Live migration workload	Port classification to be used for host live migratio...
Medium bandwidth	Port classification to be used for virtual machines t...
Host Cluster Workload	Port classification for host cluster workloads.
Low bandwidth	Port classification to be used for virtual machines t...
High bandwidth	Port classification to be used for virtual machines t...
iSCSI workload	Port classification for host iSCSI workloads.
App Fabric	

Create Port Classification...

OK Cancel

Check box **N1KV-VSM01**. Select the **Port Profile** and click **OK**.



Add Virtual Port

Configure the virtual port

Specify the port classification for the virtual port. For each switch extension associated to the logical switch, one port profile may be selected. Additionally, a native virtual network adapter port profile may be associated to the virtual port.

Port classification: App Fabric Browse...

☒ N1KV-VSM01

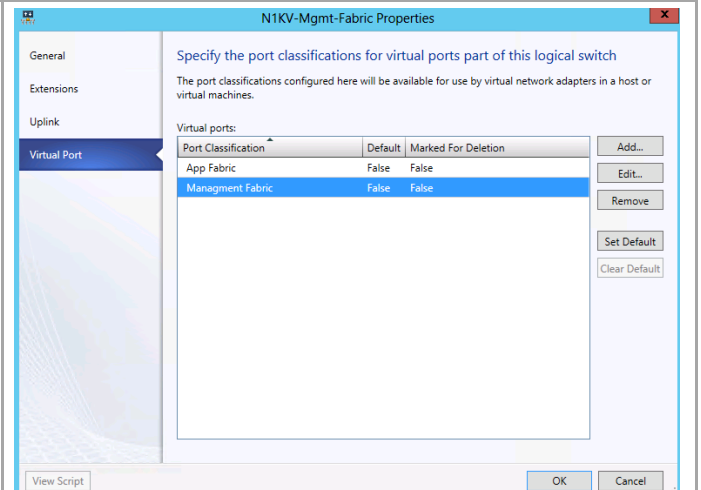
Use this port profile: AllAccess1

☐ Include a virtual network adapter port profile in this virtual port

Native virtual network adapter port profile:

OK Cancel

Click **OK** to update the logical switch properties.



N1KV-Mgmt-Fabric Properties

General

Extensions

Uplink

Virtual Port

Specify the port classifications for virtual ports part of this logical switch

The port classifications configured here will be available for use by virtual network adapters in a host or virtual machines.

Virtual ports:

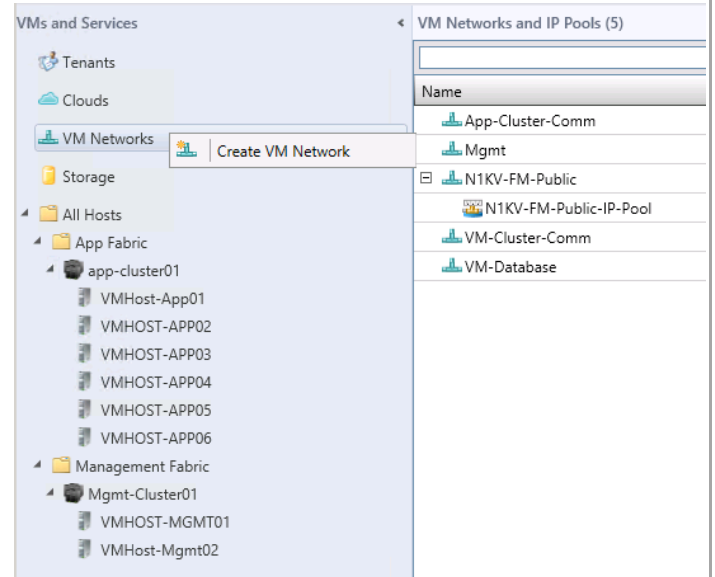
Port Classification	Default	Marked For Deletion
App Fabric	False	False
Management Fabric	False	False

