



FlexPod Validated with Microsoft Private Cloud Fast Track 2.0

Deployment Guide for FlexPod with Microsoft Windows Server 2008 R2 and Microsoft System Center 2012

Last Updated: August 7, 2012



Building Architectures to Solve Business Problems



About the Authors

Mike Mankovsky, Cisco Systems

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

Glenn Sizemore, NetApp

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

Alex Jauch, NetApp

Alex is an IT Architect with over 20 years of professional experience. Alex joined NetApp in January of 2010 as a Technical Architect within the Microsoft engineering team. He is currently responsible for the NetApp integration with System Center and Hyper-V based Private Cloud. Prior to NetApp, Alex worked for several Fortune 500 companies in a variety of Program Management, Consulting, and Architecture roles. This included 12 years at Microsoft where he was a Principal Consulting in MCS and Technical Director at the Microsoft Technology Center in Silicon Valley. Alex holds a BS in Information and Computer Science from the University of California at Irvine.

Mark Beaupre, NetApp

Mark is an experienced technology professional with over 15 years of experience who has architected and implemented solutions based on Microsoft technologies. Currently, Mark is a Microsoft Reference Architect working within the Microsoft engineering team at NetApp. Prior to his current role, Mark spent seven years in NetApp Professional Services as a Professional Services Consultant architecting and implementing Microsoft Exchange, SQL and SharePoint solutions on NetApp storage. Mark has a BS in Computer Information Systems from Arizona State University and a BS in Systems Engineering from the University of Arizona.

Adam Fazio, Microsoft

Adam Fazio is an Architect in the US Public Sector Services organization with a passion for evolving customers' IT infrastructure from a cost-center to a key strategic asset. With focus on the broad Core Infrastructure Optimization model, specialties include: Private Cloud, Datacenter, Virtualization, Management and Operations, Storage, Networking, Security, Directory Services, People & Process. In his 13 years in IT, Adam has successfully led strategic projects for Government, Education Sector, and Fortune 100 organizations. Adam is a lead architect for Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track program. Adam is a course instructor, published writer and regular conference speaker on Microsoft Private Cloud, virtualization and infrastructure solutions.

Joel Yorker, Microsoft

Joel Yorker is an Architect in the Americas Office of the Chief Technical Officer (OCTO) organization focusing on Private Cloud, Datacenter, Virtualization, Management & Operations, Storage, Networking, Security, Directory Services, Auditing and Compliance. In his 13 years at Microsoft, Joel has successfully led strategic projects for Government, Education Sector, and Fortune 100 organizations. Joel is a lead architect for Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track program and serves as course instructor, published writer and regular conference speaker on Microsoft Private Cloud, virtualization and infrastructure solutions.

David Ziembicki, Microsoft

David Ziembicki is a Senior Architect in Microsoft's Americas Office of the Chief Technical Officer organization focusing on cloud computing, virtualization, and datacenter architecture. David is a lead architect for Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track program as well as a published writer and regular conference speaker on cloud computing and virtualization.

Jeff Baker, Microsoft

Jeff Baker is an Architect in the Center of Excellence for Private Cloud at Microsoft Corporation. Jeff has worked with datacenter focused virtualization, management and operations technologies for almost a decade of his 13 plus years



in IT. Jeff has IT experience in a broad range of industries including Government, Education, Healthcare, Energy and Fortune 100 companies. Jeff has worked extensively with Microsoft's Datacenter Services Solution and the Microsoft Private Cloud Fast Track programs. Jeff is a regular conference speaker on Microsoft Private Cloud, virtualization and infrastructure solutions.

Introduction to Microsoft Private Cloud Fast Track

As the name details, the Fast Track architecture is a highly modular or “pod” like. When fully assembled this pod represents all the required components to successfully implement a Microsoft Private Cloud. While each customer's Fast Track might vary in its exact configuration, when a Fast Track is built, it can easily be scaled as requirements and demand change. This includes vertical scaling (adding additional resources within a Fast Track unit) as well as horizontal scaling (adding additional Fast Track scaling units).

Specifically, Fast Track is a defined set of hardware and software that serves as an integrated building block for all virtualization solutions. Microsoft Private Cloud Fast Track includes NetApp® storage, Cisco® networking, the Cisco Unified Computing System™ (Cisco UCS), and Microsoft software in a single package.

The default compute and network hardware includes two Cisco UCS 6248UP fabric interconnects, and one chassis of Cisco UCS blades with two fabric extenders per chassis, 4 B200 blades servers and two Cisco Nexus® 5548UP switches. Storage is provided by a NetApp FAS3240A (HA-configuration) with accompanying disk shelves. All systems and fabric links feature redundancy, providing for end-to-end high availability. For server virtualization, the deployment includes Hyper-V, System Center 2012, OnCommand Plug-in for Microsoft, and Cisco Power Tools. While this is the default base design, each of the components can be scaled flexibly to support the specific business requirements in question. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves could be deployed to improve I/O capacity and throughput, or special hardware or software features could be added to introduce new features (such as NetApp Flash Cache for dedupe-aware caching or Hyper-V virtual machines).

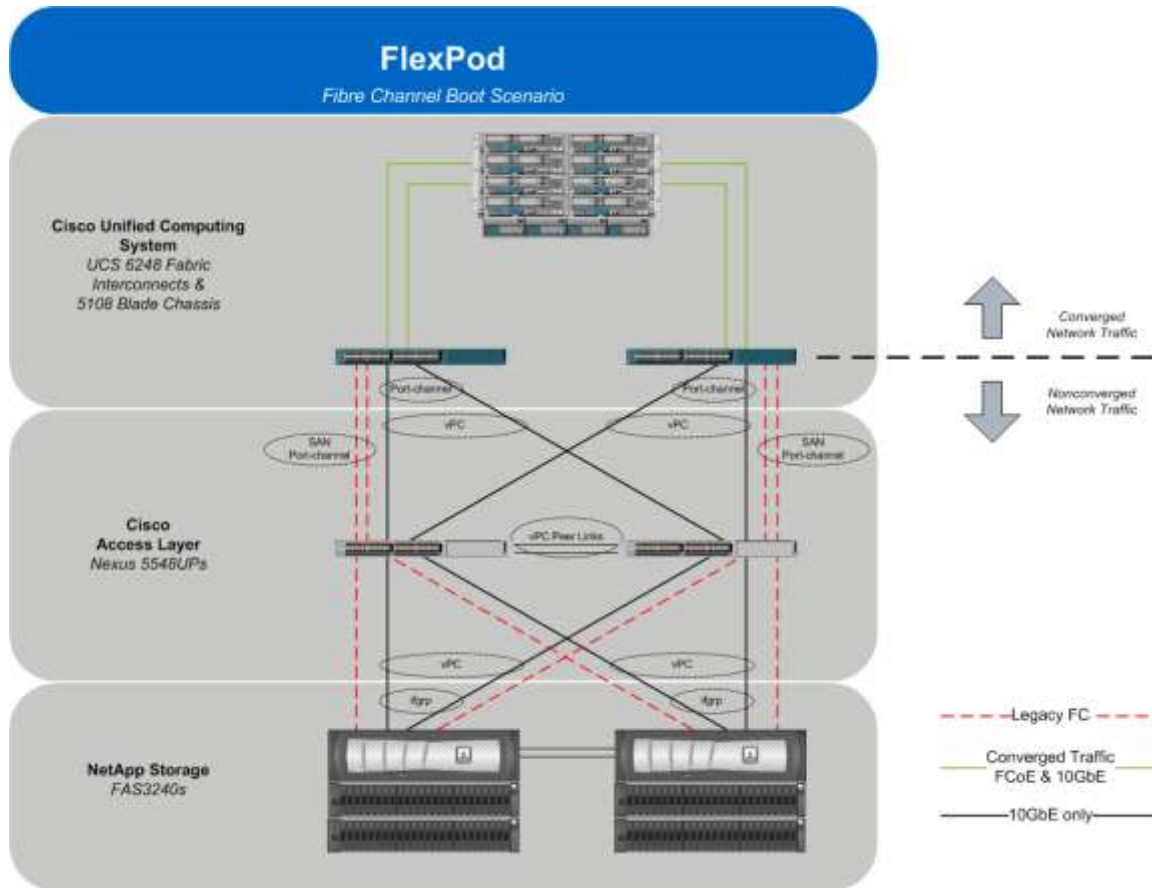
Reference Architecture

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 validated with Microsoft Private Cloud includes NetApp® FAS3200 series 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 (graphic provided by Cisco).



The reference configuration shown in Figure 1 includes:

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 6248 fabric interconnects
- One chassis of Cisco UCS blades with two fabric extenders per chassis
- One FAS3240A (HA pair)

Storage is provided by a NetApp FAS3240A (HA configuration within a single chassis) 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 the hardware series (that is, FAS3200 series) 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 Private Cloud 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.



The FlexPod with Microsoft Private Cloud Fast Track 2.0 Architecture is documented at the following link: ([FlexPod with Microsoft Private Cloud - Architecture Overview](#))

LAN and SAN Network Deployment

Nexus 5548UP Deployment Procedure: Part 1

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

Note: The configuration steps detailed in this section provides guidance for configuring the Nexus 5548UP running release 5.0(3)N2(2a).

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.

Initial Cisco Nexus 5548UP Switch Configuration

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

Cisco Nexus 5548 A

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

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



20. Enter basic FC configurations (yes/no) [n]: Enter.
21. Would you like to edit the configuration? (yes/no) [n]: Enter.
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.

Cisco Nexus 5548 B

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

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



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`.
6. Type `feature fport-channel-trunk`.

Set Global Configurations

These steps provide details for setting global configurations.

Nexus A and Nexus B

1. From the global configuration mode, type `spanning-tree port type network default` to make sure that, by default, the ports are considered as network ports in regards to spanning-tree.
2. Type `spanning-tree port type edge bpduguard default` to enable bpduguard on all edge ports by default.
3. Type `spanning-tree port type edge bpdufilter default` to enable bpdufilter on all edge ports by default.
4. Type `ip access-list classify_Silver`.
5. Type `10 permit ip <iSCSI-A net address> any`. where the variable is the network address of the iSCSI-A VLAN in CIDR notation (i.e. 192.168.102.0/24).
6. Type `20 permit ip any <iSCSI-A net address>`.
7. Type `30 permit ip <iSCSI-B net address> any`.
8. Type `40 permit ip any <iSCSI-B net address>`.
9. Type `exit`.
10. Type `class-map type qos match-all class-gold`.
11. Type `match cos 4`.
12. Type `exit`.
13. Type `class-map type qos match-all class-silver`.
14. Type `match cos 2`.
15. Type `match access-group name classify_Silver`.
16. Type `exit`.
17. Type `class-map type queuing class-gold`.
18. Type `match qos-group 3`.
19. Type `exit`.
20. Type `class-map type queuing class-silver`.
21. Type `match qos-group 4`.



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



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

Configure FC Ports

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

Nexus A and Nexus B

1. Type `slot 1`.
2. Type `port 29-32 type fc`.

Note: If you are using FCoE between the Nexus 5548 and storage, change this to: Type `port 31-32 type fc`.

3. Type `copy run start`.
4. Type `reload`.

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

Create Necessary VLANs

These steps provide details for creating the necessary VLANs.

Nexus A and Nexus B

Following switch reload, Log in as user `admin` with the password previously entered.

1. Type `config-t`.



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

Add Individual Port Descriptions for Troubleshooting

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

Cisco Nexus 5548 A

1. From the global configuration mode, type `interface Eth1/1`.
2. Type `description <Controller A:e2a>`.
3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description <Controller B:e2a>`.
6. Type `exit`.
7. Type `interface Eth1/5`.
8. Type `description <Nexus B:Eth1/5>`.
9. Type `exit`.



10. Type interface Eth1/6.
11. Type description `<Nexus B:Eth1/6>`.
12. Type exit.
13. Type interface Eth1/3.
14. Type description `<UCSM A:Eth1/19>`.
15. Type exit.
16. Type interface Eth1/4.
17. Type description `<UCSM B:Eth1/19>`.
18. Type exit.

Cisco Nexus 5548 B

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

Create Necessary Port Channels

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

Cisco Nexus 5548 A

1. From the global configuration mode, type interface Po10.
2. Type description vPC peer-link.
3. Type exit.
4. Type interface Eth1/5-6.
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 Eth1/3.
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 Eth1/4.
33. Type channel-group 14 mode active.
34. Type no shutdown.
35. Type exit.
36. Type copy run start.

Cisco Nexus 5548 B

1. From the global configuration mode, type interface Po10.
2. Type description vPC peer-link.
3. Type exit.
4. Type interface Eth1/5-6.
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 Eth1/3`.
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 Eth1/4`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `copy run start`.

Add Port Channel Configurations

These steps provide details for adding Port Channel configurations.

Cisco Nexus 5548 A

1. From the global configuration mode, type `interface Po10`.
2. Type `switchport mode trunk`.



3. **Type** switchport trunk native vlan <Native VLAN ID>.
4. **Type** switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data 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 <MGMT VLAN ID>.
11. **Type** switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID>.
12. **Type** spanning-tree port type edge trunk.
13. **Type** no shut.
14. **Type** exit.
15. **Type** interface Po12.
16. **Type** switchport mode trunk.
17. **Type** switchport trunk native vlan <MGMT VLAN ID>.
18. **Type** switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID >.
19. **Type** spanning-tree port type edge trunk.
20. **Type** no shut.
21. **Type** exit.
22. **Type** interface Po13.
23. **Type** switchport mode trunk.
24. **Type** switchport trunk native vlan <Native VLAN ID>.
25. **Type** switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
26. **Type** spanning-tree port type edge trunk.
27. **Type** no shut.
28. **Type** exit.
29. **Type** interface Po14.
30. **Type** switchport mode trunk.
31. **Type** switchport trunk native vlan <Native VLAN ID>.
32. **Type** switchport trunk allowed vlan <<MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
33. **Type** spanning-tree port type edge trunk.
34. **Type** no shut.



35. Type `exit`.
36. Type `copy run start`.

Cisco Nexus 5548 B

1. From the global configuration mode, type `interface Po10`.
2. Type `switchport mode trunk`.
3. Type `switchport trunk native vlan <Native VLAN ID>`.
4. Type `switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A, iSCSI B VLAN ID, VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data 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 <MGMT VLAN ID>`.
11. Type `switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID>`.
12. Type `spanning-tree port type edge trunk`.
13. Type `no shut`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `switchport mode trunk`.
17. Type `switchport trunk native vlan <MGMT VLAN ID>`.
18. Type `switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID>`.
19. Type `spanning-tree port type edge trunk`.
20. Type `no shut`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `switchport mode trunk`.
24. Type `switchport trunk native vlan <Native VLAN ID>`.
25. Type `switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>`.
26. Type `spanning-tree port type edge trunk`.
27. Type `no shut`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `switchport mode trunk`.



31. Type `switchport trunk native vlan <Native VLAN ID>`.
32. Type `switchport trunk allowed vlan <<MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>`.
33. Type `spanning-tree port type edge trunk`.
34. Type `no shut`.
35. Type `exit`.
36. Type `copy run start`.

Configure Virtual Port Channels

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

Cisco Nexus 5548 A

1. From the global configuration mode, type `vpc domain <Nexus vPC domain ID>`.
2. Type `role priority 10`.
3. Type `peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0 IP>`.
4. Type `exit`.
5. Type `interface Po10`.
6. Type `vpc peer-link`.
7. Type `exit`.
8. Type `interface 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`.

Cisco Nexus 5548 B

1. From the global configuration mode, type `vpc domain <Nexus vPC domain ID>`.
2. Type `role priority 20`.
3. Type `peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0 IP>`.



4. Type `exit`.
5. Type `interface Po10`.
6. Type `vpc peer-link`.
7. Type `exit`.
8. Type `interface 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`

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.

Save the Configuration

Nexus A and Nexus B

Type `copy run start`.

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.

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.

Add a Block of IP Addresses for KVM Access

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



Cisco UCS Manager

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

Synchronize Cisco UCS to NTP

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

Cisco UCS Manager

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 `Save Changes` and then `OK`.
6. Click `Add NTP Server`.
7. Input the NTP server IP and click `OK`.

Configure Unified Ports

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

Note: Modification of the unified ports leads to a reboot of the fabric interconnect in question. This reboot can take up to 10 minutes.

Cisco UCS Manager

1. Navigate to the `Equipment` tab in the left pane.
2. Select `Fabric Interconnect A`.
3. In the right pane, click the `General` tab.
4. Select `Configure Unified Ports`.
5. Select `Yes` to launch the wizard.
6. Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports.
7. Ports 31 and 32 now have the “B” indicator indicating their reconfiguration as FC uplink ports.
8. Click `Finish`.
9. Click `OK`.
10. The Cisco UCS Manager GUI will close as the primary fabric interconnect reboots.



11. Upon successful reboot, open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.
12. When prompted, enter `admin` for the username and enter the administrative password and click `Login` to log in to the Cisco UCS Manager software.
13. Navigate to the `Equipment` tab in the left pane.
14. Select `Fabric Interconnect B`.
15. In the right pane, click the `General` tab.
16. Select `Configure Unified Ports`.
17. Select `Yes` to launch the wizard.
18. Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports.
19. Ports 31 and 32 now have the “B” indicator indicating their reconfiguration as FC uplink ports.
20. Click `Finish`.
21. Click `OK`.

Edit the Chassis Discovery Policy

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

Cisco UCS Manager

1. Navigate to the `Equipment` tab in the left pane.
2. In the right pane, click the `Policies` tab.
3. Under `Global Policies`, change the `Chassis Discovery Policy` to 2-link.
4. Click `Save Changes` in the bottom right corner.

Enable Server and Uplink Ports

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

Cisco UCS Manager

1. Select the `Equipment` tab on the top left of the window.
2. Select `Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module`.
3. Expand the `Unconfigured Ethernet Ports` section.
4. Select the number of ports that are connected to the Cisco UCS chassis (2 per chassis), right-click them, and select `Configure as Server Port`.



Unconfigured Ethernet Ports

Slot	Port ID	MAC	IF Role	IF Type	Overall Status	Administrative State
1	1	54:7F:EE:3C:04:68	Unconfigured	Physical	Admin Down	Disabled
1	2	54:7F:EE:3C:04:69	Unconfigured	Physical	Admin Down	Disabled
1	3	54:7F:EE:3C:04:6A	Unconfigured	Physical	Admin Down	Disabled
1	4	54:7F:EE:3C:04:6B	Unconfigured	Physical	Admin Down	Disabled
1	5	54:7F:EE:3C:04:6C	Unconfigured	Physical	Admin Down	Disabled
1	6	54:7F:EE:3C:04:6D	Unconfigured	Physical	Admin Down	Disabled
1	7	54:7F:EE:3C:04:6E	Unconfigured	Physical	Admin Down	Disabled
1	8	54:7F:EE:3C:04:6F	Unconfigured	Physical	Admin Down	Disabled
1	9	54:7F:EE:3C:04:70	Unconfigured	Physical	Admin Down	Disabled
1	10	54:7F:EE:3C:04:71	Unconfigured	Physical	Admin Down	Disabled
1	11	54:7F:EE:3C:04:72	Unconfigured	Physical	Admin Down	Disabled
1	12	54:7F:EE:3C:04:73	Unconfigured	Physical	Admin Down	Disabled
1	13	54:7F:EE:3C:04:74	Unconfigured	Physical	Admin Down	Disabled
1	14	54:7F:EE:3C:04:75	Unconfigured	Physical	Admin Down	Disabled
1	15	54:7F:EE:3C:04:76	Unconfigured	Physical	Admin Down	Disabled
1	16	54:7F:EE:3C:04:77	Unconfigured	Physical	Admin Down	Disabled
1	17	54:7F:EE:3C:04:78	Unconfigured	Physical	Admin Down	Disabled
1	18	54:7F:EE:3C:04:79	Unconfigured	Physical	Admin Down	Disabled
1	19	54:7F:EE:3C:04:7A	Unconfigured	Physical	Admin Down	Disabled
1	20	54:7F:EE:3C:04:7B	Unconfigured	Physical	Admin Down	Disabled
1	21	54:7F:EE:3C:04:7C	Unconfigured	Physical	Admin Down	Disabled
1	22	54:7F:EE:3C:04:7D	Unconfigured	Physical	Admin Down	Disabled
1	23	54:7F:EE:3C:04:7E	Unconfigured	Physical	Admin Down	Disabled
1	24	54:7F:EE:3C:04:7F	Unconfigured	Physical	Admin Down	Disabled
1	25	54:7F:EE:3C:04:80	Unconfigured	Physical	Admin Down	Disabled
1	26	54:7F:EE:3C:04:81	Unconfigured	Physical	Admin Down	Disabled
1	27	54:7F:EE:3C:04:82	Unconfigured	Physical	Admin Down	Disabled
1	28	54:7F:EE:3C:04:83	Unconfigured	Physical	Admin Down	Disabled
1	29	54:7F:EE:3C:04:84	Unconfigured	Physical	Admin Down	Disabled

5. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue.

Server Ports

Slot	Port ID	MAC	IF Role	IF Type	Overall Status	Administrative State	License State	License Grace Period
1	1	54:7F:EE:1...	Server	Physical	Up	Enabled	License Ok	0
1	2	54:7F:EE:1...	Server	Physical	Up	Enabled	License Ok	0
1	3	54:7F:EE:1...	Server	Physical	Up	Enabled	License Ok	0
1	4	54:7F:EE:1...	Server	Physical	Up	Enabled	License Ok	0



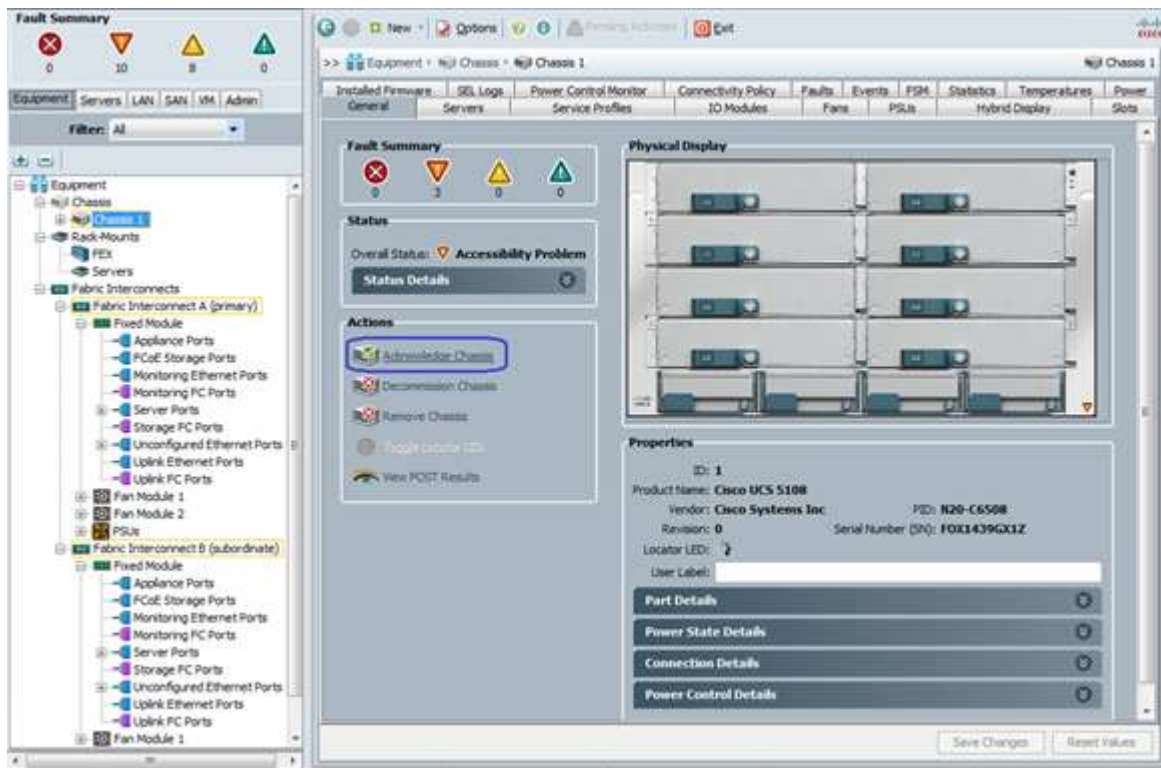
6. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select **Configure as Uplink Port**.
7. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue.
8. Select **Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module**.
9. Expand the **Unconfigured Ethernet Ports** section.
10. Select ports the number of ports that are connected to the Cisco UCS chassis (2 per chassis), right-click them, and select **Configure as Server Port**.
11. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue.
12. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select **Configure as Uplink Port**.
13. A prompt displays asking if this is what you want to do. Click **Yes**, then **OK** to continue.

Acknowledge the Cisco UCS Chassis

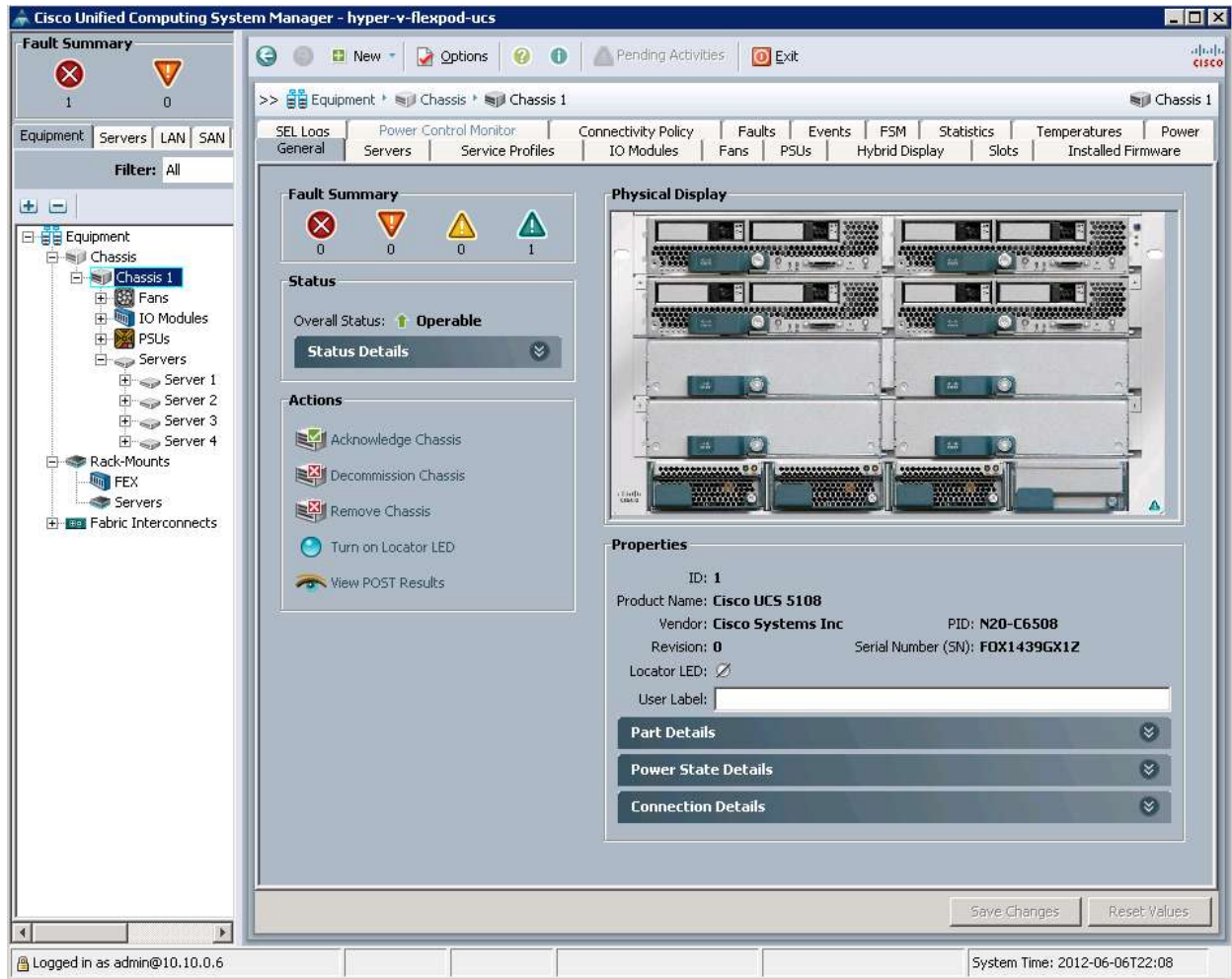
The connected chassis needs to be acknowledged before it can be managed by Cisco UCS Manager.

Cisco UCS Manager

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



Cisco UCS Manager acknowledges the chassis and the blades servers in it.



Create Uplink Port Channels to the Cisco Nexus 5548 Switches

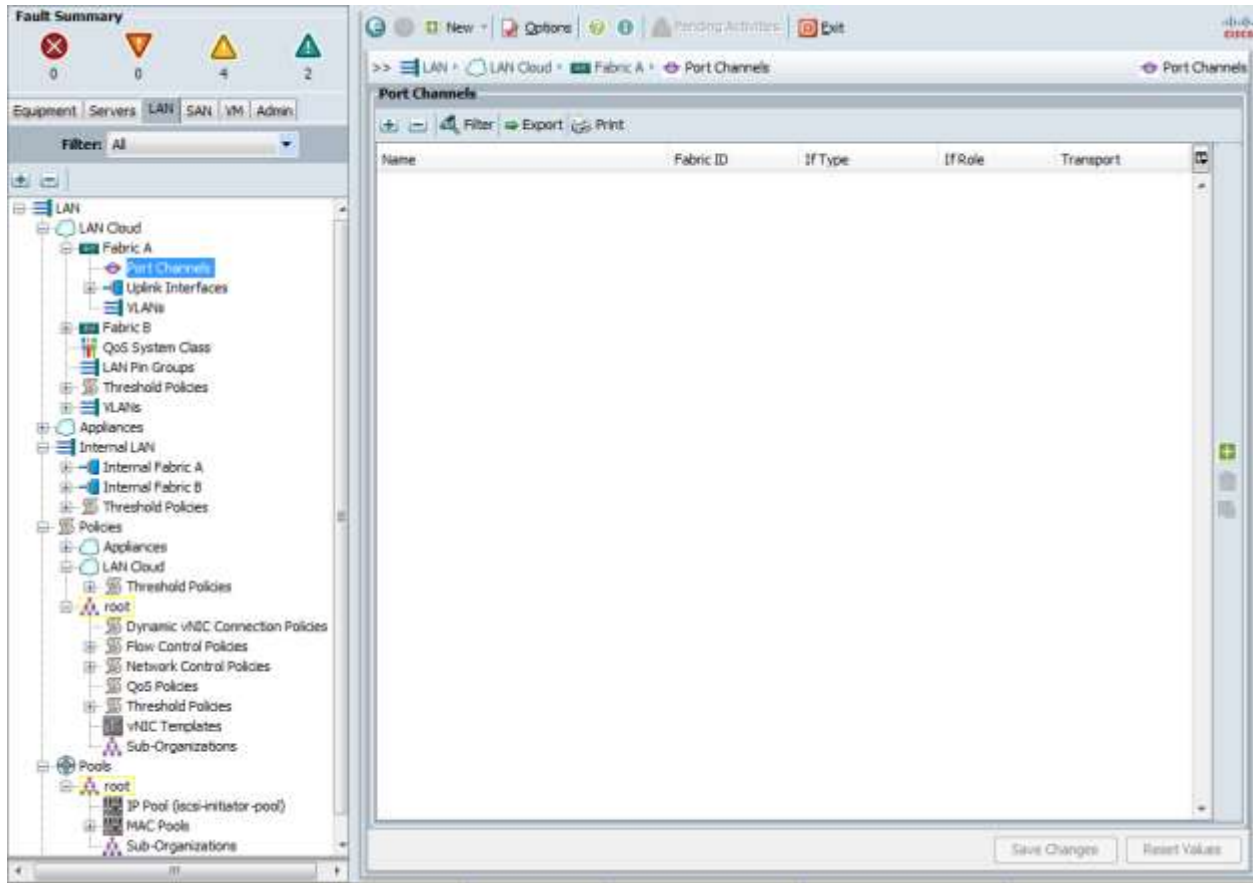
These steps provide details for configuring the necessary Port Channels out of the Cisco UCS environment.

Cisco UCS Manager

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.



Create Port Channel

Unified Computing System Manager

Create Port Channel

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

ID: 13

Name: vPC-13-H5548

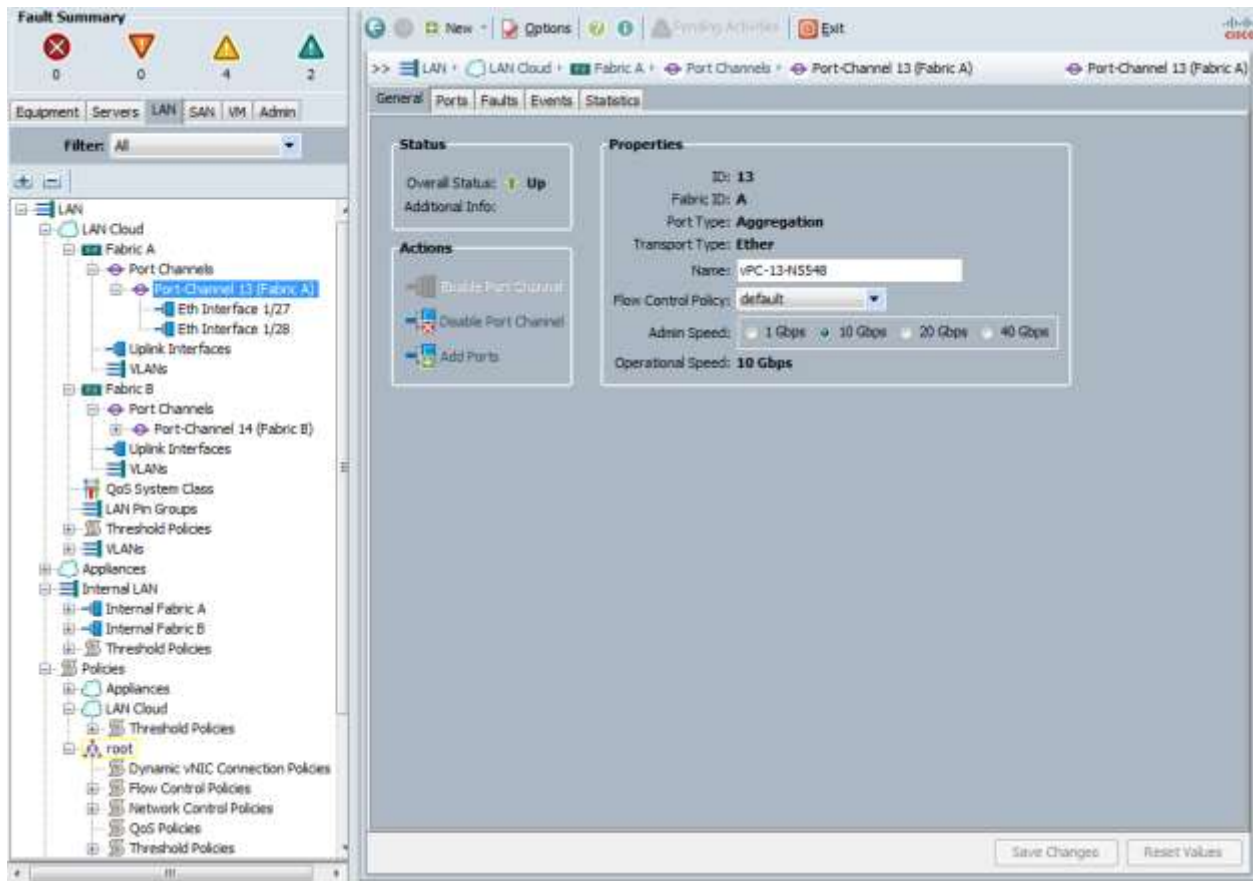
< Prev Next > Finish Cancel

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



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

16. Click OK to close the Navigator.



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



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.

Cisco UCS Manager

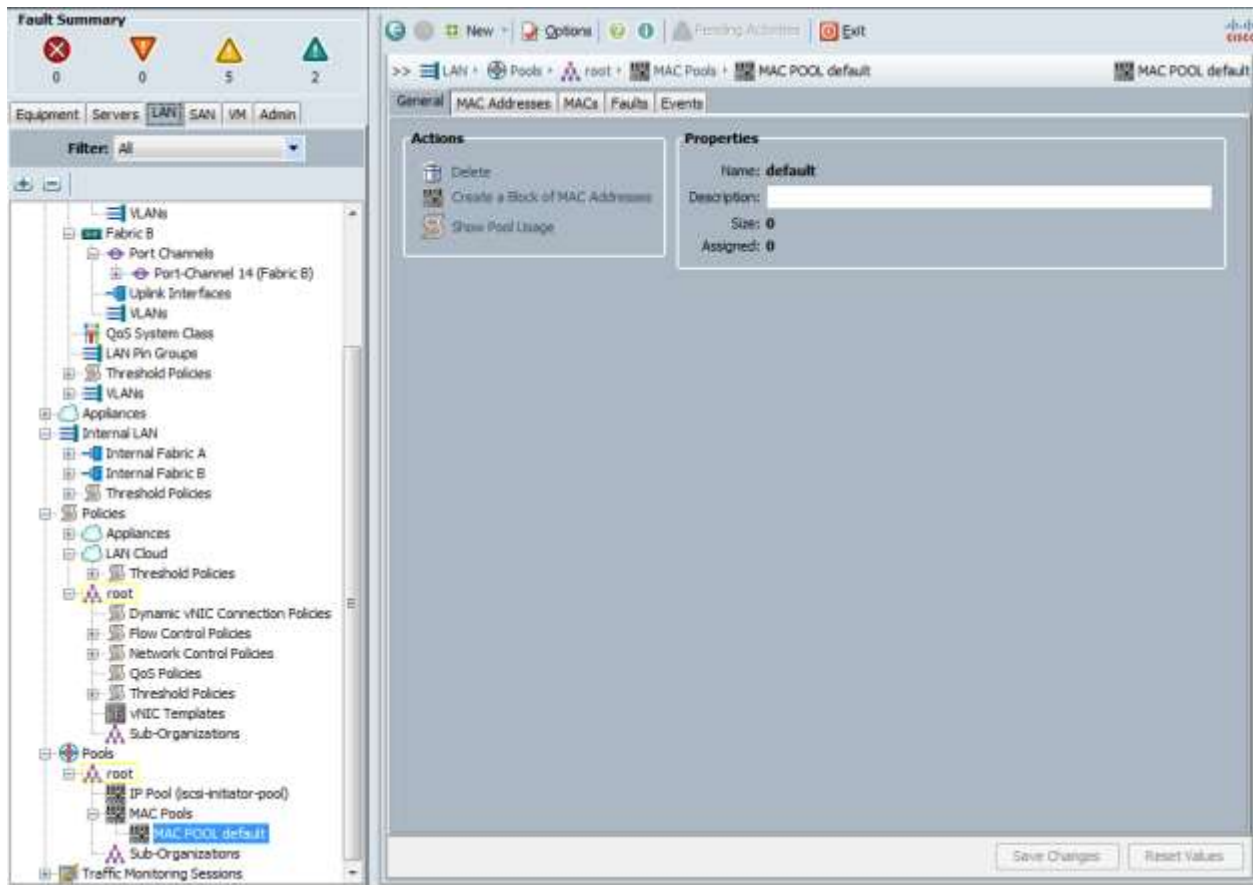
1. From the `New...` menu at the top of the window, select `Create Organization`.
2. Enter a name for the organization.
3. Enter a description for the organization (optional).
4. Click `OK`.
5. In the message box that displays, click `OK`.

Create a MAC Address Pool

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

Cisco UCS Manager

1. Select the `LAN` tab on the left of the window.
 2. Select `Pools > root`.
- Note:** One MAC address pool is created.
3. Right-click `MAC Pools` under the root organization.
 4. Select `Create MAC Pool` to create the MAC address pool.



5. Enter `MAC_Pool` for the name of the MAC pool.
6. (Optional) Enter a description of the MAC pool.
7. Click `Next`.
8. Click `Add`.
9. Specify a starting MAC address.
10. Specify a size of the MAC address pool sufficient to support the available blade resources.





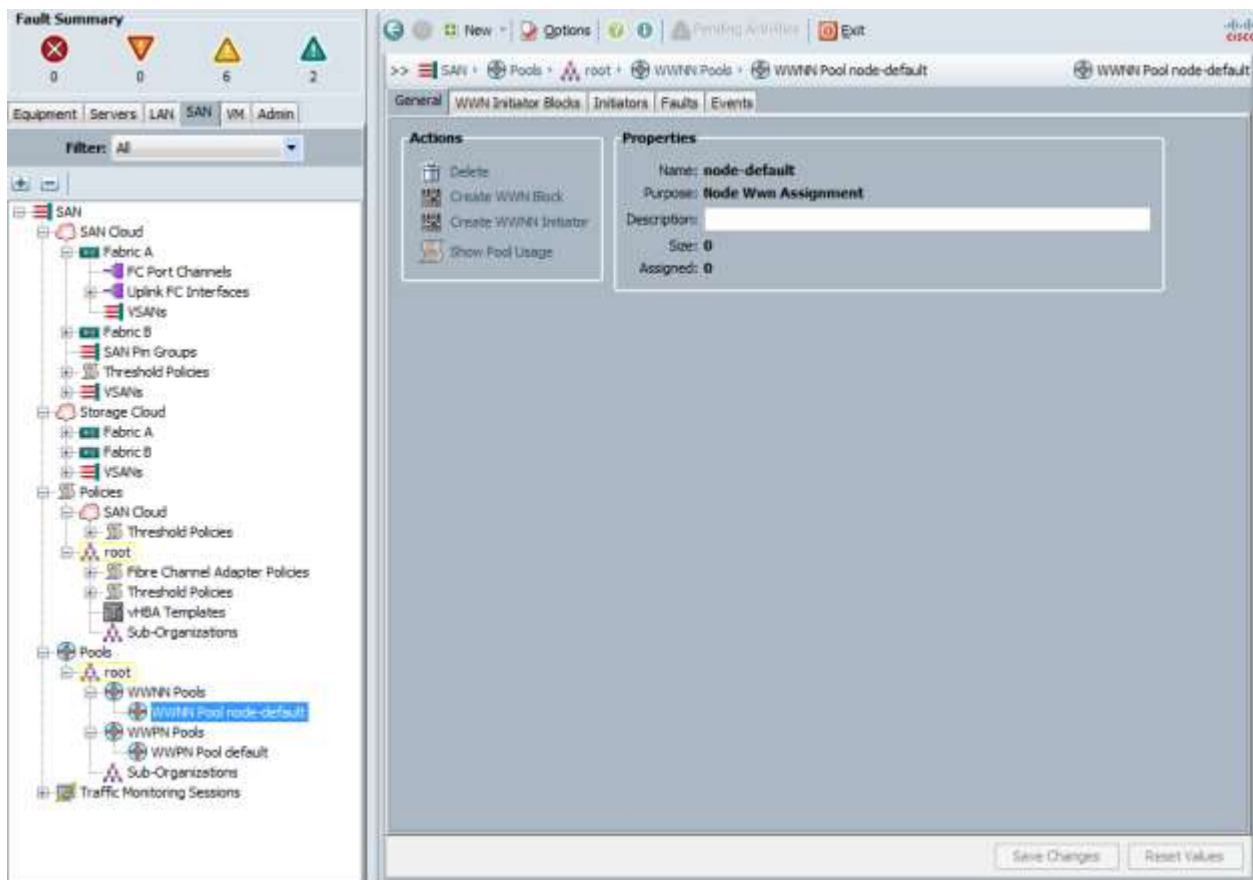
11. Click **OK**.
12. Click **Finish**.
13. In the message box that displays, click **OK**.

Create WWNN Pools

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

Cisco UCS Manager

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.
The default is fine, modify if necessary.
9. Specify a size of the WWNN block sufficient to support the available blade resources.



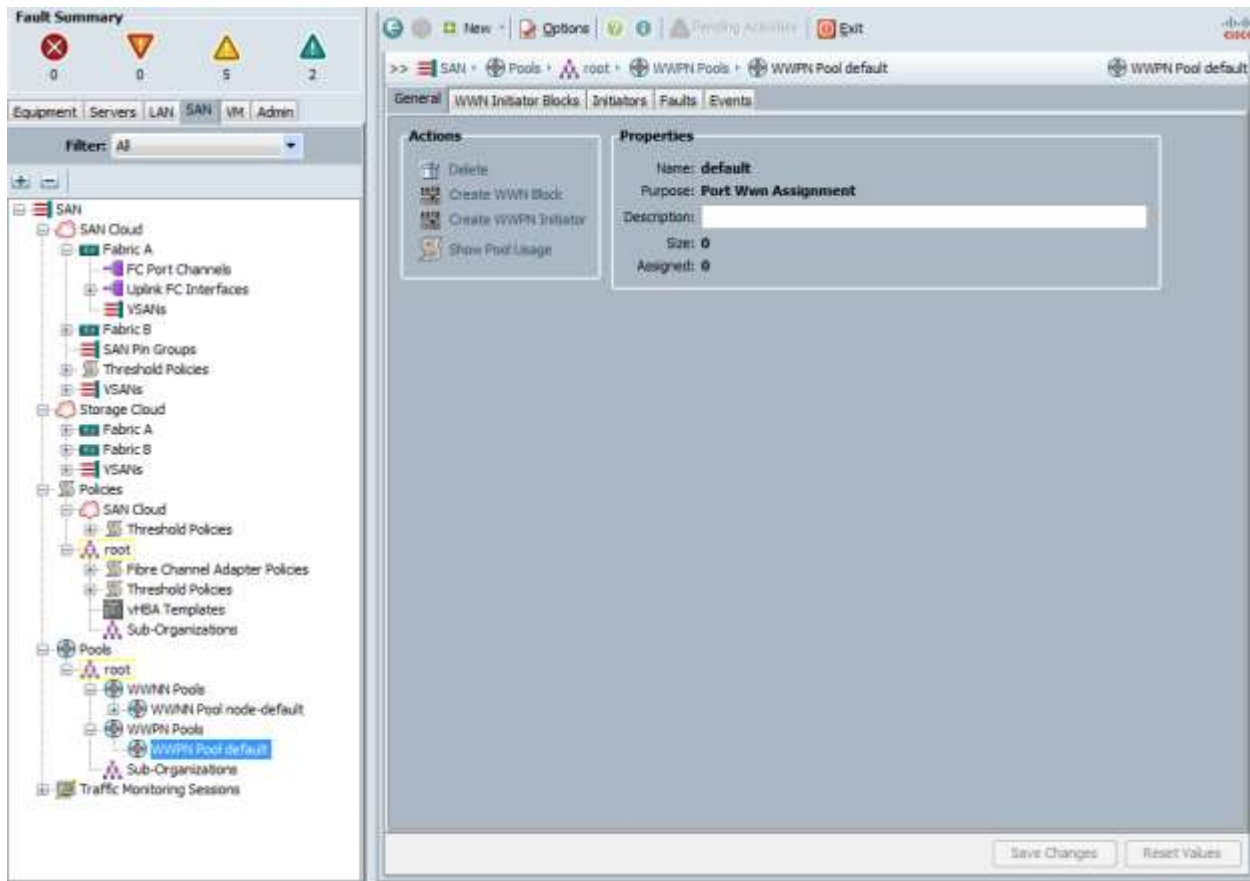
10. Click **OK** to proceed.
11. Click **Finish** to proceed.
12. Click **OK** to finish.