Add... Edit... Remove Set Default Clear Default

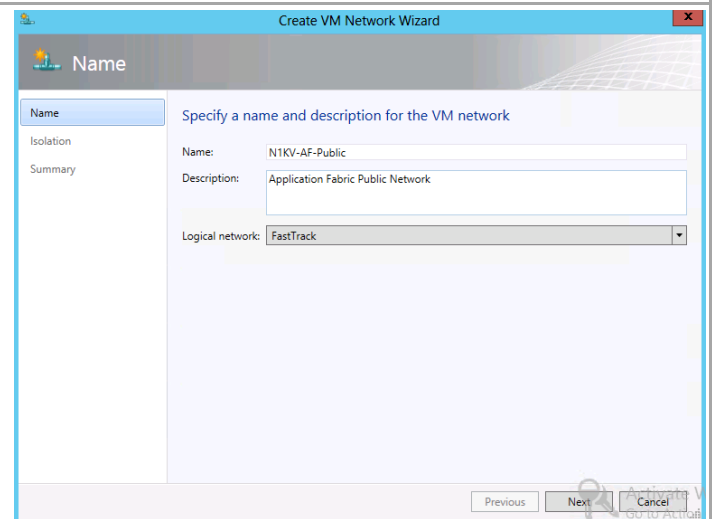
View Script OK Cancel

22.3 Create App Fabric VM Network

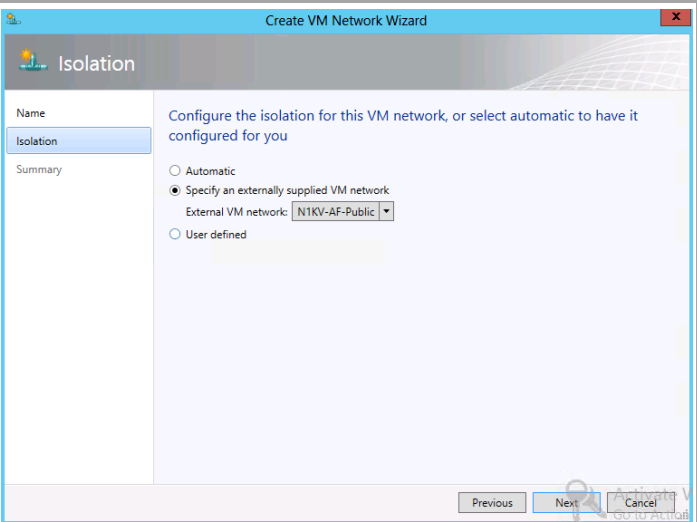
In Virtual Machine Manager, select **VMs and Services**. Right click **VM Networks** and click **Create VM Network**.



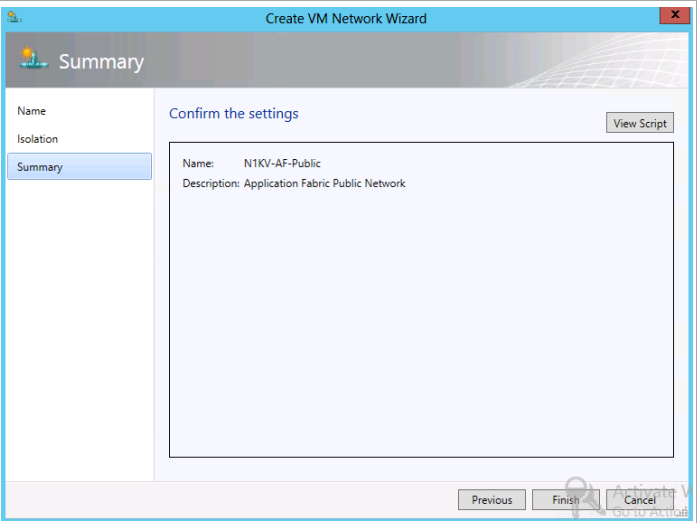
Enter the **network name**. Enter the description. Verify that the logical network FastTrack is selected and click **Next**.



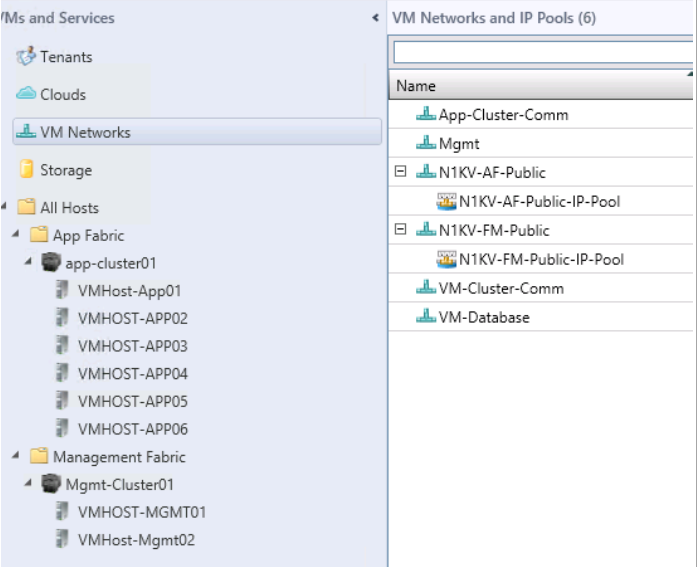
In the Isolation window, select **Specify an externally supplied VM Network** and select the External VM network **N1KV-AF-Public**. Click **Next**.



In the Summary window, click **Finish**.



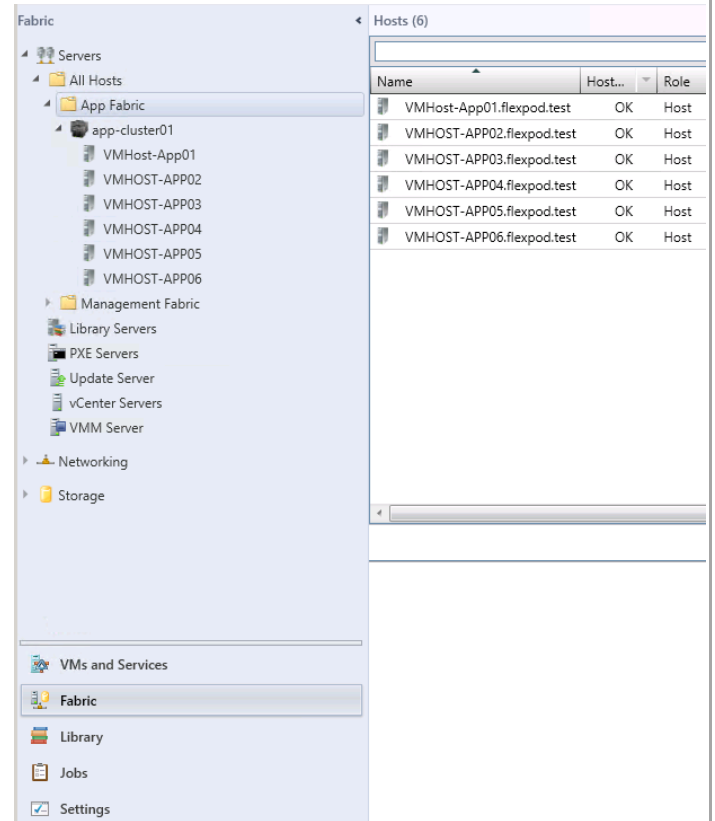
The VM Network is created.



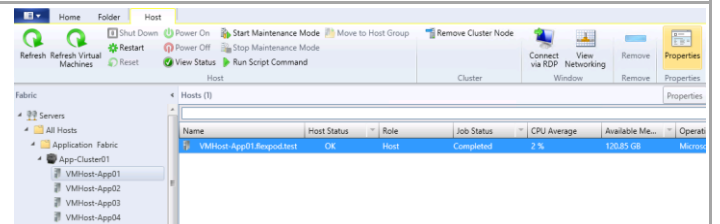
22.4 Creating the Logical Switch on the Hyper-V Hosts

Perform the following procedure on each App Fabric Cluster node.