Create WWPN Pools

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

Cisco UCS Manager

1. Select the **SAN** tab at the top left of the window.
2. Select **Pools > root**.
3. Two WWPN pools are created, one for fabric A and one for fabric B.
4. Right-click **WWPN Pools**
5. Select **Create WWPN Pool**.



13. Enter `WWPN_Pool_A` as the name for the WWPN pool for fabric A.
14. (Optional). Give the WWPN pool a description.
15. Click **Next**.
16. Click **Add** to add a block of WWPNs.
17. Enter the starting WWPN in the block for fabric A.
18. Specify a size of the WWPN block sufficient to support the available blade resources.





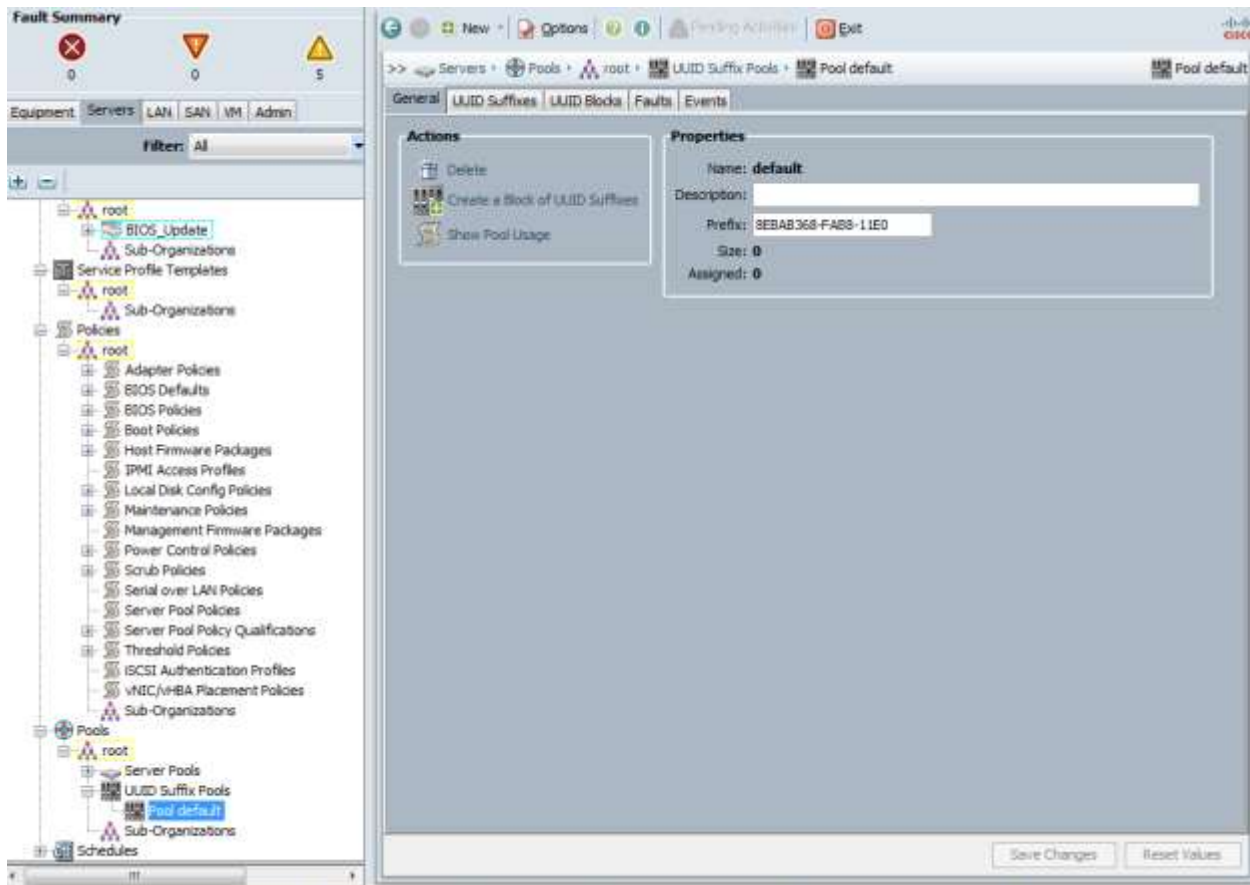
19. Click `OK`.
20. Click `Finish` to create the WWPN pool.
21. Click `OK`.
22. Right-click `WWPN Pools`
23. Select `Create WWPN Pool`.
24. Enter `WWPN_Pool_B` as the name for the WWPN pool for fabric B.
25. (Optional) Give the WWPN pool a description.
26. Click `Next`.
27. Click `Add` to add a block of WWPNS.
28. Enter the starting WWPN in the block for fabric B.
29. Specify a size of the WWPN block sufficient to support the available blade resources.
30. Click `OK`.
31. Click `Finish`.
32. Click `OK` to finish.

Create UUID Suffix Pools

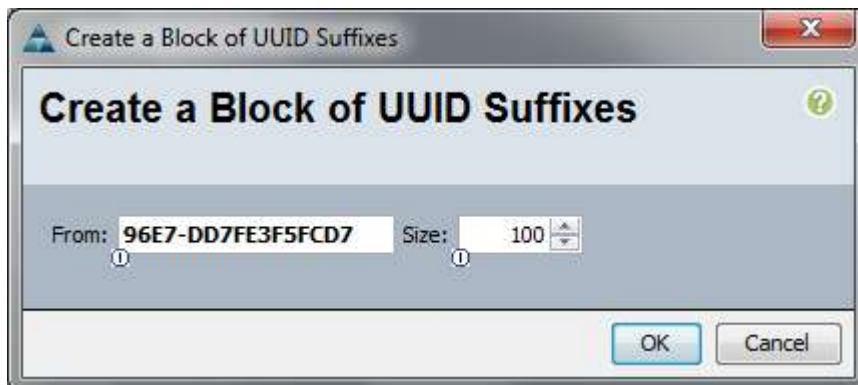
These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

Cisco UCS Manager

1. Select the `Servers` tab on the top left of the window.
2. Select `Pools > root`.
3. Right-click `UUID Suffix Pools`
4. Select `Create UUID Suffix Pool`.



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



12. Click **OK**.



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

Create Server Pools

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

Cisco UCS Manager

1. Select the `Servers` tab at the top left of the window.
2. Select `Pools > root`.
3. Right-click `Server Pools`.
4. Select `Create Server Pool`.
5. Name the server pool `Infra_Pool`.
6. (Optional) Give the server pool a description.
7. Click `Next` to continue to add servers.
8. Select two B200 servers to be added to the `Infra_Pool` server pool. Click `>>` to add them to the pool.
9. Click `Finish`.
10. Select `OK` to finish.

Create VLANs

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

Cisco UCS Manager

1. Select the `LAN` tab on the left of the window.
- Note:** Eight VLANs are created.
2. Select `LAN Cloud`.
 3. Right-click `VLANs`.
 4. Select `Create VLANs`.
 5. Enter `MGMT-VLAN` as the name of the VLAN to be used for management traffic.
 6. Keep the `Common/Global` option selected for the scope of the VLAN.
 7. Enter the VLAN ID for the management VLAN. Keep the sharing type as `none`.
 8. Click `OK`.



Create VLANs

VLAN Name/Prefix: **VM-Mgmt-VLAN**

☒ 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: **805**

Sharing Type: ☒ None ☐ Primary ☐ Isolated

Check Overlap OK Cancel

9. Right-click VLANs .
10. Select Create VLANs.
11. Enter CSV-VLAN as the name of the VLAN to be used for the CSV VLAN.
12. Keep the Common/Global option selected for the scope of the VLAN.
13. Enter the VLAN ID for the CSV VLAN.
14. Click OK.
15. Right-click VLANs .
16. Select Create VLANs.
17. Enter iSCSI-VLAN-A as the name of the VLAN to be used for the first iSCSI VLAN.
18. Keep the Common/Global option selected for the scope of the VLAN.
19. Enter the VLAN ID for the first iSCSI VLAN .
20. Click OK.



Create VLANs

VLAN Name/Prefix:

☒ 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

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



Create VLANs

VLAN Name/Prefix:

☒ 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

27. Right-click VLANs .
28. Select Create VLANs .
29. Enter Live Migration-VLAN as the name of the VLAN to be used for the live migration VLAN.
30. Keep the Common/Global option selected for the scope of the VLAN.
31. Enter the VLAN ID for the live migration VLAN.
32. Click OK, then OK.
33. Right-click VLANs .
34. Select Create VLANs .
35. Enter App-Cluster-Comm-VLAN as the name of the VLAN to be used for the VM Cluster VLAN.
36. Keep the Common/Global option selected for the scope of the VLAN.
37. Enter the VLAN ID for the VM Cluster VLAN.
38. Click OK.



Create VLANs

VLAN Name/Prefix:

☒ 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

39. Right-click VLANs .
40. Select Create VLANs.
41. Enter VM-Data-VLAN as the name of the VLAN to be used for the VM data VLAN.
42. Keep the Common/Global option selected for the scope of the VLAN.
43. Enter the VLAN ID for the VM data VLAN.
44. Click OK.
45. Right-click VLANs .
46. Select Create VLANs.
47. Enter Native-VLAN as the name of the VLAN to be used for the Native VLAN.
48. Keep the Common/Global option selected for the scope of the VLAN.
49. Enter the VLAN ID for the Native VLAN.
50. Click OK.



Create VLANs

VLAN Name/Prefix:

☒ 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

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

Create VSANs and SAN Port Channels

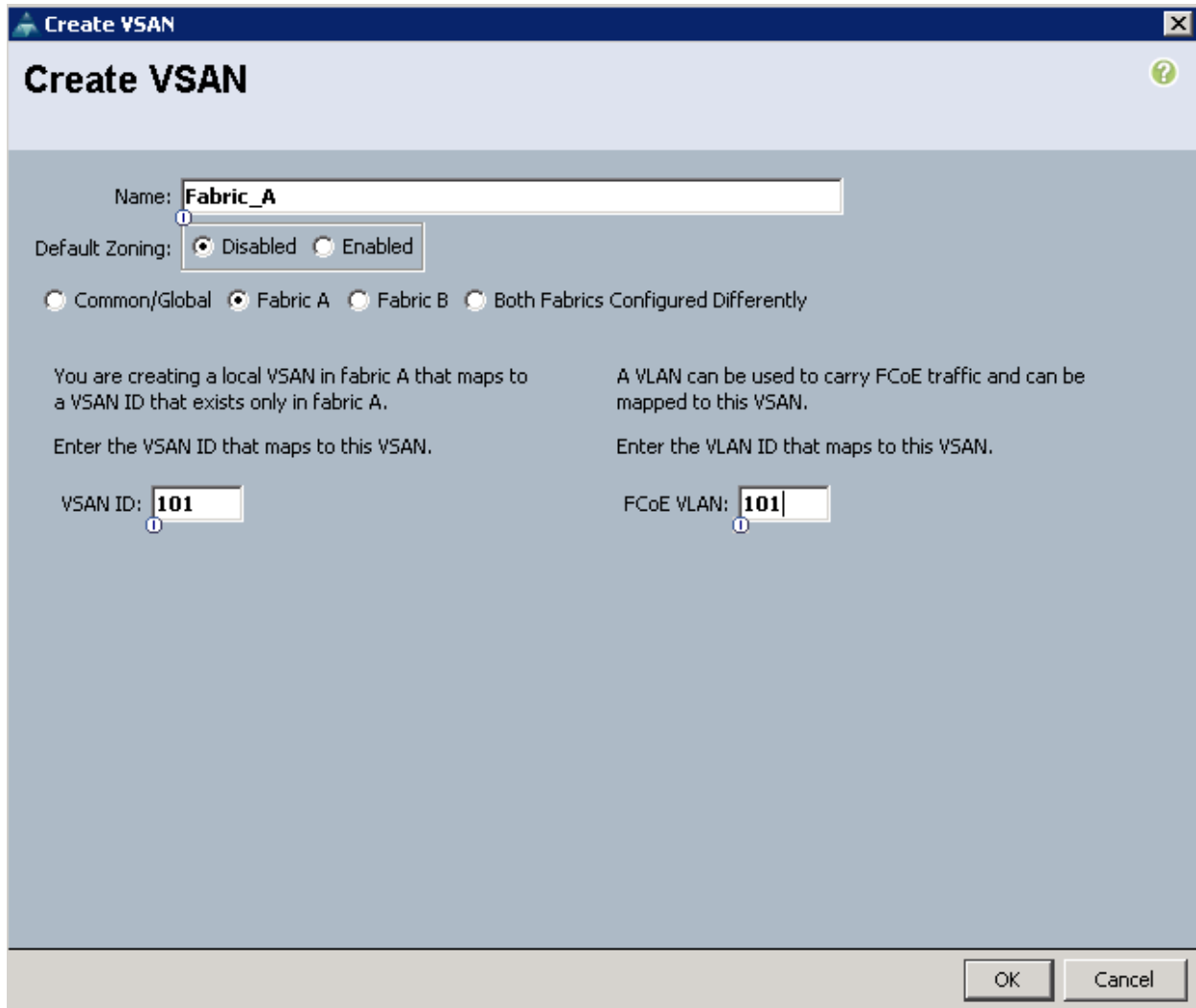
These steps provide details for configuring the necessary VSANs and SAN Port Channels for the Cisco UCS environment. By default, VSAN 1 is used created and can be used. Alternate VSANs can be created as necessary.

Cisco UCS Manager

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.



The image shows a 'Create VSAN' dialog box with a title bar containing a help icon, the text 'Create VSAN', and a close button. The main area has a light blue background. At the top, the title 'Create VSAN' is displayed in bold. Below it, the 'Name' field contains 'Fabric_A'. The 'Default Zoning' section has two radio buttons: 'Disabled' (selected) and 'Enabled'. Below this, there are four radio buttons for fabric selection: 'Common/Global', 'Fabric A' (selected), 'Fabric B', and 'Both Fabrics Configured Differently'. Two columns of explanatory text are present: the left column states 'You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.' and 'Enter the VSAN ID that maps to this VSAN.'; the right column states 'A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.' and 'Enter the VLAN ID that maps to this VSAN.'. Below the text, the 'VSAN ID' field contains '101' and the 'FCoE VLAN' field contains '101'. Both fields have a small information icon (i) to their left. At the bottom right, there are 'OK' and 'Cancel' buttons.

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:

OK **Cancel**

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:

OK Cancel

19. Under SAN Cloud, expand the Fabric A tree.
20. Right-click FC Port Channels
21. Select Create Port Channel.
22. Click Yes and then enter 1 for the Port Channel ID and SPo1 for the Port Channel name.
23. Click Next.



Create Port Channel

Unified Computing System Manager

Create Port Channel

1. ✓ Set Port Channel Name
2. ✓ Add Ports

Set Port Channel Name

ID:

Name:

< Prev Next > Finish Cancel

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

25. Click Finish.

Create Port Channel

Unified Computing System Manager

Create Port Channel

1. ✓ Set Port Channel Name
2. ✓ Add Ports

Add Ports

Port Channel Admin Speed: Auto

Port	Slot ID	WWPN	ID

Port	Slot ID	WWPN	ID
31	1	20:1F:54:7F:EE:19:...	
32	1	20:20:54:7F:EE:19:...	

Slot ID:

WWPN:

Slot ID:

WWPN:

< Prev Next > Finish Cancel

26. Select the Check box for Show navigator for FC Port-Channel 1 (Fabric A)
27. Click OK to complete creating the Port Channel.
28. In the VSAN pull-down under Properties select the vsan VSAN_A for fabric A.
29. Click Apply, then click OK.
30. Under Actions, click Enable Port Channel.
31. Click Yes and then OK to enable the Port Channel. This action also enables the two FC ports in the Port Channel.

Status

Overall Status: ↓ **Admin Down**

Additional Info: **Administratively down**

Actions

Enable Port Channel

Disable Port Channel

Add Ports

Properties

ID: **1**

Fabric ID: **A**

Port Type: **Aggregation**

Transport Type: **Fc**

Name:

VSAN:

Port Channel Admin Speed:

Operational Speed(Gbps): **16**



32. 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.

The screenshot displays a configuration window for a Port Channel. It is divided into three main sections: Status, Actions, and Properties.

- Status:** Shows 'Overall Status: Up' with a green upward arrow icon. Below it is a label 'Additional Info:'.
- Actions:** Contains three buttons: 'Enable Port Channel' (with a plug icon), 'Disable Port Channel' (with a plug and red X icon), and 'Add Ports' (with a plug and plus icon).
- Properties:** Contains the following fields:
 - ID: 1
 - Fabric ID: A
 - Port Type: Aggregation
 - Transport Type: Fc
 - Name: Fabric_A_PC_1 (text input field)
 - VSAN: Fabric dual/vsan default (1) (dropdown menu)
 - Port Channel Admin Speed: Auto (dropdown menu)
 - Operational Speed(Gbps): 16

33. Under SAN Cloud, expand the Fabric B tree.

34. Right-click FC Port Channels

35. Select Create Port Channel.

36. Click **Yes**, and then enter 2 for the Port Channel ID and SPo2 for the Port Channel name.

37. Click **Next**.



Create Port Channel

Unified Computing System Manager

Create Port Channel

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

Set Port Channel Name

ID:

Name:

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

39. Click Finish.

Create Port Channel

Unified Computing System Manager

Create Port Channel

1. ✓ Set Port Channel Name
2. ✓ Add Ports

Add Ports

Port Channel Admin Speed: Auto

Port	Slot ID	WWPN	ID
31	1	20:1F:54:7F:EE:19:...	
32	1	20:20:54:7F:EE:19:...	

Ports in the port channel

Port	Slot ID	WWPN	ID
31	1	20:1F:54:7F:EE:19:...	
32	1	20:20:54:7F:EE:19:...	

Details

Slot ID:

WWPN:

< Prev Next > Finish Cancel

40. Select Check box for Show navigator for FC Port-Channel 1 (Fabric B)
41. Click OK to complete creating the Port Channel.
42. In the VSAN pull-down under Properties select VSAN_B for fabric B.
43. Click Apply, then click OK.
44. Under Actions, click Enable Port Channel.
45. Click Yes, then OK to enable the Port Channel. This action also enables the two FC ports in the Port Channel.

Status

Overall Status: ↓ **Admin Down**

Additional Info: **Administratively down**

Actions

Enable Port Channel

Disable Port Channel

Add Ports

Properties

ID: 2

Fabric ID: B

Port Type: **Aggregation**

Transport Type: **Fc**

Name:

VSAN:

Port Channel Admin Speed: Auto

Operational Speed(Gbps): 0



46. Click **OK** to Close the Navigator.

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

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

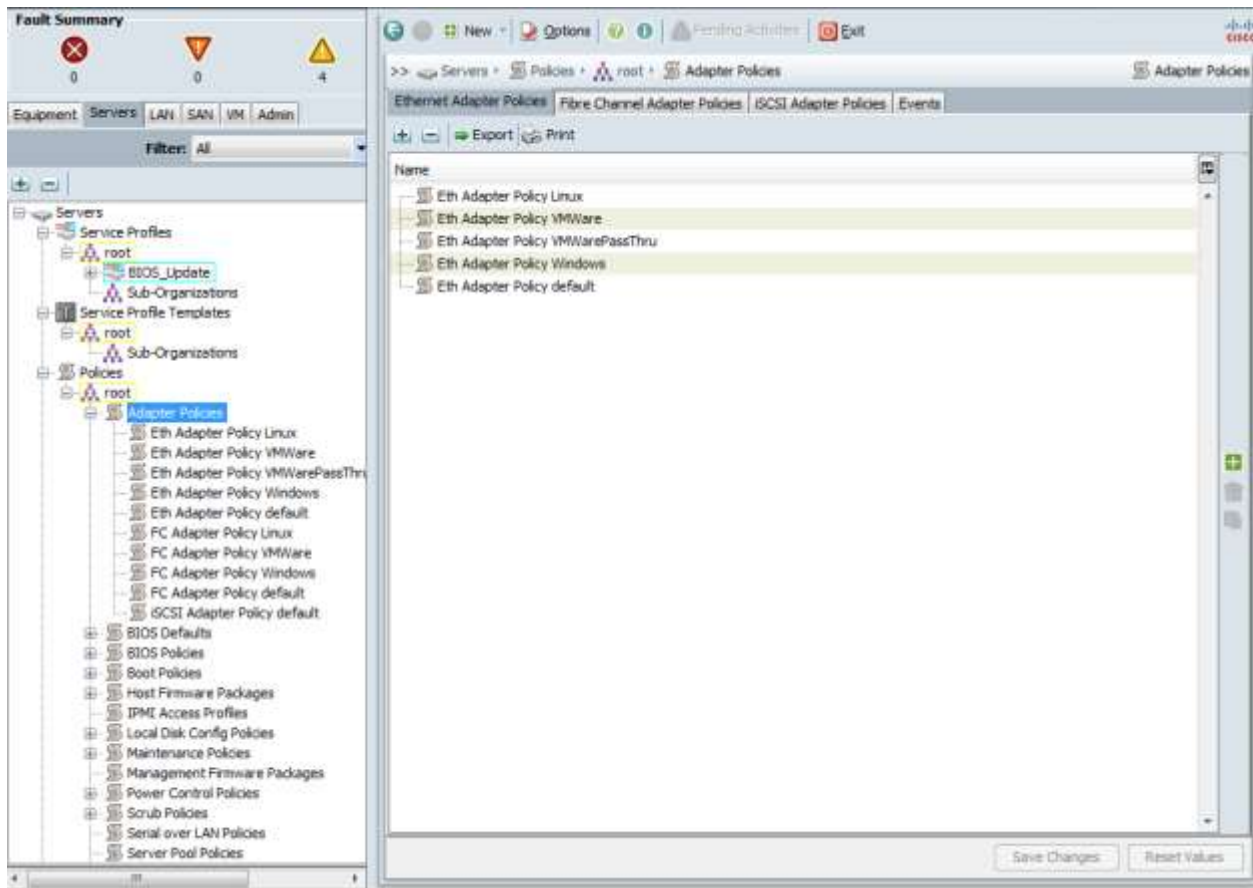
The screenshot displays a configuration window for a Fibre Channel Port Channel. It is divided into three main sections:

- Status:** Shows the Overall Status as **Up** with a green arrow icon. Below it is a label for Additional Info.
- Actions:** Contains three buttons: **Enable Port Channel** (with a plug icon), **Disable Port Channel** (with a red X icon), and **Add Ports** (with a green plus icon).
- Properties:** Displays configuration details for the port channel:
 - ID: 2
 - Fabric ID: B
 - Port Type: Aggregation
 - Transport Type: Fc
 - Name: Fabric_B_PC_2 (text input field)
 - VSAN: Fabric dual/vsan default (1) (dropdown menu)
 - Port Channel Admin Speed: Auto (dropdown menu)
 - Operational Speed(Gbps): 16

Create a FC Adapter Policy for NetApp Storage Arrays

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

1. Select to the SAN tab at the top of the left window.
2. Go to `SAN > Policies > root`.
3. Right-click `Fibre Channel Adapter Policies` and click `Create New Fibre Channel Adapter Policy`.



4. Use Windows-NetApp as the name of the Fibre Channel Adapter Policy.
5. The default values are appropriate for most configurable items. Expand the Options dropdown, and set the Link Down Timeout (MS) option to 5000.
6. Click OK to complete creating the FC adapter policy.
7. Click OK.



Create Fibre Channel Adapter Policy

Name: **Windows-NetApp**

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

OK Cancel

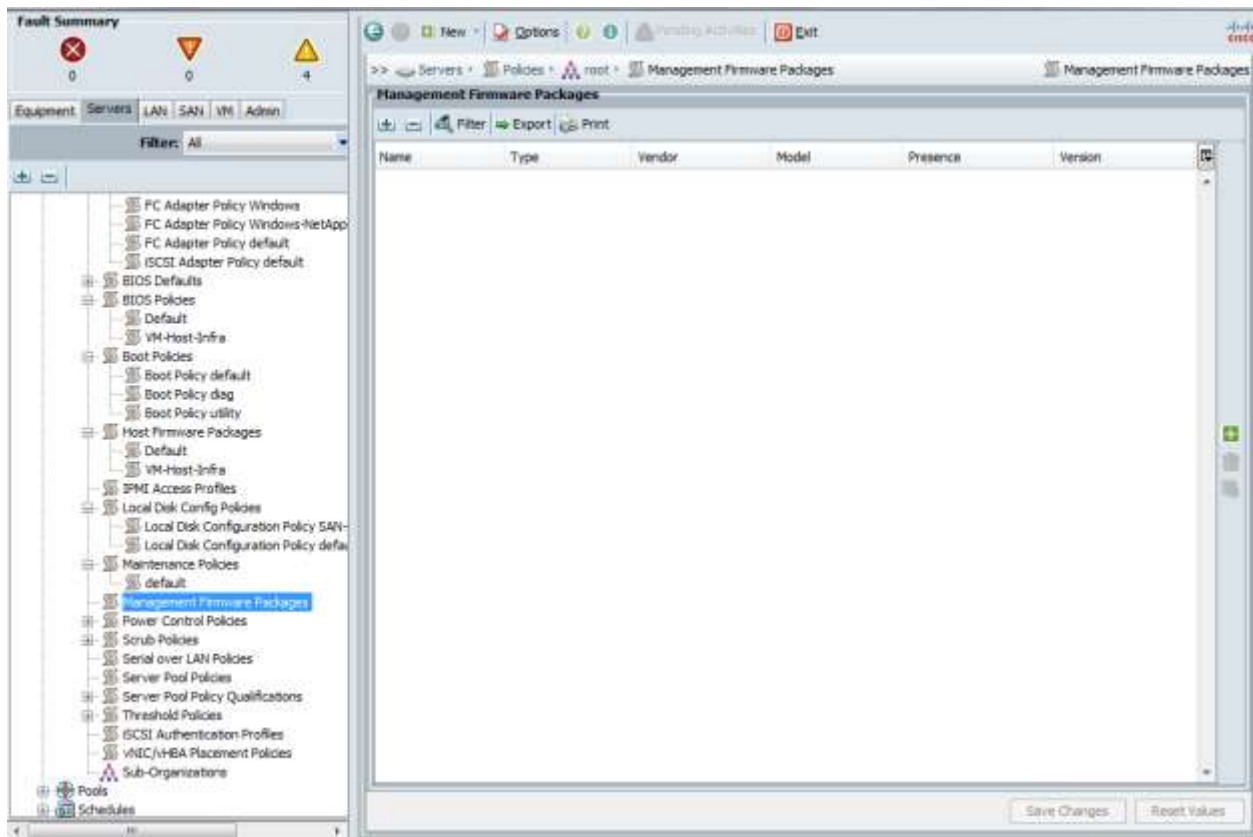
Create a Firmware Management Package

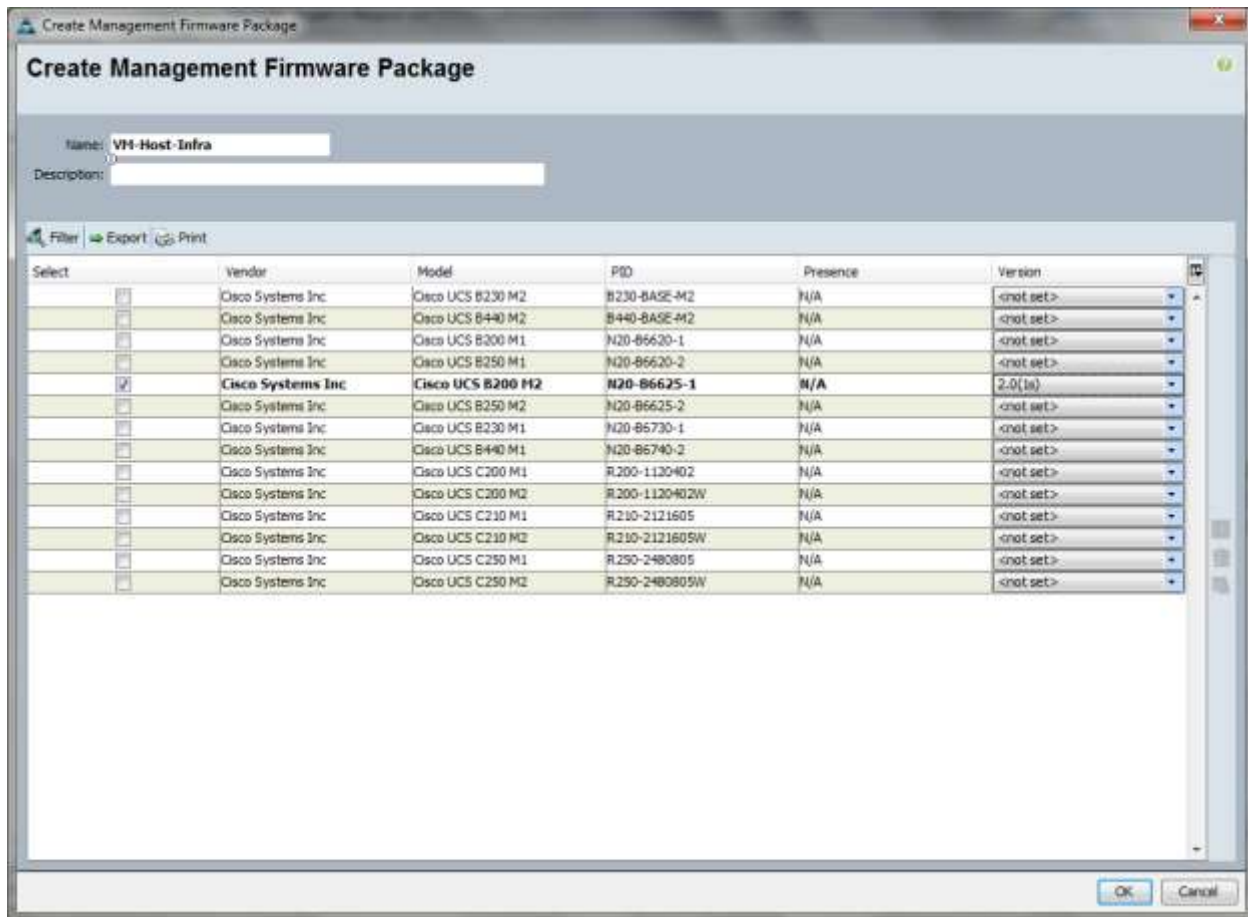
These steps provide details for a firmware management policy for n the Cisco UCS environment.



Cisco UCS Manager

1. Select the Servers tab at the top left of the window.
2. Select Policies > root.
3. Right Click Management Firmware Packages
4. Select create Management Firmware Package.
5. Enter VM-Host-Infra as the management firmware package name.
6. Select the appropriate packages and versions of the Server Management Firmware For servers that you have.
7. Click OK to complete creating the management firmware package.
8. Click OK.





Create Firmware Package Policy

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

Cisco UCS Manager

1. Select the **Servers** tab at the top left of the window.
2. Select **Policies > root**.
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.
6. Navigate the tabs of the **Create Host Firmware Package** Navigator and select the appropriate packages and versions for the server configuration.
7. Click **OK** to complete creating the host firmware package.
8. Click **OK**.



Fault Summary

0 0 4

Equipment Servers LAN SAN VM Admin

Filter: All

root

- Sub-Organizations
- Policies
 - root
 - Adapter Policies
 - Eth Adapter Policy Linux
 - Eth Adapter Policy VMWare
 - Eth Adapter Policy VMWarePassThru
 - Eth Adapter Policy Windows
 - Eth Adapter Policy default
 - FC Adapter Policy Linux
 - FC Adapter Policy VMWare
 - FC Adapter Policy Windows
 - FC Adapter Policy Windows-NetApp
 - FC Adapter Policy default
 - ISCSI Adapter Policy default
 - BIOS Defaults
 - BIOS Policies
 - Default
 - VM+Host-Infra
 - Boot Policies
 - Boot Policy default
 - Boot Policy diag
 - Boot Policy utility
 - Host Firmware Packages**
 - Default
 - IPMI Access Profiles
 - Local Disk Config Policies
 - Maintenance Policies
 - Management Firmware Packages
 - Power Control Policies
 - Scrub Policies
 - Serial over LAN Policies

Host Firmware Packages

Name	Type	Vendor	Model	Presence	Version
Default					
Cisco Systems, Inc. - N20-B6620Server B...		Cisco Systems, I...	N20-B6620-1	Present	55500.2.0.1d.0.09302...
Cisco Systems, Inc. - N20-B6625Server B...		Cisco Systems, I...	N20-B6625-1	Present	55500.2.0.1d.0.09302...

Save Changes Reset Values



Microsoft



Fault Summary

0 0 4

Equipment Servers LAN SAN VM Admin

Filter: All

root
Sub-Organizations
Policies
root
Adapter Policies
Eth Adapter Policy Linux
Eth Adapter Policy VMWare
Eth Adapter Policy VMWarePassThru
Eth Adapter Policy default
FC Adapter Policy Linux
FC Adapter Policy VMWare
FC Adapter Policy Windows
FC Adapter Policy Windows-NetApp
FC Adapter Policy default
iSCSI Adapter Policy default
BIOS Defaults
BIOS Policies
Default
VM-Host-Infra
Boot Policies
Boot Policy default
Boot Policy diag
Boot Policy utility
Host Firmware Packages
Default
VM-Host-Infra
DPMI Access Profiles
Local Disk Config Policies
Maintenance Policies
Management Firmware Packages
Power Control Policies
Scrub Policies

General Events

Actions: Delete Show Policy Usage

Properties: Name: VM-Host-Infra Description: Infrastructure Host

Adapter BIOS Board Controller FC Adapters HBA Option ROM Storage Controller

Filter Export Print

Select	Vendor	Model	PID	Presence	Version
☐	Cisco Systems Inc	Cisco UCS M5 SR-B	N20-AB0002	N/A	<not set>
☒	Cisco Systems Inc	Cisco UCS M8 SR	N20-AC0002	Present	2.0 (a)
☐	Cisco Systems Inc	Cisco UCS M7 SR-E	N20-AE0002	N/A	<not set>
☐	Cisco Systems Inc	Cisco UCS M72SR-E	N20-AE0102	N/A	<not set>
☐	Cisco Systems Inc	Cisco UCS M6 SR-I	N20-AD102	N/A	<not set>
☐	Cisco Systems Inc	Cisco UCS M7 SR-Q	N20-AQ0002	N/A	<not set>
☐	Cisco Systems Inc	Cisco UCS M72SR-Q	N20-AQ0102	N/A	<not set>
☐	Broadcom Corp.	Broadcom 10GbE Ad...	N20X-ABPC01	N/A	<not set>
☐	Cisco Systems Inc	Cisco UCS P8 SE	N20X-ACPC101	N/A	<not set>
☐	Emulex Corp.	Emulex OCe10102-F	N20X-AEPC01	N/A	<not set>
☐	Intel Corp.	Intel 10GbE Adapter	N20X-ABPC01	N/A	<not set>
☐	QLogic Corp.	QLogic QLE8152	N20X-AQPC01	N/A	<not set>

Save Changes Reset Values

Fault Summary

0 0 4

Equipment Servers LAN SAN VM Admin

Filter: All

root
Sub-Organizations
Policies
root
Adapter Policies
Eth Adapter Policy Linux
Eth Adapter Policy VMWare
Eth Adapter Policy VMWarePassThru
Eth Adapter Policy default
FC Adapter Policy Linux
FC Adapter Policy VMWare
FC Adapter Policy Windows
FC Adapter Policy Windows-NetApp
FC Adapter Policy default
iSCSI Adapter Policy default
BIOS Defaults
BIOS Policies
Default
VM-Host-Infra
Boot Policies
Boot Policy default
Boot Policy diag
Boot Policy utility
Host Firmware Packages
Default
VM-Host-Infra
DPMI Access Profiles
Local Disk Config Policies
Maintenance Policies
Management Firmware Packages
Power Control Policies
Scrub Policies

General Events

Actions: Delete Show Policy Usage

Properties: Name: VM-Host-Infra Description: Infrastructure Host

Adapter BIOS Board Controller FC Adapters HBA Option ROM Storage Controller

Filter Export Print

Select	Vendor	Model	PID	Presence	Version
☐	Cisco Systems, Inc.	Cisco UCS B230 M2	B230-BASE-M2	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS B440 M2	B440-BASE-M2	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS B200 M1	N20-B6620-1	N/A	<not set>
☐	Intel Corp.	Cisco UCS B200 M1	N20-B6620-1	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS B250 M1	N20-B6620-2	N/A	<not set>
☐	Intel Corp.	Cisco UCS B250 M1	N20-B6620-2	N/A	<not set>
☒	Cisco Systems, Inc.	Cisco UCS B200 M2	N20-B6625-1	N/A	55500.2.0.1d.0...
☐	Cisco Systems, Inc.	Cisco UCS B250 M2	N20-B6625-2	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS B230 M1	N20-B6730-1	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS B440 M1	N20-B6740-2	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C200 M1	R200-1120402	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C200 M2	R200-1120402W	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C210 M1	R210-2121605	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C210 M2	R210-2121605W	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C250 M1	R250-2480805	N/A	<not set>
☐	Cisco Systems, Inc.	Cisco UCS C250 M2	R250-2480805W	N/A	<not set>

Save Changes Reset Values

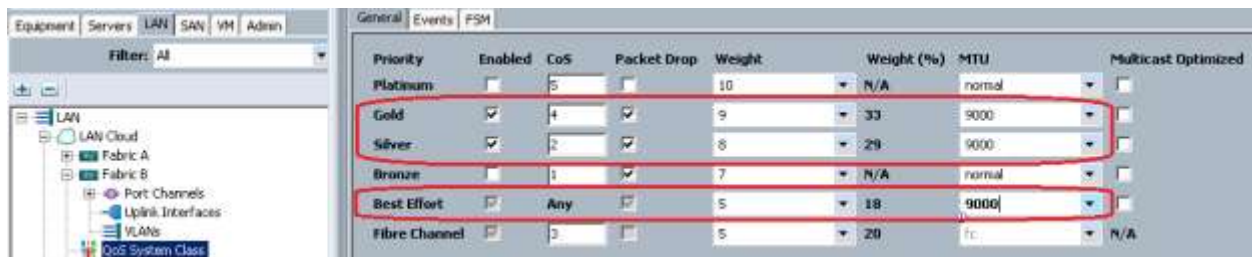


Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric

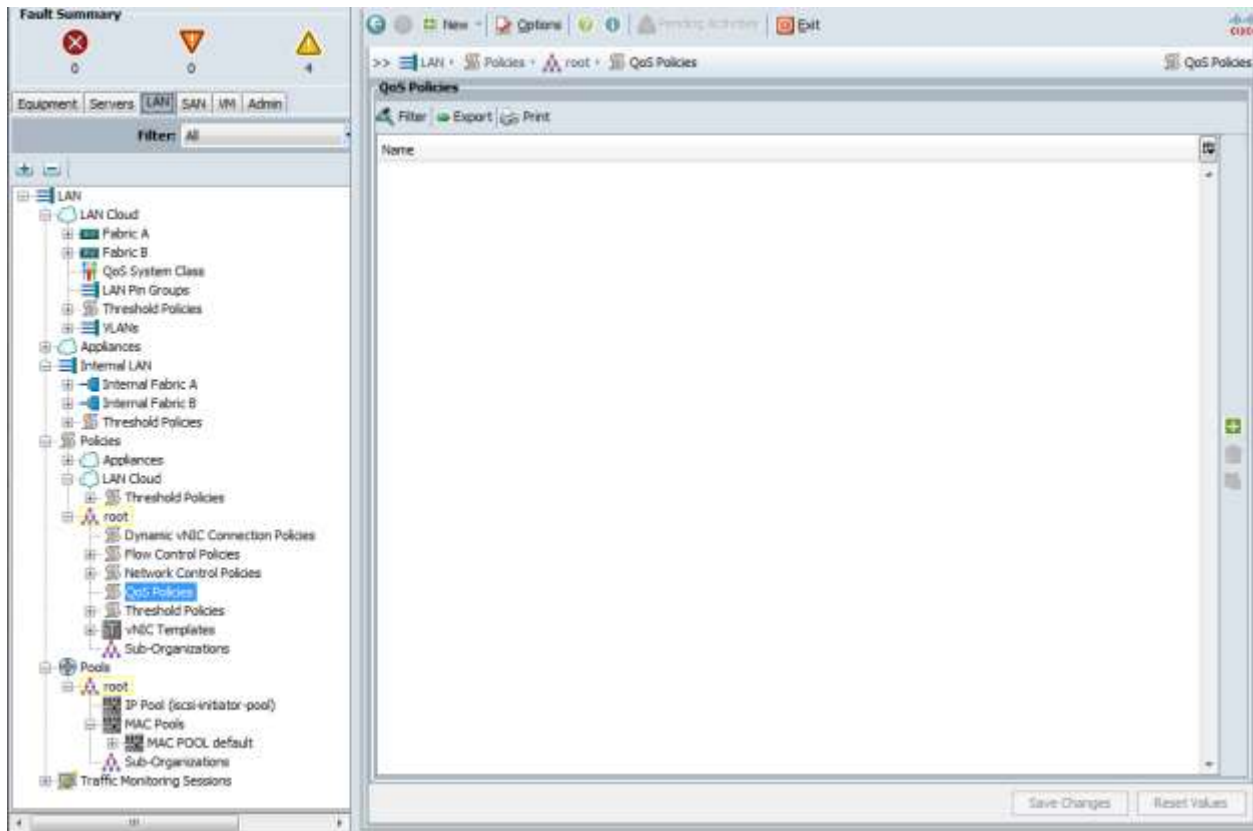
These steps provide details for setting Jumbo frames and enabling the quality of server in the Cisco UCS Fabric.

Cisco UCS Manager

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



7. Select the **LAN** tab on the left of the window.
8. Go to **LAN > Policies > Root >**.



9. Right-click QoS Policies.
10. Select Create QoS Policy.
11. Enter LiveMigration as the QoS Policy name.
12. Change the Priority to Gold. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate. Leave Host Control set to None.
13. Click OK in the bottom right corner.



Create QoS Policy

Name: **LiveMigration**

Egress

Priority: **Gold**

Burst(Bytes): 10240

Rate(Kbps): line-rate

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 Gold. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate. Leave Host Control set to None.
18. Click OK in the bottom right corner.

Create QoS Policy

Name: **CSV**

Egress

Priority: **Gold**

Burst(Bytes): 10240

Rate(Kbps): line-rate

Host Control: ☒ None ☐ Full

OK Cancel

19. Right-click QoS Policies.
20. Select Create QoS Policy.



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

Create QoS Policy

Name:

Egress

Priority:

Burst(Bytes):

Rate(Kbps):

Host Control: ☒ None ☐ Full

OK **Cancel**

Create a Power Control Policy

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

Cisco UCS Manager

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



Fault Summary

0 0 4

Equipment Servers LAN SAN VM Admin

Filter: All

- FC Adapter Policy Windows
- FC Adapter Policy Windows-NetApp
- FC Adapter Policy default
- iSCSI Adapter Policy default
- BIOS Defaults
- BIOS Policies
 - Default
- VM-Host-Infra
- Boot Policies
 - Boot Policy default
 - Boot Policy diag
 - Boot Policy utility
- Host Firmware Packages
 - Default
 - VM-Host-Infra
- IPMI Access Profiles
- Local Disk Config Policies
 - Local Disk Configuration Policy SAN
 - Local Disk Configuration Policy default
- Maintenance Policies
 - default
- Management Firmware Packages
 - VM-Host-Infra
- Power Control Policies**
 - default
- Scrub Policies
- Serial over LAN Policies
- Server Pool Policies
- Server Pool Policy Qualifications
- Threshold Policies
- iSCSI Authentication Profiles
- vNIC/vHBA Placement Policies
- Sub-Organizations

Power Control Policies

Events

Filter Export Print

Name	Power Priority
default	5

Save Changes Reset Values

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.

OK Cancel



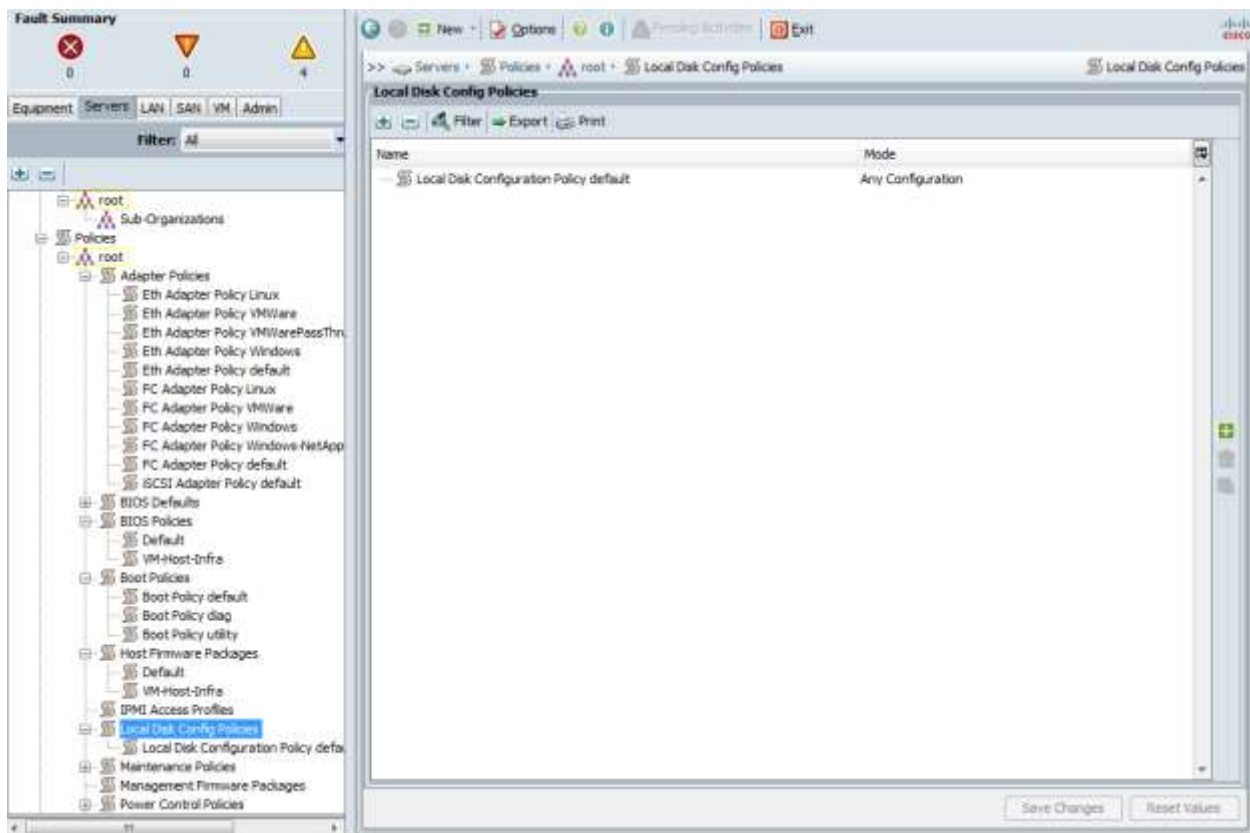
Create a Local Disk Configuration Policy

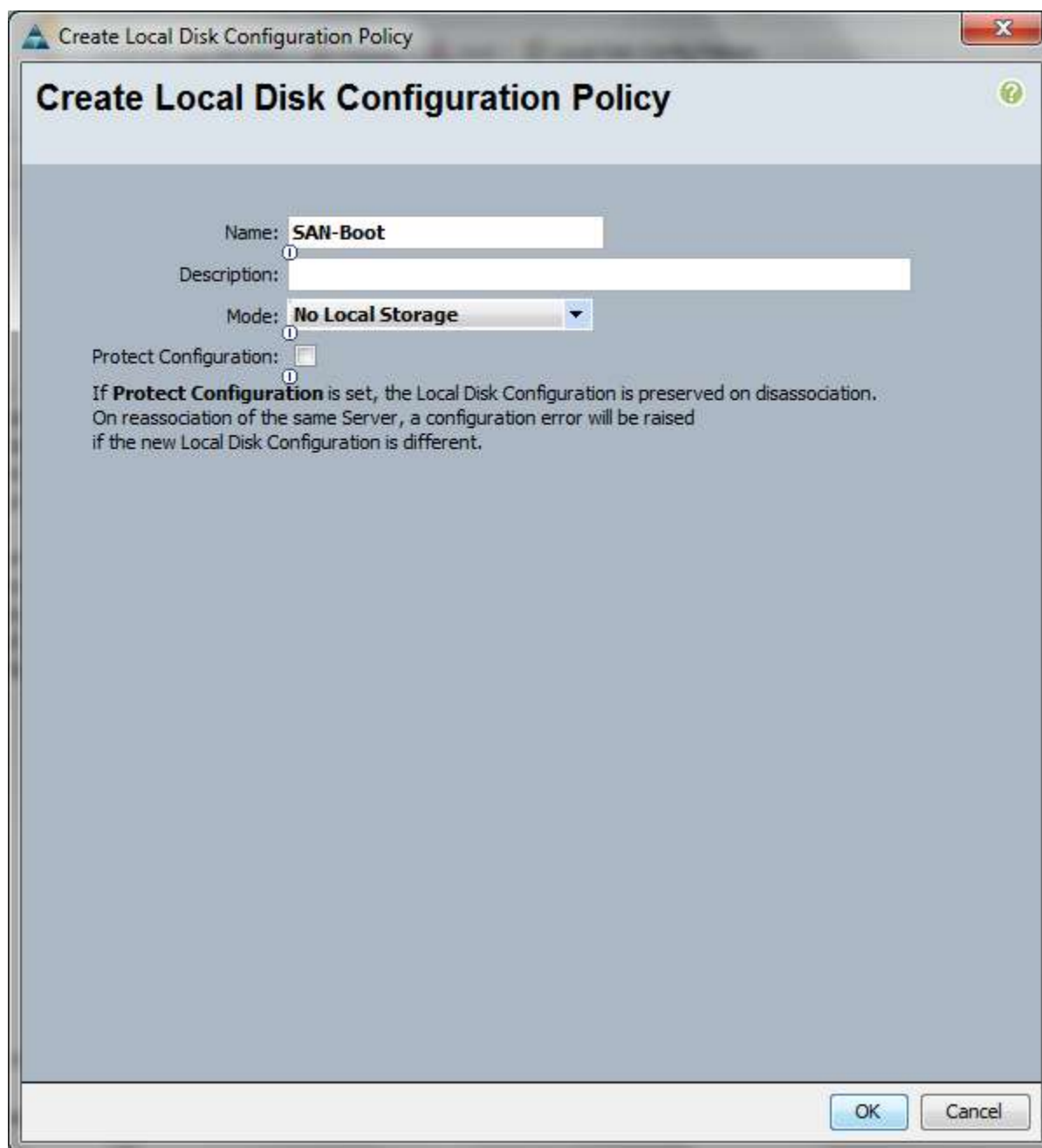
These steps provide details for creating a local disk configuration for the Cisco UCS environment, which is necessary if the servers in question do not have a local disk.

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

Cisco UCS Manager

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





Create Local Disk Configuration Policy

Name:

Description:

Mode:

Protect Configuration: ☐

If **Protect Configuration** is set, the Local Disk Configuration is preserved on disassociation. On reassociation of the same Server, a configuration error will be raised if the new Local Disk Configuration is different.

OK Cancel

Create a Server Pool Qualification Policy

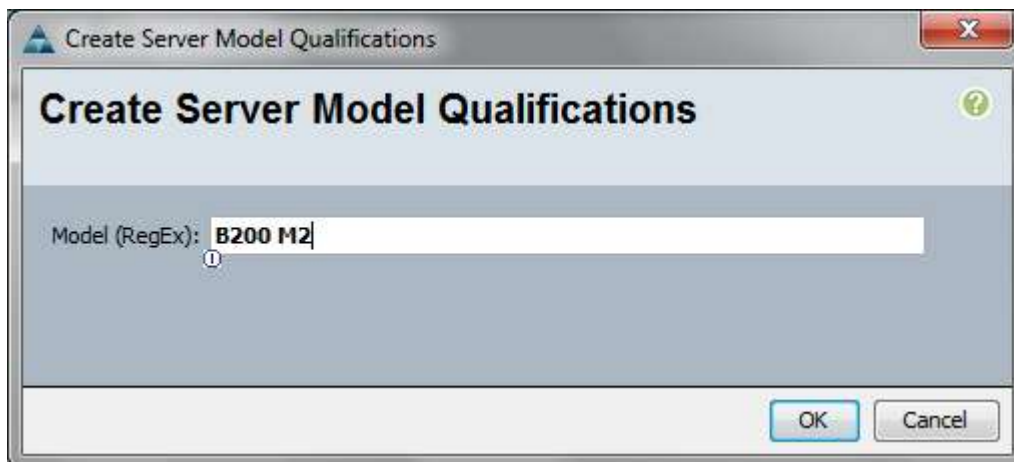
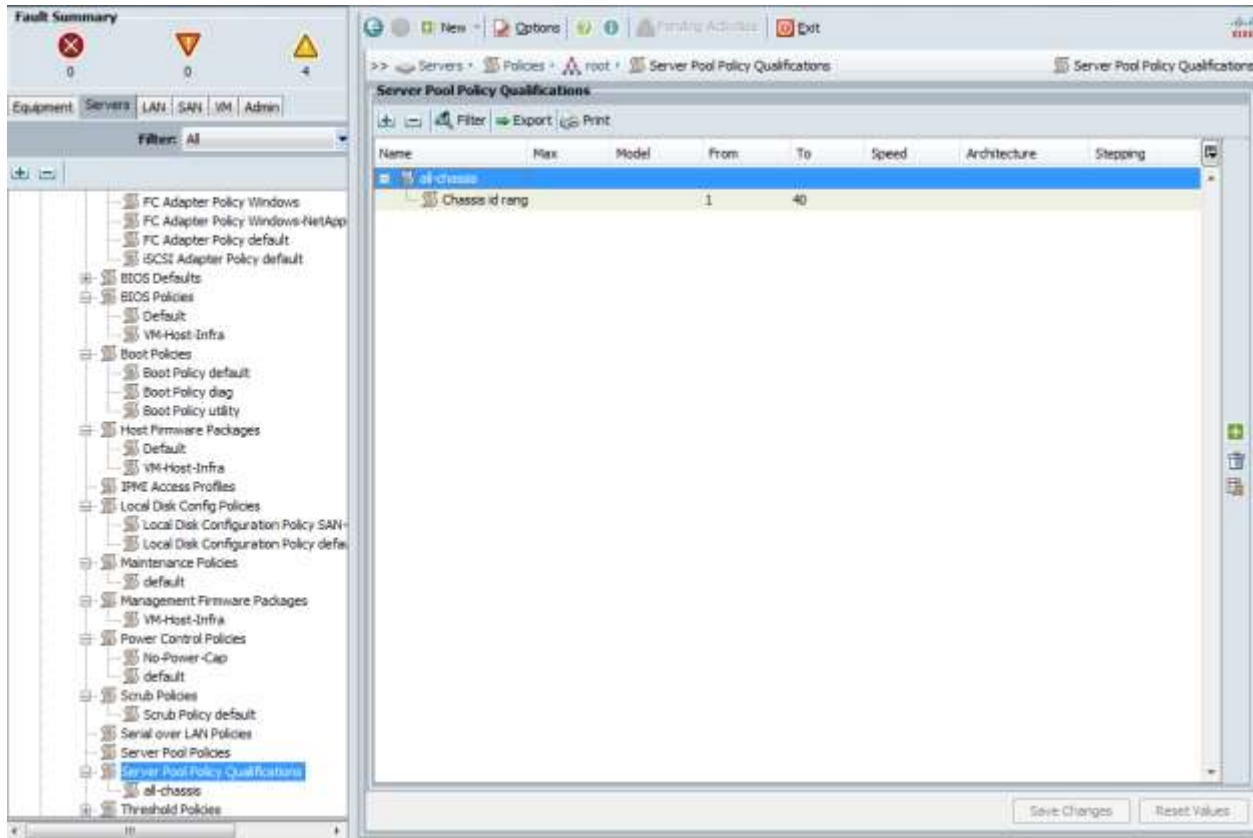
These steps provide details for creating a server pool qualification policy for the Cisco UCS environment.

Cisco UCS Manager

1. Select the `Servers` tab on the left of the window.
2. Go to `Policies > root`.
3. Right-click `Server Pool Qualification Policies`.



4. Select Create Server Pool Policy Qualification.
5. Select Server Model Qualifications.
6. Enter B200 M2 as the Model (RegEx) .
7. Click OK to complete creating the host firmware package.
8. Click OK .



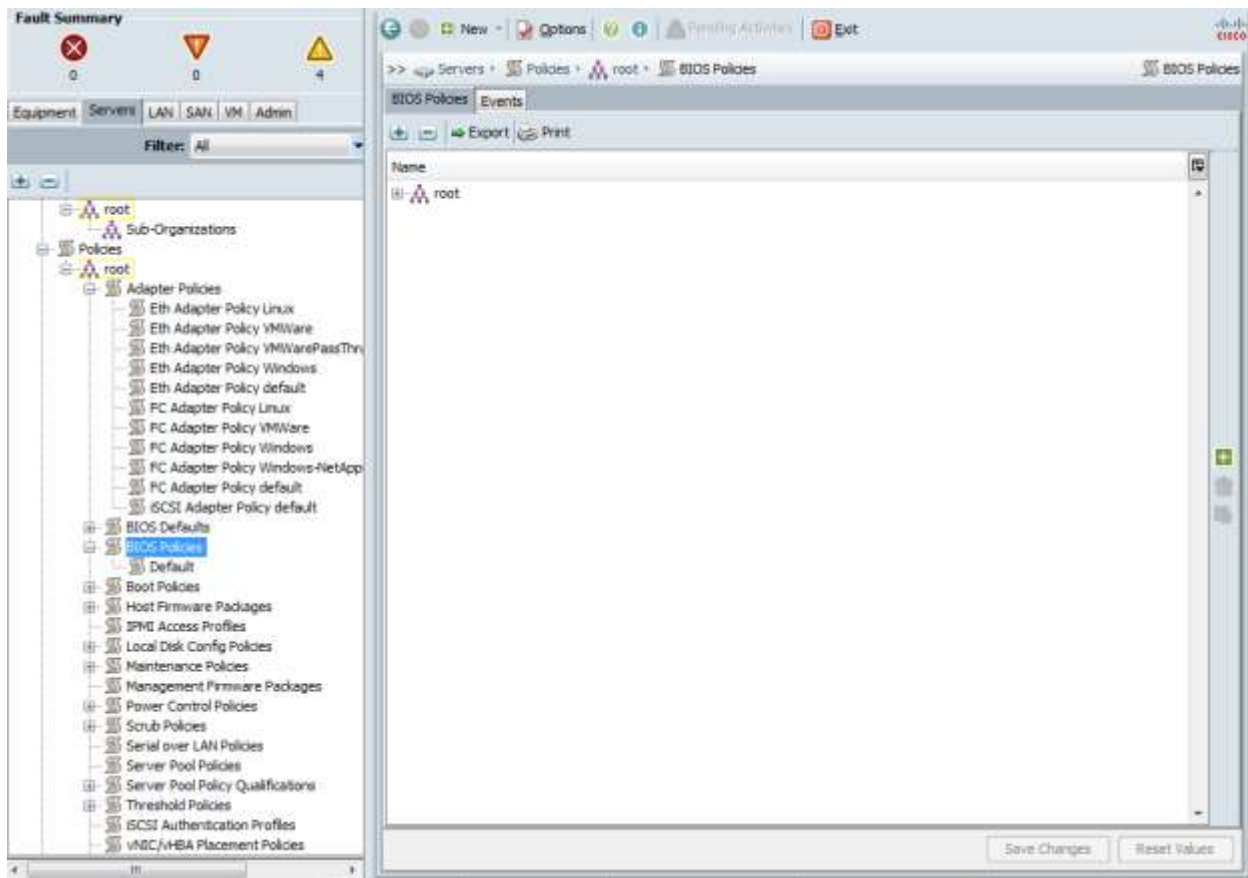
Create a Server BIOS Policy

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



Cisco UCS Manager

1. Select the **Servers** tab on the left of the window.
2. Go to **Policies > root**.
3. Right-click **BIOS Policies**.
4. Select **Create BIOS Policy**.
5. Enter **VM-Host-Infra** as the BIOS policy name.
6. Change the **Quiet Boot** property to **Disabled**.
7. Click **Finish** to complete creating the BIOS policy.
8. Click **OK**.





Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts

Cisco UCS Manager

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

Create Placement Policy

Create Placement Policy

Name: VM-Host-Infra

Filter

Export

Print

Virtual Slot	Selection Preference
1	All
2	All
3	Assigned Only
4	Exclude Dynamic
	Exclude Unassigned

OK

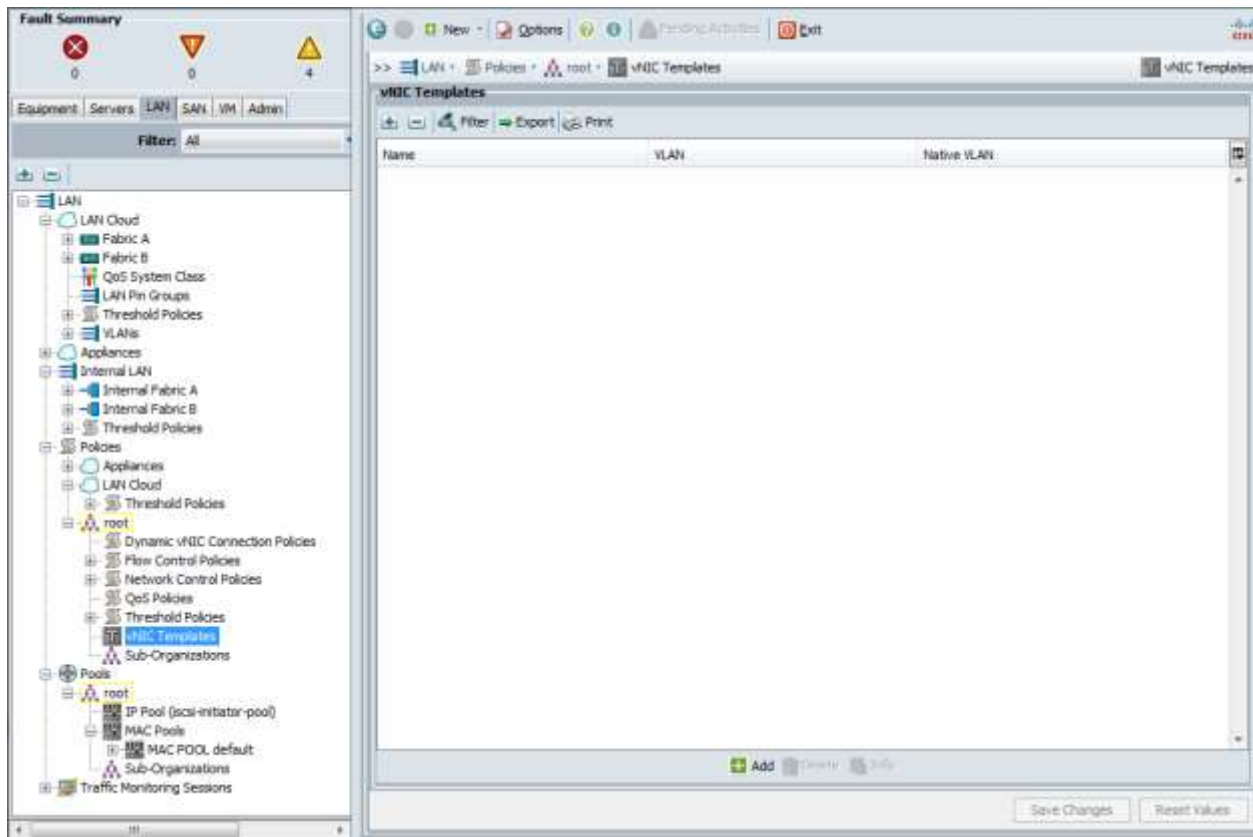
Cancel

Create a vNIC Template

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

Cisco UCS Manager

1. Select the `LAN` tab on the left of the window.
2. Go to `Policies > root`.
3. Right-click `vNIC Templates`.



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

Create vNIC Template

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
☐	default	☐
☐	App-Cluster-Comm	☐
☒	CSV-VLAN	☒
☐	LiveMigration-VLAN	☐

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: default

QoS Policy: CSV

Network Control Policy: <not set>

Pin Group: <not set>

Stats Threshold Policy: default

OK

Cancel

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

10. Go to Policies > root.

11. Right-click vNIC Templates.



12. Select `Create vNIC Template`.
13. Enter `LiveMigration` as the vNIC template name.
14. Check `Fabric B`. Check the `Enable Failover` box. Under `target`, unselect the `VM` box. Select `Updating Template` as the `Template Type`. Under `VLANs`, select `Live-Migration-VLAN` and set as `Native VLAN`. Under `MTU`, enter `9000`. Under `MAC Pool`:, select `Default`. 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
☐	default	☐
☐	CSV-VLAN	☐
☒	LiveMigration-VLAN	☒
☐	VM-Data-VLAN	☐

[+ 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:

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 VM-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 MAC_Pool.
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
☐	VM-Data-VLAN	☐
☒	VM-Mgmt-VLAN	☒
☐	iSCSI-Fabric-A	☐
☐	iSCSI-Fabric-B	☐

+ Create VLAN

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

OK Cancel

25. Select the LAN tab on the left of the window.
26. Go to Policies > root.



27. Right-click vNIC Templates.
28. Select Create vNIC Template.
29. Enter App-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 default.
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
☐	default	☐
☒	App-Cluster-Comm	☐
☐	CSV-VLAN	☐
☐	LiveMigration-VLAN	☐

Create VLAN

MTU:

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Stats Threshold Policy:

OK Cancel

33. Select the LAN tab on the left of the window.
34. Go to Policies > root.
35. Right-click vNIC Templates.



36. Select **Create vNIC Template**.
37. Enter **VM-Data** 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**. Do not set a **Native VLAN**. Under **MAC Pool**, select **Default**.
39. Click **OK** to complete creating the vNIC template.
40. Click **OK**.

Create vNIC Template

Name: **VM-Data**

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
☐	default	☐
☐	CSV-VLAN	☐
☐	LiveMigration-VLAN	☐
☒	VM-Data-VLAN	☐

+ Create VLAN

MTU: 1500

MAC Pool: default

QoS Policy: <not set>

Network Control Policy: <not set>

Pin Group: <not set>

Stats Threshold Policy: default

OK Cancel

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 iSCSI-A as the vNIC template name.
46. Check Fabric A. Uncheck the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select iSCSI-VLAN-A. Do not set a Native VLAN. Under MTU, enter 9000. Under MAC Pool, select MAC_Pool. Under QoS Policy, select iSCSI.
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
☐	PXE-Boot	☐
☐	VM-Data-VLAN	☐
☐	VM-Mgmt-VLAN	☐
☒	iSCSI-VLAN	☐

+ 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:

OK Cancel

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



50. Go to Policies > root.
51. Right-click vNIC Templates.
52. Select Create vNIC Template.
53. Enter iSCSI-B as the vNIC template name.
54. Check Fabric B. Uncheck the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select iSCSI-VLAN-B. Do not set a Native VLAN. Under MTU, enter 9000. Under MAC Pool, select MAC_Pool. Under QoS Policy, select iSCSI.
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
☐	PXE-Boot	☐
☐	VM-Data-VLAN	☐
☐	VM-Mgmt-VLAN	☐
☒	iSCSI-VLAN	☐

+ 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:

OK Cancel

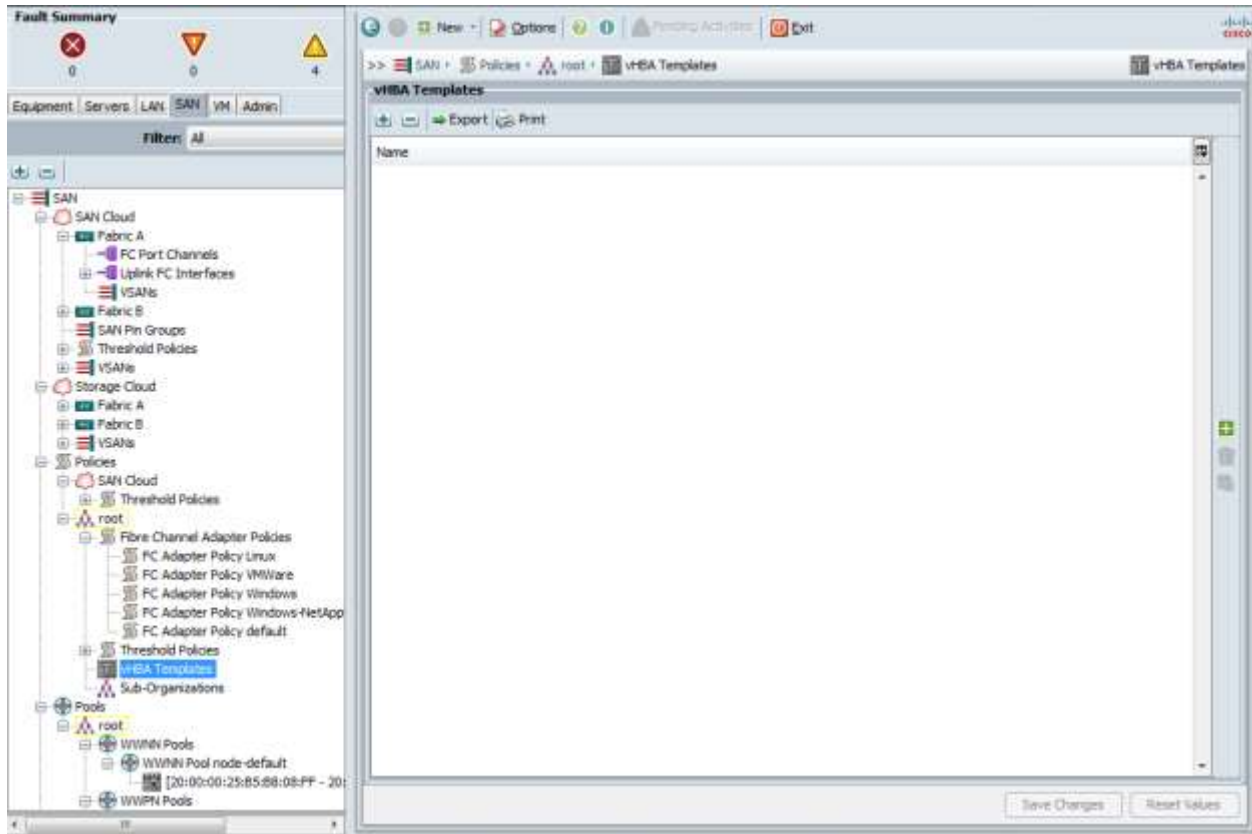
Create vHBA Templates for Fabric A and B

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

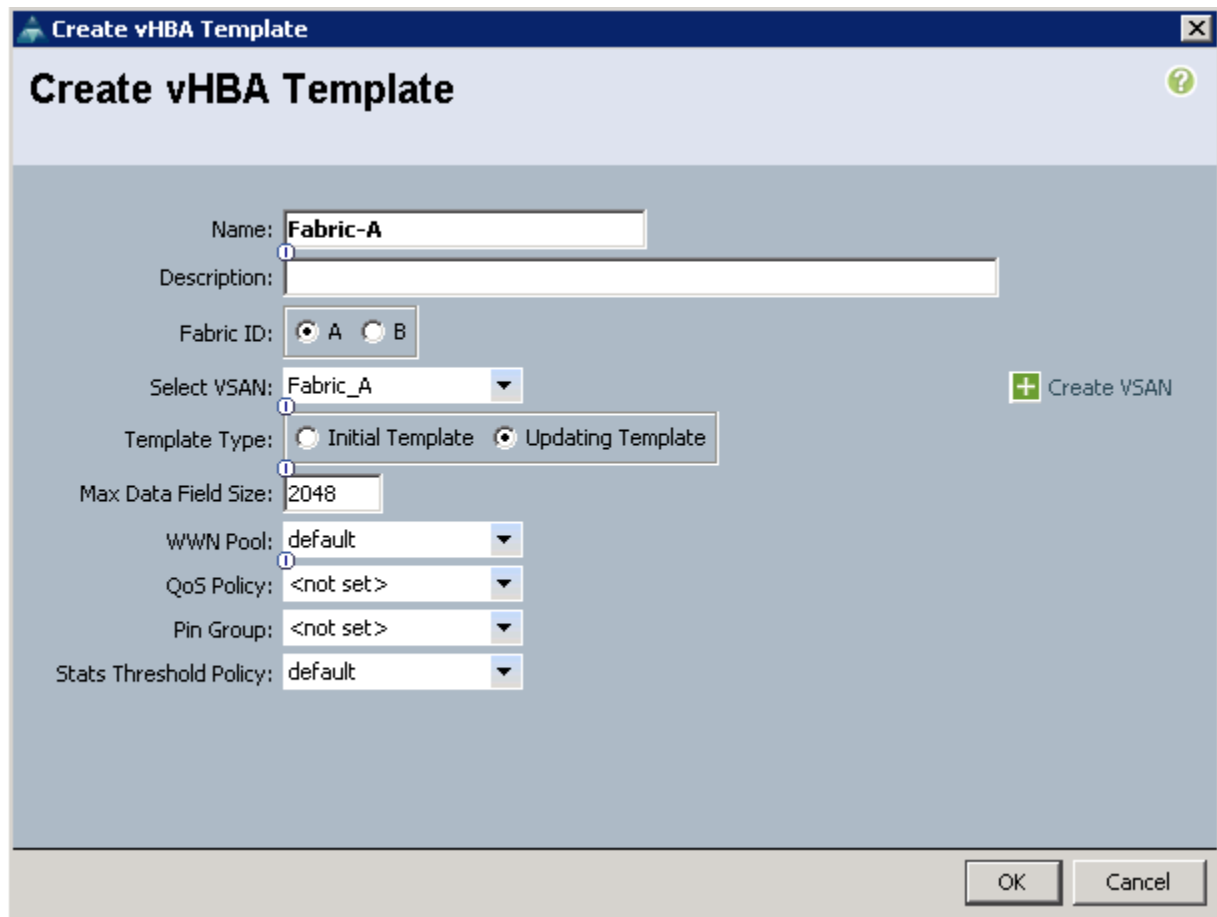


Cisco UCS Manager

1. Select the VSAN tab on the left of the window.
2. Go to Policies > root.
3. Right-click vHBA Templates.



4. Select Create vNIC Template.
5. Enter VHBA-Template-A as the vHBA template name.
6. Select Fabric A. Under Select VSAN, select VSAN_A. Under WWN Pool, select WWPN_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:

WWN Pool:

QoS Policy:

Pin Group:

Stats Threshold Policy:

OK Cancel

9. Select the VSAN tab on the left of the window.
10. Go to Policies > root.
11. Right-click vHBA Templates.
12. Select Create vHBA Template.
13. Enter VHBA-Template-B as the vHBA template name.
14. Select Fabric B. Under Select VSAN, select VSAN_B. Under WWN Pool, select WWPN_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:

WWN Pool:

QoS Policy:

Pin Group:

Stats Threshold Policy:

OK Cancel

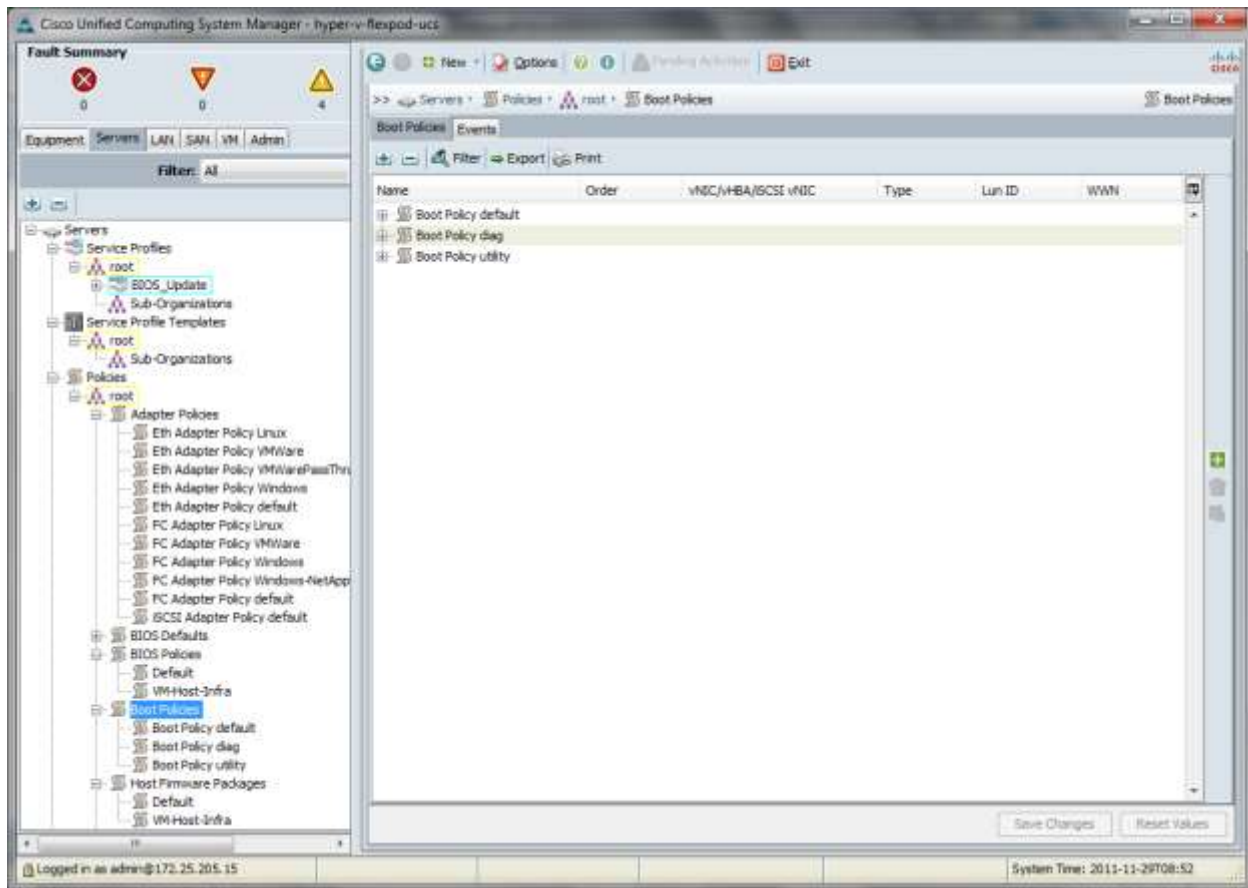
Create Boot Policies

These steps provide details for creating boot policies for the Cisco UCS environment. These directions apply to an environment in which each storage controller 0c port is connected to fabric A and each storage controller 0d port is connected to fabric B. In these steps, 2 boot policies will be configured. The first policy will configure the primary target to be controller A port 0c and the second boot policy primary target will be controller B port 0d.

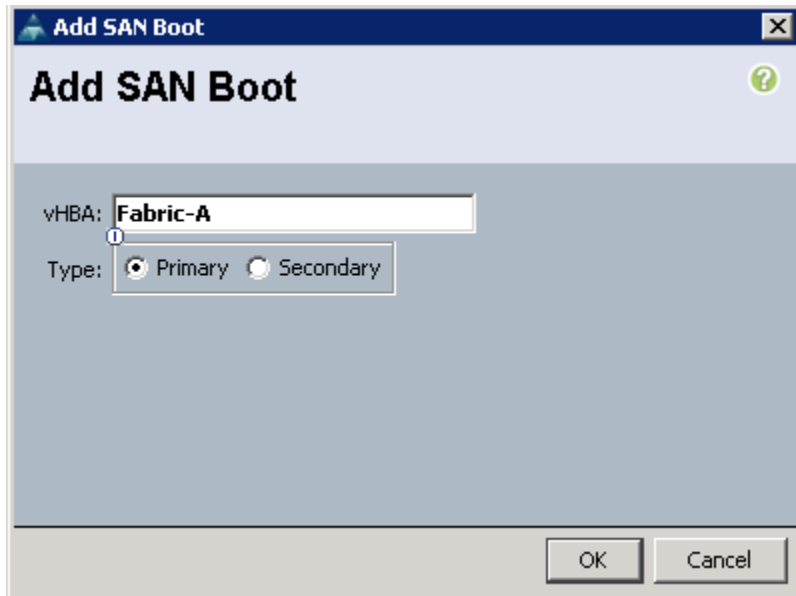
Note: If you are using FCoE between the Nexus 5548 and the NetApp Storage systems substitute port 2a for port 0c and port 2b for port 0d in this procedure.

Cisco UCS Manager

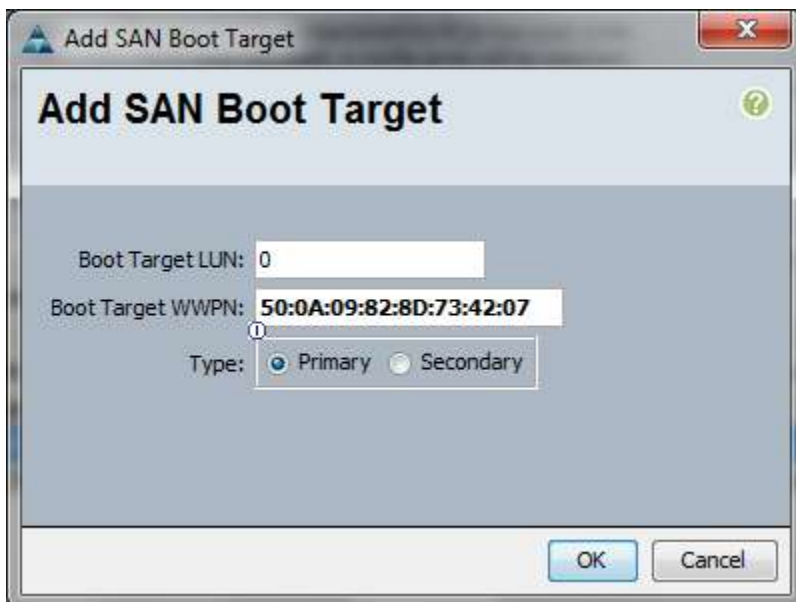
1. Select the **Servers** tab at the top left of the window.
2. Go to **Policies > root**.
3. Right-click **Boot Policies**.



4. Select Create Boot Policy.
5. Name the boot policy Boot-Fabric-A.
6. (Optional) Give the boot policy a description.
7. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
8. Expand the Local Devices drop-down menu and select Add CD-ROM.
9. Expand the vHBAs drop-down menu and select Add SAN Boot.
10. Enter Fabric-A in the vHBA field in the Add SAN Boot window that displays.
11. Make sure that Primary is selected as the type.
12. Click OK to add the SAN boot initiator.



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



18. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
19. Enter the WWPN for the primary FC adapter interface 0c of controller B. To obtain this information, log in to the controller B and run the `fcv show adapters` command.



20. Be sure to use the FC portname for port 0c and not the FC node name.

21. Click **OK** to add the SAN boot target.

The 'Add SAN Boot Target' dialog box is shown. It has a title bar with a close button. The main area contains the following fields and controls:

- Boot Target LUN:** A text box containing the value '0'.
- Boot Target WWPN:** A text box containing the value '50:0A:09:82:9D:73:42:07'. A small blue circle with the number '1' is next to this field.
- Type:** Two radio buttons labeled 'Primary' and 'Secondary'. The 'Secondary' radio button is selected.

At the bottom right, there are 'OK' and 'Cancel' buttons.

22. Select **Add SAN Boot** under the vHBA drop-down menu.

23. Enter **Fabric-B** in the vHBA field in the Add SAN Boot window that displays.

24. The type should automatically be set to **Secondary** and it should be grayed out. This is fine.

25. Click **OK** to add the SAN boot target.

The 'Add SAN Boot' dialog box is shown. It has a title bar with a close button. The main area contains the following fields and controls:

- vHBA:** A text box containing the value 'Fabric-B'. A small blue circle with the number '1' is next to this field.
- Type:** Two radio buttons labeled 'Primary' and 'Secondary'. The 'Secondary' radio button is selected.

At the bottom right, there are 'OK' and 'Cancel' buttons.

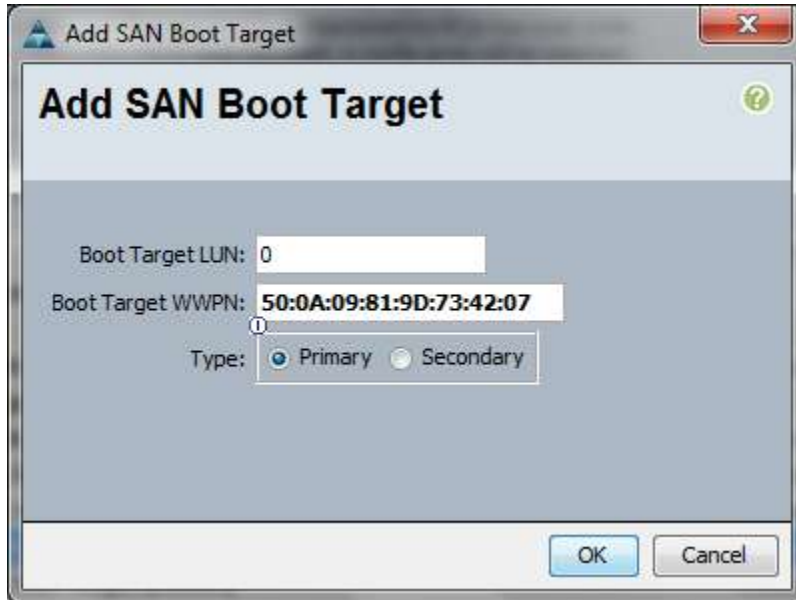
26. Select **Add SAN Boot Target** under the vHBA drop-down menu.

27. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.

28. Enter the WWPN for the primary FC adapter interface 0d of the controller B. To obtain this information, log in to controller B and run the `fcpl show adapters` command.



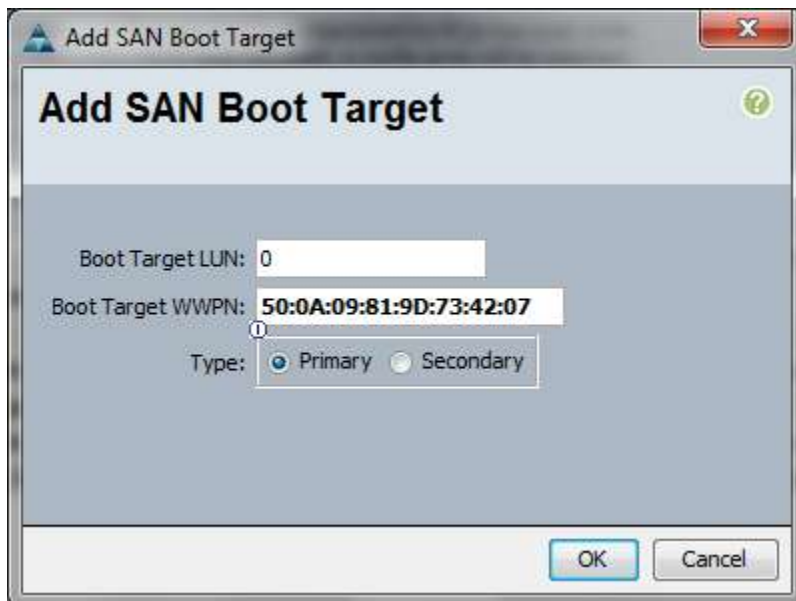
29. Be sure to use the FC portname for port 0d and not the FC node name.
30. Keep the type as Primary.
31. Click **OK** to add the SAN boot target.



The dialog box titled "Add SAN Boot Target" contains the following fields and controls:

- Boot Target LUN:** A text box containing the value "0".
- Boot Target WWPN:** A text box containing the value "50:0A:09:81:9D:73:42:07".
- Type:** A radio button group with two options: "Primary" (selected) and "Secondary".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

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 FC adapter interface 0d of controller A. To obtain this information, log in to controller A and run the `fcv show adapters` command.
34. Be sure to use the FC portname for port 0d and not the FC node name.
35. Click **OK** to add the SAN boot target.



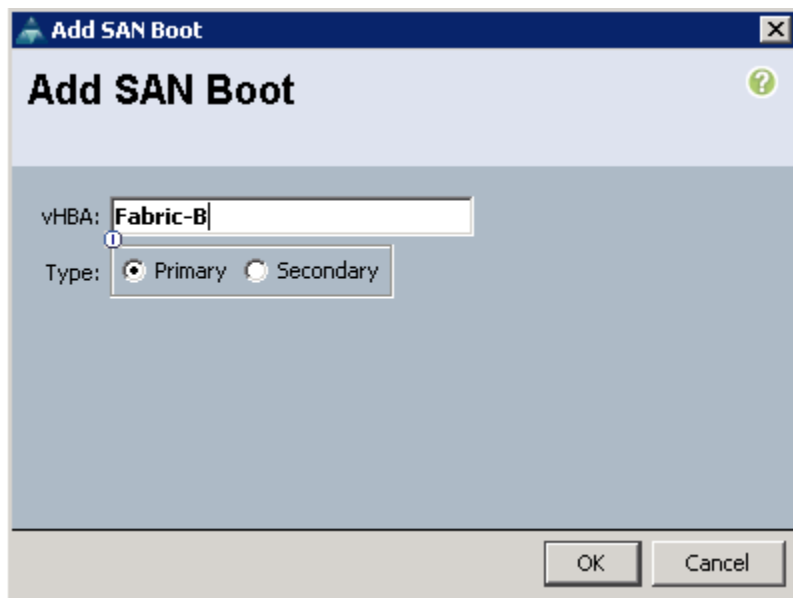
The dialog box titled "Add SAN Boot Target" contains the following fields and controls:

- Boot Target LUN:** A text box containing the value "0".
- Boot Target WWPN:** A text box containing the value "50:0A:09:81:9D:73:42:07".
- Type:** A radio button group with two options: "Primary" (selected) and "Secondary".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

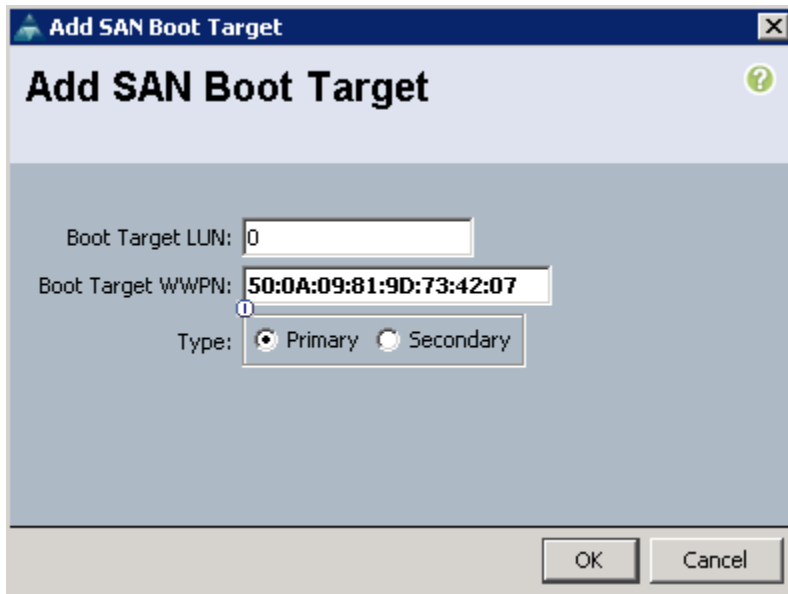


Creating Boot Policy for Fabric B

1. Right-click `Boot Policies` again.
2. Select `Create Boot Policy`.
3. Name the boot policy `Boot-Fabric-B`.
4. (Optional) Give the boot policy a description.
5. Leave `Reboot on Boot Order Change` and `Enforce vNIC/vHBA Name` unchecked.
6. Expand the `Local Devices` drop-down menu and select `Add CD-ROM`.
7. Click the `vHBA` drop-down menu and select `Add SAN Boot`.
8. Enter `Fabric-B` in the `vHBA` field in the `Add SAN Boot` window that displays.
9. Make sure that `Primary` is selected as the type.
10. Click `OK` to add the SAN boot target.

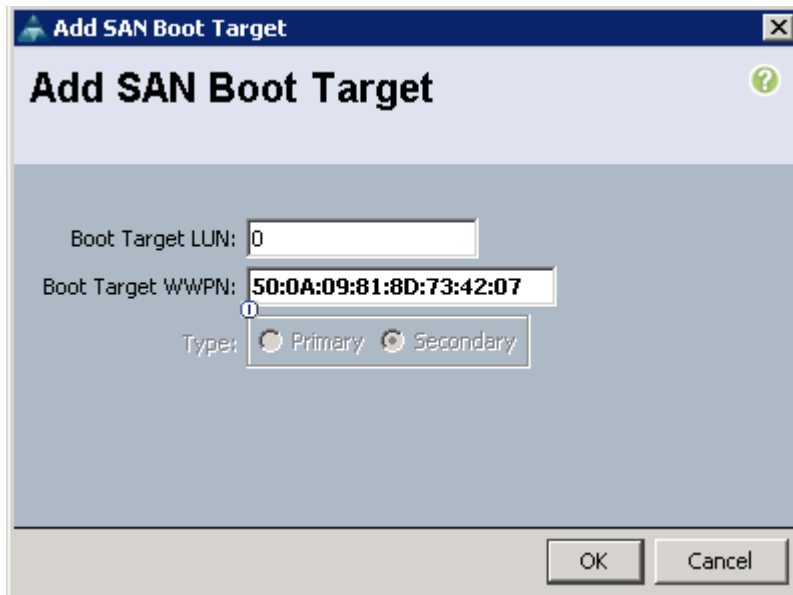


11. Under the `vHBA` drop-down menu, select `Add SAN Boot Target`. Keep the value for `Boot Target LUN` as `0`.
12. Enter the WWPN for the primary FC adapter interface `0d` of controller B. To obtain this information, log in to controller B and run the `fcv show adapters` command.
13. Be sure to use the FC portname for port `0d` and not the FC node name.
14. Keep the type as `Primary`.
15. Click `OK` to add the SAN boot target.