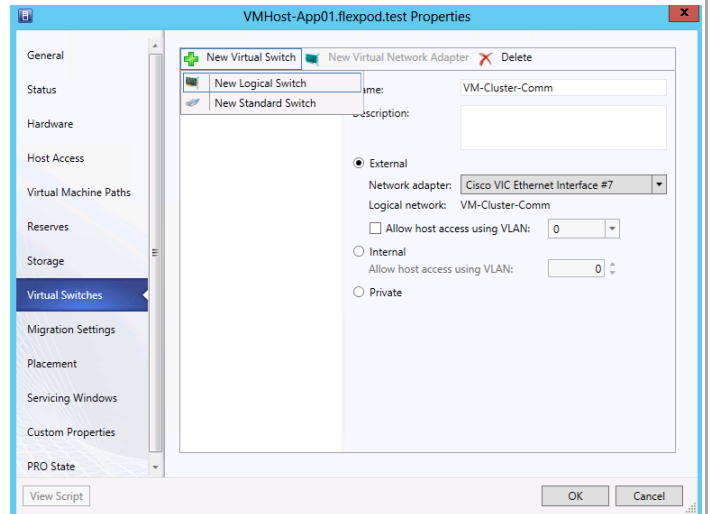
In the active Virtual Machine Manager instance, select **Fabric**. Expand **All Hosts** and **App Fabric**.



Select the first App Fabric host and click **Properties**.

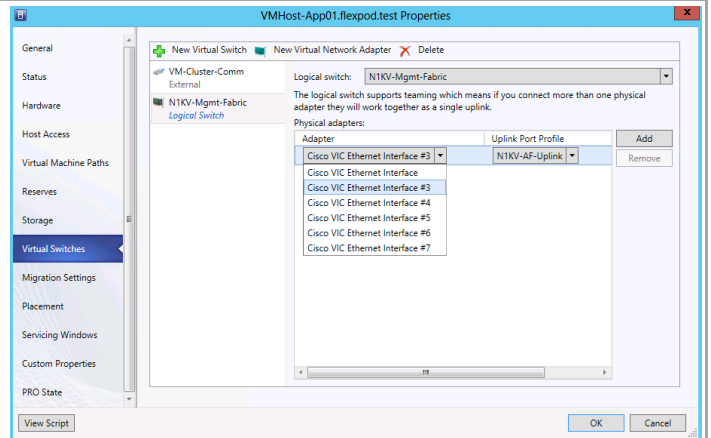


Select **Virtual Switch** in the left pane and **New Virtual Switch**. Select New Logical Switch.



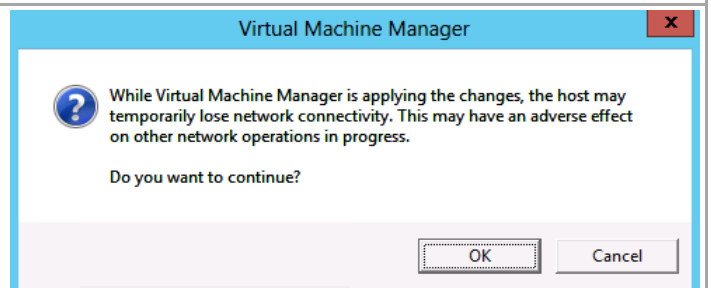
Select the new logical switch in the middle pane and in the right pane select the Ethernet adapter for the AF Public network. Click **OK**.

Note: Obtain the adapter number from the application host computer.



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.