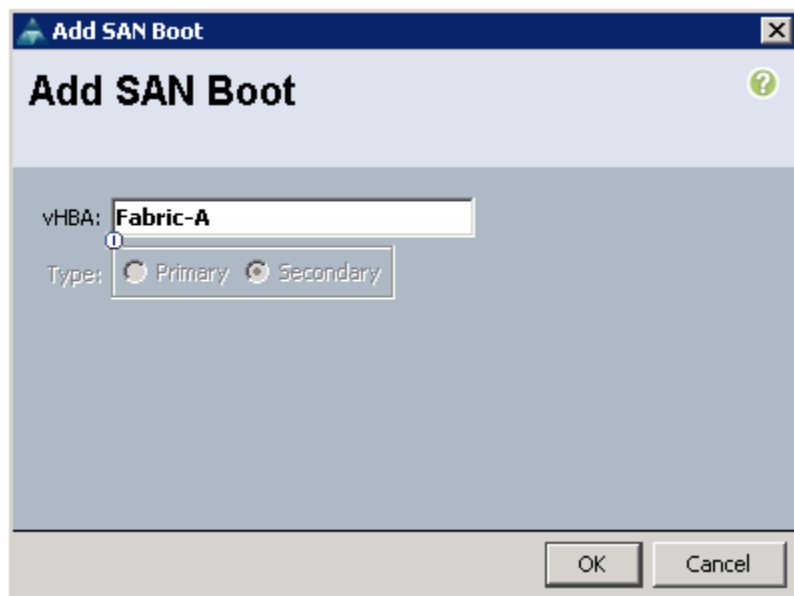
The dialog box titled "Add SAN Boot Target" has a title bar with a close button. The main area contains three fields: "Boot Target LUN:" with the value "0", "Boot Target WWPN:" with the value "50:0A:09:81:9D:73:42:07", and "Type:" with radio buttons for "Primary" (selected) and "Secondary". At the bottom right are "OK" and "Cancel" buttons.

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



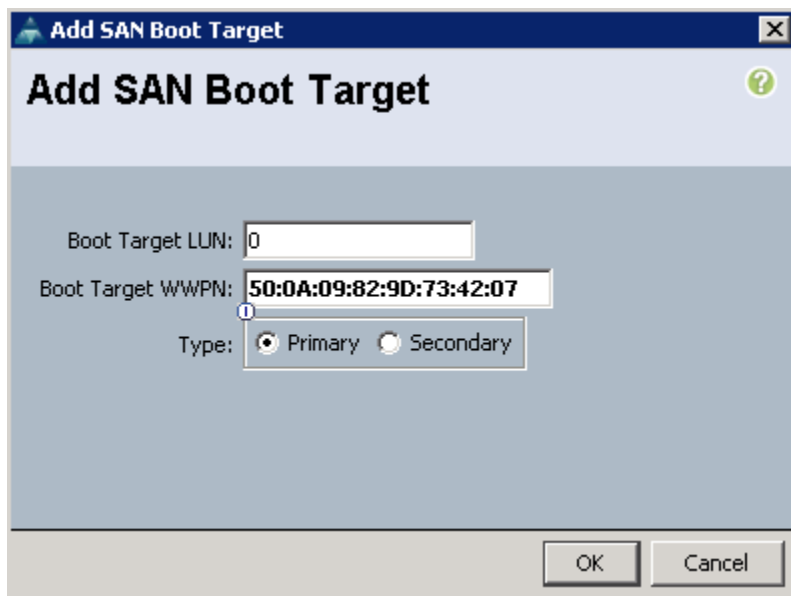
The dialog box titled "Add SAN Boot Target" has a title bar with a close button. The main area contains three fields: "Boot Target LUN:" with the value "0", "Boot Target WWPN:" with the value "50:0A:09:81:8D:73:42:07", and "Type:" with radio buttons for "Primary" and "Secondary" (selected). At the bottom right are "OK" and "Cancel" buttons.

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



The 'Add SAN Boot' dialog box has a title bar with a green icon, the text 'Add SAN Boot', and a close button. The main area has a light blue header with the title 'Add SAN Boot' and a green help icon. Below this, there is a 'vHBA:' label followed by a text box containing 'Fabric-A'. A small blue circle with the number '1' is next to the text box. Below the text box is a 'Type:' label followed by two radio buttons: 'Primary' and 'Secondary'. The 'Secondary' radio button is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

24. Select Add SAN Boot Target under the vHBA drop-down menu.
25. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.
26. Enter the WWPN for the primary FC adapter interface 0c of controller A. To obtain this information, log in to controller A and run the `fcv show adapters` command.
27. Be sure to use the FC portname for port 0c and not the FC node name.
28. Keep the type as Primary.
29. Click OK to add the SAN boot target.

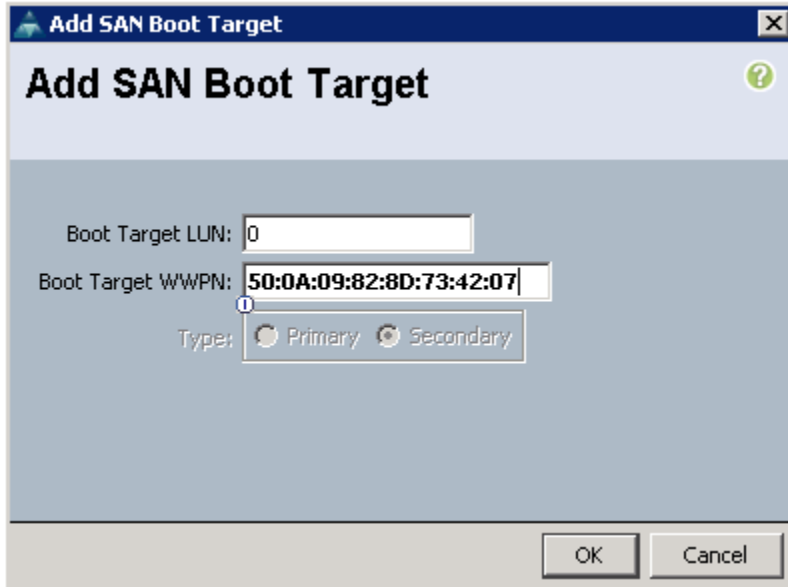


The 'Add SAN Boot Target' dialog box has a title bar with a green icon, the text 'Add SAN Boot Target', and a close button. The main area has a light blue header with the title 'Add SAN Boot Target' and a green help icon. Below this, there is a 'Boot Target LUN:' label followed by a text box containing '0'. Below that is a 'Boot Target WWPN:' label followed by a text box containing '50:0A:09:82:9D:73:42:07'. A small blue circle with the number '1' is next to the WWPN text box. Below the WWPN text box is a 'Type:' label followed by two radio buttons: 'Primary' and 'Secondary'. The 'Primary' radio button is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

30. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
31. Enter the WWPN for the primary FC adapter interface 0c of controller B. To obtain this information, log in to controller B and run the `fcv show adapters` command.



32. Be sure to use the FC portname for port 0c and not the FC node name.
33. Click **OK** to add the SAN boot target.



The image shows a Windows-style dialog box titled "Add SAN Boot Target". It has a blue header bar with the title and a close button. Below the header, the title "Add SAN Boot Target" is repeated in a larger font. The main area contains three input fields: "Boot Target LUN:" with the value "0", "Boot Target WWPN:" with the value "50:0A:09:82:8D:73:42:07", and "Type:" with two radio buttons, "Primary" (selected) and "Secondary". At the bottom right are "OK" and "Cancel" buttons.

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

Create Service Profile Templates

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

Cisco UCS Manager

1. Select the **Servers** tab at the top left of the window.
2. Go to **Service Profile Templates > root**.
3. Right-click **root**.
4. Select **Create Service Profile Template**.
5. The Create Service Profile Template window displays.
 - a. These steps detail configuration info for the **Identify the Service Profile Template** Section.
 - b. Name the service profile template **VM-Host-Infra-Fabric-A**. This service profile template is configured to boot from controller A port 0c.
 - c. Select **Updating Template**.
 - d. In the **UUID** section, select **UUID_Pool** as the UUID pool.
 - e. Click **Next** to continue to the next section.



6. Storage section

- a. Select `Default` for the Local Storage field.
- b. Select the appropriate local storage policy if the server in question does not have local disk.
- c. Select `SAN-Boot` for the local disk configuration policy.
- d. Select the `Expert` option for the How would you like to configure SAN connectivity field.
- e. In the `WWNN Assignment` field, select `WWNN_Pool`.
- f. Click the `Add` button at the bottom of the window to add vHBAs to the template.
- g. The `Create vHBA` window displays. Name the vHBA `Fabric-A`.
- h. Check the box for `Use SAN Connectivity Template`.
- i. Select `Fabric-A` in the `vHBA Template` field.
- j. Select `Windows-NetApp` in the `Adapter Policy` field.
- k. Click `OK` to add the vHBA to the template.



Create vHBA

Name:

Use SAN Connectivity Template: ☒

+ Create vHBA Template

vHBA Template:

Adapter Performance Profile

Adapter Policy: + Create Fibre Channel Adapter Policy

OK Cancel

7. Click the Add button at the bottom of the window to add vHBAs to the template.
8. The Create vHBA window displays. Name the vHBA Fabric-B.
9. Check the box for Use SAN Connectivity Template.
10. Select Fabric-B in the vHBA Template field.
11. Select Windows-NetApp in the Adapter Policy field.



12. Click **OK** to add the vHBA to the template.

The image shows a 'Create vHBA' dialog box with the following fields and options:

- Name:** Fabric-B
- Use SAN Connectivity Template:** ☒
- Create vHBA Template:** ☐
- vHBA Template:** Fabric-B
- Adapter Performance Profile:**
 - Adapter Policy:** Windows-NetApp
 - Create Fibre Channel Adapter Policy:** ☐

Buttons: OK, Cancel



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

The screenshot shows the 'Create Service Profile Template' wizard in the Unified Computing System Manager (UCSM). The 'Storage' section is active, showing options for local disk configuration and SAN connectivity. The 'Local Storage' is set to 'SAN-Boot' and the 'Mode' is 'No Local Storage'. The 'Protect Configuration' is set to 'no'. The 'How would you like to configure SAN connectivity?' section has 'Simple' selected. Below this, the 'World Wide Node Name' section shows a 'WWNN Assignment' of 'node-default(100/100)'. A table at the bottom lists the vHBAs created:

Name	WWNN
vHBA Fabric-A	Derived
vHBA Fabric-B	Derived

At the bottom of the wizard, there are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

14. Click Next to continue to the next section.
15. Networking Section
 - a. Leave the Dynamic vNIC Connection Policy field at the default.



- b. Select Expert for the How would you like to configure LAN connectivity? option.

- c. Click Add to add a vNIC to the template.
- d. The Create vNIC window displays. Name the vNIC CSV.
- e. Check the Use LAN Connectivity Template checkbox.
- f. Select CSV for the vNIC Template field.
- g. Select Windows in the Adapter Policy field.



- h. Click **OK** to add the vNIC to the template.

Create vNIC

Name:

Use LAN Connectivity Template: ☒

[+ Create vNIC Template](#)

vNIC Template:

Adapter Performance Profile

Adapter Policy: [+ Create Ethernet Adapter Policy](#)

OK **Cancel**

- i. Click **Add** to add a vNIC to the template.
- j. The **Create vNIC** window displays. Name the vNIC **LiveMigration**.
- k. Check the **Use LAN Connectivity Template** checkbox.
- l. Select **LiveMigration** for the vNIC Template field.
- m. Select **Windows** in the Adapter Policy field.



- n. Click **OK** to add the vNIC to the template.

Create vNIC

Name:

Use LAN Connectivity Template: ☒

+ Create vNIC Template

vNIC Template:

Adapter Performance Profile

Adapter Policy: + Create Ethernet Adapter Policy

OK Cancel

- o. Click **Add** to add a vNIC to the template.
- p. The **Create vNIC** window displays. Name the vNIC **VM-MGMT**.
- q. Check the **Use LAN Connectivity Template** checkbox.
- r. Select **VM-MGMT** for the vNIC Template field.
- s. Select **Windows** in the Adapter Policy field.



- t. Click **OK** to add the vNIC to the template.

Create vNIC

Name:

Use LAN Connectivity Template: ☒

+ Create vNIC Template

vNIC Template:

Adapter Performance Profile

Adapter Policy: + Create Ethernet Adapter Policy

OK Cancel

- u. Click **Add** to add a vNIC to the template.
- v. The **Create vNIC** window displays. Name the vNIC **AppApp-Cluster-Comm**.
- w. Check the **Use LAN Connectivity Template** checkbox.
- x. Select **AppApp-Cluster-Comm** for the vNIC Template field.
- y. Select **Windows** in the Adapter Policy field.
- z. Click **OK** to add the vNIC to the template.
- aa. Click **Add** to add a vNIC to the template.
- bb. The **Create vNIC** window displays. Name the vNIC **VM-Data**.
- cc. Check the **Use LAN Connectivity Template** checkbox.
- dd. Select **VM-Data** for the vNIC Template field.
- ee. Select **Windows** in the Adapter Policy field.



- ff. Click **OK** to add the vNIC to the template.

Create vNIC

Name: **VM-Data**

Use LAN Connectivity Template: ☒

+ Create vNIC Template

vNIC Template: **VM-Data**

Adapter Performance Profile

Adapter Policy: **Windows** **+ Create Ethernet Adapter Policy**

OK Cancel

- gg. Click **Add** to add a vNIC to the template.
- hh. The **Create vNIC** window displays. Name the vNIC **iSCSI-Fabric-A**.
- ii. Check the **Use LAN Connectivity Template** checkbox.
- jj. Select **iSCSI-Fabric-A** for the vNIC Template field.
- kk. Select **Windows** in the Adapter Policy field.



- II. Click **OK** to add the vNIC to the template.

Create vNIC

Name:

Use LAN Connectivity Template: ☒

+ Create vNIC Template

vNIC Template:

Adapter Performance Profile

Adapter Policy: + Create Ethernet Adapter Policy

OK Cancel

16. Click **Add** to add a vNIC to the template.
17. The **Create vNIC** window displays. Name the vNIC **iSCSI-Fabric-B**.
18. Check the **Use LAN Connectivity Template** checkbox.
19. Select **iSCSI-Fabric-B** for the vNIC Template field.
20. Select **Windows** in the Adapter Policy field.



21. Click **OK** to add the vNIC to the template.



The image shows a 'Create vNIC' dialog box with the following fields and options:

- Name:** iSCSI-Fabric-B
- Use LAN Connectivity Template:** ☒
- + Create vNIC Template** (button)
- vNIC Template:** iSCSI-Fabric-B (dropdown menu)
- Adapter Performance Profile** (section header)
 - Adapter Policy:** Windows (dropdown menu)
 - + Create Ethernet Adapter Policy** (button)

At the bottom right, there are **OK** and **Cancel** buttons.



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

The screenshot shows the 'Create Service Profile Template' wizard in the Unified Computing System Manager (UCSM). The 'Networking' section is active, showing a table of vNICs and options for LAN connectivity.

Create Service Profile Template

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

Networking
Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy:

How would you like to configure LAN connectivity? ☐ Simple ☐ Expert ☐ No vNICs

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
vNIC VM-Mgmt	Derived	derived	
vNIC VM-Data	Derived	derived	
vNIC CSV	Derived	derived	
vNIC LiveMigration	Derived	derived	
vNIC iSCSI-Fabric-A	Derived	derived	

iSCSI vNICs

< Prev Next > Finish Cancel

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

24. vNIC/vHBA Placement Section



25. Select the VM-Host-Infra Placement 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: **VM-Host-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

vNICs vHBAs

Name
iSCSI-Fabri...
iSCSI-Fabri...
VM-Mgmt
CSV
LiveMigrati...
App-Cluste...
VM-Data

>> assign >>
<< remove <<

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

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

- VM-Data
- App-Cluster-Comm
- LiveMigration
- CSV
- VM-Mgmt
- iSCSI-Fabric-A



- g. iSCSI-Fabric-B

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: VM-Host-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

vNICs

vHBAs

Name

>> assign >>

<< remove <<

Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
vCon 1		Assigned Only
vNIC VM-Data	1	
vNIC App-Cluster-Comm	2	
vNIC LiveMigration	3	
vNIC CSV	4	
vNIC VM-Mgmt	5	
vNIC iSCSI-Fabric-A	6	
vNIC iSCSI-Fabric-B	7	

▲ Move Up ▼ Move Down

27. Click the vHBA tab and add the vHBAs in the following order:
- Fabric-A
 - Fabric-B
28. Verify: Review the table to make sure that all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not



important.

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: VM-Host-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

vNICs

vHBAs

Name

>> assign >>

<< remove <<

Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
vNIC LiveMigration	3	
vNIC CSV	4	
vNIC VM-Mgmt	5	
vNIC iSCSI-Fabric-A	6	
vNIC iSCSI-Fabric-B	7	
vHBA Fabric-A	8	
vHBA Fabric-B	9	
vCon 2		All

▲ Move Up

▼ Move Down

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

30. Server Boot Order Section

- Select **Boot Fabric-A** in the **Boot Policy** field.
- 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.



- c. Click **Next** to continue to the next section.

Create Service Profile (expert)

Unified Computing System Manager

Create Service Profile (expert)

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

Server Boot Order

Optionally specify the boot policy for this service profile.

Select a boot policy.

Boot Policy: **Boot-Fabric-A**

Name: **Boot-Fabric-A**

Description:

Reboot on Boot Order Change: **no**

Enforce vNIC/vHBA/iSCSI Name: **no**

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

Boot Order

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN
CD-ROM	1				
Storage	2				
SAN primary		FC-Fabric-A	Primary		
SAN Target primary			Primary	0	50:0A:09:82:8D:73:42:07
SAN Target secondary			Secondary	0	50:0A:09:82:9D:73:42:07
SAN secondary		FC-Fabric-B	Secondary		
SAN Target primary			Primary	0	50:0A:09:81:8D:73:42:07
SAN Target secondary			Secondary	0	50:0A:09:81:9D:73:42:07

< Prev Next > Finish Cancel

31. Maintenance Policy Section

- a. Keep the default of no policy used by default.
- b. Click **Next** to continue to the next section.

32. Server Assignment Section

- a. Select **Default** in the **Pool Assignment** field.
- b. Select **VM-Host-Infra** for the **Server Pool Qualification** field.
- c. Select **Up** for the **power state**.
- d. Select **VM-Host-Infra** in the **Host Firmware** field.
- e. Select **VM-Host-Infra** in the **Management Firmware** field.



- f. Click **Next** to continue to the next section.

The screenshot shows the 'Create Service Profile Template' wizard in the Unified Computing System Manager (UCSM). The wizard is titled 'Unified Computing System Manager' and 'Create Service Profile Template'. On the left, a list of steps is shown: 1. Identify Service Profile Template, 2. Storage, 3. Networking, 4. vNIC/vHBA Placement, 5. Server Boot Order, 6. Maintenance Policy, 7. **Server Assignment**, and 8. Operational Policies. The main area is titled 'Server Assignment' and contains the following text: 'Optionally specify a server pool for this service profile template. You can select a server pool you want to associate with this service profile template.' Below this, there is a 'Pool Assignment' dropdown menu set to 'default', a 'Create Server Pool' button, and a 'Select the power state to be applied when this profile is associated with the server.' section with 'Up' and 'Down' radio buttons. Further down, it states: '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.' Below this, there is a 'Server Pool Qualification' dropdown menu set to 'VM-Host-Infra' and a 'Restrict Migration' checkbox. At the bottom, there is a 'Firmware Management (BIOS, Disk Controller, Adapter)' section with the text: 'If you select a host or management firmware policy for this service profile template, the profile will update the firmware on the server that is associated with. Otherwise the system uses the firmware already installed on the associated server.' Below this, there are two dropdown menus: 'Host Firmware' and 'Management Firmware', both set to 'VM-Host-Infra', each with a 'Create Firmware Package' button. At the bottom right, there are navigation buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

33. Operational Policies Section

- a. Select **VM-Host-Infra** in the **BIOS Policy** field.
- b. Expand **Power Control Policy Configuration**.
- c. Select **No-Power-Cap** in the **Power Control Policy** field.
- d. Click **Finish** to create the Service Profile template.



- e. Click OK in the pop-up window to proceed.

Create Service Profile Template

Unified Computing System Manager

Create Service Profile Template

1. ✓ Identify Service Profile Template
2. ✓ Storage
3. ✓ Networking
4. ✓ vNIC/vHBA Placement
5. ✓ Server Boot Order
6. ✓ Maintenance Policy
7. ✓ Server Assignment
8. ✓ 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)

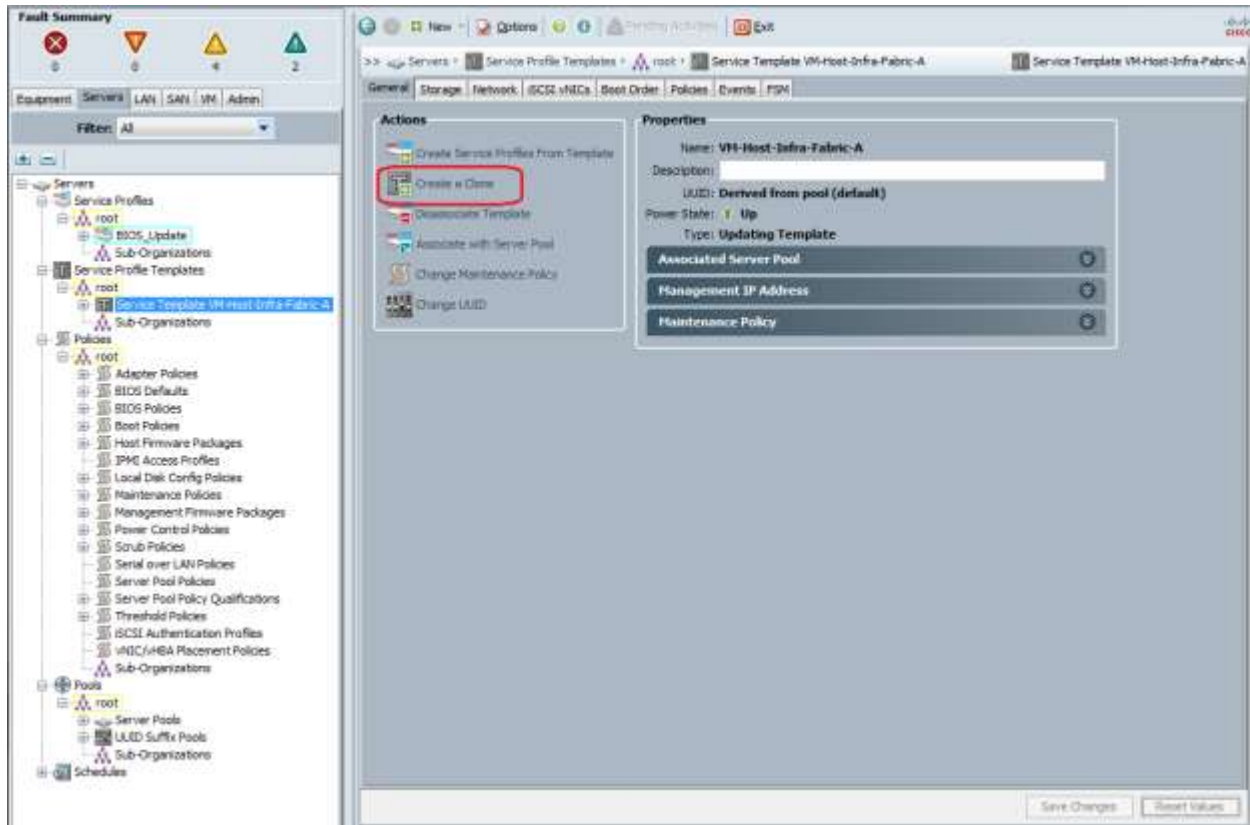
Power Control Policy Configuration

Scrub Policy

Scrub Policy: default Create Scrub Policy

< Prev Next > Finish Cancel

34. Select the Servers tab at the top left of the window.
35. Go to Service Profile Templates > root.
36. Select the previously created VM-Host-Infra-Fabric-A template
37. Click Create a Clone.



38. Enter VM-Host-Infra-Fabric-B in the Clone Name field and click OK.



39. Select the newly created service profile template and select the Boot Order tab.

40. Click Modify Boot Policy.

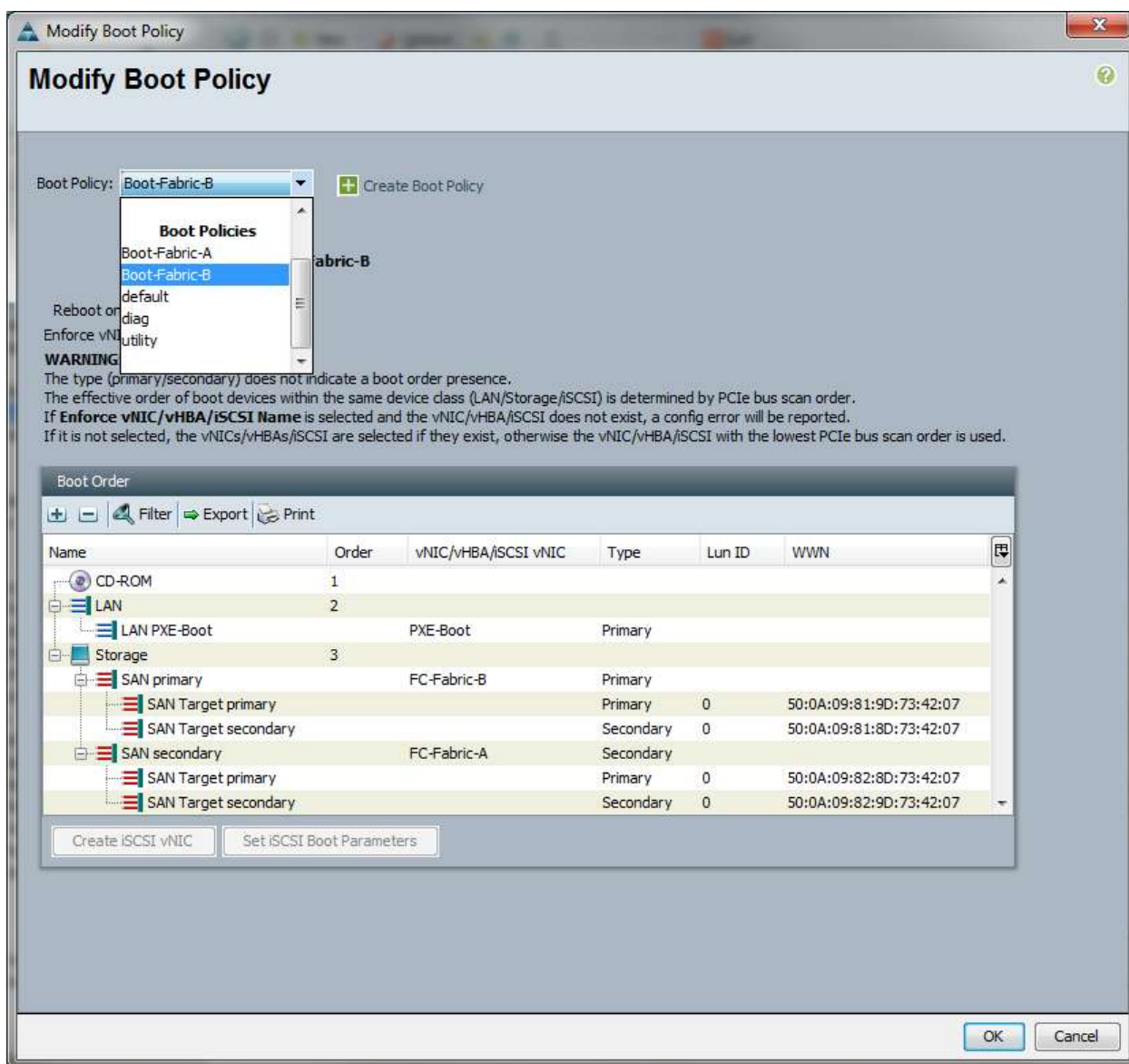


The screenshot shows the Cisco UCS Manager interface. On the left, a tree view under 'Policies' shows 'Boot Policies' expanded, with 'Boot Policy Boot-Fabric-A' selected. The main pane displays the 'Modify Boot Policy' dialog for 'Boot-Fabric-A'. The 'Boot Order' tab is active, showing a table of boot devices. The table has columns: Name, Order, vNIC/vHBA/SCSI vNIC, Type, Lun ID, and WWN. The boot order is as follows:

Name	Order	vNIC/vHBA/SCSI vNIC	Type	Lun ID	WWN
CD-ROM	1				
Storage	2				
SAN primary		PC-Fabric-A	Primary		
SAN Target primary			Primary	0	50:0A:09:62:80:73:42:07
SAN Target secondary			Secondary	0	50:0A:09:62:90:73:42:07
SAN secondary		PC-Fabric-B	Secondary		
SAN Target primary			Primary	0	50:0A:09:61:80:73:42:07
SAN Target secondary			Secondary	0	50:0A:09:61:90:73:42:07

Buttons at the bottom of the dialog include 'Create SCSI vNIC', 'Set SCSI Boot Policy', 'Save Changes', and 'Reset Values'.

41. Select Boot-Fabric-B Boot Policy and click OK.



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



Virtual Slot	Selection Reference	ID
1	Assigned Only	
2	All	
3	All	
4	All	

Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Native VLAN
vNIC VM-Mgmt	Derived	1	Unspecified	A B	1	Any	
Network VM-Mgmt-VLAN							
vNIC App-Cluster-Conn	Derived	2	Unspecified	B A	1	Any	
Network App-Cluster-Conn							
vNIC LiveMigration	Derived	3	Unspecified	B A	1	Any	
Network LiveMigration-VLAN							
vNIC CSW	Derived	4	Unspecified	A B	1	Any	
Network CSW-VLAN							
vNIC VM-Mgmt	Derived	5	Unspecified	A B	1	Any	
Network VM-Mgmt-VLAN							
vNIC SCSI-Fabric-A	Derived	6	Unspecified	A	1	Any	
Network SCSI-Fabric-A							
vNIC SCSI-Fabric-B	Derived	7	Unspecified	B	1	Any	
Network SCSI-Fabric-B							

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

Select Placement: VM-Host-Infra

Virtual Network Interfaces Policy (read only)

Name	Order	Selection Preference
vNIC VM-Mgmt	5	All
vNIC SCSI-Fabric-A	6	All
vNIC SCSI-Fabric-B	7	All
vNIC App-Cluster-Conn	8	All
vNIC LiveMigration	9	All
vHBA Fabric-B	10	All
vHBA Fabric-A	11	All

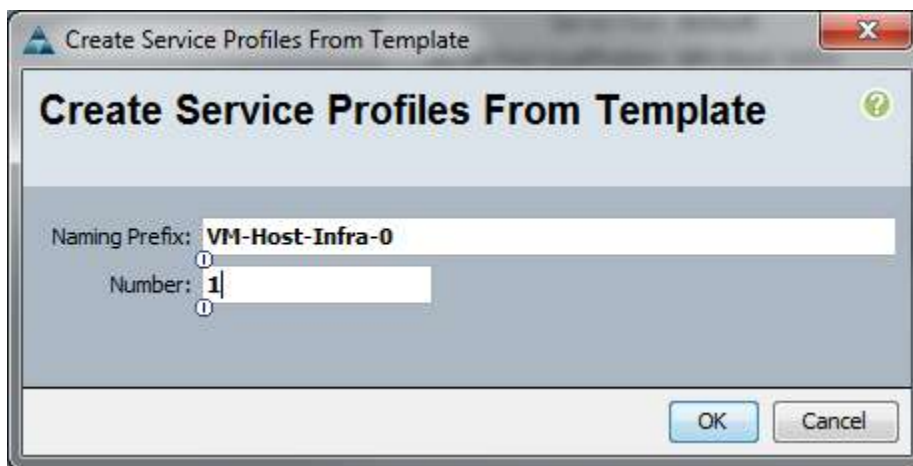


Create Service Profiles

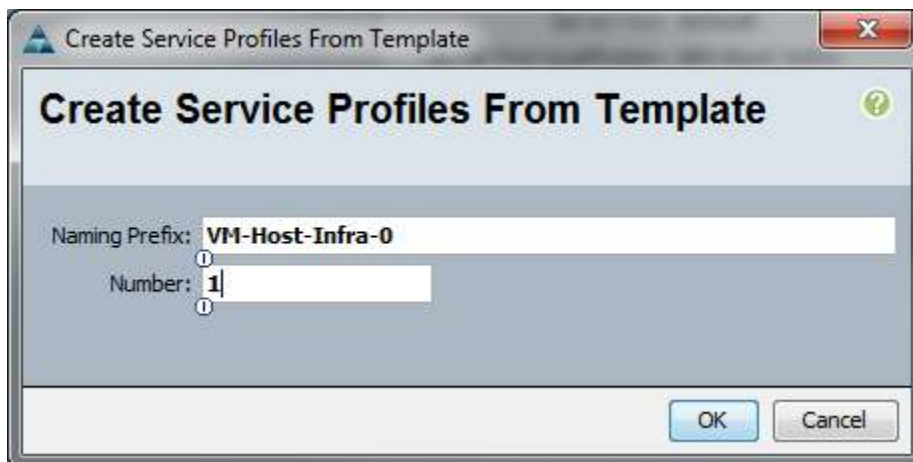
These steps provide details for creating a service profile from a template.

Cisco UCS Manager

1. Select the **Servers** tab at the top left of the window.
2. Select **Service Profile Templates VM-Host-Infra-Fabric-A**
3. Right-click and select **Create Service Profile From Template**.
4. Enter **VM-Host-Infra-0** for the service profile prefix.
5. Enter **1** for the number of service profiles to create.
6. Click **OK** to create the service profile.



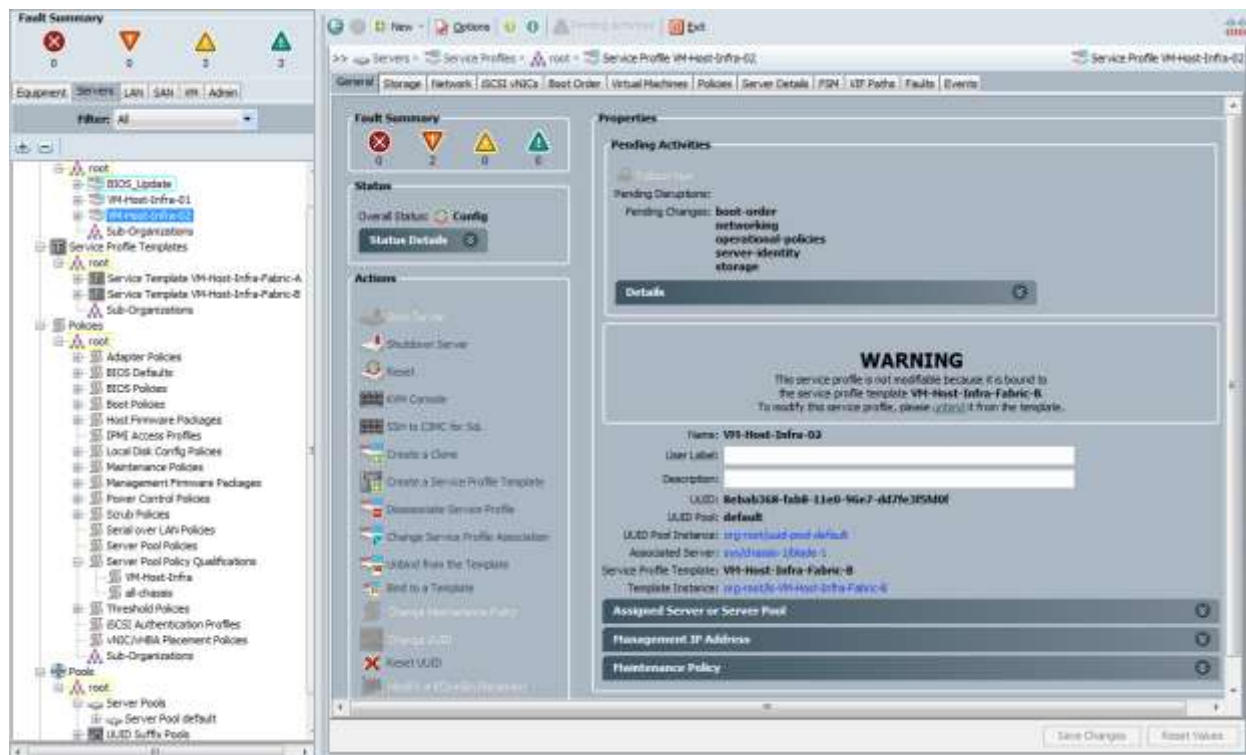
7. Click **OK** in the message box.
8. Select **Service Profile Templates VM-Host-Infra-Fabric-B**
9. Right-click and select **Create Service Profile From Template**.
10. Enter **VM-Host-Infra-0** for the service profile prefix.
11. Enter **1** for the number of service profiles to create.
12. Click **OK** to create the service profile.





13. Click OK in the message box.

14. Verify that Service Profiles VM-Host-Infra-01 and VM-Host-Infra-02 are created. The service profiles will automatically be associated with the servers in their assigned server pools.



15. Repeat steps x through 130 to create Service Profiles VM-Host-Infra-03 and VM-Host-Infra-04. The odd numbered service profiles are created from service profile template VM-Host-Infra-Fabric-A and the even numbered service profiles are created from service profile template VM-Host-Infra-Fabric-B

Add More Server Blades to the FlexPod Unit

Add server pools, service profile templates, and service profiles in the respective organizations to add more servers to the FlexPod unit. All other pools and policies are at the root level and can be shared among the organizations.

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 blade and from the NetApp controllers. Insert the required information in the tables below.

NetApp Controller	FC Port	FC Portname
Controller A	0c	
	0d	
Controller B	0c	



	0d	

Note: On each NetApp controller use `show fcp adapters` to gather the information above. If using FCoE between storage and the Cisco Nexus 5548s, substitute 2a for 0c and 2b for 0d.

Cisco UCS Service Profile Name	Fabric-A WWPN	Fabric-B WWPN
VM-Host-Infra-01		
VM-Host-Infra-02		
VM-Host-Infra-03		
VM-Host-Infra-04		

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.

Cisco Nexus 5548 Deployment Procedure: Part 2

These steps provide details for completing the configuration of the Nexus infrastructure for the FlexPod environment.

Create VSANs, Assign FC Ports, Turn on FC Ports

These steps provide details for configuring VSANs, assigning FC ports and enabling FC ports.

Note: This procedure sets up Fibre Channel connections between the Cisco Nexus 5548s and the NetApp storage systems. If you want to use FCoE connections between the Cisco Nexus 5548s and the NetApp storage systems using the NetApp Unified Target Adapter (UTA) use the Alternate Cisco Nexus 5548 Deployment Procedure: Part 2.

Cisco Nexus 5548 A

1. From the global configuration mode, type `interface san-port-channel 1`.
2. Type `channel mode active`.
3. Type `exit`.
4. Type `vsan database`.
5. Type `vsan <VSAN A ID> name Fabric_A`.
6. Type `vsan <VSAN A ID> interface fc1/29-32`.
7. Type `vsan <VSAN A ID> interface san-port-channel 1`.
8. Type `exit`.
9. Type `interface fc1/31-32`.
10. Type `channel-group 1 force`.
11. Type `no shutdown`.
12. Type `exit`.



13. Type `interface fc1/29-30`.
14. Type `no shutdown`.
15. Type `exit`.
16. Type `show int san-port-channel 1` to confirm connectivity.
17. Type `interface fc1/29`.
18. Type `switchport description <Controller A:0c>`.
19. Type `exit`.
20. Type `interface fc1/30`.
21. Type `switchport description <Controller B:0c>`.
22. Type `exit`.
23. Type `interface fc1/31`.
24. Type `switchport description <UCSM A:fc1/31>`.
25. Type `exit`.
26. Type `interface fc1/32`.
27. Type `switchport description <UCSM A:fc1/32>`.
28. Type `exit`.

Cisco Nexus 5548 B

1. From the global configuration mode, type `interface san-port-channel 2`.
2. Type `channel mode active`.
3. Type `exit`.
4. Type `vsan database`.
5. Type `vsan <VSAN B ID> name Fabric_B`.
6. Type `vsan <VSAN B ID> interface fc1/29-32`.
7. Type `vsan <VSAN B ID> interface san-port-channel 2`.
8. Type `exit`.
9. Type `interface fc1/31-32`.
10. Type `channel-group 2 force`.
11. Type `no shutdown`.
12. Type `exit`.
13. Type `interface fc1/29-30`.
14. Type `no shutdown`.
15. Type `exit`.
16. Type `show int san-port-channel 2` to confirm connectivity.
17. Type `interface fc1/29`.
18. Type `switchport description <Controller A:0d>`.
19. Type `exit`.
20. Type `interface fc1/30`.



21. Type `switchport description <Controller B:0d>`.
22. Type `exit`.
23. Type `interface fc1/31`.
24. Type `switchport description <UCSM B:fc1/31>`.
25. Type `exit`.
26. Type `interface fc1/32`.
27. Type `switchport description <UCSM B:fc1/32>`.
28. Type `exit`.

Create Device Aliases and Create Zones

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.

Cisco Nexus 5548 A

1. From the global configuration mode, type `device-alias database`.
2. Type `device-alias name VM-Host-Infra-01_A pwwn <Fabric-A WWPN>`.
3. Type `device-alias name VM-Host-Infra-02_A pwwn <Fabric-A WWPN>`.
4. Type `device-alias name controller_A_0c pwwn <Controller A 0c WWPN>`.
5. Type `device-alias name controller_B_0c pwwn <Controller B 0c WWPN>`.
Get this information from the table in section Gather Necessary Information.
6. After all of the necessary device-alias are created, type `exit`.
7. Type `device-alias commit`.
8. Create the zone for each service profile.
 - a. Type `zone name VM-Host-Infra-01_A vsan <Fabric A VSAN ID>`.
 - b. Type `member device-alias VM-Host-Infra-01_A`.
 - c. Type `member device-alias controller_A_0c`.
 - d. Type `exit`.
9. After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.
10. Create the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric A VSAN ID>`.
 - b. Type `member VM-Host-Infra-01_A`.
 - c. Type `exit`.
11. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan < Fabric A VSAN ID>`.
 - b. Type `exit`.
12. Type `copy run start`.



Cisco Nexus 5548 B

1. From the global configuration mode, type `device-alias database`.
 2. Type `device-alias name VM-Host-Infra-01_B pwwn <Fabric-B WWPN>`.
 3. Type `device-alias name VM-Host-Infra-02_B _B pwwn <Fabric-B WWPN>`.
 4. Type `device-alias name controller_A_0d pwwn <Controller A 0d WWPN>`.
 5. Type `device-alias name controller_B_0d pwwn <Controller B 0d WWPN>`.
- Get this information from the tables in the section Gather Necessary Information.
6. After all of the necessary device-alias are created, type `exit`.
 7. Type `device-alias commit`.
 8. Create the zones for each service profile.
 - a. Type `zone name VM-Host-Infra-02_B vsan <Fabric B VSAN ID>`.
 - b. Type `member device-alias VM-Host-Infra-02_B _B`.
 - c. Type `member device-alias controller_B_0d`.
 - d. Type `exit`.
 9. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
 10. Create the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `member VM-Host-Infra-02_B`.
 - c. Type `exit`.
 11. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `exit`.
 12. Type `copy run start`.

Storage

NetApp FAS3240

The following section provides a detailed procedure for configuring the NetApp FAS3240A for use in a FlexPod Validated with Microsoft Private Cloud environment. These steps should be followed precisely. Failure to do so could result in an improper configuration.

Note: The configuration steps detailed in this section provides guidance for configuring the FAS3240A running Data ONTAP 8.1

Assign Controller Disk Ownership

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

Controller A

1. During controller boot, when prompted for Boot Menu, press **CTRL-C**.
2. At the menu prompt, select option 5 for Maintenance mode boot.
3. Type **yes** if prompted with `Continue to boot?`



4. Type `disk show`. No disks should be assigned to the controller.
5. Refer to the `Local System ID:` value for the following disk assignment.
6. Half the total number of disks in the environment are assigned to this controller and half to the other controller. Divide the number of disks in half and use the result in the following command for the `<# of disks>`.
7. Assign disk to controller.

```
disk assign -n <# of disks>
```

8. Type `halt` to reboot the controller.
9. If the controller stops at a `LOADER-A>` prompt, type `autoboot` to start Data ONTAP.
10. During controller boot, when prompted, press `CTRL-C`.
11. At the menu prompt, select option 4 for clean configuration and initialize all disks.
12. The installer asks if you want to zero the disks and install a new file system. Answer `y`.
13. A warning is displayed that this will erase all of the data on the disks. Answer `y` that you are sure this is what you want to do.

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.

Controller B

1. During controller boot, when prompted for Boot Menu, press `CTRL-C`.
2. At the menu prompt, select option 5 for Maintenance mode boot.
3. Type `yes` if prompted with `Continue to boot?`
4. Type `disk show`. No disks should be assigned to the controller.
5. Refer to the `Local System ID:` value for the following disk assignment.
6. Half the total number of disks in the environment are assigned to this controller and half to the other controller. Divide the number of disks in half and use the result in the following command for the `<# of disks>`.
7. Assign disk to controller.

```
disk assign -n <# of disks>
```

8. Type `halt` to reboot the controller.
9. If the controller stops at a `LOADER-A>` prompt, type `autoboot` to start Data ONTAP.
10. During controller boot, when prompted, press `CTRL-C`.
11. At the menu prompt, select option 4 for clean configuration and initialize all disks.
12. The installer asks if you want to zero the disks and install a new file system. Answer `y`.
13. A warning is displayed that this will erase all of the data on the disks. Answer `y` that you are sure this is what you want to do.

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



The Setup Process

Configuration Worksheet

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

Configuration Worksheet	http://now.netapp.com/NOW/knowledge/docs/ontap/rel80/pdfs/ontap/setup.pdf	Requires access to now.netapp.com

Initial system setup is via the supplied serial cable to a PC with a serial port. When the system first boots, it will automatically run the setup program shown below. You can use this setup program to set up the initial networks and security settings before attaching the FAS series controllers to a production network. The setup script collects information to populate configuration files and to configure the installed functionality of your system. Connect to the controller's serial ports and start the setup process as shown below.

Controller A

1. After the disk initialization and the creation of the root volume, Data ONTAP setup begins.
2. Enter the hostname of the storage system.

```
Please enter the new hostname []: <<var_fas3240_a_hostname>>
```

3. Answer **n** for enabling ipv6.

```
Do you want to enable IPv6? [n]: n
```

4. Answer **y** for setting up interface groups.

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

5. Enter **1** for the number of interface groups to configure.

```
Number of interface groups to configure? [1] 1
```

6. Name the interface **vif0**.

```
Name of interface group #1 []: vif0
```

7. Enter **1** to specify the interface as LACP.

```
Is vif0 a single [s], multi [m] or a lacp [l] interface group? [] 1
```

8. Enter **i** to specify IP load balancing

```
Is vif0 to use IP-based [i], MAC-based [m], Round-robin based [r] or Port based [p] load balancing? [] i
```

9. Enter **2** for the number of links for **vif0**.

```
Number of links for vif0? [] 2
```

10. Enter **e2a** for the name of the first link.

```
Name of link #1 for vif0 [e0a]: e2a
```

11. Enter **e2b** for the name of the second link.

```
Name of link #1 for vif0 [e0a]: e2a
```



12. Enter the controller in-band management address when prompted for an IP address for vif0.

```
Please enter the IP address for Network Interface vif0 []:<<var_fas3240_a_vif0_ip>>
```

13. Enter the netmask for the controller in-band management address.

```
Please enter the netmask for Network interface e0M []:<<var_fas3240_a_vif0_netmask>>
```

14. Enter y for interface group vif0 taking over a partner interface.

```
Should interface vif0 take over a parnet IP address during failover? [n]: y
```

15. Enter vif0 for the name of the interface to be taken over.

```
Please enter the IP address of or interface name to be taken over by vif0 []: vif0
```

Press Enter to accept the blank IP address for e0a.

```
Please enter the IP address for Network Interface e0a [] [Enter]
```

16. Enter n for interface e0a taking over a partner interface.

```
Should interface e0a take over a partner IP address during failover? [n]: [Enter]
```

17. Press Enter to accept the blank IP address for e0b.

```
Please enter the IP address for Network Interface e0b [] [Enter]
```

18. Enter n for interface e0b taking over a partner interface.

```
Should interface e0b take over a partner IP address during failover? [n]: [Enter]
```

19. Enter the IP address of the out-of-band management interface, e0M.

```
Please enter the IP address for Network Interface e0M []:<<var_fas3240_a_mgmt_ip>>
```

20. Enter the subnet mask for e0M.

```
Please enter the netmask for Network interface e0M []:<<var_fas3240_a_mgmt0_netmask>>
```

21. Enter y for interface e0M taking over a partner IP address during failover.

```
Should interface e0M take over a parnet IP address during failover? [n]: y
```

22. Enter e0M for the name of the interface to be taken over.

```
Please enter the IP address of or interface name to be taken over by e0M []: e0m
```

Press Enter to accept the default flow control of full.

```
Please enter flow control for EOM [full]: [Enter]
```

23. Answer n to continuing setup through the Web interface.

```
Would you like to continue setup through the Web interface? [n]: n
```

24. Enter the IP address for the default gateway for the storage system.

```
Please enter the name or IP address of the Default Gateway []:<<var_fas3240_a_gateway>>
```

25. Enter the IP address for the administration host, or hit enters to allow all hosts.

```
Please enter the name of the administraton host: [Enter]
```

26. Enter the local timezone (for example, PST, MST, CST, or EST).

```
Please enter timezone []:<<var_fas3240_timezone>>
```

27. Enter the location for the storage system.



Where is the Filer Located ? [] [Enter]

28. Enter the language for multi-protocol files.

What language will be used for multi-protocol files (Type ? for list)?: <<var_fas3240_language>>

29. Answer **y** to enable DNS resolution.

Do you want to run DNS resolver? [n]: **y**

30. Enter the DNS domain name.

Please enter DNS domain name []:<<var_fas3240_dnsdomain>>

31. Enter the IP address for the first nameserver.

Please enter the IP address for first nameserver []:<<var_fas3240_dns1>>

32. Answer **y** to enter an alternate nameserver server.

Do you want another nameserver? [y]: **y**

33. Enter the IP address for the alternate nameserver.

Please enter the IP address for alternate nameserver []:<<var_fas3240_dns2>>

34. Answer **n** to finish entering DNS servers, or answer **y** to add up to two more DNS servers.

Do you want another nameserver? [n]: **n**

35. Answer **n** for running the NIS client.

Do you want to run NIS client? [n]: **n**

36. Press Enter to acknowledge the AutoSupport message.

37. Answer **y** to configuring the SP LAN interface.

The Service Processor (SP) provides remote management capabilities including console redirection, logging and power control. It also extends autosupport by sending additional system event alerts. Your autosupport settings are used for sending these alerts via email over the SP LAN interface.
Would you like to configure the SP LAN interface [y]: **y**

38. Answer **n** to setting up DHCP on the SP LAN interface.

Would you like to enable DHCP on the SP LAN interface [y]: **n**

39. Enter the IP address for the SP LAN interface.

Please enter the IP address for the SP: <<var_fas3240_a_sp_ip>>

40. Enter the subnet mask for the SP LAN interface.

Please enter the netmask for the SP []:<<var_fas3240_a_sp_netmask>>

41. Enter the IP address for the default gateway for the SP LAN interface.

Please enter the IP address for the SP gateway: <<var_fas3240_a_sp_gateway>>

42. Enter the fully qualified domain name for the mail host to receive SP messages and AutoSupport.

The mail host is required by your system to send SP alerts and local autosupport email.
Please enter the name or IP address of the mail host [mailhost]: <<var_fas3240_mailhost>>

43. Enter the new administrative (root) password.

44. Enter the new administrative (root) password again to confirm.



45. After these steps are completed, the controller should display a password prompt. Enter the administrative password to login as root.

Controller B

1. After the disk initialization and the creation of the root volume, Data ONTAP setup begins.
2. Enter the hostname of the storage system.

```
Please enter the new hostname []: <<var_fas3240_b_hostname>>
```

3. Answer n for enabling ipv6.

```
Do you want to enable IPv6? [n]: n
```

4. Answer y for setting up interface groups.

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

5. Enter 1 for the number of interface groups to configure.

```
Number of interface groups to configure? [1] 1
```

6. Name the interface vif0.

```
Name of interface group #1 []: vif0
```

7. Enter 1 to specify the interface as LACP.

```
Is vif0 a single [s], multi [m] or a lacp [l] interface group? [] 1
```

8. Enter i to specify IP load balancing

```
Is vif0 to use IP-based [i], MAC-based [m], Round-robin based [r] or Port based [p] load balancing? [] i
```

9. Enter 2 for the number of links for vif0.

```
Number of links for vif0? [] 2
```

10. Enter e2a for the name of the first link.

```
Name of link #1 for vif0 [e0a]: e2a
```

11. Enter e2b for the name of the second link.

```
Name of link #1 for vif0 [e0a]: e2a
```

12. Enter the controller in-band management address when prompted for an IP address for vif0.

```
Please enter the IP address for Network Interface vif0 []:<<var_fas3240_b_vif0_ip>>
```

13. Enter the netmask for the controller in-band management address.

```
Please enter the netmask for Network interface e0M []:<<var_fas3240_b_vif0_netmask>>
```

14. Enter y for interface group vif0 taking over a partner interface.

```
Should interface vif0 take over a parnet IP address during failover? [n]: y
```

15. Enter vif0 for the name of the interface to be taken over.

```
Please enter the IP address of or interface name to be taken over by vif0 []: vif0
```

Press Enter to accept the blank IP address for e0a.

```
Please enter the IP address for Network Interface e0a [] [Enter]
```

16. Enter n for interface e0a taking over a partner interface.



Should interface e0a take over a partner IP address during failover? [n]: **[Enter]**

Press Enter to accept the blank IP address for e0b.

Please enter the IP address for Network Interface e0b [] **[Enter]**

17. Enter n for interface e0b taking over a partner interface.

Should interface e0b take over a partner IP address during failover? [n]: **[Enter]**

18. Enter the IP address of the out-of-band management interface, e0M.

Please enter the IP address for Network Interface e0M []:<<var_fas3240_b_mgmt0_ip>>

19. Enter the subnet mask for e0M.

Please enter the netmask for Network interface e0M []:<<var_fas3240_b_mgmt0_netmask>>

20. Enter y for interface e0M taking over a partner IP address during failover.

Should interface e0M take over a partner IP address during failover? [n]: **y**

21. Enter e0M for the name of the interface to be taken over.

Please enter the IP address of or interface name to be taken over by e0M []: **e0m**

22. Press Enter to accept the default flow control of full.

Please enter flow control for EOM [full]: **[Enter]**

23. Answer n to continuing setup through the Web interface.

Would you like to continue setup through the Web interface? [n]: **n**

24. Enter the IP address for the default gateway for the storage system.

Please enter the name or IP address of the Default Gateway []:<<var_fas3240_b_gateway>>

25. Enter the IP address for the administration host, or hit enters to allow all hosts.

Please enter the name of the administrator host: **[Enter]**

26. Enter the local timezone (for example, PST, MST, CST, or EST).

Please enter timezone []:<<var_fas3240_timezone>>

27. Enter the location for the storage system.

Where is the Filer Located ? [] **[Enter]**

28. Enter the language for multi-protocol files.

What language will be used for multi-protocol files (Type ? for list)?: <<var_fas3240_language>>

29. Answer y to enable DNS resolution.

Do you want to run DNS resolver? [n]: **y**

30. Enter the DNS domain name.

Please enter DNS domain name []:<<var_fas3240_dnsdomain>>

31. Enter the IP address for the first nameserver.

Please enter the IP address for first nameserver []:<<var_fas3240_dns1>>

32. Answer y to enter an alternate nameserver server.

Do you want another nameserver? [y]: **y**



33. Enter the IP address for the alternate nameserver.

```
Please enter the IP address for alternate nameserver []:<<var_fas3240_dns2>>
```

34. Answer **n** to finish entering DNS servers, or answer **y** to add up to two more DNS servers.

```
Do you want another nameserver? [n]: n
```

35. Answer **n** for running the NIS client.

```
Do you want to run NIS client? [n]: n
```

36. Press Enter to acknowledge the AutoSupport message.

37. Answer **y** to configuring the SP LAN interface.

```
The Service Processor (SP) provides remote management capabilities
including console redirection, logging and power control.
It also extends autosupport by sending
additional system event alerts. Your autosupport settings are used
for sending these alerts via email over the SP LAN interface.
Would you like to configure the SP LAN interface [y]: y
```

38. Answer **n** to setting up DHCP on the SP LAN interface.

```
Would you like to enable DHCP on the SP LAN interface [y]: n
```

39. Enter the IP address for the SP LAN interface.

```
Please enter the IP address for the SP: <<var_fas3240_b_sp_ip>>
```

40. Enter the subnet mask for the SP LAN interface.

```
Please enter the netmask for the SP []:<<var_fas3240_b_sp_netmask>>
```

41. Enter the IP address for the default gateway for the SP LAN interface.

```
Please enter the IP address for the SP gateway: <<var_fas3240_b_sp_netmask>>
```

42. Enter the fully qualified domain name for the mail host to receive SP messages and AutoSupport.

```
The mail host is required by your system to send SP
alerts and local autosupport email.
Please enter the name or IP address of the mail host [mailhost]: <<var_fas3240_mailhost>>
```

43. Enter the new administrative (root) password.

44. Enter the new administrative (root) password again to confirm.

45. After these steps are completed, the controller should display a password prompt. Enter the administrative password to login as root.

Install Data ONTAP to Onboard Flash Storage

These steps provide details for installing Data ONTAP to the onboard flash storage.

Controller A and Controller B

Install the Data ONTAP image to the onboard flash device by using the `software install` and indicating the http or https Web address of the NetApp Data ONTAP 8.1 flash image.

```
Software install http://server/81_q_image.tgz
```

1. After this is complete, type `download` and press Enter to download the software to the flash device.

```
download
```



Harden Storage System Logins and Security

These steps provide details for hardening the storage system logins and security.

Controller A and Controller B

1. Disable all protocol access to the storage system.

```
secureadmin disable all
```

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

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

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

```
options ssh.idle.timeout 600
```

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

```
secureadmin setup -q ssl t US Wa Bellevue NetApp Eng FAS3210FT.example.com user@example.com
```

5. Use the following options configure and enable SSL and HTTPS for API access.

```
Options httpd.access none
```

The following steps provide details for adding VLAN interfaces on the storage controllers.

Controller A

1. Create iSCSI-A Vlan Interface.

```
vlan add vif0-<<var_iscsi_a_vlanid>>
```

2. Configure iSCSI-A Vlan Interface.

```
ifconfig          vif0-<<var_iscsi_a_vlanid>>          <<var_fas3240_a_iscsi_a_ip>>          netmask  
<<var_fas3240_a_iscsi_a_netmask>> mtusize <<var_iscsi_a_mtu>> partner vif0-<<var_iscsi_a_vlanid>>
```

3. Make new interface persistent by saving to the /etc/rc file.

```
wrfile -a /etc/hosts <<var_fas3240_a_iscsi_a_ip>>    <<var_fas3240_a_hostname>>--  
<<var_iscsi_a_vlanid>>  
wrfile -a /etc/rc vlan add vif0-<<var_iscsi_a_vlanid>>  
wrfile -a /etc/rc ifconfig vif0-<<var_iscsi_a_vlanid>> `hostname`-<<var_iscsi_a_vlanid>> netmask  
<<var_fas3240_a_iscsi_a_netmask>> mtusize <<var_iscsi_a_mtu>> partner vif0-<<var_iscsi_a_vlanid>>
```

4. Create iSCSI-B VLAN Interface.

```
vlan add vif0-<<var_iscsi_b_vlanid>>
```

5. Configure iSCSI-B VLAN Interface.

```
ifconfig          vif0-<<var_iscsi_b_vlanid>>          <<var_fas3240_a_iscsi_b_ip>>          netmask  
<<var_fas3240_a_iscsi_b_netmask>> mtusize <<var_iscsi_b_mtu>> partner vif0-<<var_iscsi_b_vlanid>>
```

6. Make new interface persistent by saving to the /etc/rc file.

```
wrfile -a /etc/hosts <<var_fas3240_a_iscsi_a_ip>>    <<var_fas3240_a_hostname>>--  
<<var_iscsi_b_vlanid>>  
wrfile -a /etc/rc vlan add vif0-<<var_iscsi_b_vlanid>>  
wrfile -a /etc/rc ifconfig vif0-<<var_iscsi_b_vlanid>> `hostname`-<<var_iscsi_b_vlanid>> netmask  
<<var_fas3240_a_iscsi_b_netmask>> mtusize <<var_iscsi_b_mtu>> partner vif0-<<var_iscsi_b_vlanid>>
```



Controller B

1. Create iSCSI-A Vlan Interface.

```
vlan add vif0-<<var_iscsi_a_vlanid>>
```

2. Configure iSCSI-A Vlan Interface.

```
ifconfig vif0-<<var_iscsi_a_vlanid>> <<var_fas3240_b_iscsi_a_ip>> netmask  
<<var_fas3240_b_iscsi_a_netmask>> mtusize <<var_iscsi_a_mtu>> partner vif0-<<var_iscsi_a_vlanid>>
```

3. Make new interface persistent by saving to the /etc/rc file.

```
wrfile -a /etc/hosts <<var_fas3240_b_iscsi_a_ip>> <<var_fas3240_b_hostname>>-  
<<var_iscsi_a_vlanid>>  
wrfile -a /etc/rc vlan add vif0-<<var_iscsi_a_vlanid>>  
wrfile -a /etc/rc ifconfig vif0-<<var_iscsi_a_vlanid>> `hostname`-<<var_iscsi_a_vlanid>> netmask  
<<var_fas3240_b_iscsi_a_netmask>> mtusize <<var_iscsi_a_mtu>> partner vif0-<<var_iscsi_a_vlanid>>
```

4. Create iSCSI-B VLAN Interface.

```
vlan add vif0-<<var_iscsi_b_vlanid>>
```

5. Configure iSCSI-B VLAN Interface.

```
ifconfig vif0-<<var_iscsi_b_vlanid>> <<var_fas3240_b_iscsi_b_ip>> netmask  
<<var_fas3240_b_iscsi_b_netmask>> mtusize <<var_iscsi_b_mtu>> partner vif0-<<var_iscsi_b_vlanid>>
```

6. Make new interface persistent by saving to the /etc/rc file.

```
wrfile -a /etc/hosts <<var_fas3240_b_iscsi_b_ip>> <<var_fas3240_b_hostname>>-  
<<var_iscsi_b_vlanid>>  
wrfile -a /etc/rc vlan add vif0-<<var_iscsi_b_vlanid>>  
wrfile -a /etc/rc ifconfig vif0-<<var_iscsi_b_vlanid>> `hostname`-<<var_iscsi_b_vlanid>> netmask  
<<var_fas3240_b_iscsi_b_netmask>> mtusize <<var_iscsi_b_mtu>> partner vif0-<<var_iscsi_b_vlanid>>
```

Install Required Licenses

These steps provide details about storage licenses that are used in this reference architecture for feature enablement.

Recommended licenses include:

- near_store: To enable the NearStore® personality on a controller
- a_sis: To enable advanced single instance storage availability
- cluster (cf): To configure storage controllers into an HA pair
- MultiStore: To enable secure tenant storage delegation.
- CIFS: To enable the CIFS protocol
- FCP: To enable the FCP protocol
- iSCSI: To enable the iSCSI protocol
- flash_cache: To enable usage of the Flash Cache module
- flex_clone: To enable the provisioning of NetApp FlexClone® volumes
- snapdrive_windows: To enable storage-based usage of NetApp SnapDrive® for Windows
- snapmanager_hyperv: To enable the use of NetApp SnapManager® for Microsoft Hyper-V

Note: If deduplication is required, license NearStore before licensing a_sis.

Controller A and Controller B

1. Add licenses to the storage system.



```
license add <necessary licenses>
```

2. Reboot the storage controller.

```
reboot
```

Configure SNMP

Controller A and Controller B

1. Create SNMP Requests Role and Assign SNMP Login Privileges

```
useradmin role add snmplogin -a login-snmp
```

2. Create SNMP Management Group and Assign SNMP Request Role

```
useradmin group add snmp -r snmplogin
```

3. Create SNMP User and Assign to SNMP Management Group

```
useradmin user add snmp -g snmp
```

Note: After the user is created, the system prompts for a password. Enter the SNMP password when prompted.

4. Set Up SNMP v1 Communities on Storage Controllers

```
snmp community delete all.  
snmp community add ro <<var_fas3240_snmp>>
```

5. Set up SNMP.

```
snmp                                contact                                "<<var_Customer_defined_SNMPContact>>"  
snmp location "<<var_Customer_defined_location>>"  
snmp init 1  
options snmp.enable on
```

Enable Flash Cache

This step provides details for enabling the NetApp Flash Cache module, if installed.

Controller A and Controller B

Enter the following command to enable Flash Cache on each controller:

```
options flexscale.enable on.
```

FCP and iSCSI Service

Controller A and Controller B

1. Start the iSCSI service and the FCP service.

```
fcv start  
iscsi start
```

2. Define the Fibre Channel Interfaces on the FAS controller to act as Target Devices instead of Initiator Devices.

```
fcadmin config -d 0c  
fcadmin config -t target 0c  
fcadmin config -e target 0c  
fcadmin config -d 0d
```



```
fcadmin config -t target 0d
fcadmin config -e 0d
```

- Record the WWPN for interfaces 0c and 0d by running:

```
fcportname show
```

- Reboot controller for change to take effect.

```
reboot
```

Set Up Storage System NTP Time Synchronization and CDP Enablement

These steps provide details for setting up storage system NTP time synchronization and the enablement of Cisco Discovery Protocol (CDP).

Controller A and Controller B

- Set the current date time on the controller.

```
date CCyyMMddhhmm
```

Note: CCyy is the four-digit year, MM is the two-digit month, dd is the two-digit day of the month, hh is the two-digit hour, and mm is the two-digit minute.

- Configure NTP to sync with windows.

```
options timed.proto ntp
options timed.servers <<var_fas3240_dnsdomain>>
options timed.enable on
```

- Enable CDP.

```
options cdpd.enable on
```

Enable Active-Active Controller Configuration Between Two Storage Systems

This step provides details for enabling active-active controller configuration between the two storage systems.

Controller A

- Enable active-active controller configuration.

```
Cf enable
```

Joining a Windows Domain

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

Controller A and Controller B

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

```
CIFS setup
Do you want to make the sysmt visible via WINS? [N] n
Choose (2) NTFS-only filer [2] 2
Enter the password for the root user []: <<var_root_password>>
Reenter the password: <<var_root_password>>
Would you like the change this name? [n]: Enter
Choose (1) Active Directory Domain Authentication : 1 Enter
Configure the DNS Resolver Service ?[y]: y
What is the filers DSN Domain name? []: <<var_fas3240_dnsdomain>>
What the IPv4 Addresses of your Authoritative DNS servers? []: <<var_ip_DNSserver>>
```



```
What is the name of the Active Directory Domain Controller? : <<var_fas3240_dnsdomain>>
Would you like to configure time services? [y]: [Enter]
Enter the time server host []:<<var_fas3240_dnsdomain>>
Enter the ame of the windows user [administrator@<<var_fas3240_dnsdomain>>] [Enter]
Password for <<var_domainAccountUsed>>: <<password>>
Choose (1) Create the filers machine account in the "computers" container: 1
Do you want to configure a <<var_ntap_hostname>>/administrator account [Y]: [Enter]
Password for the <<var_ntap_hostname>>/Administrator <<var_password>> [Enter]
Would you like to specify a user or group that can administer CIFS [n]: [Enter]
```

Create Data Aggregate aggr1

This step provides details for creating the data aggregate.

Note: In most cases, the following command finishes quickly, but depending on the state of each disk, it might be necessary to zero some or all of the disks in order to add them to the aggregate. This might take up to 60 minutes to complete.

Controller A and Controller B

```
aggr create <<var_aggr01>> -r 22 -B 64 44
```

Note: Above command assumes base configuration with x4 DS2246 disk shelves. If installing a larger environment adjust accordingly.

Add Infrastructure Volumes

Controller A

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

```
vol create ucs_boot -s none aggr1 1t
vol create hyperv_quorum -s none aggr1 10g
```

2. Configure volume dedupe.

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

3. Create a Qtree to house the goldmaster boot LUN, and Cluster Quorum.

```
qtree create /vol/ucs_boot/goldmaster
qtree create /vol/hypervft_quorum/cluster1
```

4. Create the goldmaster initiator group, create the goldmaster LUN and map that LUN to the iGroup.

```
igroup create -f -t windows goldmaster
lun create -s 120g -t windows_2008 -o noreserve /vol/ucs_boot/goldmaster/goldmaster.lun
lun map /vol/ucs_boot/goldmaster/goldmaster.lun goldmaster 0
```

Controller A

1. Create a 500GB FlexVol volume in Aggr1 to host the management infrastructure virtual machines.

```
vol create fabric_mgmt_csv -s none aggr1 5t
```

2. Configure dedupe.

```
sis config -s auto /vol/mgmt_infra_csv
sis on /vol/mgmt_infra_csv
sis start -s /vol/mgmt_infra_csv
```

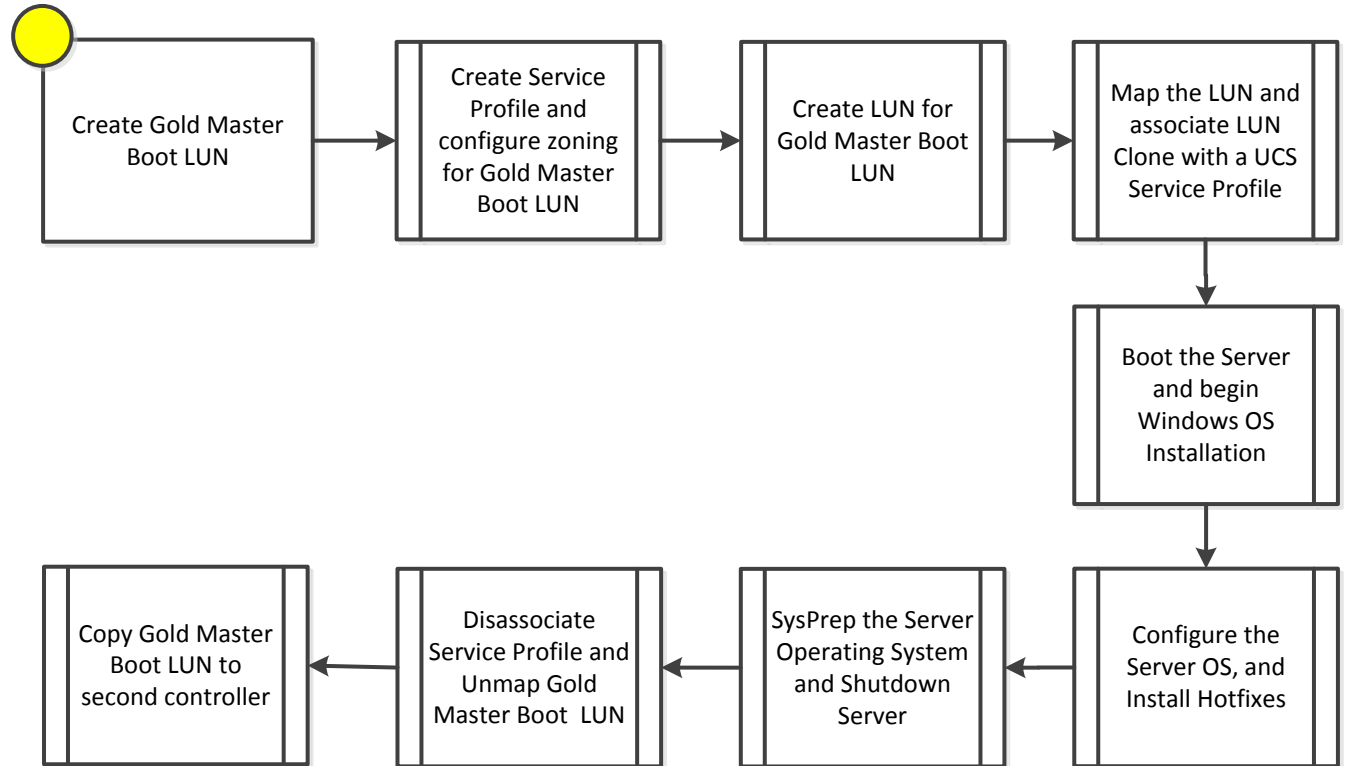


3. Create a Qtree to house the management infrastructure CSV LUN.

```
qtree create /vol/mgmt_infra_csv/csv01
```

Create Gold Master Boot LUN

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



Overview

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

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

- NetApp PowerShell Toolkit 1.7 or higher installed on an administrative host
- Access to Windows 2008R2 installation ISO image
- Access to Cisco UCS FCoE driver installation ISO image



- Access to Cisco UCS Ethernet driver installation ISO image

Creation of Gold Master Boot LUN Workflow

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

Perform the following PowerShell commands with an account that has local administrator rights on the NetApp **Controller A** storage controller.

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

```
import-module dataontap
```

Connect to the NetApp controller:

```
connect-nacontroller <<var_ntap_A_hostname>> -credential root
```

Create the NetApp flexible volume that will store the Gold Master Boot LUN.

```
new-navol ucsboot aggr1 500g
```

Set the NetApp flexible volume options that will store the Gold Master Boot LUN.

```
set-navoloption ucs_boot create_ucose on  
set-navoloption ucs_boot convert_ucose on  
set-navoloption fractional_reserve 0
```

```
set-nasnapshotschedule ucs_boot -Weeks 0 -Days 0 -Hours 0 -Minutes 0  
set-nasnapshotsreserve ucs_boot 0
```

```
new-naqtree /vol/ucs_boot/goldmaster
```

Create the NetApp LUN for the Gold Master Boot LUN.

```
new-nalun /vol/ucs_boot/goldmaster/goldmaster.lun 130g -type windows_2008 -unreserved
```

Perform the following PowerShell commands with an account that has local administrator rights on the NetApp **Controller B** storage controller.

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

```
import-module dataontap
```

Connect to the NetApp controller:

```
connect-nacontroller <<var_ntap_B_hostname>> -credential root
```

Create the NetApp flexible volume that will store the Gold Master Boot LUN.

```
new-navol ucsboot aggr1 500g
```




Set the NetApp flexible volume options that will store the Gold Master Boot LUN.

```
set-navoloption ucs_boot create_ucose on  
set-navoloption ucs_boot convert_ucose on  
set-navoloption fractional_reserve 0
```

```
set-nasnapshotschedule ucs_boot -Weeks 0 -Days 0 -Hours 0 -Minutes 0  
set-nasnapshotreserve ucs_boot 0
```

We will not create another Gold Master Boot LUN on NetApp Controller B. When the Gold Master Boot LUN is created on Controller A, the Gold Master Boot LUN will be copied via ndmp to Controller B.

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 object.
3. Right-click <<Service_Template_Fabric_A>> and select the action "Create Service Profiles From Template".
4. Enter goldmaster_<<Hyper-V_A_hostname>> for the service profile suffix.
5. Enter 1 for the number of service profiles to create.
6. Select <<Hyper_A_Template>> for the Service Profile Template field. It should be under Organizations > root.
7. Click OK to create the service profile, and OK again to acknowledge the creation.
8. Select the newly created service profile, and select the Boot Order tab at the top right.
9. Click the Modify Boot Policy link at the top right.
10. Select the initial_<<Hyper-V_A_hostname>> boot policy, and click OK > OK to acknowledge the action.
11. From the left hand management pane expand initial_<<Hyper-V_A_hostname>> > vHBAs.
12. Select vHBA vHBA_A and write down the WWPN.
13. Log in to the <<var_ntap_A_hostname>> controller with PowerShell.
14. Add the WWPN to the goldmaster igroup.

Perform the following PowerShell commands with an account that has local administrator rights on the NetApp **Controller A** storage controller.

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

```
import-module dataontap
```

Connect to the NetApp controller:

```
connect-nacontroller <<var_ntap_A_hostname>> -credential root
```

Create the NetApp igroup for the Gold Master Boot LUN.

```
new-naigroup goldmaster fcp windows  
set-naigroup goldmaster alua true
```

Add the WWPN from the <<vHBA_A>> vHBA in the goldmaster_<<Hyper-V_A_hostname>> service profile to the Gold Master Boot LUN igroup.

```
add-naigroupinitiator goldmaster <vHBA_A WWPN>
```



Map the igroup to the Gold Master Boot LUN.

```
add-nalunmap /vol/ucs_boot/goldmaster/goldmaster.lun goldmaster
```

15. While connected to the <<var_ntap_A_hostname>> issue the following command to retrieve the WWPN for the 0c interface.

```
get-nafcpcadapter 0c
```

16. Create the device alias for goldmaster_<<var_ntap_a_hostname>>_A using the WWPN recorded above. Create the zone for the goldmaster_<<var_ntap_A_hostname>> service profile.

Using an ssh client, log into the Cisco Nexus 5548 A - <<var_nexus_A_hostname>> with administrative rights on the switch.

```
configure terminal
device-alias database
device-alias name goldmaster_<<Hyper-V_A_hostname>>_A pwwn <vHBA_A WWPN>
device-alias name goldmaster_<<var_ntap_A_hostname>>_A pwwn <HBA_0c WWPN>
exit
device-alias commit
```

```
zone name goldmaster_<<Hyper-V_A_hostname>>_A vsan 1
member device-alias goldmaster_<<Hyper-V_A_hostname>>_A
member device-alias goldmaster_<<var_ntap_A_hostname>>_A
exit
```

17. After the device aliases and the goldmaster zone for the goldmaster_<<Hyper-V_A_hostname>> service profile have been created, create a zoneset to organize and manage them.

18. Create the zoneset and add the necessary members.

```
zoneset name Hyper-V_FastTrack vsan 1
member goldmaster_<<Hyper-V_A_hostname>>_A
exit
```

19. Activate the zoneset.

```
zoneset activate name Hyper-V_FastTrack vsan 1
zoneset distribute full vsan 1
exit
copy run start
```

20. Back in UCSM, right-click goldmaster_<<Hyper-V_A_hostname>> and select Boot Server.

21. Right-click goldmaster_<<Hyper-V_A_hostname>> and select KVM Console.

22. When the KVM console opens, select Tools > Launch Virtual Media.



23. When the Virtual Media Session manager opens, click Add Image.
24. Browse to the Windows® Server 2008 R2 ISO and click Open.
25. Select the Mapped checkbox next to the Windows ISO.
26. Boot the server from the ISO and start Windows setup. Do not close the virtual media manager or it will disconnect the ISO image. The “Boot Server” button is on the Server KVM Screen. Click OK to proceed, and then OK again to acknowledge.
27. If needed, modify Language, Time/currency format, and Keyboard settings. Click Next > Install Now.
28. Select Windows Server 2008 R2 Datacenter (Full Installation) and click Next.
29. Click I accept the license terms and click Next.
30. Select Custom (advanced) installation.
31. In the Virtual Media Session manager clear the Mapped checkbox for the Windows ISO and select yes when it asks you to confirm the action.
32. Click Add Image.
33. Browse to the Cisco fNIC driver ISO, click Open.
34. Select the Mapped checkbox next to the Cisco fNIC Driver ISO. Again, do not close the virtual media manager as it will disconnect the ISO image.
35. Back in the KVM Console, click the Load Driver option, and click OK.
36. The Cisco VIC FCoE Storport Miniport driver should auto detect, Click Next.
37. You should see a LUN listed in the drive selection screen.
38. 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.
39. Select the Mapped checkbox for the Windows ISO in the virtual media session manager.
40. Back in the KVM console click refresh to update the cdrom drive status.
41. Select the new LUN, and click the Windows cannot be installed to this disk link.
42. Click OK to online the LUN.
43. Select the LUN and click Next.
44. When Windows is finished installing, enter a new Administrator Password.
45. In the Virtual Media Session manager, clear the Mapped checkbox for the Windows ISO.
46. Click Add Image.
47. Browse to the Cisco eNIC driver ISO and click Open.
48. Select the Mapped checkbox for the Cisco eNIC driver ISO.
49. Back in the KVM console open Server Manager, and select Diagnostics > Device Manager.
50. Right-click one of the Ethernet Controller and select Update Driver Software.
51. Click Browse my computer for driver software.
52. Click Browse, and select the CDROM drive, click OK.
53. Click Next > Close.
54. Now that Windows has an instance of the Ethernet controller right-click the computer name at the top of device manager, and select Scan for Hardware Changes. This will load the correct driver on any remaining Ethernet controllers.
55. Close Device Manager.
56. Click Start > Run > ncpa.cpl. This action will open the Network Connections Control Panel.
57. One at a time, right-click each eNIC and select Status.
58. Click details, and note the Physical Address.
59. Back in the Cisco USC Manager, open the Servers tab, and select Service Profile > root > <hyper-v Hostname>_vNICs.
60. Identify the vNIC with the MAC Address noted in step 61.
61. Back in Windows rename the LAN adapter to reflect the network it is associated with.



62. Set the appropriate IP settings for that adapter.
63. Repeat for each eNIC in Windows.
64. Click the Start menu > Administrator Tools. Select the iSCSI initiator and choose Yes to start the iSCSI initiator service. When the service has started you can close the iSCSI initiator tool.
65. Select the iSCSI interface, and clear both File and Print Sharing for Microsoft® Networks and Client for Microsoft Networks.
66. Add the following features via Windows PowerShell, .Net Framework 3.5.1(exclude WCF Activation), Failover Clustering, and Multipath I/O. This process does not require a reboot.

```
import-module servermanager  
add-windowsfeature net-framework-core,multipath-io,failover-clustering
```

Verify that the features have been added.

```
get-windowsfeature
```

This command will generate a list of features installed on the server.

67. Configure MS MPIO to claim NetApp LUNs. This command will automatically reboot the server.

From the Windows PowerShell session on the Hyper-V Server, run the following command.

```
mpclaim -r -i -d "NETAPP LUN"
```

68. After the server has restarted, log in and review that the Microsoft DSM (MPIO) has claimed (supports) NetApp LUNs.

From the Windows PowerShell session on the Hyper-V Server, run the following command.

```
mpclaim -h
```

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

From the Windows PowerShell session on the Hyper-V host, run the following command.

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

70. When the server is off, open the Cisco USC Manager. Select and expand the Service Profile Templates > root object.
71. Right-click goldmaster_<<Hyper-V_A_hostname>> and select Disassociate Service Profile.
72. Log in to the <<var_ntap_A_hostname>> controller with PowerShell.
73. Unmap the goldmaster igroup from the Gold Master Boot LUN.

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

74. Copy the Gold Master Boot LUN from <<var_ntap_A_hostname>> to <<var_ntap_B_hostname>>



```
invoke-nassh ndmpcopy -sa root:password -da root:password
<<var_ntap_A_hostname>>:/vol/ucs_boot/goldmaster/goldmaster.lun
<<var_ntap_B_hostname>>:/vol/ucs_boot
```

After copying the LUN to the <<var_ntap_B_hostname>> storage controller, the lun has to be brought online and moved into a qtree.

```
connect-nacontroller <<var_ntap_B_hostname>> -credentials root
set-nalun /vol/ucs_boot/goldmaster.lun -Online
new-naqtree /vol/ucs_boot/goldmaster
rename-nalun /vol/ucs_boot/goldmaster.lun /vol/ucs_boot/goldmaster/goldmaster.lun
```

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

Using an ssh client, log into the Cisco Nexus 5548 A - <<var_nexus_A_hostname>> with administrative rights on the switch.

```
configure terminal
zoneset name Hyper-V_FastTrack vsan 1
no member goldmaster_<<Hyper-V_A_hostname>>_A
exit

no zone name goldmaster_<<Hyper-V_A_hostname>>_A vsan 1
```

```
device-alias database
no device-alias name goldmaster_<<Hyper-V_A_hostname>>_A pwwn <vHBA_A WWPN>
no device-alias name goldmaster_<<var_ntap_A_hostname>>_A pwwn <HBA_0c WWPN>
exit
device-alias commit
```

76. After all of the goldmaster device aliases and the goldmaster zone for the goldmaster_<<var_ntap_A_hostname>> service profile have been deleted, aactivate and distribute the zoneset.

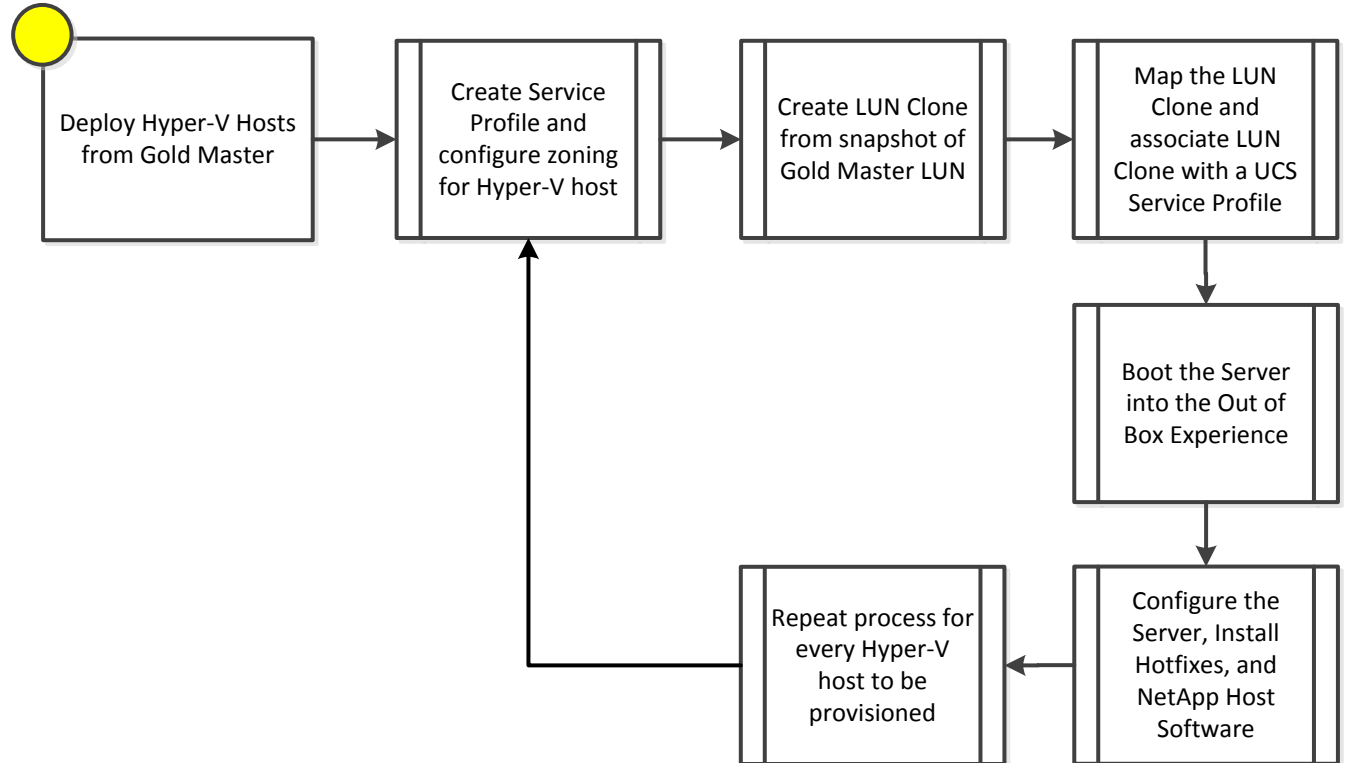
```
zoneset activate name Hyper-V_FastTrack vsan 1
zoneset distribute full vsan 1
exit
copy run start
```

Deploy Hyper-V Hosts from Gold Master

The deployment of Hyper-V hosts from a Gold Master process is comprised of the following high-level steps:



Microsoft



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 deploy Hyper-V hosts for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

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

Pre-requisites

The following environment prerequisites must be met before proceeding.



Cisco UCS Service Profile Templates

Open the Cisco UCS Manager application, expand the Service Profile Templates object and then verify that the Cisco UCS Service Profile Templates have been created:

Cisco UCS Service Profile Template	Purpose
Service Template <<Service Template Fabric A>>	Template for service profile to boot from Controller A
Service Template <<Service Template Fabric B>>	Template for service profile to boot from Controller B

Gold Master boot LUN

The Gold Master boot LUN will be used to create the boot LUNs for the Hyper-V hosts. Prior to deployment you need to ensure that the Gold Master boot LUN exists on each controller.

Perform the following steps using the NetApp PowerShell Toolkit connected to NetApp **Controller A** storage controller with an account which has local Administrator rights on the storage controller.

Using the NetApp PowerShell Toolkit, connect to the storage controller and issue the following command:

```
get-nalun /vol/ucs_boot/goldmaster/goldmaster.lun
```

The output of the command will display the Gold Master boot LUN. If the message 'LUN not found' is returned. Verify the path of the Gold Master boot LUN.

Perform the following steps using the NetApp PowerShell Toolkit connected to NetApp **Controller B** storage controller with an account which has local Administrator rights on the storage controller.

Using the NetApp PowerShell Toolkit, connect to the storage controller and issue the following command:

```
get-nalun /vol/ucs_boot/goldmaster/goldmaster.lun
```

The output of the command will display the Gold Master boot LUN. If the message 'LUN not found' is returned. Verify the path of the Gold Master boot LUN.

Deployment of Hyper-V Host Workflow

1. Open the Cisco USC Manager, select and expand the Service Profile Templates > root object.
2. Right-click root and select Create Service Profiles from Template.
3. Enter <<Hyper-V Hostname>> for the service profile suffix.
4. Enter 1 for the number of service profiles to create.
5. Select <<Service Template Fabric A>> for the Service Profile Template field. It should be under Organizations > root object.
6. Click OK to create the service profile, and OK again to acknowledge. This service profile will SAN boot from the <<var_ntap_A_hostname>> NetApp storage controller.
7. You will now see the service profile populate under the Service Profile Template > root object. Under that server name, expand the vHBAs and record the WWPN for each of the adapters.
8. Retrieve the WWPN for the 0c and 0d FCP target interfaces on the <<var_ntap_A_hostname>> and <<var_ntap_B_hostname>> NetApp storage controllers. Record the WWPN for each of the adapters.



Using the NetApp PowerShell Toolkit, connect to the <<var_ntap_A_hostname>> NetApp storage controller.

```
connect-nacontroller <<var_ntap_A_hostname>> -credential root
get-nafcadapter 0c
get-nafcadapter 0d

connect-nacontroller <<var_ntap_B_hostname>> -credential root
get-nafcadapter 0c
get-nafcadapter 0d
```

9. Connect to Cisco Nexus 5548 A - <<var_nexus_A_hostname>> and create the device aliases and zoning for the <<Hyper-V hostname>> service profile. The zoning will be single initiator zoning.

Using an ssh client, log into the Cisco Nexus 5548 A - <<var_nexus_A_hostname>> with administrative rights on the switch.

```
configure terminal
device-alias database
device-alias name <Service Profile>_<<var_ntap_A_hostname>>_A pwwn <vHBA_A WWPN>
device-alias name <<var_ntap_A_hostname>>_A pwwn <var_ntap_A_hostname 0c WWPN>
device-alias name <<var_ntap_B_hostname>>_A pwwn <var_ntap_B_hostname 0c WWPN>
exit
device-alias commit

zone name <Service Profile>_<<Hyper-V_hostname>>_A vsan 1
member device-alias <Service Profile>_A
member device-alias <<var_ntap_A_hostname>>_A
member device-alias <<var_ntap_B_hostname>>_B
exit

zoneset name Hyper-V_FastTrack vsan 1
member <Service Profile>_<<var_ntap_A_hostname>>_A
exit
```

10. Activate and distribute the zoneset.

```
zoneset activate name Fast Track vsan 1
zoneset distribute vsan 1
exit
copy run start
```

11. Connect to Cisco Nexus 5548 B - <<var_nexus_B_hostname>> and create the device aliases and zoning for the <<Hyper-V hostname>> service profile. The zoning will be single initiator zoning.