Status:	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %																																			
Command:	Set-SCVMHost																																			
Result name:	VMHost-App02.flexpod.test																																			
Started:	5/28/2013 2:18:25 PM																																			
Duration:	00:00:03																																			
Owner:	FLEXP0D \Administrator																																			
<table><tr><th>Step</th><th>Name</th><th>Status</th><th>Start Time</th><th>End Time</th></tr><tr><td> 1</td><td>Change pr...</td><td><div><div></div><div></div><div></div><div></div><div></div></div> 99 %</td><td>5/28/2013...</td><td></td></tr><tr><td> 1.1</td><td>Change pr...</td><td>Completed</td><td>5/28/2013...</td><td>5/28/2013...</td></tr><tr><td> 1.2</td><td>New Host...</td><td><div><div></div><div></div><div></div><div></div><div></div></div> 99 %</td><td>5/28/2013...</td><td></td></tr><tr><td> 1.2.1</td><td>Install virt...</td><td><div><div></div><div></div><div></div><div></div><div></div></div> 99 %</td><td>5/28/2013...</td><td></td></tr><tr><td> 1.2.1.1</td><td>Deploy dri...</td><td><div><div></div><div></div><div></div><div></div><div></div></div> 99 %</td><td>5/28/2013...</td><td></td></tr><tr><td> 1.2.1.1.1</td><td>Deploy fil...</td><td>Completed</td><td>5/28/2013...</td><td>5/28/2013...</td></tr></table>		Step	Name	Status	Start Time	End Time	1	Change pr...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...		1.1	Change pr...	Completed	5/28/2013...	5/28/2013...	1.2	New Host...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...		1.2.1	Install virt...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...		1.2.1.1	Deploy dri...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...		1.2.1.1.1	Deploy fil...	Completed	5/28/2013...	5/28/2013...
Step	Name	Status	Start Time	End Time																																
1	Change pr...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...																																	
1.1	Change pr...	Completed	5/28/2013...	5/28/2013...																																
1.2	New Host...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...																																	
1.2.1	Install virt...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...																																	
1.2.1.1	Deploy dri...	<div><div></div><div></div><div></div><div></div><div></div></div> 99 %	5/28/2013...																																	
1.2.1.1.1	Deploy fil...	Completed	5/28/2013...	5/28/2013...																																

Step	Name	Status	Start Time	End Time
1	Change properties...	Completed	5/28/2013 2:21:59...	5/28/2013 2:23:16...
1.1	Change properties...	Completed	5/28/2013 2:21:59...	5/28/2013 2:21:59...
1.2	New Host instance...	Completed	5/28/2013 2:21:59...	5/28/2013 2:23:16...
1.2.1	Install virtual switch...	Completed	5/28/2013 2:22:00...	5/28/2013 2:22:48...
1.2.1.1	Deploy driver and i...	Completed	5/28/2013 2:22:00...	5/28/2013 2:22:48...
1.2.1.1.1	Deploy file (using L...	Completed	5/28/2013 2:22:00...	5/28/2013 2:22:06...
1.2.2	Install virtual switch...	Completed	5/28/2013 2:22:48...	5/28/2013 2:22:50...
1.2.3	Configure virtual s...	Completed	5/28/2013 2:23:10...	5/28/2013 2:23:10...

Open the App-Cluster01 properties and verify that the N1KV-Fabric Switch is in the list of switch installed on all cluster nodes.

app-cluster01.flexpod.test Properties

General

Status

Available Storage

File Share Storage

Shared Volumes

Virtual Switches

Migration Settings

PRO Configuration

PRO State

Custom Properties

Virtual Switches (2)

Name	Logical Networks
N1KV-Mgmt-Fabric	FastTrack
VM-Cluster-Comm	VM-Cluster-Comm

Create...

View Script

OK

Cancel

APPENDIX A: Installing Cisco UCS PowerTool

The Cisco UCS PowerTool should be installed on the FlexPod Management server.