Using an ssh client, log into the Cisco Nexus 5548 B - <<var_nexus_B_hostname>> with administrative rights on the switch.

```
configure terminal
device-alias database
device-alias name <Service Profile>_<<var_ntap_A_hostname>>_B pwwn <vHBA_B_WWPN>
device-alias name <<var_ntap_A_hostname>>_B pwwn <var_ntap_A_hostname 0d_WWPN>
device-alias name <<var_ntap_B_hostname>>_B pwwn <var_ntap_B_hostname 0d_WWPN>
exit
device-alias commit

zone name <Service Profile>_<<Hyper-V_A_hostname>>_A vsan 1
member device-alias <Service Profile>_A
member device-alias <<var_ntap_A_hostname>>_B
member device-alias <<var_ntap_B_hostname>>_B
exit

zoneset name Hyper-V_FastTrack vsan 1
member <Service Profile>_<<Hyper-V_hostname>>_B
exit
```

12. Activate and distribute the zoneset.

```
zoneset activate name Fast Track vsan 1
zoneset distribute vsan 1
exit
copy run start
```

13. Select <Hyper-V Hostname> >vHBAs. You'll need these WWPNs in a minute.

14. Log in to <<var_ntap_A_hostname>>.

15. Create a Qtree to house the Hyper-V host boot LUN.

```
new-naqtree /vol/ucs_boot/<Hyper-V Hostname>
```

16. Create and configure an initiator group to map the host to the storage.

```
new-naigroup <Hyper-V Hostname> fcp hyper_v
set-naigroup <Hyper-V Hostname> alua true
add-naigroupinitiator <Hyper-V Hostname> <vHBA_A_WWPN>
add-naigroupinitiator <Hyper-V Hostname> <vHBA_B_WWPN>
```

17. Create a Snapshot® copy for the LUN clone.

```
new-nasnapshot ucs_boot clone_base
```

18. Clone the boot LUN from the goldmaster boot LUN.



```
new-nalunclone /vol/ucs_boot/<Hyper-V Hostname>/<Hyper-V Hostname>.lun  
/vol/ucs_boot/goldmaster/goldmaster.lun -unreserved clone_base
```

19. Split the clone into a full LUN. Due to ASIS this should take seconds to complete.

```
start-nalunclonesplit /vol/ucs_boot/<Hyper-V Hostname>/<Hyper-V Hostname>.lun
```

20. Monitor the status of the split using the following command.

```
get-nalunclonesplit /vol/ucs_boot/<Hyper-V Hostname>/<Hyper-V Hostname>.lun
```

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

```
set-nalunsignature /vol/ucs_boot/<Hyper-V Hostname>/<Hyper-V Hostname>.lun -generaterandom
```

22. When the split is finished, remove the Snapshot copy from the LUN clone.

```
remove-nasnapshot ucs_boot clone_base
```

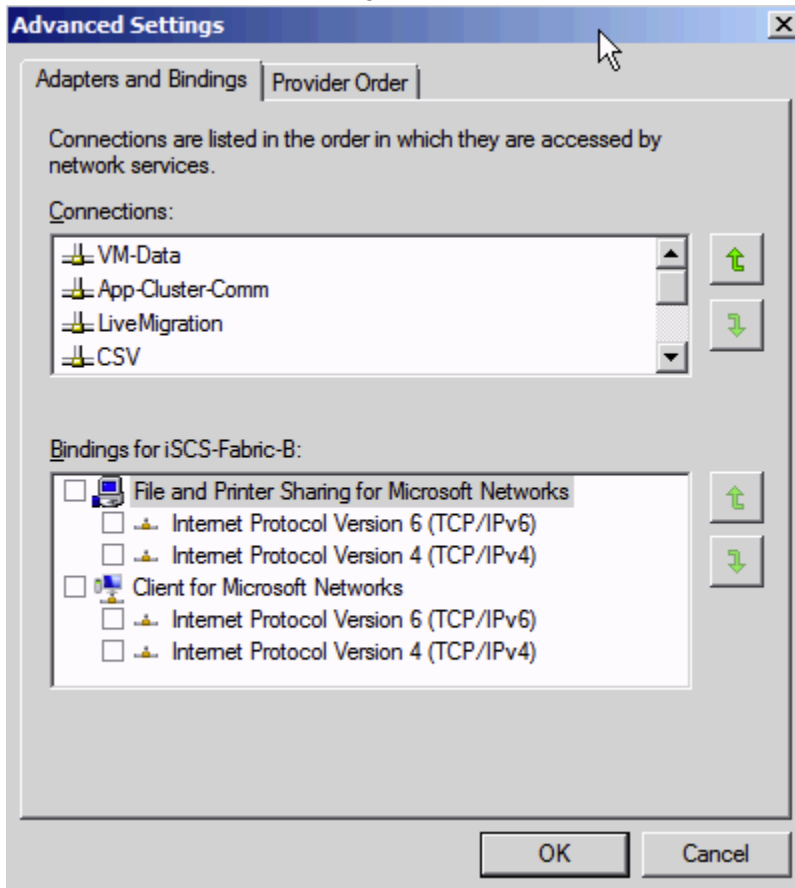
23. Map the boot LUN to the new iGroup.

```
add-nalunmap /vol/ucs_boot/<Hyper-V Hostname>/<Hyper-V Hostname>.lun <Hyper-V Hostname> -ID 0
```

24. Back in the Cisco USC Manager, right-click <Hyper-V Hostname>, and select Associate with Server Pool.
25. From the Pool Assignment box, select the Infra_Pool and click OK, and OK again to acknowledge.
26. Right-click the <Hyper-V hostname> and select KVM Console.
27. Click Boot Server, the service profile will then pull a server from the Infra_Pool, and configure the hardware per the service profile.
28. Back in the Cisco USC Manager, right-click <Hyper-V Hostname>, and select KVM Console.
29. Click Boot Server, the service profile will then pull a server from the Infra_Pool, and configure the hardware per the service profile.
30. When the server has fully booted Windows will enter the out of box experience. Select the Language, Time/currency format, and Keyboard settings. Click Next.
31. Enter the product key and click Next.
32. Click I accept the license terms and click Start.
33. When Windows is finished setup. Enter a new Administrator Password.
34. From the Initial Configuration Tasks pane select Configure Networking.
35. One at a time, right-click each eNIC and select Status.
36. Click details, and note the Physical Address.
37. Back in the Cisco USC Manager, open the Servers tab, and select Service Profile > root > <<hyper-v Hostname>>_vNICs. Record the MAC Address of the vNIC.



38. From the Windows Network Connections Control Panel, rename the LAN adapter to reflect the network it is associated with.
39. Set the appropriate IP settings for that adapter.
40. Repeat for each eNIC in Windows.
41. Configure the Binding Order on the network adapters.
 - a. Click start > run, then type `ncpa.cpl` and press return.
 - b. Press the ALT key to display the advanced Menu Bar.
 - c. Click Advanced and then Advanced Settings.
 - d. Select the adapter and use the arrows to move it up or down in binding order.
42. The recommended binding order is:
 - e. VM-Data
 - f. App-Cluster-Comm
 - g. LiveMigration
 - h. CSV
 - i. VM-Mgmt
 - j. iSCSI-Fabric-A
 - k. iSCSI-Fabric-B
43. Clear the File and Print Sharing for the iSCSI networks checkbox.





44. Open the TCP/IP Properties for each of the Private Networks (CSV, LiveMigration, iSCSIA, iSCSIB and App-Cluster-Comm. Click on the Advanced button and then select the DNS tab. Clear the "Register this connection's addresses in DNS" checkbox. Click OK twice and then click Close.
45. Open Server Manager, Click Roles > Add Roles. Add the Hyper-V role.
46. Add the Hyper-V role via Windows PowerShell. This process requires a reboot.

```
import-module servermanager  
add-windowsfeature hyper-v -restart
```

47. Install the following Microsoft Windows Hotfixes and reboot after installation of all patches:
KB2494016
KB2517329
KB2520235
KB2522766
KB2528357
KB2531907
KB2552040
KB2639032
48. After the server has completed the boot process, log into the server with Administrative rights and set the page file size to an amount appropriate for your environment. To set the page file size, open the Control Panel > System > Advanced System Settings > Advanced > Performance Settings Button > Advanced > Change. Changing the page file size will require a reboot.
49. Install the NetApp Host Utilities Kit 6.0, selecting the MPIO option. Disregard the informational message that no FC settings needed update. Choose to manually restart later.
50. Install the NetApp MPIO DSM version 3.5. Enter the MPIO license found in your license package. Use the SYSTEM account to run the NetApp DSM service. Install the Hyper-V Guest Utilities. Disregard the message about the FC configuration tool not finding HBAs. Reboot the server.
51. Open the Hyper-v Manager and click Virtual Network Manager. Create Virtual Network Switches with the following properties:

Virtual Network Name	Connection Type	Interface Name	Share Network with Management Host
VM-Data	External	VM-Data	No
App-Cluster-Comm	External	App-Cluster-Comm	No
iSCSI-Fabric-A	External	iSCSI-Fabric-A	No
iSCSI-Fabric-B	External	iSCSI-Fabric-B	No

Note: You will need to open the Network Connections Control Panel to view the underlying Device Name for each interface.

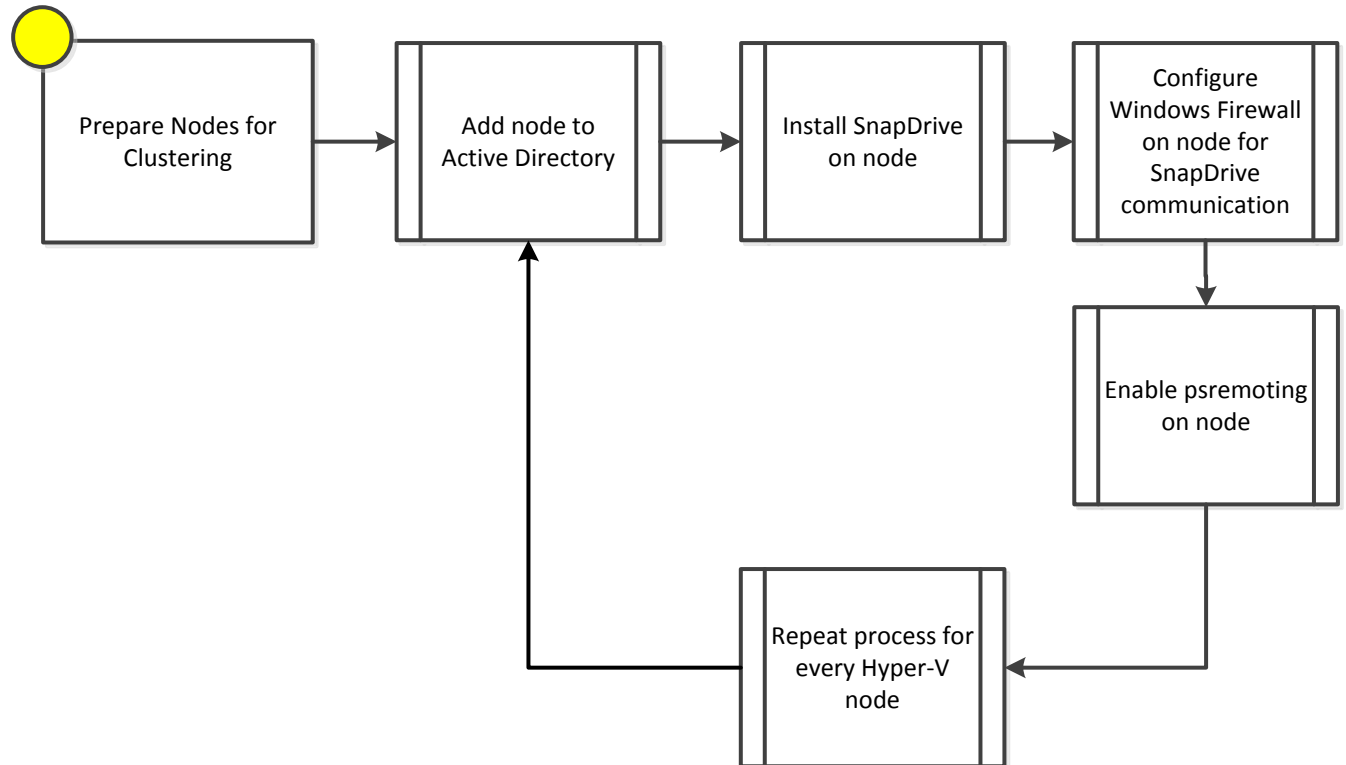
52. Repeat for each Hyper-V node to be provisioned.



Create Window Failover Cluster and Clustered Virtual Machines

Prepare Nodes for Clustering

The deployment of Hyper-V hosts from a Gold Master process is comprised of the following high-level steps:



Overview

This section provides high-level walkthrough on how to prepare the Hyper-V hosts to participate in a Windows Failover Cluster that will be used in the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- Administrative access to the Hyper-V cluster nodes
- SnapDrive Service Account created
- Permission to add computers to Active Directory



- Storage controllers are members of Active Directory

Prerequisites

The following environment prerequisites must be met before proceeding.

Service Account

Verify that the following service account has been created:

UserName	Purpose	Permissions
<DOMAIN>\<snapdriveAccountName>	SnapDrive Service Account	This account will have local administrator rights and Log on As a Service rights on each Hyper-V node. This account will also be a member of the local Administrators group on the NetApp storage controllers (and vFilers, if applicable)



Hyper-V Node Preparation Workflow

1. Join the Hyper-V node to your active directory domain (reboot required).
2. Add the SnapDrive service account to the local administrators group on each Hyper-V node.
3. Add the SnapDrive service account to the local administrators group on each NetApp Storage controller (or vFiler as applicable).
4. Install NetApp SnapDrive 6.4. When prompted for the account to use as the service account, use the SnapDrive account in the above step. The account will be granted the Log on as a Service right on the local server. When prompted for the License type, select Per Storage System. When prompted for the Transport Protocol Default setting, select HTTPS and choose the SnapDrive service account, <domainname>\<snapdriveAccountName>.
5. Create an inbound Windows firewall rule via Server Manager > Configuration > Windows Firewall > Inbound Rules, for %programfiles%\NetApp\SnapDrive\SWSvc.exe. Creating an inbound rule automatically creates the outbound rule as well. Alternatively, you can turn off the Windows Firewall. Deploy a Windows Firewall configuration appropriate for your environment.
6. Open the System Control Panel and click on Remote Settings. Set the appropriate Remote Desktop policy appropriate for your environment.
7. Open the PowerShell console via a right-click and run as administrator and execute `Enable-psremoting -force` to enable remote management.
8. Repeat the above steps on additional nodes that will become members of a Hyper-V cluster.

Hyper-V Node Preparation Workflow

Overview

This section provides high-level walkthrough on how to create the Hyper-V cluster that will be used in the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- Administrative access to the Hyper-V cluster nodes
- Permission to add computers to Active Directory

Hyper-V Node Preparation Workflow

Overview

This section provides high-level walkthrough on how to create the Hyper-V cluster that will be used in the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

Administrative access to the Hyper-V cluster nodes

Permission to add computers to Active Directory

Hyper-V Cluster Formation Workflow

1. Log in to the servers using a Domain account with permissions to add a domain machine account. Open Server Manager and browse to Features > Failover Cluster Manager.
2. Validate cluster.



Validate a Configuration Wizard

 **Select Servers or a Cluster**

Before You Begin

Select Servers or a Cluster

Testing Options

Confirmation

Validating

Summary

To validate a set of servers, add the names of all the servers.
To test an existing cluster, add the name of the cluster or one of its nodes.

Enter name:

Selected servers:

- VMHost-Infra-01.flexpod.test (Infra-Clus-01)
- VMHost-Infra-02.flexpod.test (Infra-Clus-01)
- vmhost-infra-03.flexpod.test (Infra-Clus-01)
- vmhost-infra-04.flexpod.test (Infra-Clus-01)

< Previous Next > Cancel

3. Select "Run all tests" when performing cluster validation.



Validate a Configuration Wizard

 **Testing Options**

Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary

Choose between running all tests or running selected tests.

The tests include Inventory tasks, Network tests, Storage tests, and System Configuration tests.

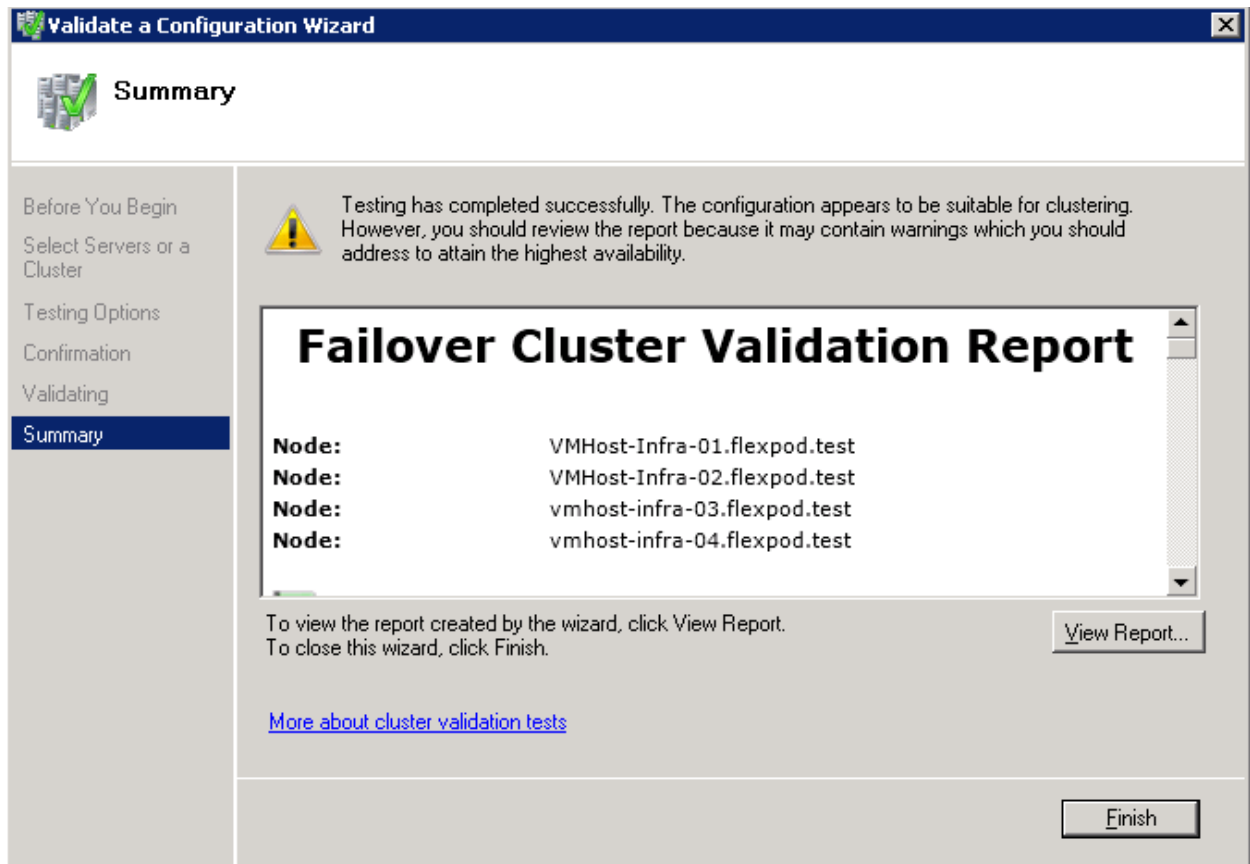
Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in this wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2008 R2".

☒ Run all tests (recommended)
☐ Run only tests I select

[More about cluster validation tests](#)

< Previous Next > Cancel

4. Validation will complete successfully with warnings. The warning exists because there is not yet any shared disk resources.



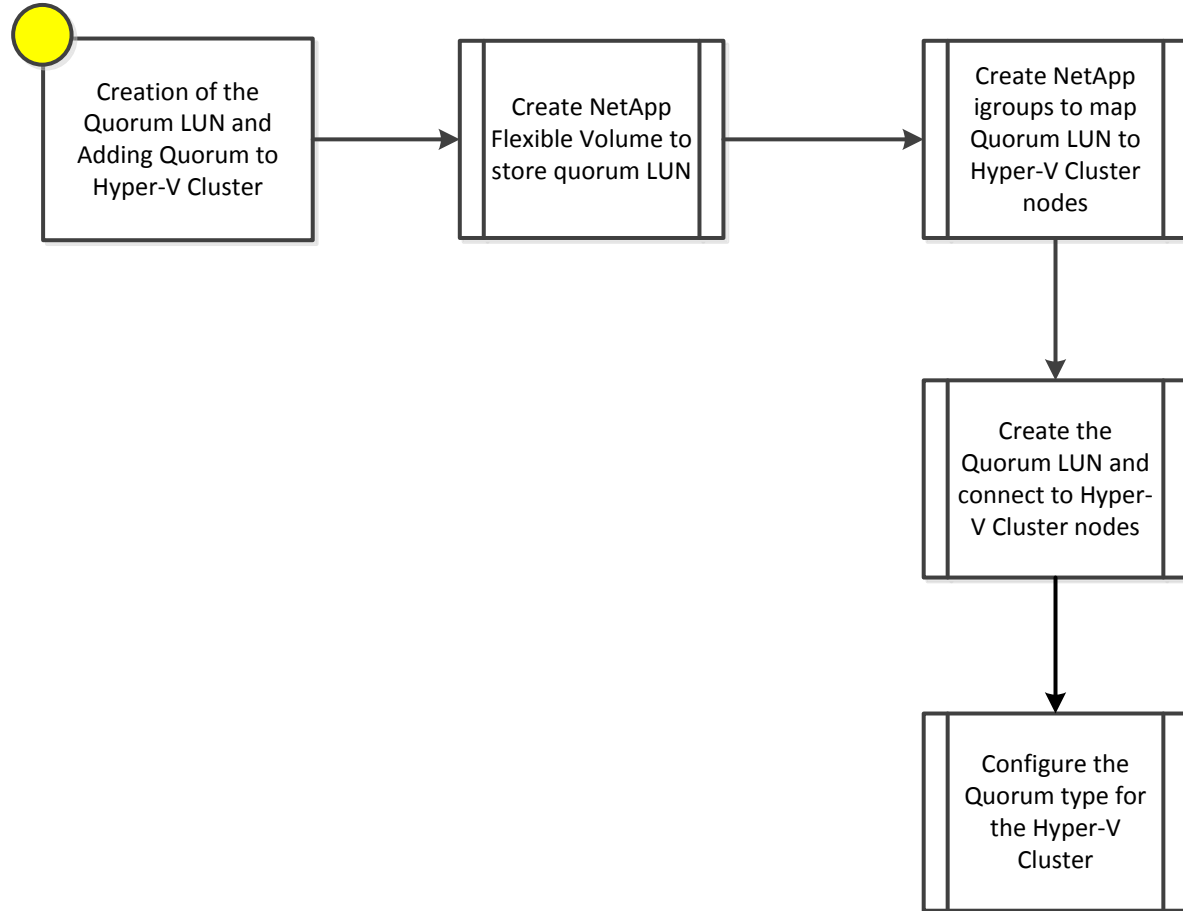
5. When validation successfully completes, create the cluster naming it <FastTrack_Cluster>FastTrack.

Creation of the Quorum LUN and Adding Quorum to the Hyper-v Cluster

The creation of the Quorum LUN and adding Quorum to the Hyper-V Cluster process is comprised of the following high-level steps:



Microsoft



Overview

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

- NetApp PowerShell Toolkit 1.7 or higher installed on Hyper-V cluster nodes
- NetApp SnapDrive 6.4 or higher installed on Hyper-V cluster nodes

Creation of Quorum LUN and adding Quorum to Hyper-V Cluster Workflow

1. Connect to NetApp Controller A using administrative rights on the controller.



Start a Windows PowerShell session on the Hyper-V cluster node, <<Hyper-V Hostname A>>, with administrative rights on the cluster node. Import the PowerShell Toolkit module and the Windows Failover Cluster PowerShell modules

```
import-module dataontap  
import-module failoverclusters
```

Connect to the NetApp controller with credentials that have administrative rights on the controller.

```
connect-nacontroller <<var_ntap_B_hostname>> -credential root
```

2. Create a flexible volume and qtree to store the Quorum LUN.

```
new-navol vm_host_infra_cluster_quorum aggr1 5g  
set-navoloption vm_host_infra_cluster_quorum fractional_reserve 0  
set-navoloption vm_host_infra_cluster_quorum create_ucose on  
set-navoloption vm_host_infra_cluster_quorum convert_ucose on  
  
set-nasnapshotreserve vm_host_infra_cluster_quorum 0  
set-nasnapshotschedule vm_host_infra_cluster_quorum -Weeks 0 -Days 0 -Hours 0 -Minutes 0  
  
new-naqtree /vol/vm_host_infra_cluster_quorum/quorum
```

3. Create the Quorum LUN as a shared LUN and connect to the Hyper-V cluster nodes with Snapdrive. Use the same NetApp igroups that map the Hyper-V Boot LUN to the storage.

Determine which cluster node owns the cluster group "Available Storage".

```
import-module failoverclusters  
get-clustergroup "Available Storage"
```

If the "Available Storage" cluster group is not on <<Hyper-V Hostname A>>, move the cluster group to <<Hyper-V Hostname A>>.

```
move-clustergroup "Available Storage" -node <<Hyper-V Hostname A>>
```

Verify the location of the "Available Storage" cluster group is on <<Hyper-V Hostname A>>.

```
get-clustergroup "Available Storage"
```

Create the new Quorum LUN as a 5GB shared LUN with SnapDrive to the Hyper-V cluster and assign Q: as the mountpoint. The below command assumes that you have two nodes in your Hyper-V cluster. If you have more than two nodes, modify the following command to include the additional Hyper-V nodes.

```
sdcli disk create -d q -p <<var_ntap_A_hostname>>:/vol/vm_host_infra_cluster_quorum/quorum/  
vm_host_infra_cluster_quorum.lun -dtype shared -z 5120 -rs y -IG <<Hyper-V Hostname A>> <<Hyper-V  
Hostname A>> <<Hyper-V Hostname B>> <<Hyper-V Hostname B>> -e "Available Storage"
```



Confirm the new disk has been created. Note the name of the Cluster Disk Resource name of the shared LUN that was created.

```
get-clustergroup "Available Storage" | get-clusterresource | fl
```

The name of the new Cluster Disk Resource will be Q:\.

4. Configure the Quorum Type for the Hyper-V cluster. The device name for your environment may be different.

```
set-clusterquorum nodeanddiskmajority "Cluster Disk 7"
```

5. Confirm the Quorum disk has been assigned to the Cluster Group and that the Cluster Quorum type is set to Node and Disk Majority.

```
get-clustergroup "Cluster Group" | get-clusterresource | fl  
get-clusterquorum
```

6. Move the Cluster Group cluster group from <<Hyper V HostName A>> and back. If your cluster has more than two nodes, move the Cluster Group cluster group between all of the nodes.

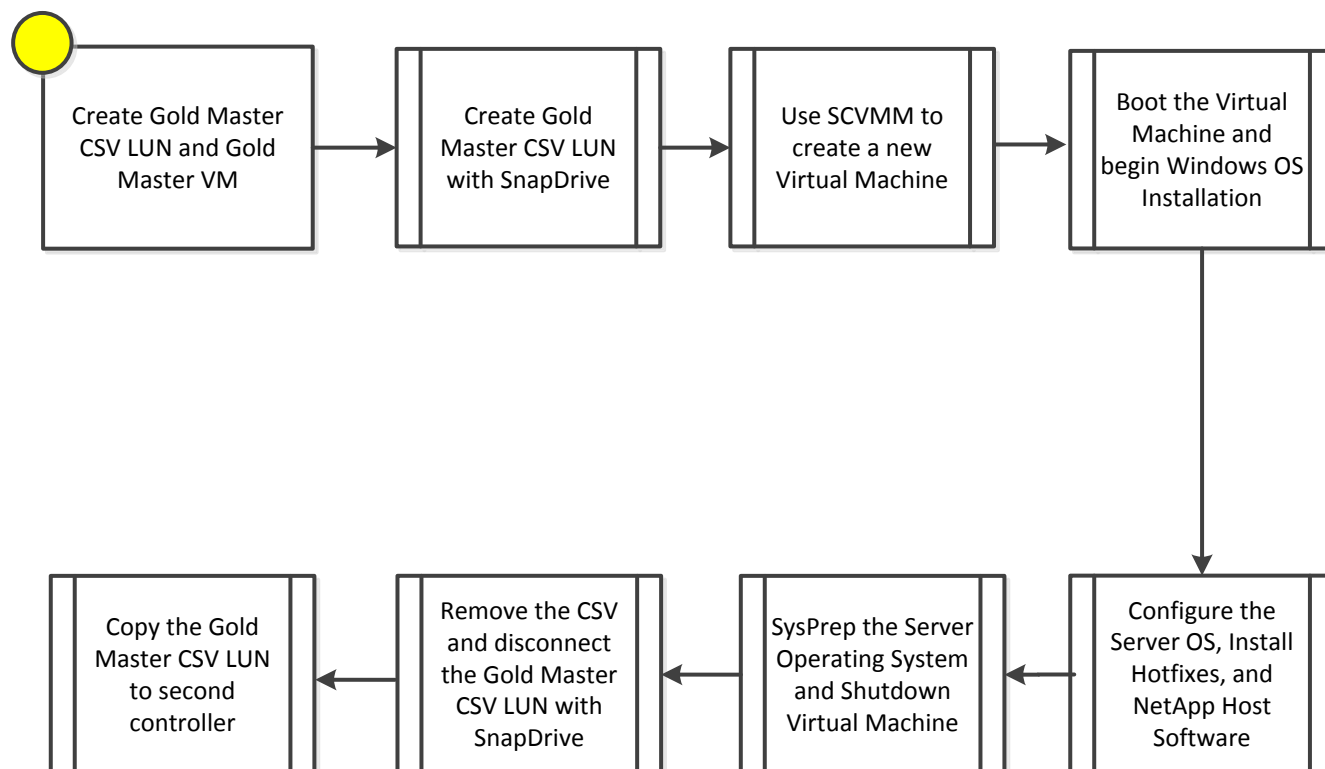
```
move-clustergroup "Cluster Group" -node <<Hyper V HostName B>>  
move-clustergroup "Cluster Group" -node <<Hyper V HostName A>>
```

Create Gold Master CSV LUN and Gold Master VHD

The process to create a Gold Master CSV LUN and Gold Master Virtual Machine is comprised of the following high-level steps:



Microsoft



Overview

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

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

- NetApp PowerShell Toolkit 1.7 or higher installed on Hyper-V cluster nodes
- PowerShell Management Library for Hyper-V installed on Hyper-V cluster nodes
<http://pshyperv.codeplex.com/releases/view/62842>
- Access to Windows 2008R2 installation ISO image

Creation of Gold Master CSV LUN Workflow

1. Perform the following steps to configure the NetApp storage needed for the Gold Master CSV LUN:



Perform the following PowerShell commands with an account that has local administrator rights on the NetApp **Controller B** storage controller.

Start a Windows PowerShell session on the <<Hyper-V Hostname A>> node and import the Data ONTAP PowerShell Toolkit module.

```
import-module dataontap
```

Connect to the NetApp controller:

```
connect-nacontroller <<var_ntap_B_hostname>> -credential root
```

Create the NetApp flexible volume that will store the Gold Master CSV LUN.

```
new-navol CSV_B aggr1 600g
```

Set the NetApp flexible volume options that will store the Gold Master CSV LUN.

```
set-navoloption CSV_B create_ucose on  
set-navoloption CSV_B convert_ucose on  
set-navoloption CSV_B fractional_reserve 0
```

```
set-nasnapshotschedule CSV_B -Weeks 0 -Days 0 -Hours 0 -Minutes 0  
set-nasnapshotreserve CSV_B 0
```

```
new-naqtree /vol/CSV_B/goldmaster
```

2. Create the Gold Master CSV LUN with SnapDrive. Use the NetApp igroups created previously for each Hyper-V cluster node.

Determine which cluster node owns the cluster group “Available Storage”.

```
import-module failoverclusters  
get-clustergroup “Available Storage”
```

If the “Available Storage” cluster group is not on <<Hyper-V Hostname A>>, move the cluster group to <<Hyper-V Hostname A>>.

```
move-clustergroup “Available Storage” -node <<Hyper-V Hostname A>>
```

Verify the location of the “Available Storage” cluster group is on <<Hyper-V Hostname A>>.

```
get-clustergroup “Available Storage”
```

Create a 500GB shared LUN with SnapDrive on <<Hyper-V Hostname A>> with no mountpoint. The following example assumes two Hyper-V cluster nodes. Modify the following command to include additional Hyper-V cluster nodes.

```
sdcli disk create -p <<var_ntap_B_hostname>>:/vol/CSV_B/goldmaster/goldmaster_csv.lun -dtype shared -z  
512000 -rs n -IG <<Hyper-V Hostname A>> <<Hyper-V Hostname A>> <<Hyper-V Hostname B>> <<Hyper-  
V Hostname B>> -e “Available Storage”
```



Confirm the new disk has been created. Note the name of the Cluster Disk Resource name of the shared LUN that was created. get-clustergroup "Available Storage" get-clusterresource fl The name of the new Cluster Disk Resource will be in a GUID format.
Rename the Cluster Disk Resource. \$resource = "<<Name of the shared LUN that was created>>" Get-ClusterResource \$resource %{ \$_.Name = "CSV_GoldMaster" }
Create new clustered shared volume using the Cluster Disk Resource name of the shared LUN that was just created. add-clustersharedvolume "CSV_GoldMaster"
Confirm that the new cluster shared volume has been created. get-clustersharedvolume

Creation of Gold Master Virtual Machine Workflow

1. Perform the following steps to configure the NetApp storage needed for the Gold Master CSV LUN:

Perform the following PowerShell commands with an account that has local administrator rights on the Hyper-V cluster.
Start a Windows PowerShell session on <<Hyper-V Hostname A>> cluster node and import the Data ONTAP PowerShell Toolkit module, the Windows Failover Clustering module, and the PowerShell Management Library for Hyper-V. import-module dataontap import-module failoverclusters import-module hyperv
Run the following commands to create the Gold Master Virtual Machine on the Gold Master CSV LUN. \$VMName = <<Insert VM Name Here>> New-VM -Name \$VMName -Path C:\ClusterStorage\Volume1 New-NaVirtualDisk -FullName C:\ClusterStorage\Volume1\TempGoldMaster.vhd -Size 100gb Add-VMNIC -VM \$VMName -VirtualSwitch <<Name of Management Network>> Add-VMNIC -VM \$VMName -VirtualSwitch <<Name of Data Network>> Add-VMdisk -VM \$VMName -Path C:\ClusterStorage\Volume1\TempGoldMaster.vhd Add-VMdrive -VM \$VMName -ControllerID 1 -lun 1 -DVD Add-ClusterVirtualMachineRole -Name <<Insert VM Name Here>> -VirtualMachine \$VMName

2. Open Hyper-V Manager on <<Hyper-V Hostname A>>
3. Select the GoldMaster Virtual Machine and then right click and select Properties.
4. On the VM-Data, Network Bus Adapter, check the "Enable virtual LAN identification" and set the VLAN ID number for the VM-Data network. Click Apply to save changes.



5. On the Memory Object, configure the desired memory configuration for the Gold Master Virtual Machine. Click Apply to save changes.
6. On the Processor Object, configure the desired processor configuration for the Gold Master Virtual Machine. Click Apply to save changes.
7. On the DVD Drive, select "Image File" in the Media section and then specify the path to the Windows® Server 2008 R2 ISO. Click Apply to save changes.
8. Make any additional changes to the Gold Master Virtual Machine configuration. Click Apply to save changes.
9. On the BIOS Object, ensure that "Boot from CD" is configured. Click OK.
10. Use the Hyper-V Manager to connect to the Gold Master Virtual Machine.
11. Start the Gold Master Virtual Machine.
12. If needed, modify Language, Time/currency format, and Keyboard settings. Click Next > Install Now.
13. Select Windows Server 2008 R2 Enterprise Edition (Full Installation) and click Next.
14. Click I accept the license terms and click Next.
15. Select Custom (advanced) installation.
16. When Windows is finished installing, enter a new Administrator Password.
17. In the Virtual Media Session manager, clear the Mapped checkbox for the Windows ISO.
18. Add the .NET 3.51 Framework Core (add-windowsfeature net-framework-core) and install the following hotfixes for NetApp SnapDrive support: KB977096, KB2494016, KB2520235, and KB2531907. Install any other hotfixes as required.
19. When the Gold Master Virtual Machine configuration is complete, start the sysprep process.
20. Click Start > Run > C:\Windows\System32\Sysprep\sysprep.exe /generalize /shutdown /oobe.
21. After the Gold Master Virtual Machine has completed shutdown, we will use the NetApp PowerShell Toolkit command, copy-nahostfile, to create the final copy of the Gold Master Virtual Machine in a Thin-Fixed VHD format.

```
copy-nahostfile C:\ClusterStorage\Volume1\tempgoldmaster.vhd C:\ClusterStorage\Volume1\sysprep.vhd
```

After the file has been copied, remove the GoldMaster virtual machine.

```
Remove-VM -VM "GoldMaster"
```

Remove the Gold Master Cluster Shared Volume and the Gold Master cluster group.

```
remove-clustershared volume "CSV_GoldMaster"
```

```
remove-clustergroup "GoldMaster" -RemoveResources
```

22. After the Gold Master Virtual Machine has been removed. Use SnapDrive to disconnect the Gold Master CSV LUN from the Hyper-V cluster.

```
sdcli disk disconnect -p <<var_ntap_B_hostname>>:/vol/CSV_B/goldmaster/goldmaster_csv.lun
```

23. Log in to the secondary NetApp controller <<var_ntap_A_hostname>> with PowerShell and create the volume that will store the copy of the Gold Master CSV LUN.



```
import-dataontap
connect-nacontroller <<var_ntap_A_hostname>> -credential root

new-navol CSV_A aggr1 600g
```

Set the NetApp flexible volume options that will store the Gold Master CSV LUN.

```
set-navoloption CSV_A create_ucose on
set-navoloption CSV_A convert_ucose on
set-navoloption CSV_A fractional_reserve 0

set-nasnapshotschedule CSV_A -Weeks 0 -Days 0 -Hours 0 -Minutes 0
set-nasnapshotreserve CSV_A 0

new-naqtree /vol/CSV_A/goldmaster
```

24. Now copy the Gold Master CSV LUN to the NetApp controller <<var_ntap_A_hostname>> using the ndmpcopy command.

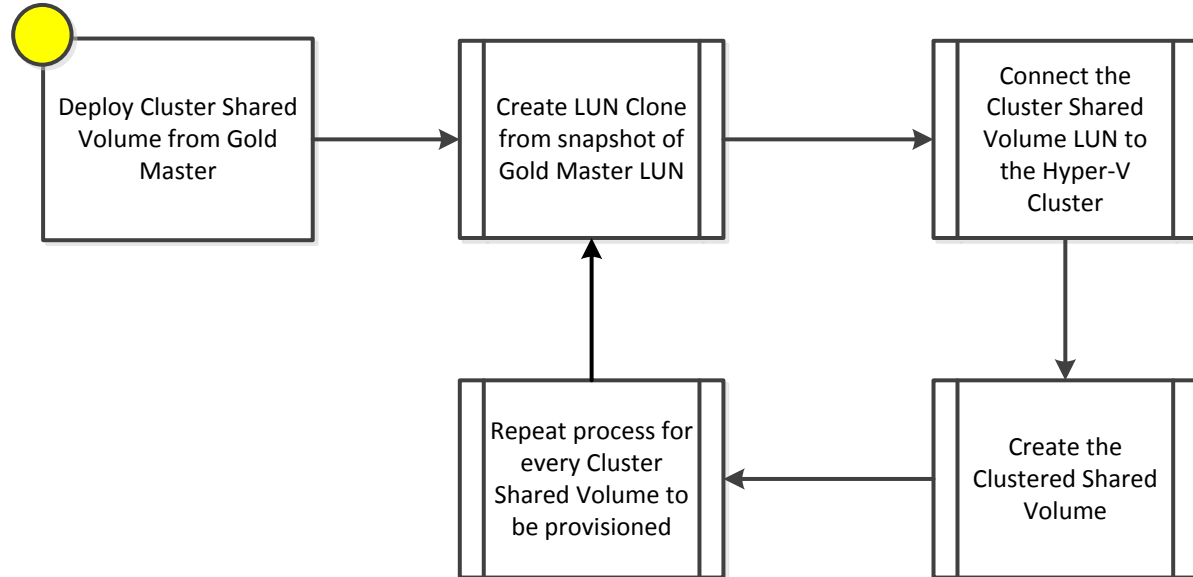
```
invoke-nassh ndmpcopy -sa root:password -da root:password
<<var_ntap_B_hostname>>:/vol/CSV_B/goldmaster/goldmaster_csv.lun
<<var_ntap_A_hostname>>:/vol/CSV_A/goldmaster
```

Deploy Cluster Shared Volume from Gold Master

The deployment of a Cluster Shared Volume from a Gold Master process is comprised of the following high-level steps:



Microsoft



Overview

The deployment process of Cluster Shared Volumes 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 Cluster Shared Volumes from a Gold Master CSV LUN for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- A Gold Master CSV LUN has been created
- NetApp PowerShell Toolkit 1.7 or higher installed on Hyper-V cluster nodes
- NetApp SnapDrive 6.4 or higher installed on Hyper-V cluster nodes

Prerequisites

The following environment prerequisites must be met before proceeding.



Gold Master Cluster Shared Volume LUN

The Gold Master CSV LUN will be used to create new Cluster Shared Volumes for the Hyper-V cluster. Prior to deployment you need to ensure that the Gold Master CSV LUN exists on a controller.

Perform the following PowerShell commands with an account that has local administrator rights on the NetApp **Controller A** storage controller.

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

```
import-module dataontap
```

View the status of the Gold Master CSV LUN.

```
get-nalun /vol/CSV_B/goldmaster/goldmaster_csv.lun
```

The output of the command will display the Gold Master CSV LUN. If the message 'No such LUN exists' is returned. Verify the path of the Gold Master CSV LUN and resubmit the command with the proper path

Deployment of Cluster Shared Volume

1. While connected to the NetApp storage controller with PowerShell, create a Snapshot® copy for the LUN clone.

```
new-nasnapshot CSV_B clone_base
```

2. Clone the Cluster Shared Volume LUN from the Gold Master CSV LUN snapshot.

```
new-nalunclone /vol/CSV_B/prod_csv.lun /vol/CSV_B/goldmaster/goldmaster_csv.lun -unreserved
```

3. Split the clone into a full LUN. Due to ASIS this should take seconds to complete.

```
start-nalunclonesplit /vol/CSV_B/goldmaster/prod_csv.lun
```

4. Monitor the status of the split using the following command.

```
get-nalunclonesplit /vol/CSV_B/goldmaster/prod_csv.lun
```

5. When the split is finished, remove the Snapshot copy from the LUN clone.

```
remove-nasnapshot CSV_B clone_base
```

6. Create a qtree and place cloned LUN into qtree.

```
new-naqtree /vol/CSV_B/prod/prod_csv.lun  
rename-nalun /vol/CSV_B/goldmaster/prod_csv.lun /vol/CSV_B/prod/prod_csv.lun
```



7. Change disk signature of the LUN.

```
set-nalunsignature /vol/CSV_B/prod/prod_csv.lun -generaterandom
```

8. Connect the Cluster Shared Volume LUN as a shared LUN to the Hyper-V cluster with Snapdrive.

Determine which cluster node owns the cluster group “Available Storage”.

```
import-module failoverclusters  
get-clustergroup “Available Storage”
```

If the “Available Storage” cluster group is not on <<Hyper-V Hostname A>>, move the cluster group to <<Hyper-V Hostname A>>.

```
move-clustergroup “Available Storage” –node <<Hyper-V Hostname A>>
```

Verify the location of the “Available Storage” cluster group is on <<Hyper-V Hostname A>>.

```
get-clustergroup “Available Storage”
```

Connect to the new CSV LUN as a shared LUN with SnapDrive to the Hyper-V cluster with no mountpoint. Modify the following command to include additional Hyper-V nodes.

```
sdcli disk connect –p <<var_ntap_B_hostname>>:/vol/CSV_B/prod/prod_csv.lun –dtype shared –rs n –IG  
<<Hyper-V Hostname A>> <<Hyper-V Hostname A>> <<Hyper-V Hostname B>> <<Hyper-V Hostname>> –e  
“Available Storage”
```

Confirm the new disk has been created. Note the name of the Cluster Disk Resource name of the shared LUN that was created.

```
get-clustergroup “Available Storage” | get-clusterresource | fl
```

The name of the new Cluster Disk Resource will be in a GUID format.

Rename the Cluster Disk Resource.

```
$resource = “<<Name of the shared LUN that was created>>”  
Get-ClusterResource $resource | %{ $_.Name = “CSV_Prod” }
```

Create new clustered shared volume using the Cluster Disk Resource name of the shared LUN that was just created.

```
add-clustersharedvolume “CSV_Prod”
```

Confirm that the new cluster shared volume has been created and is available.

```
get-clustersharedvolume
```

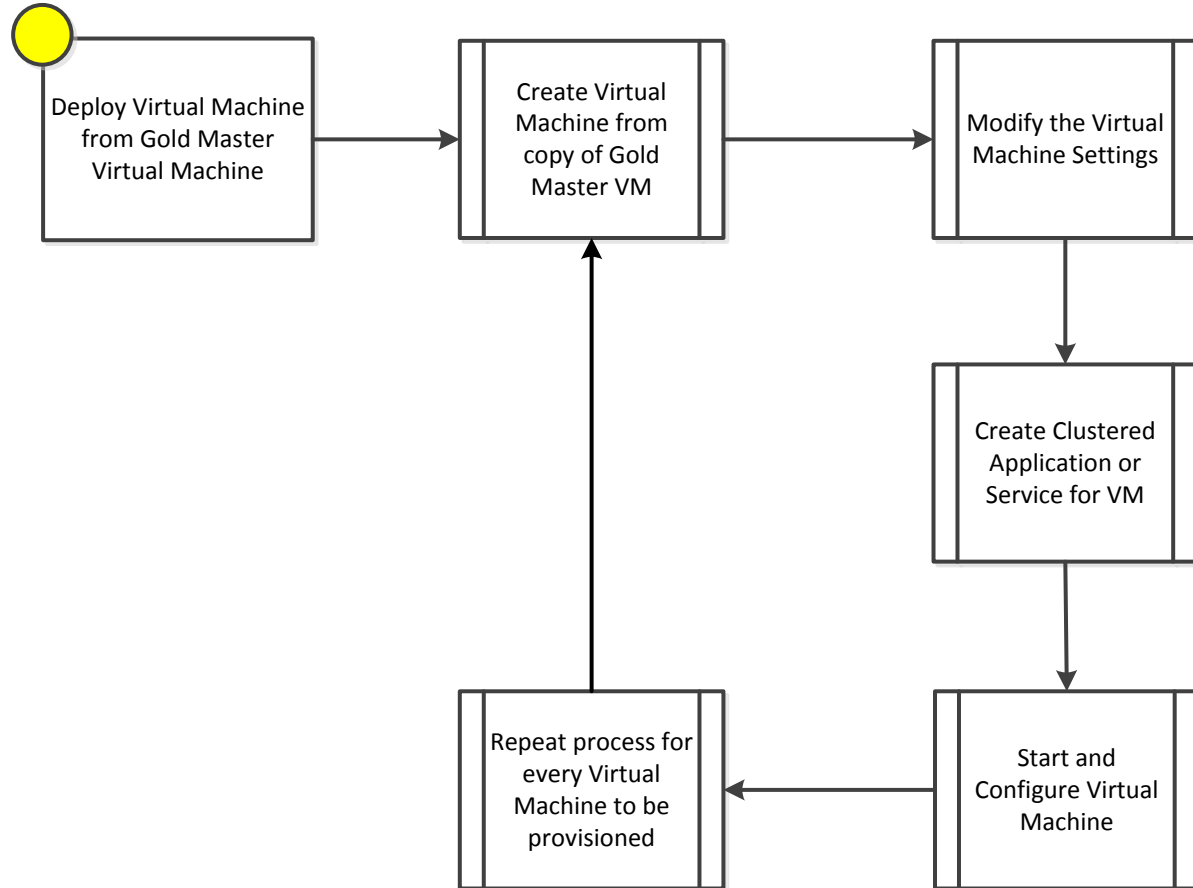
9. Repeat for each Cluster Shared Volume to be provisioned.

Deploy Virtual Machine from Gold Master Virtual Machine

The deployment of a Virtual Machine from Gold Master Virtual Machine process is comprised of the following high-level steps:



Microsoft



Overview

The deployment process of a Virtual Machine takes advantage of the built-in cloning capabilities of the NetApp storage.

This section provides high-level walkthrough on how to deploy Hyper-V Virtual Machines from a Gold Master Virtual Machine image for use into the Fast Track Fabric Management (FM). The following assumptions are made prior to deployment:

- A Gold Master Virtual Machine image has been created and stored on Cluster Shared Volume
- NetApp PowerShell Toolkit 1.7 or higher installed on Hyper-V cluster nodes

Deploy the Virtual Machine

1. Start a PowerShell session on Hyper-V cluster node <<Hyper-V hostname A>> with administrative rights on the Hyper-V node.



```
import-module dataotap
import-module failoverclusters
import-module hyperv
```

2. Create a virtual machine file from a clone of the Gold Master Virtual Machine file.

```
copy-naostfile C:\ClusterStorage\CSV\goldmaster.vhd C:\ClusterStorage\CSV\prod.vhd
```

3. After the virtual machine file has been created, open the Hyper-V Manager. Right click on the Hyper-V server <<Hyper-V hostname A>>, select New > Virtual Machine. Provide the name of the virtual machine and set the location of the virtual machine to be the Cluster Shared Volume. Click Next.

The screenshot shows the 'New Virtual Machine Wizard' window with the title bar 'New Virtual Machine Wizard'. The main window has a left sidebar with a list of steps: 'Before You Begin', 'Specify Name and Location' (which is highlighted), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area of the wizard is titled 'Specify Name and Location' and contains the following text: 'Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' Below this text is a 'Name:' label followed by a text box containing 'VM-Prod'. Another paragraph of text follows: 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.' Below this is a checkbox labeled 'Store the virtual machine in a different location' which is checked. To the right of the checkbox is a 'Location:' label followed by a text box containing 'C:\ClusterStorage\CSV_Gold' and a 'Browse...' button. At the bottom of the main area is a yellow warning icon followed by the text: 'If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.' At the bottom of the wizard window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

4. Assign the memory for the virtual machine. Click Next.



New Virtual Machine Wizard

 **Assign Memory**

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 65536 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

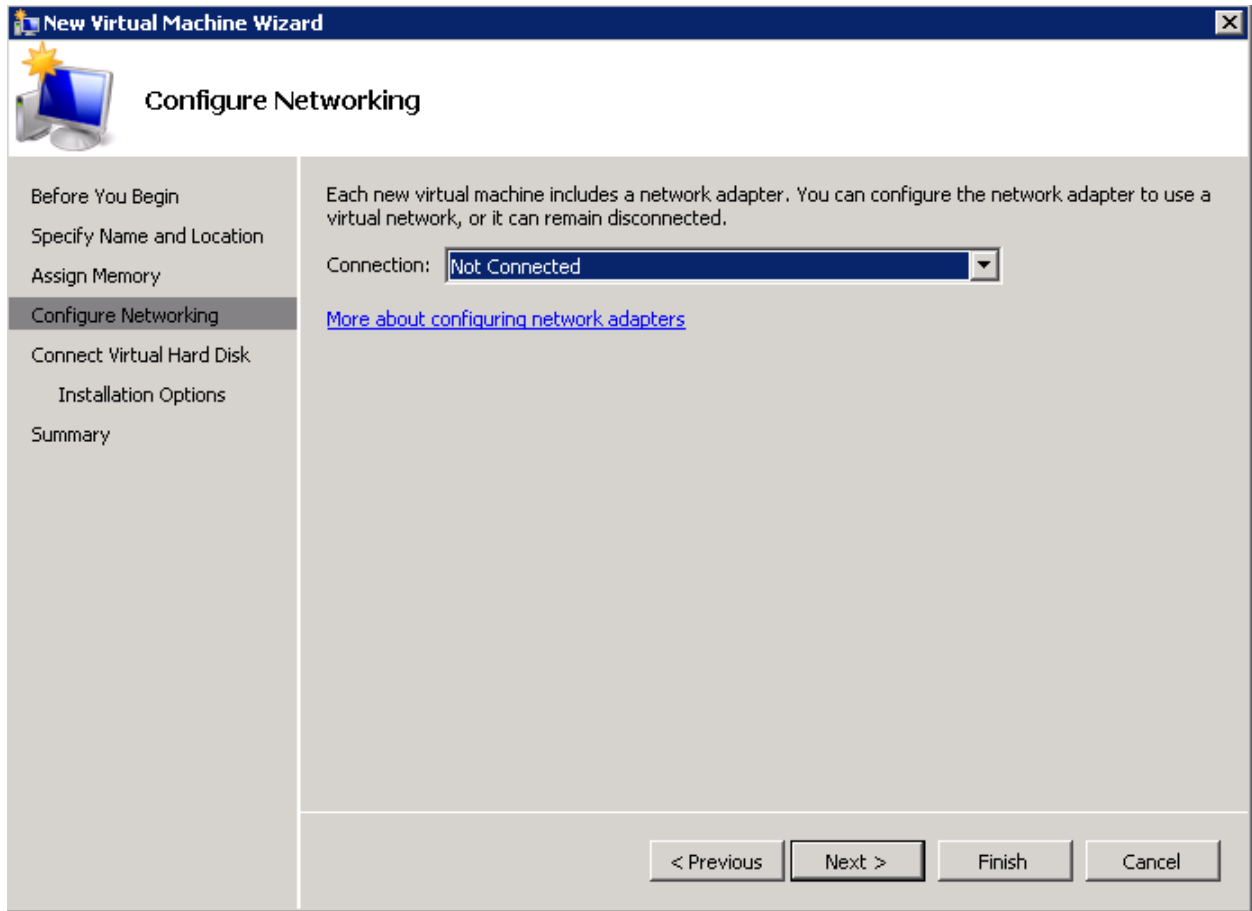
Memory: MB

 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

[More about determining the memory to assign to a virtual machine](#)

< Previous Next > Finish Cancel

5. In the Configure Networking dialog, leave the default setting of Not Connected. The network settings for the virtual machine will be set later. Click Next.



6. Select "Use an existing virtual hard disk" and set the path to the virtual disk file that was created from the Gold Master virtual machine file. Click Next.

New Virtual Machine Wizard

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ Create a virtual hard disk

Name: VM-Prod.vhd
Location: C:\ClusterStorage\CSV_Gold\VM-Prod\ Browse...
Size: 127 GB (Maximum: 2040 GB)

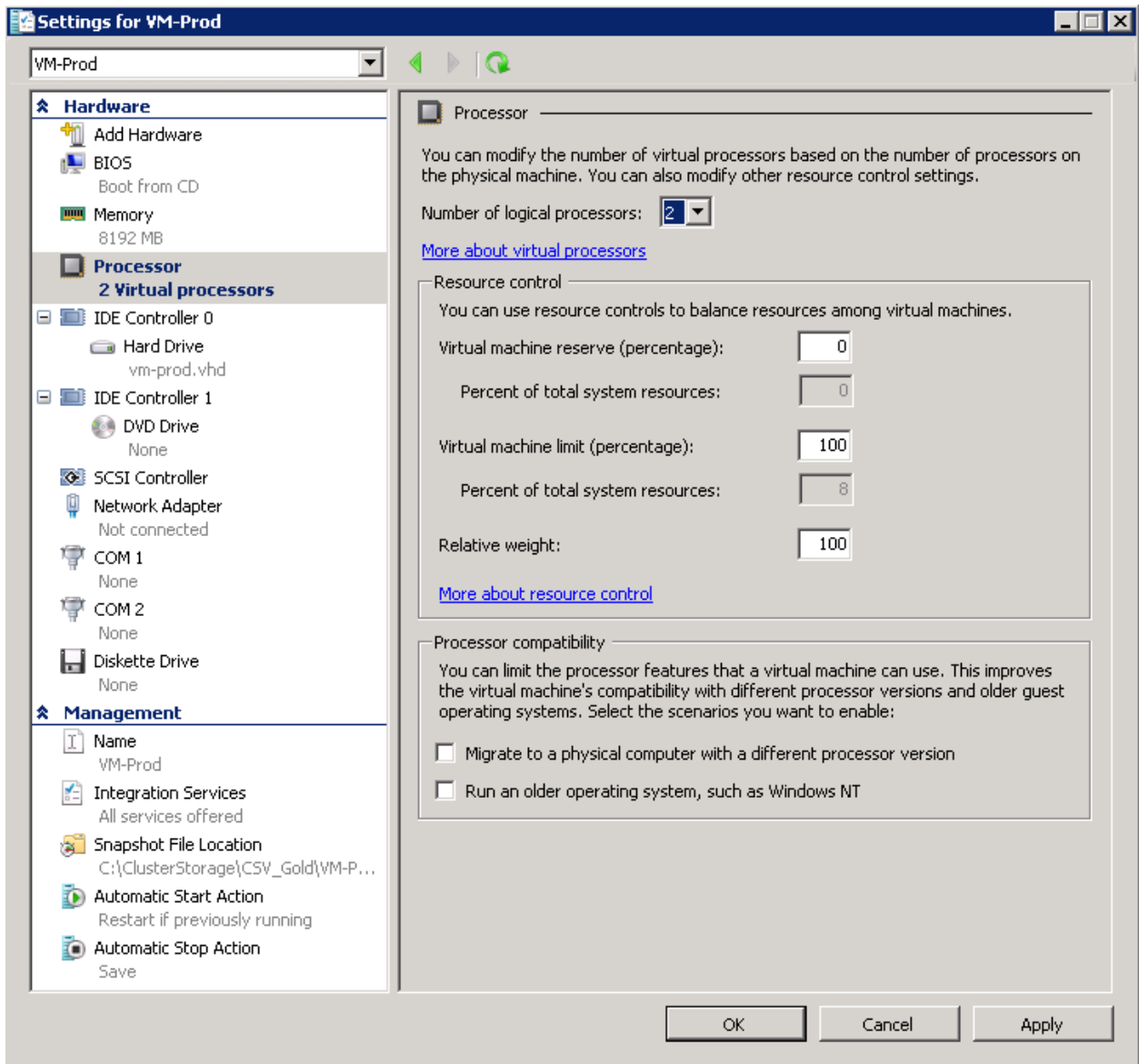
☒ Use an existing virtual hard disk

Location: C:\ClusterStorage\CSV_Gold\vm-prod.vhd Browse...

☐ Attach a virtual hard disk later

< Previous Next > Finish Cancel

7. Click Finish to complete the wizard.
8. In Hyper-V Manager, right click on the virtual machine that was created and select Settings.
Configure the number of logical processors and resource control settings for the logical processors.



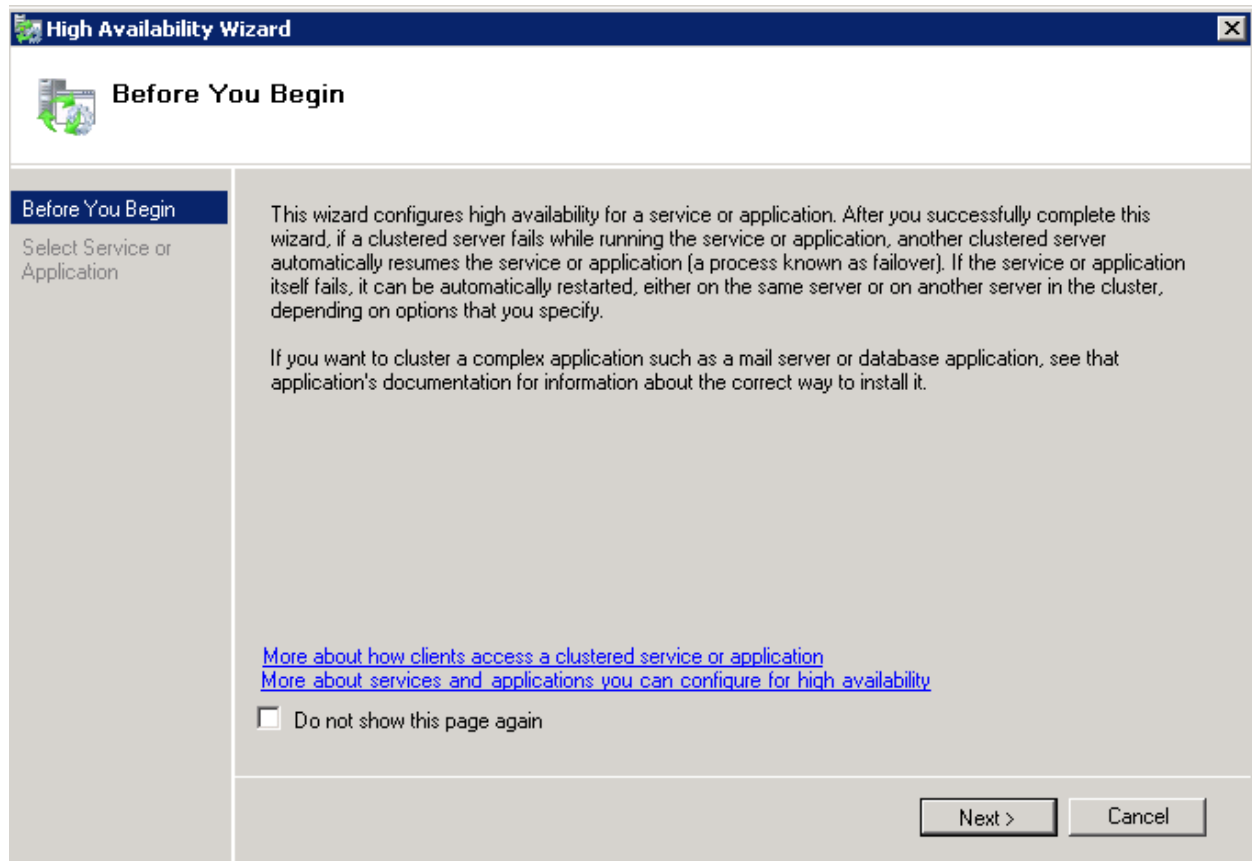
9. Add four network adapters to the virtual machine. Configure the virtual adapters with the following network settings:

Network	VLAN ID
VM-Data	804
iSCSI-Fabric-A	802
iSCSI-Fabric-B	807
App-Cluster-Comm	806

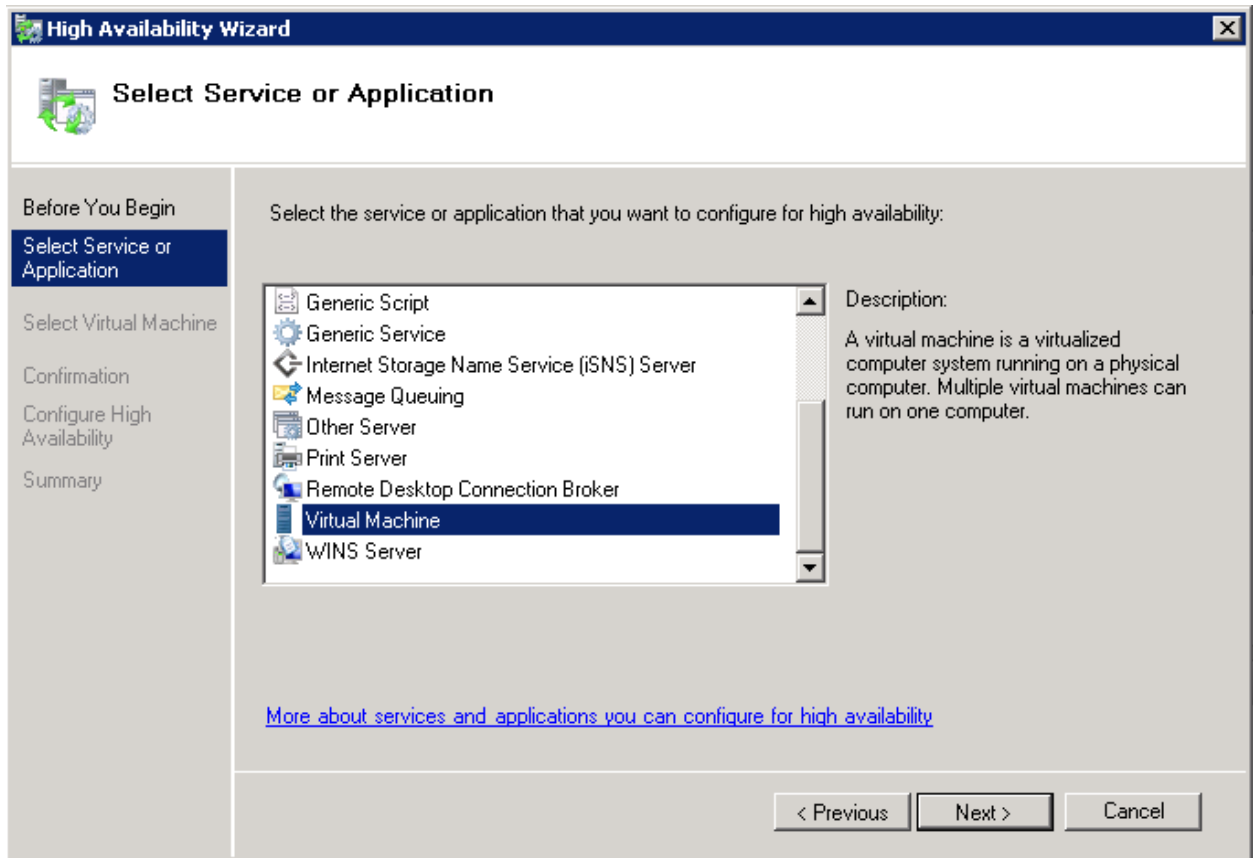
10. After configuring the virtual machine settings, open Window Failover Cluster Management to make the virtual machine highly available via Windows Failover Clustering.
11. Select the cluster name, right click and select the "Configure a Service or Application" action.



12. Click Next to start the High Availability Wizard.



13. Select Virtual Machine from the list of services and applications. Click Next.



14. Select the virtual machine that you created to add it to the cluster. Click Next.



High Availability Wizard

Select Virtual Machine

Before You Begin
Select Service or Application
Select Virtual Machine
Confirmation
Configure High Availability
Summary

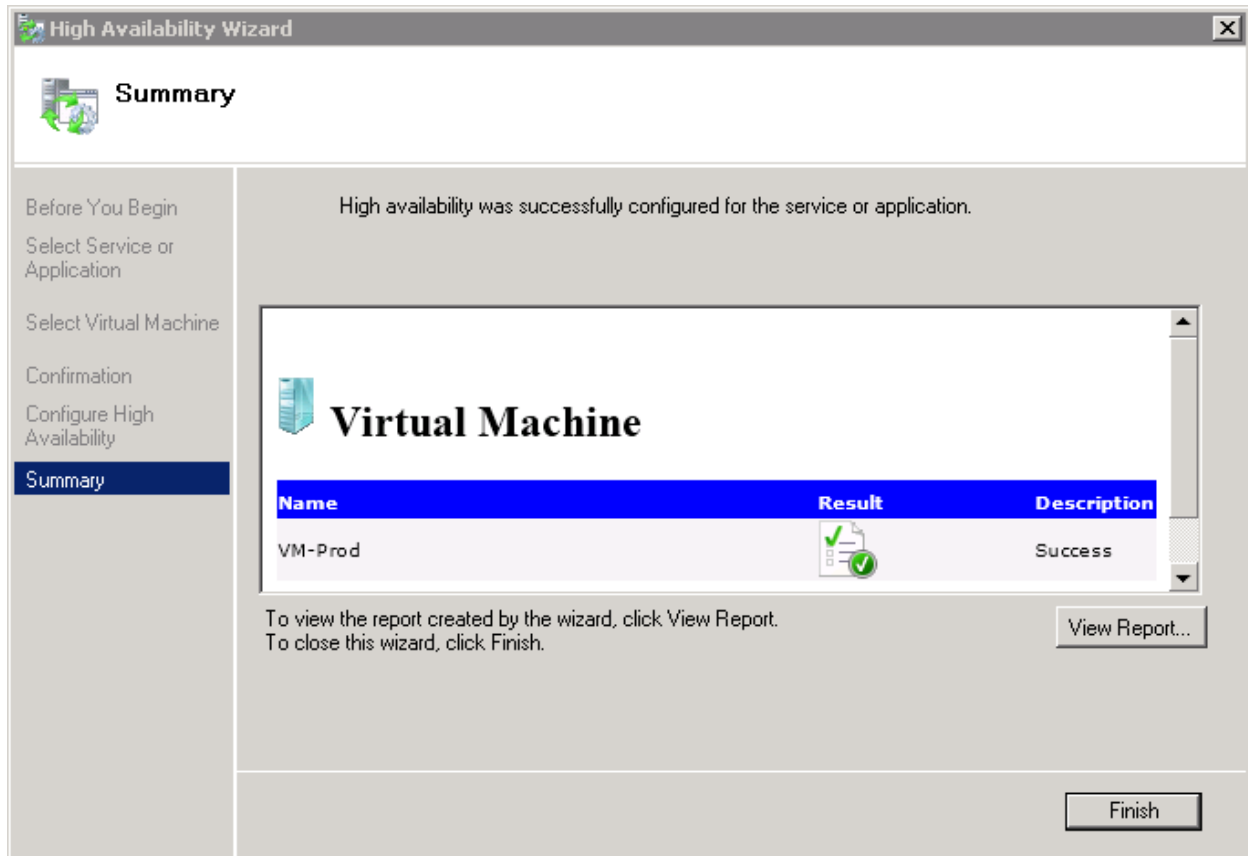
Select the virtual machine(s) that you want to configure for high availability.

Name	Status	Host Server
☐ Infra-DC-01	Running	VMHost-Infra-01.flexpod.test
☐ Infra-DC-02	Running	VMHost-Infra-02.flexpod.test
☒ VM-Prod	Off	VMHost-Infra-02.flexpod.test

[Refresh](#)

< Previous Next > Cancel

15. If the virtual machine was added successfully, click Finish. If the virtual machine was not added successfully, review the cluster log for troubleshooting assistance.



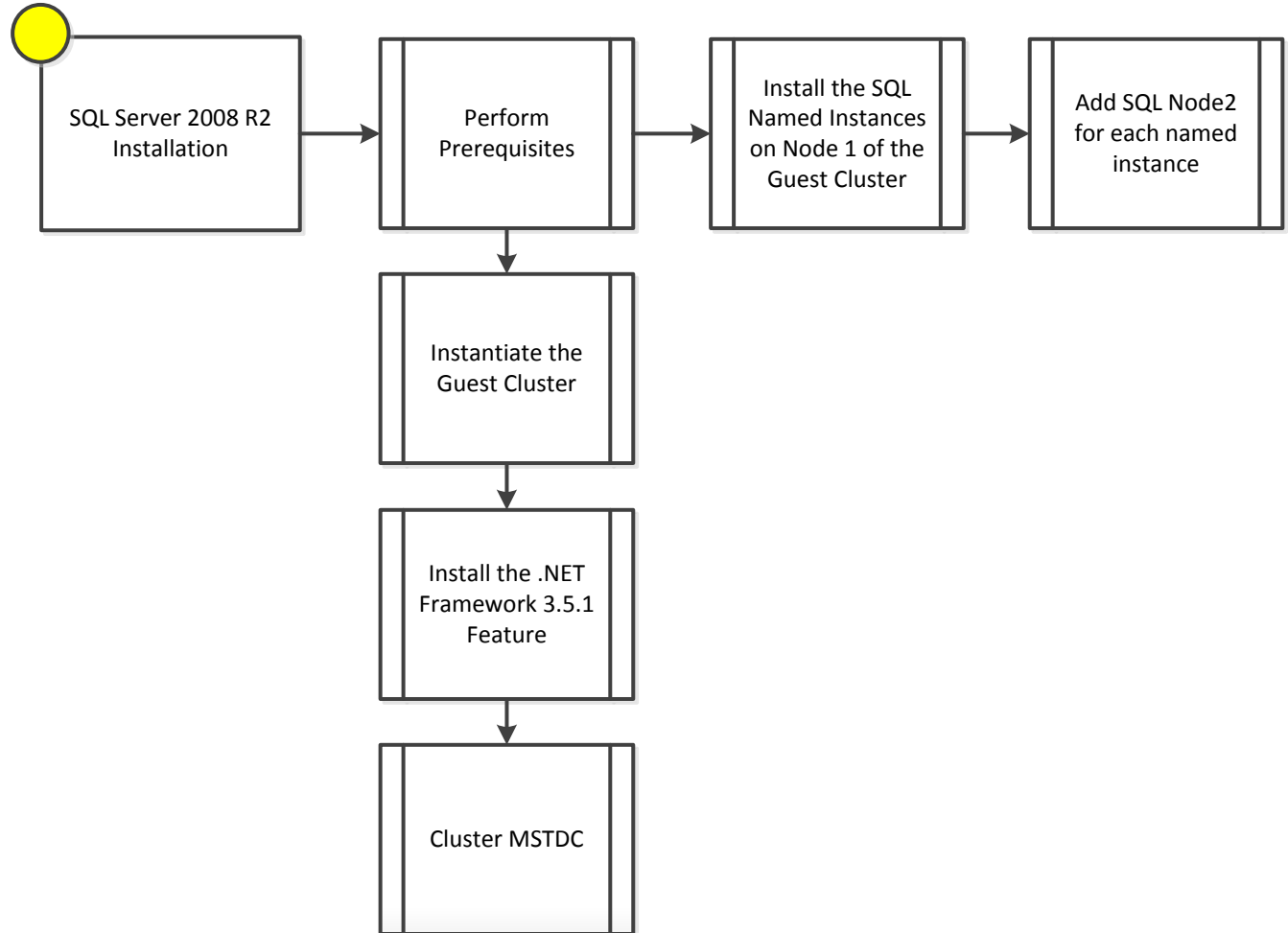
16. Click on the Cluster Group that was created when the Virtual Machine was added to the cluster. In the center pane of the console, select the virtual machine and then right click on the virtual machines and select "Properties".
17. Click on the "Network for live migration" tab. Clear all Checkboxes except LiveMigration. Click Ok.
18. Start the virtual machine from the Windows Failover Cluster management tool. Connect to the virtual machine.
19. The virtual machine will go into mini-setup. Set the keyboard and language settings. Set the license key on the virtual machine. Accept the EULA.
20. After logging into the virtual machine, assign IP addresses to the virtual machine network interfaces.
21. Change the virtual machine name and add the virtual machine to the Active Directory. This change will require a reboot of the virtual machine.
22. After reboot, install hotfixes and any roles or features required for your environment.
23. Repeat for each Virtual Machine to be provisioned.

SQL Server 2008 R2 Cluster Installation

The SQL Server 2008 R2 installation process includes the following high-level steps:



Microsoft



Overview

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

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

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



This section provides high-level walkthrough on how to install SQL Server 2008 R2 SP1 with Cumulative Update 4 (CU4) (version 10.50.2796.0) into the Fast Track fabric management.¹ The following assumptions are made prior to installation:

- Two to four base virtual machines running Windows Server 2008 R2 (x64) have been provisioned for SQL Server
- 20 iSCSI LUNs have been assigned to the virtual machine guests
- One LUN – quorum (1 GB)
- One LUN – Microsoft Distribution Transaction Coordinator service (MSDTC) (1 GB)
- Two LUNs for each fabric management component database (18 LUNs for all components)

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

Table 1 Database Instances and Requirements

Virtual Machine Manager	SCVMMDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Operations Manager	SCOMDB	Database Engine, Full-Text Search	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Operations Manager Data Warehouse	SCOMDW	Database Engine, Full-Text Search	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Service Manager	SCSMDB	Database Engine, Full-Text	SQL_Latin1_General_CP1_CI_AS	2 LUNs

¹ The SQL Server 2008 R2 builds that were released after SQL Server 2008 R2 was released - <http://support.microsoft.com/kb/981356>.

² The default SQL Server collation settings are not supported for multi-lingual installations of the Service Manager component. Only use the default SQL Server collation if multiple languages are not required. Note that the same collation must be used for all Service Manager databases (Management, Data Warehouse, and Reporting Services).



Search				
Service Manager Data Warehouse	SCSMDW	Database Engine, Full-Text Search	SQL_Latin1_General_CP1_CI_AS	2 LUNs
	SCSMAS	Analysis Services	SQL_Latin1_General_CP1_CI_AS	2 LUNs
	SCSPFarm	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Orchestrator	SCODB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
App Controller	SCACDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs
Windows Server Update Services (optional)	SCWSUSDB	Database Engine	SQL_Latin1_General_CP1_CI_AS	2 LUNs

Appendix C outlines the required SQL Server instances and associated recommended node placements.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following accounts have been created:

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



Groups

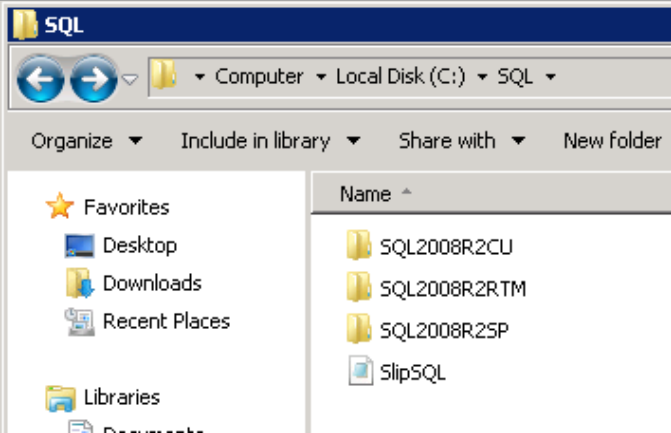
Verify that the following security groups have been created:

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

Create the SQL Server 2008 R2 Slipstreamed Source

For Fast Track, the SQL Server installation will use SQL Server 2008 R2. In order to perform the installation, a slipstreamed version of the SQL Server 2008 R2 with SP1 and CU4 must be created. To support this operation, a script has been created to automate this process. Creating slipstreamed builds of SQL Server with this script (SLIPSQL.PS1) is a non-destructive action and does not modify the source files. To create a slipstreamed build using this automation, follow the provided steps.³

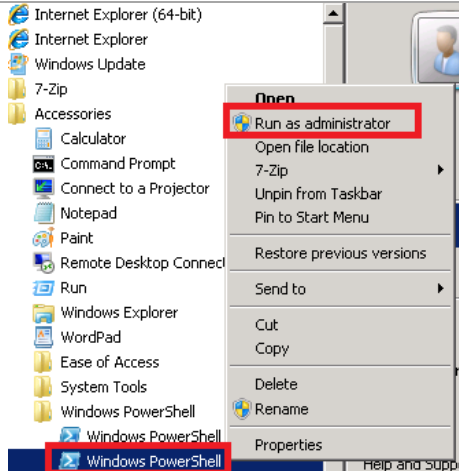
When completed, perform the following steps:

Perform the following steps on the First Fabric Management Host computer.	
On a local drive with sufficient space create a directory called "SQL". ⁴	
Within the \SQL folder, create the following subfolders: \SQL2008R2CU \SQL2008R2RTM \SQL2008R2SP	
Copy the original SQL Server 2008 R2 source media to \SQL\SQL2008R2RTM created in the previous step.	

³ The actions in the script are adapted from <http://blogs.msdn.com/b/petersad/archive/2011/07/13/how-to-slipstream-sql-server-2008-r2-and-a-sql-server-2008-r2-service-pack-1-sp1.aspx>.

⁴ The final slipstreamed source is ~6.5GB in size.



Copy the three Service Pack files to the folder named SQL\SQL2008R2SP created in the previous step. Note: SQL Server 2008 R2 Service Pack 1 can also be downloaded from http://www.microsoft.com/download/en/details.aspx?id=26727. The three architectures of Service Pack 1 should be included. The required package names are listed in the next pane.	SQLServer2008R2SP1-KB2528583-IA64-ENU.exe SQLServer2008R2SP1-KB2528583-x64-ENU.exe SQLServer2008R2SP1-KB2528583-x86-ENU.exe
Copy the three SQL Server 2008 R2 SP1 Cumulative Update 4 (CU4) files to the folder named SQL\SQL2008R2CU created in the previous step. Note: SQL 2008 R2 Service Pack 1 CU4 can also be downloaded from http://support.microsoft.com/kb/2633146. The three architectures of CU4 should be included. The required package names are listed in the next pane.	Expand zip to → SQLServer2008R2-KB2633146-IA64.exe Expand zip to → SQLServer2008R2-KB2633146-x64.exe Expand zip to → SQLServer2008R2-KB2633146-x86.exe
Run Microsoft Windows PowerShell® command line interface as an Administrator.	 The screenshot shows a Windows Start menu search for 'Windows PowerShell'. The search results list various applications including Internet Explorer, Windows Update, 7-Zip, Accessories, Calculator, Command Prompt, Connect to a Projector, Notepad, Paint, Remote Desktop Connection, Run, Windows Explorer, WordPad, Ease of Access, System Tools, Windows PowerShell, and another Windows PowerShell entry at the bottom. A right-click context menu is open over the bottom 'Windows PowerShell' entry, with the 'Run as administrator' option highlighted by a red rectangle.



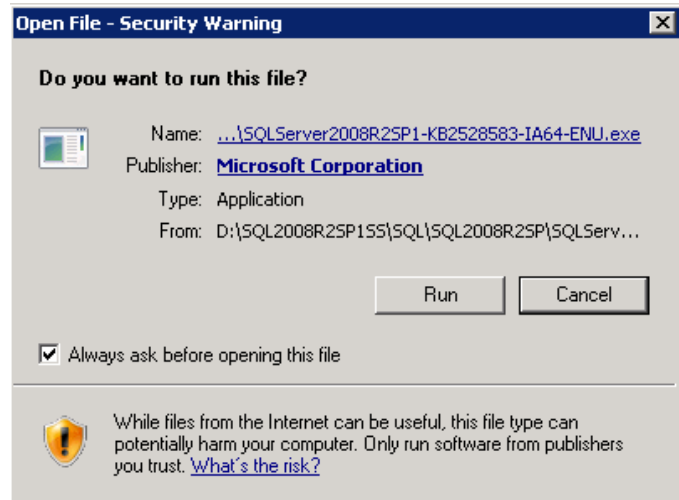
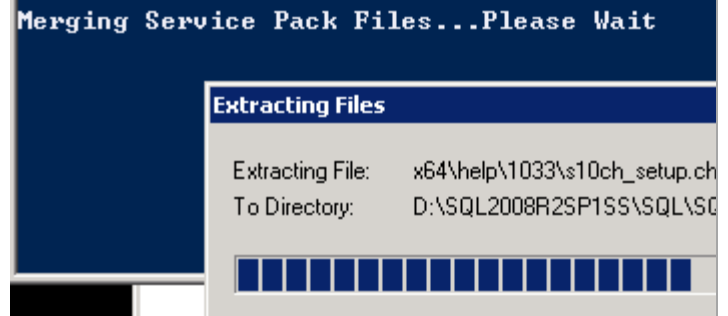
Copy the text for <i>SLIPSQL.PS1</i> from Appendix B and save it in a file named <i>SLIPSQL.PS1</i> in the SQL directory. Run the script SLIPSQL.PS1 in PowerShell. Note: before this script can be run the execution policy in PowerShell must be set to Bypass or Unrestricted. This can be performed with the following command: Get-ExecutionPolicy Note: capture the policy state for later use Set-ExecutionPolicy –ExecutionPolicy Bypass When the script is complete, the execution policy can be returned to its previous state by running the Set-ExecutionPolicy command and specifying the prior state.	<pre>Administrator: Windows PowerShell PS C:\SQL2008> .\slipsql.ps1</pre>
The SQL Server Slipstream Script will launch. At each prompt, provide the location of the following folders: • SQL RTM Source Path – (<drive>\SQL\SQL2008R2RTM). • SQL Service Pack Source Path – (<drive>\SQL\SQL2008R2SP). • SQL Cumulative Update Source Path – (<drive>\SQL\SQL2008R2CU). Note: folder paths must NOT contain spaces.	<pre>SQL Server Slipstream Script ***** * This script will merge a SQL 2008 R2 Service Pack and * * Cumulative Update into a single slipstreamed build * ***** Enter the SQL RTM Source Path Enter the location <folder>: C:\SQL\SQL2008R2RTM Enter the SQL Service Pack Source Path Enter the location <folder>: C:\SQL\SQL2008R2SP Enter the SQL Cumulative Update Source Path Enter the location <folder>: C:\SQL\SQL2008R2CU Provided Source Paths SQLRTMPath: C:\SQL\SQL2008R2RTM SQLFCUPath: C:\SQL\SQL2008R2SP SQLCUPath: C:\SQL\SQL2008R2CU</pre>
When prompted, provide a path for the new slipstreamed build to be created. Note that this folder must not exist prior to running this script. Note: if a folder exists with this name, the script will return an error and exit gracefully.	<pre>Enter the desired SQL Slipstream Target Path <Note this path should not previously exist> Enter the location <folder>: C:\SQL\SQL2008R2SP1CU4</pre>
A confirmation page will be presented. Verify that the correct locations are specified. If not, type “N” to re-enter the values. If they are correct, type “Y” and press Enter.	<pre>Confirm Source and Target Folders ----- SQL RTM Source Path: C:\SQL\SQL2008R2RTM SQL Service Pack Source Path: C:\SQL\SQL2008R2SP SQL Cumulative Update Source Path: C:\SQL\SQL2008R2CU SQL Cumulative Update Source Path: C:\SQL\SQL2008R2SP1CU4 Are these values correct? [Y] Yes [N] No [?] Help <default is "Y">: _</pre>
The script will begin to create the slipstreamed build. The initial phase requires the duplication of the source RTM media to the new location. This can take several minutes and the script may not appear to be performing any actions. Please be patient during this process and do not perform any action that may otherwise interrupt the process.	<pre>Path does not exist, creating C:\SQL\SQL2008R2SP1CU4 Copying files, please be patient... _</pre>



After a few minutes the Service Pack files will be extracted one by one. This process may require interaction depending on the source of the downloaded Service Pack and security settings of the operating system.

Note: if security warnings are displayed due to the platform security configuration, please click **Run**.

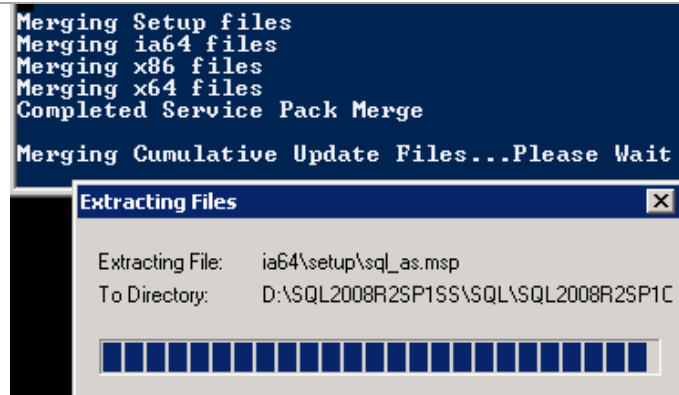
When complete, each architecture will be integrated with the source build to update the media to include SP1.



Cumulative Update files will be extracted one by one. This process may require interaction depending on the source of the downloaded Cumulative Update files and security settings of the operating system.

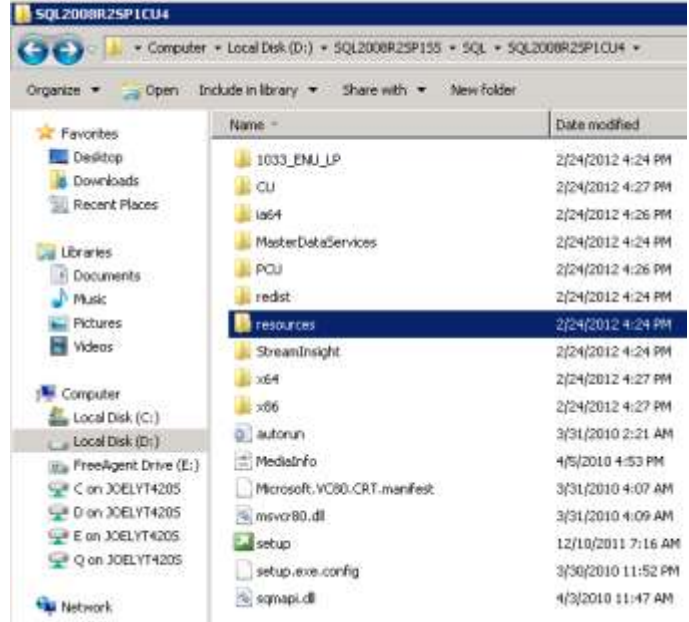
Note: if a security warning is displayed due to the platform security configuration, please click **Run**.

When complete, each architecture will be integrated with the source build to update the media to include SP1 CU4.

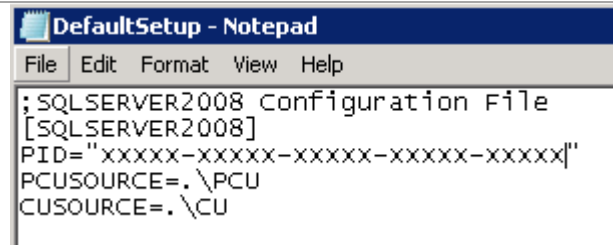




When completed, the folder specified for the destination build will be created containing the newly slipstreamed SQL Server build.

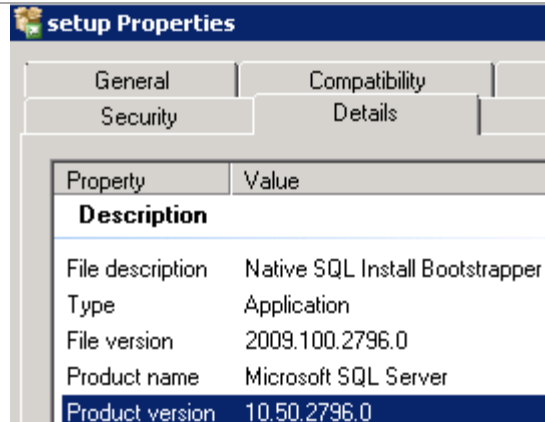


Verify that each architecture folder (\x86, \x64 and \ia64) has a DefaultSetup.ini with the edited PCUSOURCE and CUSOURCE. These values can also be supplied in a command line installation.



In order to verify if SQL Server 2008 R2 SP1 CU4 was properly slipstreamed, right-click the setup.exe file and select the **Details** tab. The **File version** property should read 10.50.2796.0 to reflect the updated, slipstreamed version.

When completed, copy the folder to an accessible share for installation into the virtual machine.





Establish the SQL Server Guest Cluster

Assuming storage with iSCSI interface is available and the customer is implementing a SQL Server guest cluster, the following steps can be followed to create the SQL Server guest cluster.

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

- One LUN – quorum (1 GB).
- One LUN – MSDTC (1 GB).
- Two LUNs for each fabric management component instance (20 LUNs for all products).

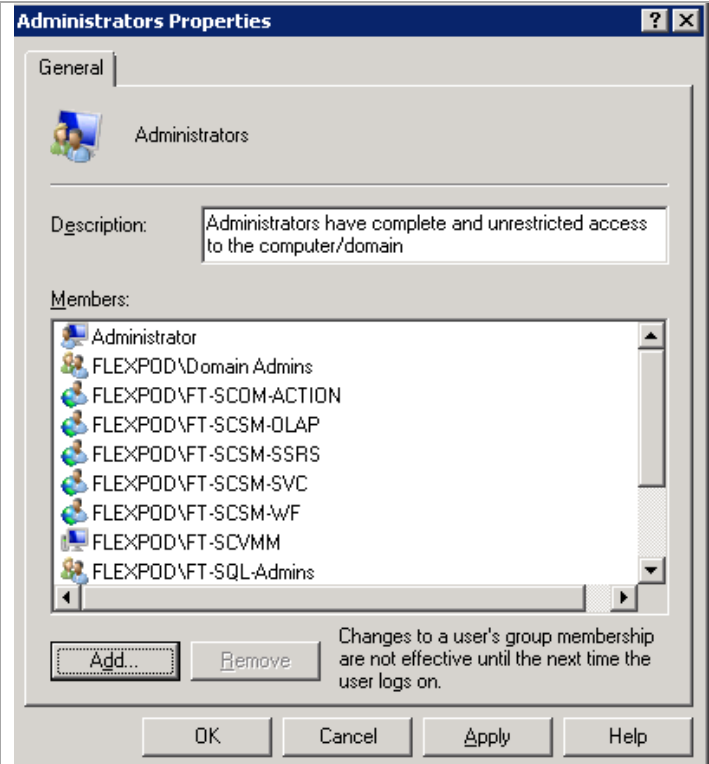
During the provisioning process, four virtual machines were built to the specifications outlined in the Fast Track Reference Architecture Guide to support SQL Server operations for fabric management. When created, the iSCSI targets must be configured within each virtual machine to make them accessible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

Perform the following steps on **both Fabric Management SQL Server** virtual machines.

Logon to the First node in the SQL Cluster, with a user with Local Admin rights.

Ensure the following accounts and/or groups are members of the Local Administrators group on the first and second SQL Nodes.

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

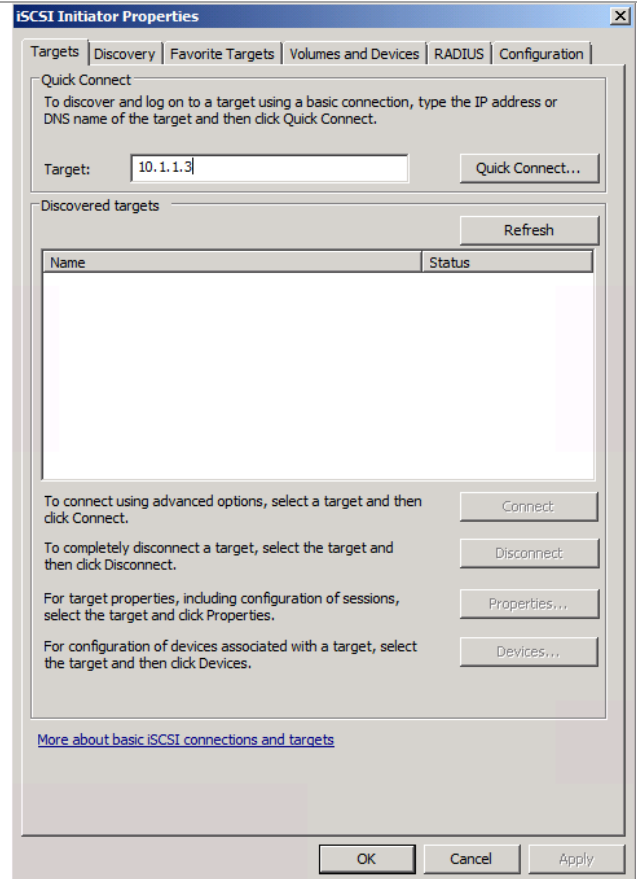




To attach the guest cluster to the iSCSI LUNs, the iSCSI Initiator must be configured on each SQL Server virtual machine.

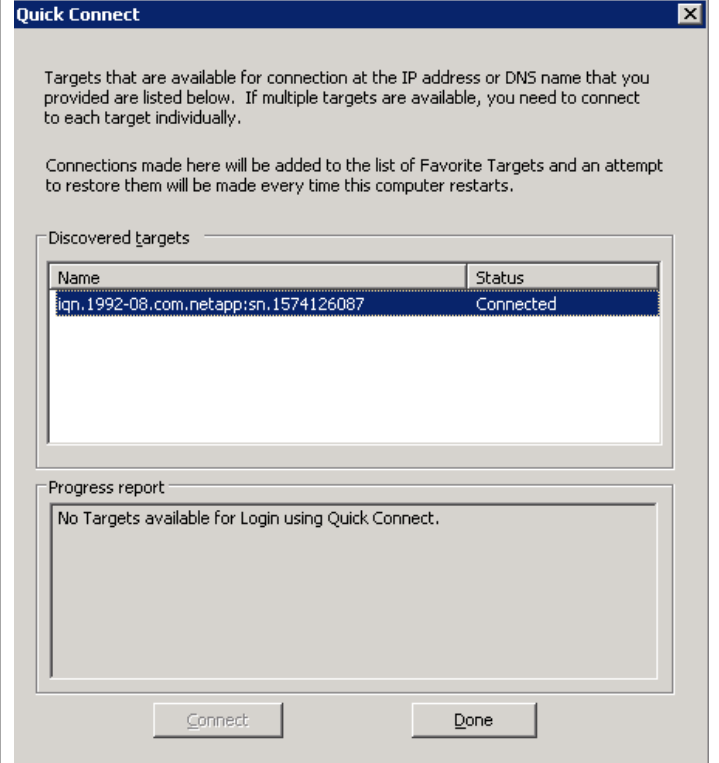
Note: third-party Storage Area Network (SAN) connectivity software can be used in place of the in-box iSCSI Initiator. If a third-party solution is used, the in-box iSCSI Initiator steps can be skipped.