Download the Cisco UCS PowerTool version 1.0.1.0 or newer from the Cisco. It can be found at the following link.
<http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.0.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

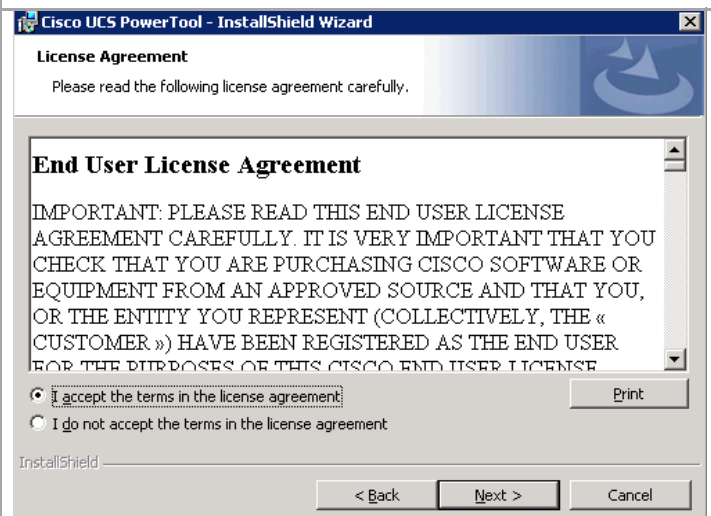
Extract the zip file and execute the extracted exe file.

Perform the following steps on the FlexPod management server.

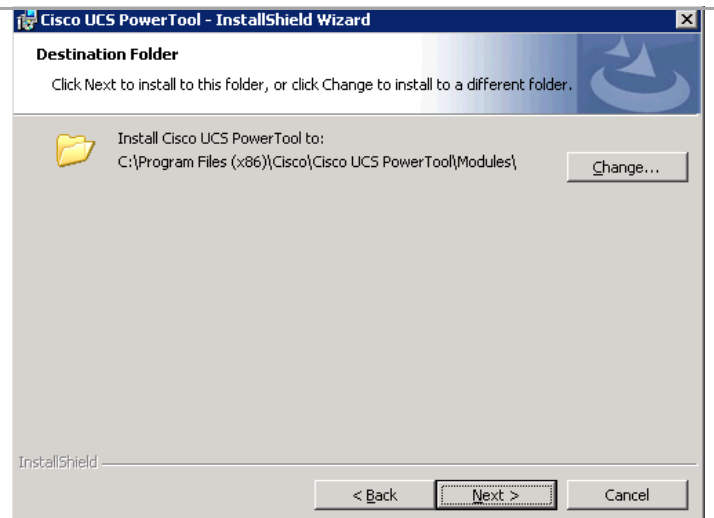
Launch the Cisco UCS PowerTool Installer. The **Setup Wizard** screen appears.



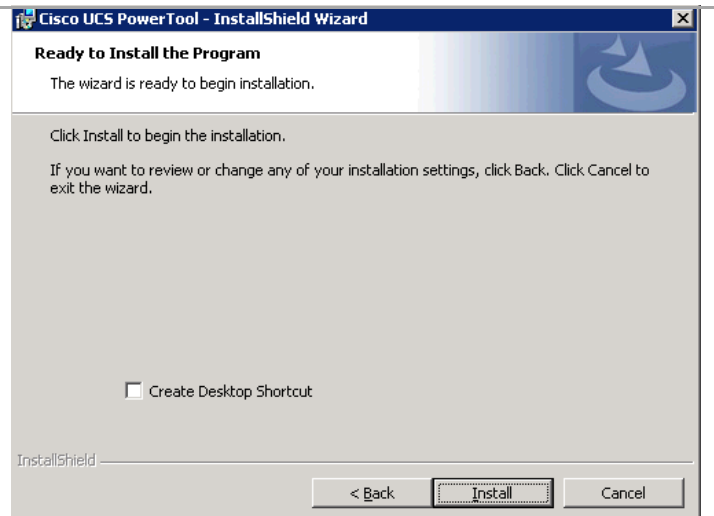
Read and accept the end user license agreement. Click **Next** to continue.



Select the **Destination Folder** and click **Next** to continue.



Cisco UCS PowerTool is ready to install. Click **Next** to complete the installation.



After the installation completes successfully click **Finish** to close the installation wizard.

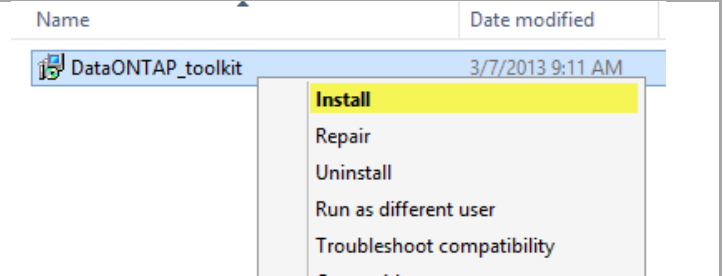
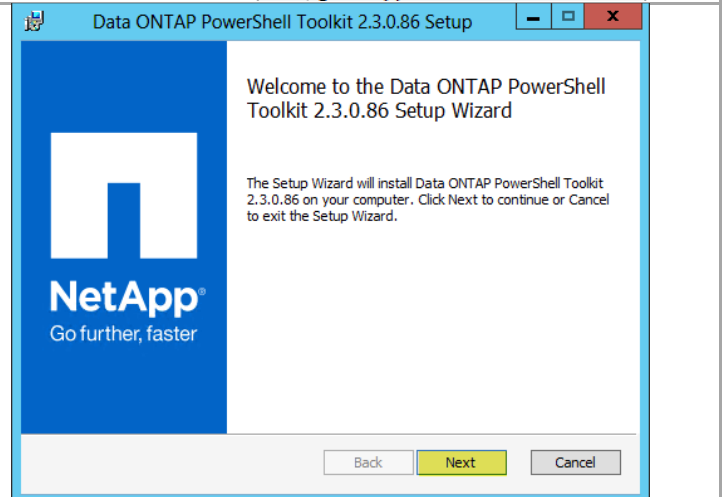
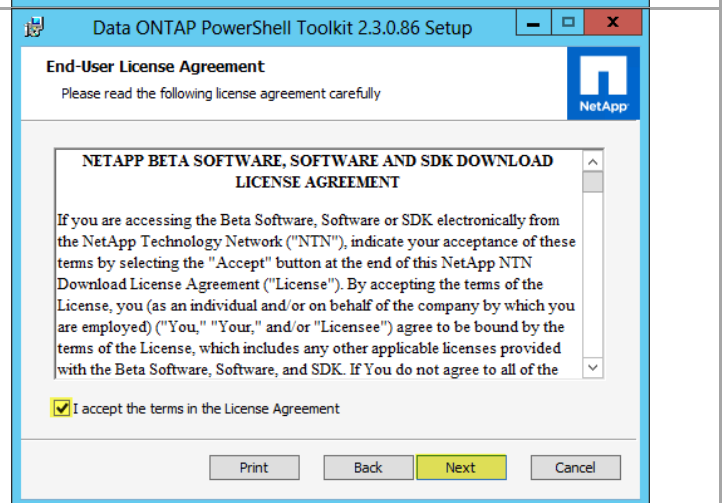


APPENDIX B: Installing the Data ONTAP PowerShell Toolkit.

The Data ONTAP PowerShell Toolkit should be installed on the FlexPod Management server.

Download the DataONTAP PowerShell toolkit from the NetApp Communities https://communities.netapp.com/community/products_and_solutions/microsoft/powershell

Perform the following steps on the FlexPod management server.

Run DataONTAP windows installation package.	
Click Next on the welcome page.	
Accept the ELUA and click Next .	

<p>Validate the Installation path and click Next.</p>	
<p>Click Install.</p>	
<p>Click Finish.</p>	