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



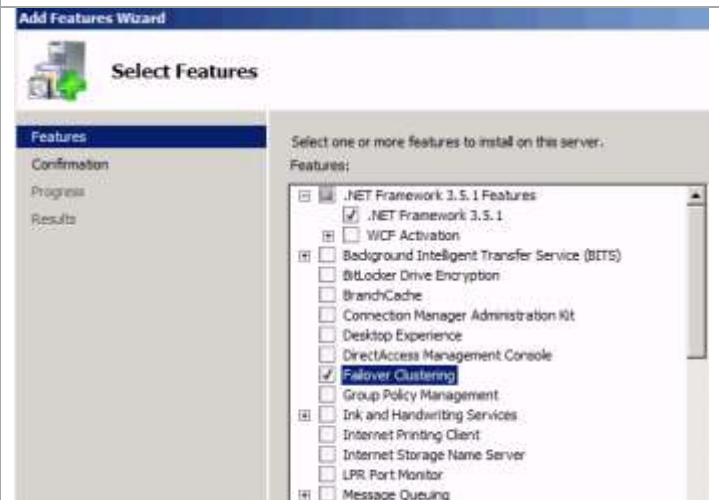


The **Quick Connect** dialog will provide a list of discovered targets. When the **Progress report** section shows *Login Succeeded*, click **Done** to close the dialog.



- **Windows Features**

Open Server Manager and select Features.
Click the Add Features link launching the Add Features wizard.
Expand .NET Framework 3.5.1 Features.
Select the .NET Framework 3.5.1 Feature. Leave the WCP Activation check box unselected.
Select the Failover Clustering feature.
Click Next > Install.



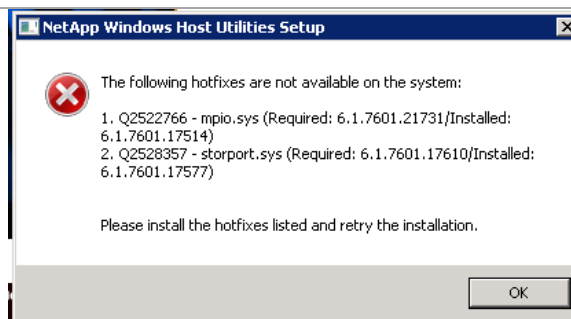


- **NetApp Windows Host Utilities Kit**
 1. Download and NetApp Windows Host Utilities Kit from the NOW.netapp.com Site.
 2. Launch the Installer, click next, Accept the EULA, and click Next.
 3. Select Yes, Install support for Multipath I/O, and click Next.
 4. Click Next > Finish.

Ignore the HBA error. There is no HBA support in Hyper-V.

If you receive an error stating that you do not have correct versions of MPIO.SYS and/or STORPORT.SYS, this is because your system is not fully patched.

Install the requested HotFixes and repeat this step.



- **NetApp DSM MPIO**

Download and NetApp DSM MPIO package from the [NOW](http://NOW.netapp.com) site.

Launch the Installer.

Click Next then click OK to acknowledge the ALUA requirement.

Accept the EULA and click Next.

Enter the DSM License Key and click Next.

Leave the system account selected and click Next.

Click Next > Next > Install and when complete restart the system.

Ignore the HBA error. There is no HBA support for Hyper-V.



- **NetApp SnapDrive**
 1. Download and NetApp SnapDrive.
 2. Launch the Installer, click Next, Accept the EULA, and click Next.
 3. Select the Storage based Licensing method and click Next.
 4. Enter your User Name, and Organization information, and click Next.
 5. Enter the Account information for the <SnapDrive > account created earlier.
 6. Click Next and the select the “Enable Transport Protocol Settings Option.
 7. Select HTTPS.
 8. Enter the UserName: <domain>\<snapdrive> and enter the service account password.
 9. Click Next > Next > Next > Install > Finish.

The screenshot shows the 'SnapDrive® - Installation Wizard' window, specifically the 'Transport Protocol Default Setting' step. The window title bar includes the NetApp logo and the text 'SnapDrive® - Installation Wizard'. The main heading is 'Transport Protocol Default Setting' with a subtitle 'Specify Default Transport Setting for Storage System(s)'. A checkbox labeled 'Enable Transport Protocol Settings' is checked. Below this, there are three radio button options: 'RPC', 'HTTP', and 'HTTPS', with 'HTTPS' being selected. A text box below the radio buttons says 'Specify the user name and password for the HTTP/HTTPS Protocol selection.' followed by 'User Name:' and a text field containing 'netapp\SnapDrive'. Below that is 'Password:' and a text field with masked characters '.....'. At the bottom, there is a 'Port ID:' label and a text field containing '443'. The bottom of the window features three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner of the window.



- Set Firewall exceptions:

Open Windows Firewall with Advanced Security, by clicking Start > Administrative Tools > Windows Firewall with Advanced Security.

SnapDrive

1. Highlight Inbound Rules and click New Rule.
2. Select Program and click Next.
3. Enter the program path for the SnapDrive Service i.e. %ProgramFiles%\NetApp\SnapDrive\SWSvc.exe.
4. Click Next, then select the Allow the Connection options and click Next > Next.
5. Enter the rule Name <SnapDrive>, Description, and click Finish.

SQL Server

1. Click New Rule.
2. Select Port and click Next.
3. Select TCP and enter the Specific local port 1433. Click Next.
4. Select Allow the connection, and click Next > Next.
5. Give a rule Name <SQL Server>, and Description, and click Finish.
6. Repeat a-g for the Data warehouse SQL Server instance using a port of your specification (e.g, 1444).

SQL Server Discovery

1. Click New Rule.
2. Select Port and click Next.
3. Select TCP and enter the Specific local port 445. Click Next.
4. Select Allow the connection, and click Next, then click Next again.
5. Give a rule Name <SQL Server Discovery>, and Description, and click Finish.



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

When complete, the storage should be brought online one at a time, initialized and formatted using SnapDrive.

Important Note: The installation of a SQL Cluster creates computer accounts in Active Directory for each instance in the cluster called cluster name objects (CNO). By default these objects are created in the default Computers container (e.g. cn=Computers) of the target Active Directory domain. The account used to perform the installation of the SQL Cluster requires the rights in Active Directory to create the associated CNOs for each product SQL instance. This occurs as a standard part of the SQL installation process. There are several approaches to mitigate this including using a higher privileged account for installation, delegation of rights in Active Directory for the account used for installation, or pre-creation of the computer accounts in the target Active Directory domain. Further discussion of this aspect of Windows Server Failover Cluster installation (and mitigation strategies) can be found in the Windows Server 2008 R2 Failover Cluster Step-by-Step Guide⁵.

To assist with the actual creation of the cluster, the following steps and automation have been provided:

Perform the following steps on the **First Fabric Management SQL Node** virtual machine with an account which has both local Administrator rights and permissions in Active Directory to create the SQL cluster name objects.

Validate cluster feasibility:

1. Open Server Manager and browse to Features > Failover Cluster Manager.
2. Select Validate a Configuration, then click Next.
3. Add both nodes one at a time into the Enter Name text field, and click Next.
4. Select Run only tests I select and click Next.
5. Scroll down to the storage section and clear all the storage related checks checkboxes.
 - a. *Note these will be run after we attach our iSCSI storage.
6. Click Next > Next.
7. Review the report and resolve any issues found by the validation wizard before continuing.



⁵ Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory - [http://technet.microsoft.com/en-us/library/cc731002\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731002(WS.10).aspx)



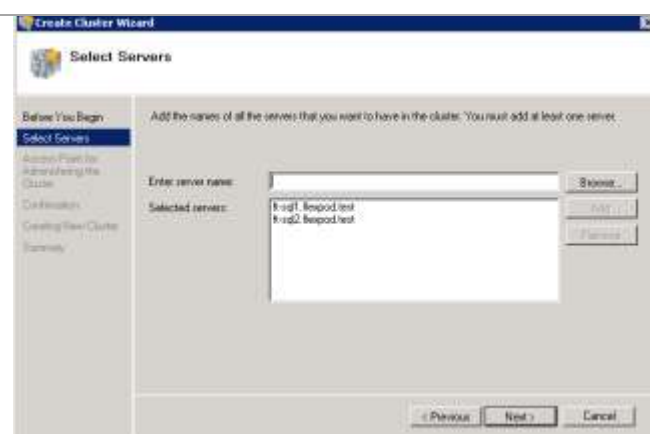
Navigate to %TEMP% and review the **Failover Cluster Validation Report** for errors and warnings. Perform any required remediation and re-perform the cluster tests above as required.

Note that you may ignore the storage warnings. We will provision storage for the cluster when we create the cluster.



Create majority node cluster:

1. In the Failover Cluster Manager, select Create a Cluster.
2. In the welcome screen, click Next.
3. Add both nodes one at a time into the Enter Name text field, and click Next.
4. Select Yes to run all validation tests, and click Next, then Next again.
5. Select Run all test and click Next, then Next again.
6. Click Finish, at this time you may safely ignore any warnings or errors related to clustered disks.
7. Enter the Cluster Name, Cluster IP, and click Next.
8. Review the configuration, and click Next > Finish.





Create quorum:

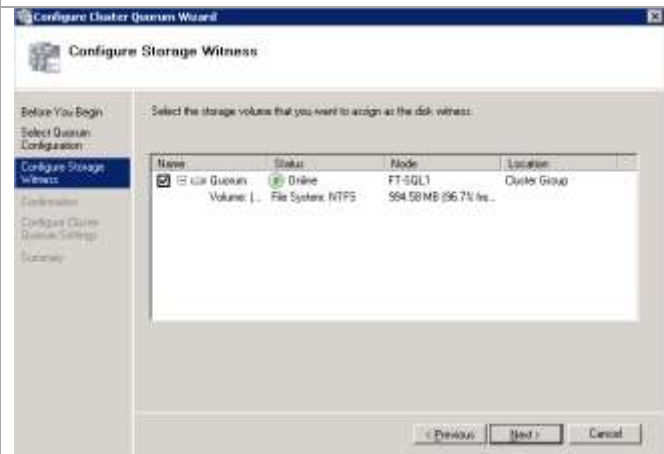
1. Log in to the cluster host server and open SnapDrive.
2. Select Disks and click Create Disk.
3. In the Welcome screen, click Next.
4. Enter the IP/FQDN for the vFiler0 Controller and click Add.
5. When enumeration has completed, select the target volume where you intend to add the LUN.
6. Add a LUN Name, LUN Description and click Next.
7. Select Shared (Microsoft Cluster Services only) and click Next.
8. Verify both nodes are shown for your cluster and click Next.
9. Select Assign a Drive Letter and pick a drive letter.
10. Set the LUN Size to the size designated earlier, click next then next again.
11. Highlight each node in the Cluster and select the iSCSI initiators to map the new LUN to.
12. Click Next, then Select Automatic and click Next.
13. Make sure that Select a cluster group by this node is selected.
14. Select the Cluster Group name, and click Next and then click Finish.
15. Repeat for SQL Server Data, and SQL Server Log LUNs.



In cluster manager, confirm that the disk was recognized. Rename it to Quorum by right clicking on the storage object and selecting “Properties”.



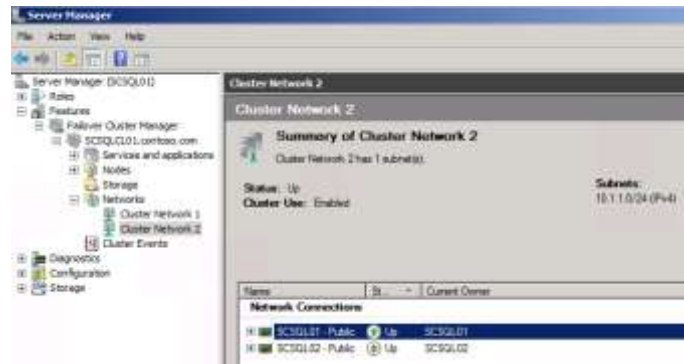
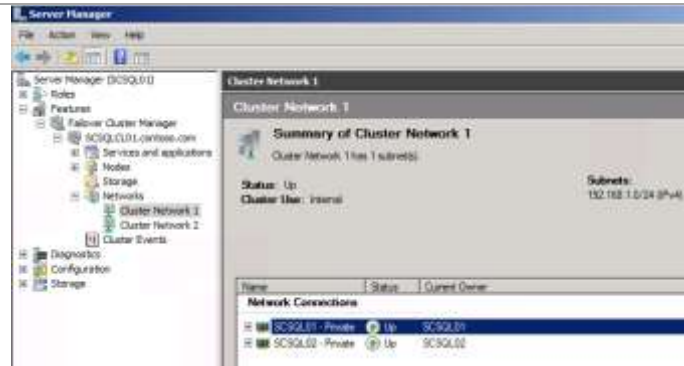
Change the Cluster quorum settings, by selecting the cluster object in the tree view to the left, right clicking and selecting “More Actions.” Select “Node and Disk Majority” and then select the new LUN as your Quorum disk.



Continue to create LUNs in SnapDrive and assign them to the cluster as with the Quorum disk. There should be one 1 GB LUN for MSDTC and 2 LUNs for each Fabric Component database (18 LUNs total).



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



Document all disk assignments in the cluster. Create a mapping table of available storage (by name) to drive letters. This information will be used during the SQL installation.

Storage		
Storage: 10 Total Disks - 10 online 9 Available Disks - 9 online 1 In Use Disks - 1 online	Total Capacity: Total: 81.97 GB Free Space: 81.28 GB Percent Free: 99.2%	Available Capacity: Total: 80.97 GB Free Space: 80.32 GB Percent Free: 99.2%
Disk	Status	Current Owner
Disk Witness in Quorum		
Cluster Disk 1 Volume: (G)	Online File System: NTFS	SCSQL01 1,021 MB (99.7% free)
Available Storage		
Cluster Disk 10 Volume: (L)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 2 Volume: (H)	Online File System: NTFS	SCSQL01 1,021 MB (99.8% free)
Cluster Disk 3 Volume: (E)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 4 Volume: (F)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 5 Volume: (G)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 6 Volume: (H)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 7 Volume: (I)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 8 Volume: (J)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)
Cluster Disk 9 Volume: (K)	Online File System: NTFS	SCSQL01 10 GB (99.2% free)



Clustering MSDTC on Node 1

Prior to performing the installation of SQL, the MSDTC service must be clustered. Please note that prior to installation, the first node of the SQL Server cluster must have ownership of the LUNs. The following steps and automation are provided to assist with the clustering of this service.

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 Active Directory to create the SQL Server CNOS.

To cluster the MSDTC service, from an elevated Powershell prompt, run the following commands:

Import-Module FailoverClusters

Add-ClusterServerRole -Name
<DTCClusterGroupName> -Storage
<DTCClusterDisk> -StaticAddress
<DTCClusterIPAddress>

Get-ClusterGroup <DTCClusterGroupName> |
Add-ClusterResource -Name
<DTCClusterResName> -ResourceType
"Distributed Transaction Coordinator"

Add-ClusterResourceDependency
<DTCClusterResName>
<DTCClusterGroupName>

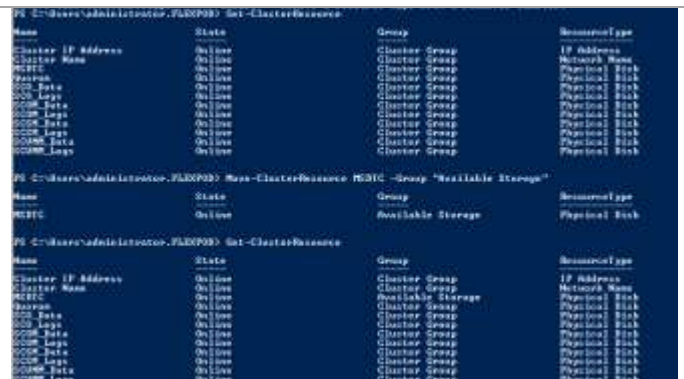
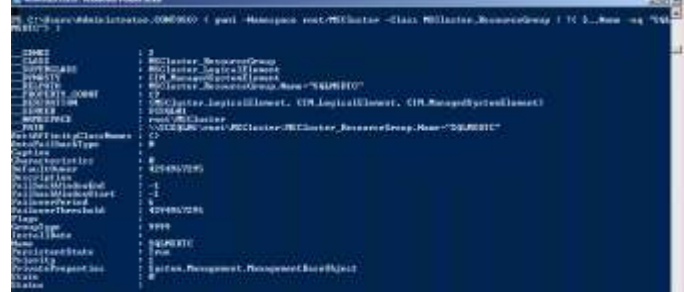
Add-ClusterResourceDependency
<DTCClusterResName> <DTCClusterDisk>

Start-ClusterGroup <DTCClusterGroupName>

(gwmi -Namespace root/MSCluster -Class
MSCluster_ResourceGroup | ?{ \$_.Name -eq
<DTCClusterGroupName>}
) .SetGroupType(103)

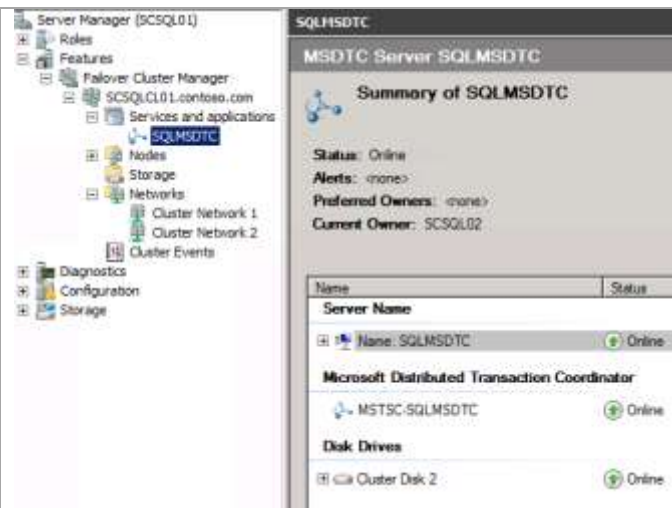
Move-ClusterGroup <DTCClusterGroupName> -
Node <Node1>

You may need to move the MSDTC LUN into the "Available Storage" group depending on how you created the LUN. You can do this with the Move-ClusterResource cmdlet.





Within the Failover Clustering MMC, verify that the MSDTC service has been properly created and clustered. It is important to verify that the icon for MSDTC is not that of a generic service to promote proper operation.



When the clustering of the MSDTC service is completed and verified, the installation of SQL in a cluster configuration can proceed.

Installation

Installing 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.

SQL Server Instance Name	SCVMM DB	SCACDB	SCODB	SCOMDB	SCOMDW	SCSMDB	SCSMAS	SCSMDW	SCSPFarm
SQL Server Instance Failover Cluster Network Name	SQLSCV MMDB	SQL SCACDB	SQL SCODB	SQLSCOMD B	SQLSCOMDW	SQLSCSMDB	SQLSCS MAS	SQLSCS MDW	SQLSCSPFa rm
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	Cluster Disk 16	Cluster Disk 18
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	Cluster Disk 17	Cluster Disk 19



SQL Server Instance Install Drive	E:	G:	I:	K:	M:	O:	Q:	S:	U:
SQL Server Instance DATA Drive	E:	G:	I:	K:	M:	O:	Q:	S:	U:
SQL Server Instance LOG Drive	F:	H:	J:	L:	N:	P:	R:	T:	V:
SQL Server Instance TEMPDB Drive	F:	H:	J:	L:	N:	P:	R:	T:	V:
Cluster Service Name	SQL Server (SCVMM DB)	SQL Server (SCACDB)	SQL Server (SCODB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)	SQL Server (SCSMDB)	SQL Server (SCSMA S)	SQL Server (SCSMD W)	SQL Server (SCSPFarm)
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	10.1.1.29	10.1.1.30
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	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	Cluster Network 2	Cluster Network 2

The template provided in Appendix A of this document should assist with capturing this information for the installation process. When 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 Serve Node** virtual machine with an account which has both local Administrator rights and permissions in Active Directory to create the SQL CNOS.



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

SCACDB (App Controller database instance).

SCODB (Orchestrator database instance).

SCOMDB (Operations Manager database instance).

SCOMDW (Operations Manager Data Warehouse instance).

SCSMAS (Service Manager SQL Analysis Services instance).

SCSMDB (Service Manager database instance).

SCSMDW (Service Manager Data Warehouse instance).

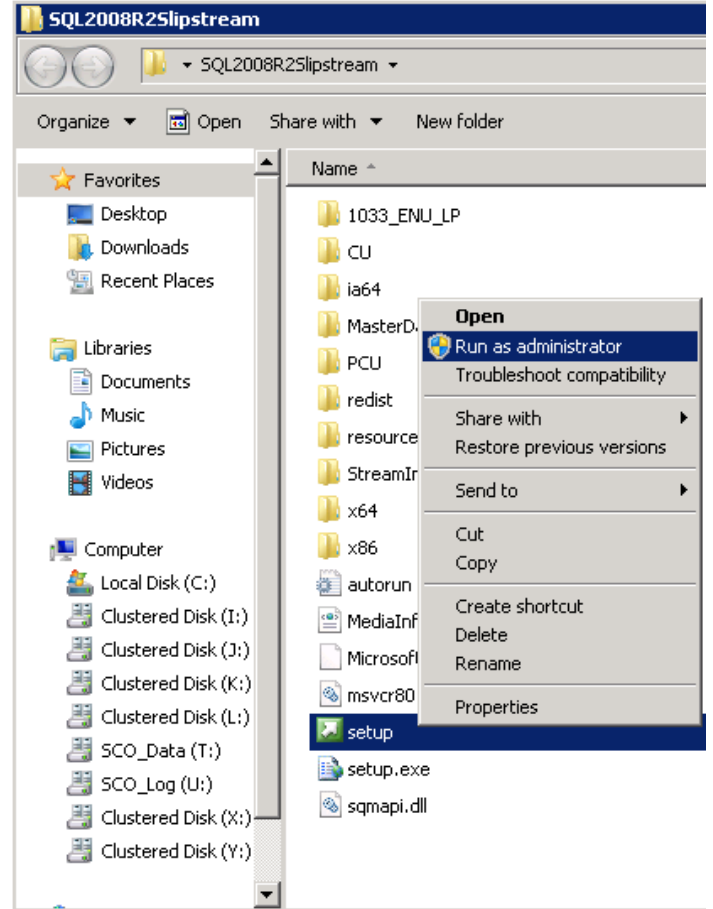
SCSPFarm (Service Manager self-service portal Microsoft SharePoint® Foundation 2010 services instance).

SCVMMDB (Virtual Machine Manager database instance and optional WSUS database instance).

For multi-instance failover clusters, installation for SQL Server 2008 R2 must be performed when for each instance. As such, these steps must be performed for each instance sequentially.



From the SQL Server 2008 R2 slipstreamed 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 New SQL Server failover cluster installation link.

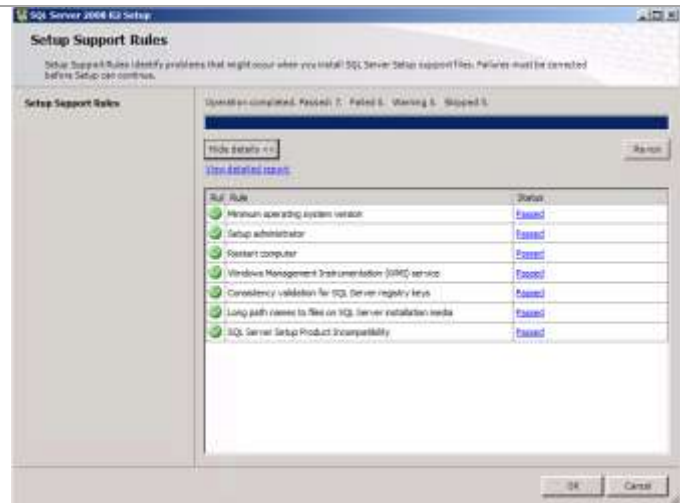


New SQL Server failover cluster installation

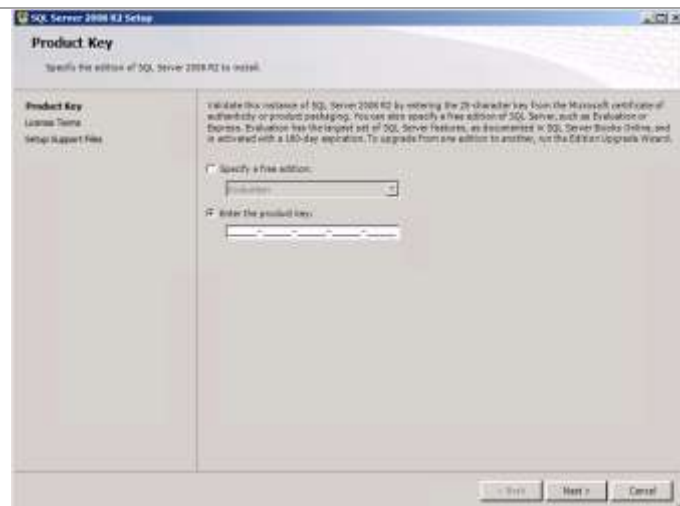
Launch a wizard to install a single-node SQL Server 2008 R2 failover cluster.



The **SQL Server 2008 R2 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.

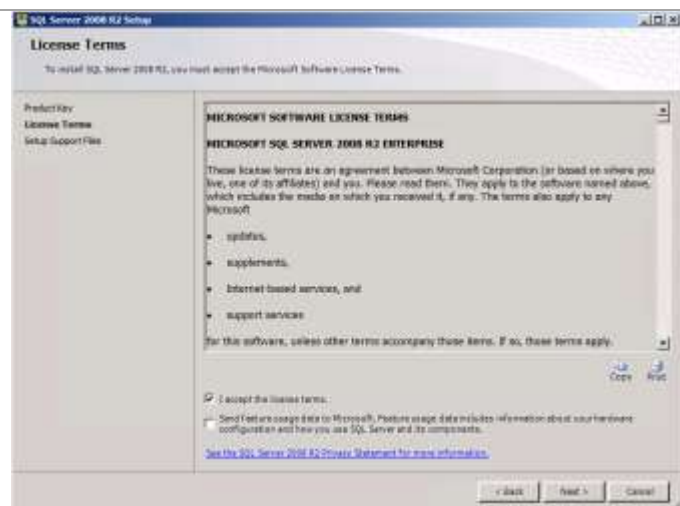


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.



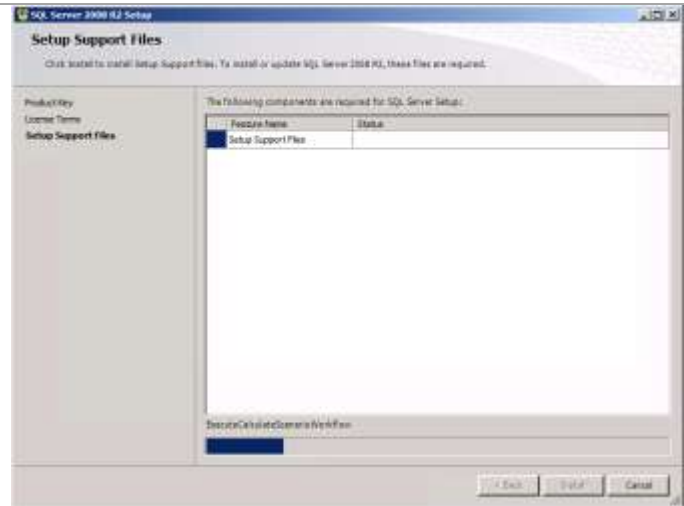
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.

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

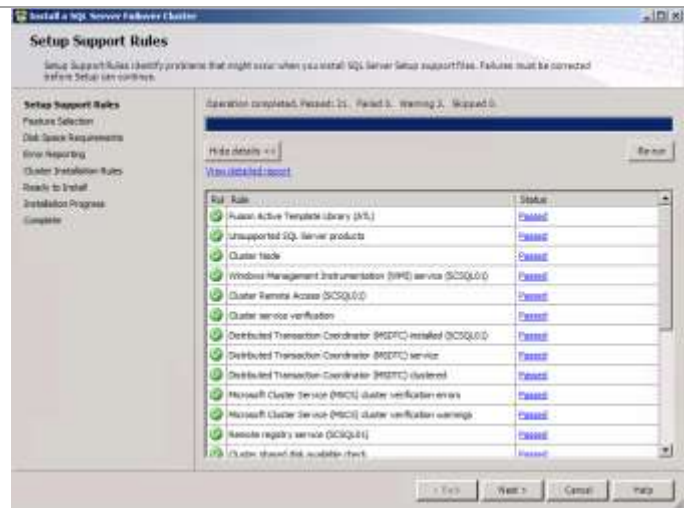




In the **Setup Support Files** dialog, click install and allow the support files to install.



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. Click **Next** to continue.



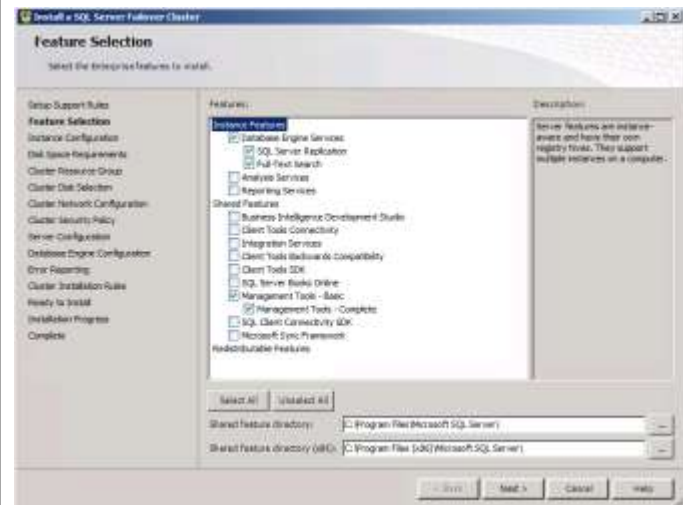


In the **Feature Selection** dialog, features for the various instances will be selected. Note that not all features are supported for failover cluster installations, so the features for Fast Track are limited to the features as listed below. SQL Server with failover clusters requires the selection of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

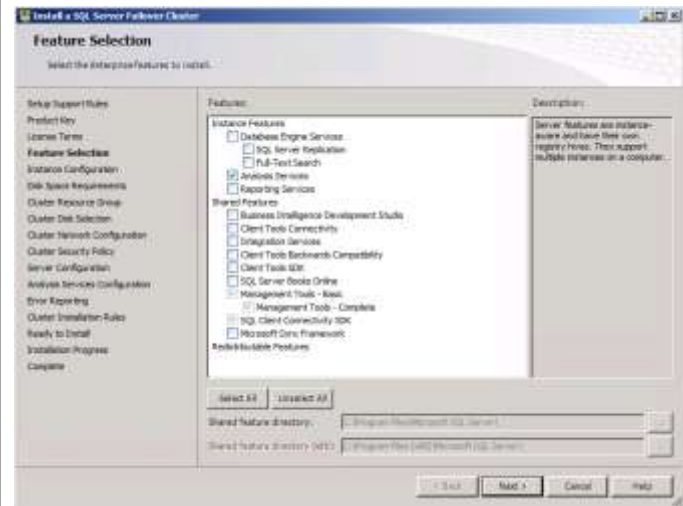
- SCACDB
- Database Engine Services
- SCODB
- Database Engine Services
- SCOMDB
- Database Engine Services
- SCOMDW
- Database Engine Services
- SCSMAS
- Analysis Services
- SCSMDB
- Database Engine Services
- SCSMDW
- Database Engine Services
- SCSPFarm
- Database Engine Services
- SCVMMDB
- Database 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 **Instance Configuration** dialog, make the following selections (refer to the worksheet created earlier):

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

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

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

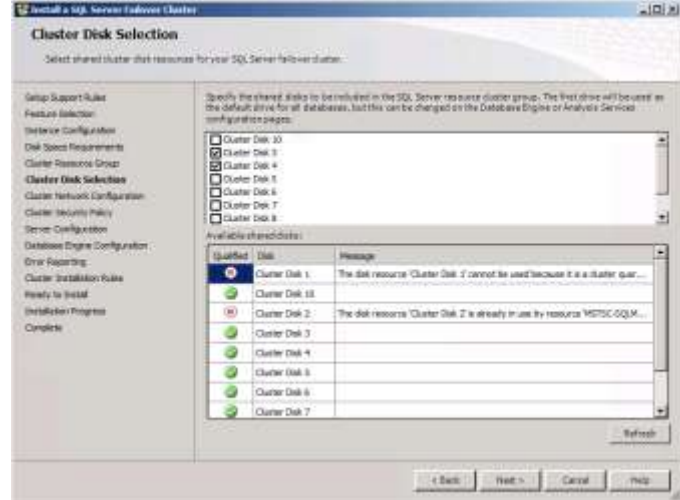
Click **Next** to continue.

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

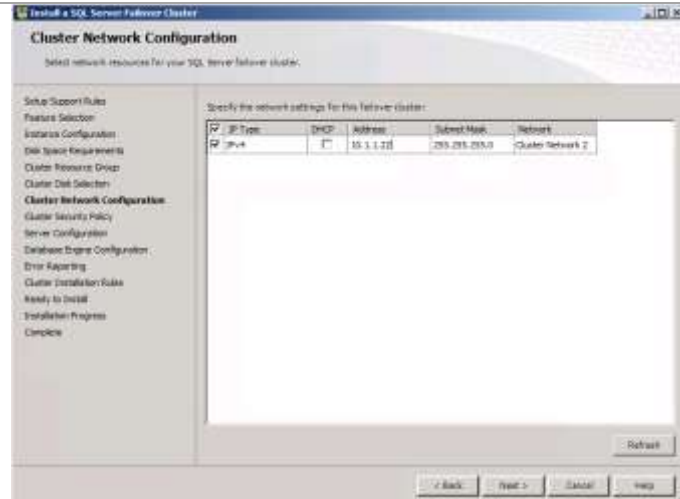
In the **Cluster Resource Group** dialog, in the **SQL Server cluster resource group name** drop-down menu, accept the default value of **SQL Server (<InstanceName>)**. Click **Next** to continue.



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



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 in the TCP and/or IP address in the **Address** field text box. When complete, click **Next** to continue.



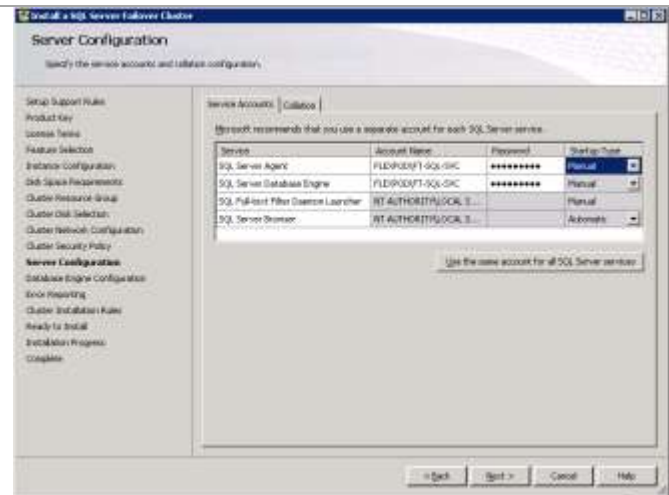
In the **Cluster Security Policy** dialog, select the **Use service SIDs (recommended)** option and click **Next** to continue.





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

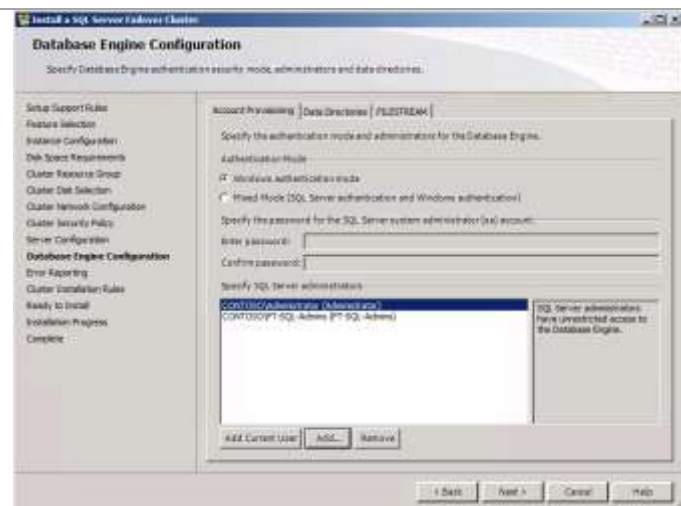
Note: the Fast Track SQL Server Service Account will also be used for the SQL Server Analysis Services service for the instances where these feature are selected.



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

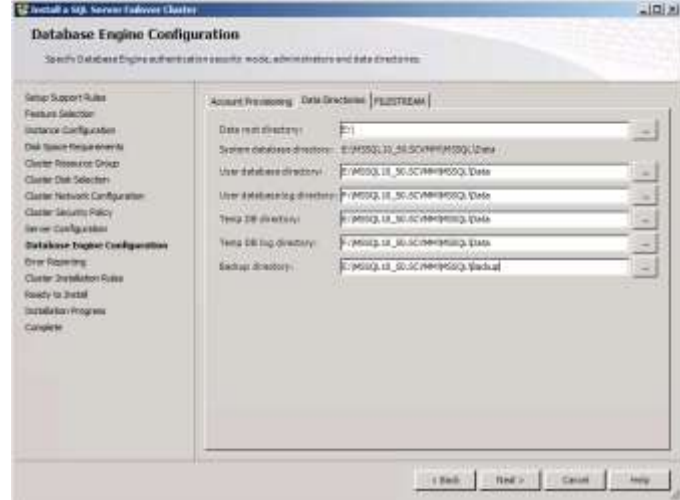


In the Database Engine Configuration dialog, select the Account Provisioning tab. In the Authentication Mode section, select the Windows authentication mode option. In the Specify SQL Server administrators section, click the Add Current User button to add the current installation user. Click the Add... 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. When complete, click **Next** to continue.

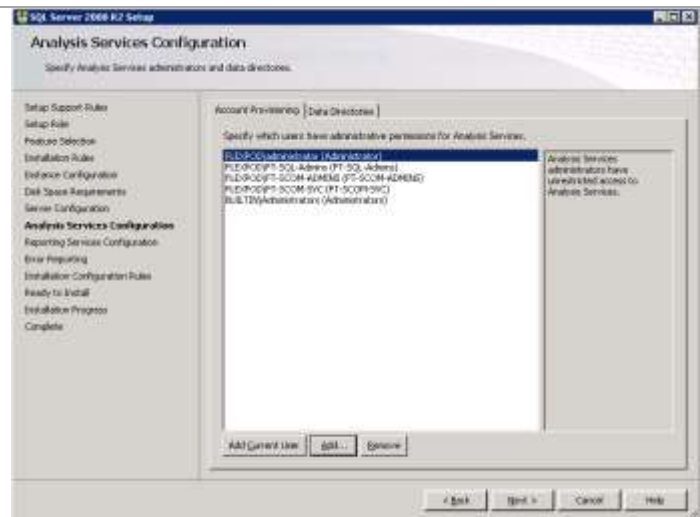


In the Analysis Services Configuration dialog, select the Account Provisioning tab. In the Specify which users have administrative permissions for Analysis Services section, click the Add Current User button to add the current installation user. Click the Add... button to select the following groups:

Service Manager instance:

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

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.





Cluster Installation Rules

Setup is running rules to determine if the failover cluster installation operation will be successful. For more information, click Help.

Operation completed. Passed 6, Failed 0, Warning 0, Skipped 1.

View Details >>>

View Details >>>

Rule Name	Status
Cluster supported for edition	Passed
Operating system supported for edition	Passed
Windows Server 2003 FILESTREAM Health Check	Not applicable
Cluster Resource DLL update health check	Passed
PATL File System	Passed
SQL Server 2008 Analysis Services (SSAS) install action	Not applicable
Instance name	Not applicable
Previous releases of Microsoft Visual Studio 2008	Passed
Update Setup Media Language Compatibility	Passed

< Back Next > Cancel Help

The screenshot shows the "Ready to Install" window of the SQL Server 2008 R2 Setup program. On the left, a sidebar lists various configuration steps: Setup Support Rules, Feature Selection (which is highlighted), Instance Configuration, Disk Space Requirements, Cluster Resource Group, Cluster Disk Selection, Cluster Network Configuration, Cluster Security Policy, Server Configuration, Database Engine Configuration, Error Reporting, and Cluster Installation Role. Below this list, the "Ready to install" section shows "Installation Progress" as "Complete".

The main area of the window displays the selected features for installation. At the top, it says "Ready to install the SQL Server 2008 R2 feature(s) below:". A tree view shows the following selection:

- ☒ Enterprise Edition
 - ☒ General Configuration
 - ☒ Features
 - ☒ Database Engine Services
 - ☒ SQL Server Replication
 - ☒ Full-Text Search
 - ☒ Management Tools – Basic
 - ☒ Management Tools – Complete
 - ☒ Instance Configuration
 - ☒ Instance Name (MUST BE UNIQUE)
 - ☒ Instance ID= MSSQLSERVER
 - ☒ Instance Collation
 - ☒ SQL_Collation= Latin1_General_CI_AS_KS_WS
 - ☒ Shared component root directory
 - ☒ Shared Feature Directory=C:\Program Files\Microsoft SQL Server\90\Shared
 - ☒ Error and Usage Reporting
 - ☒ Usage Reporting= False
 - ☒ Error Reporting= False

At the bottom, the "Configuration File Path:" field contains the path: C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\SQLRS\sqlrs\sqlrsinst.exe. Navigation buttons at the very bottom include "< Back", "Install", "Cancel", and "Help".

Install a SQL Server Failover Cluster

Installation Progress

Setup Support Files
Feature Selection
Instance Configuration
Disk Space Requirements
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Cluster Security Policy
Server Configuration
SQL Server Engine Configuration
Error Reporting
Cluster Installation Rules
Ready to Install
Installation Progress
Complete

Performing Windows Installer actions.

Back Cancel Next

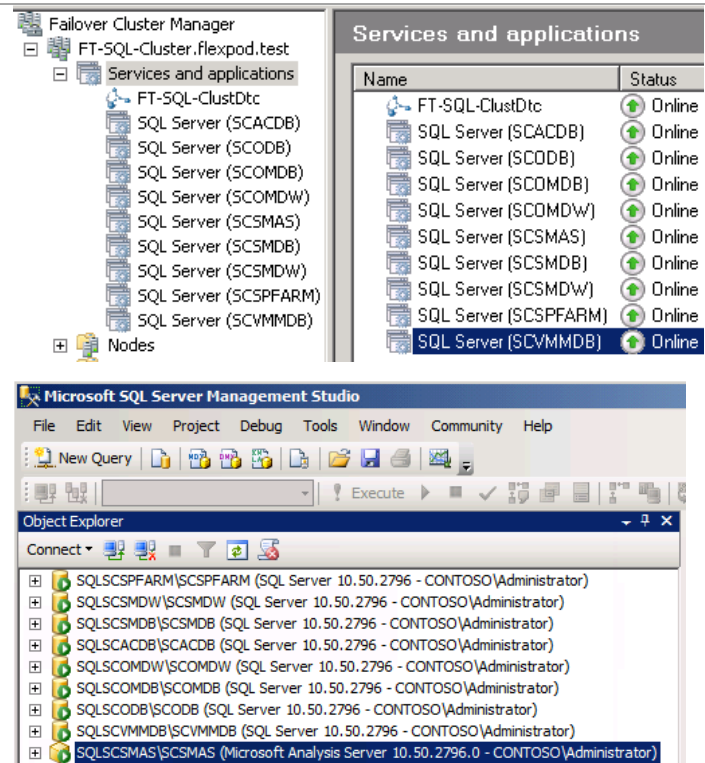


When complete the **Complete** dialog will appear. Click Close to complete the installation of this SQL database instance.



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

Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server® 2008 Management Studio (SSMS) prior to moving to the next step of installation.

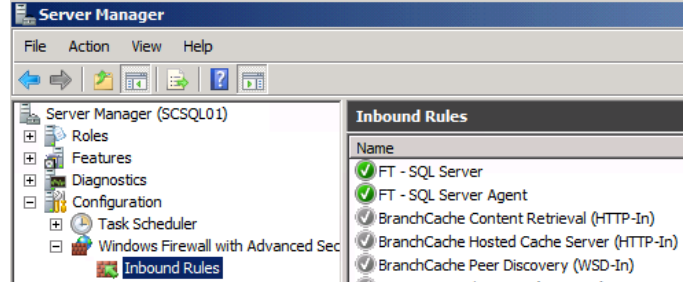




Configure Microsoft Windows Firewall for SQL:

By default, named SQL Server instances will use a unique dynamic port for each instance. If you wish to leave the Windows Firewall enabled, you must set each SQL Server instance to a static port and open the corresponding port in the Windows Firewall. In addition to each instance port, you will need to open the standard SQL Server ports of 1433 and 1434 for SQL Server to function.

Note: the process for setting SQL Server named instances to use static ports is documented at <http://support.microsoft.com/kb/823938>.



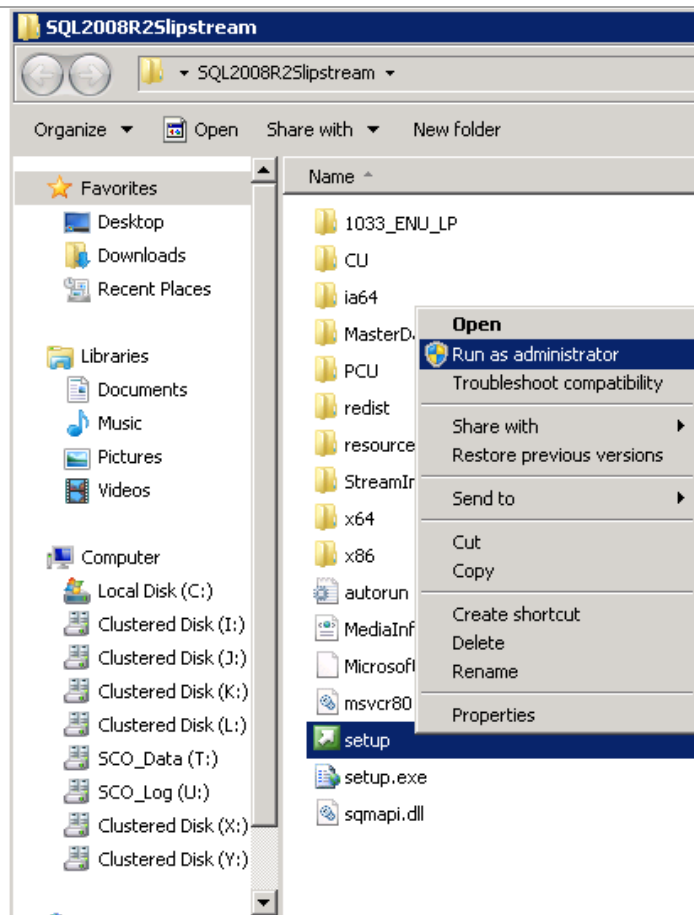


Installing the SQL Server Named Instances on the Guest Cluster (Node 2)

When the creation of all required SQL Server instances on Node 1 is complete, a second node (Node 2) can be added to each instance of the cluster. Follow the steps below to begin the installation of the second node of the cluster.

Perform the following steps on the **Second fabric management SQL Server Node** virtual machine.

From the SQL Server 2008 R2 slipstreamed 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.



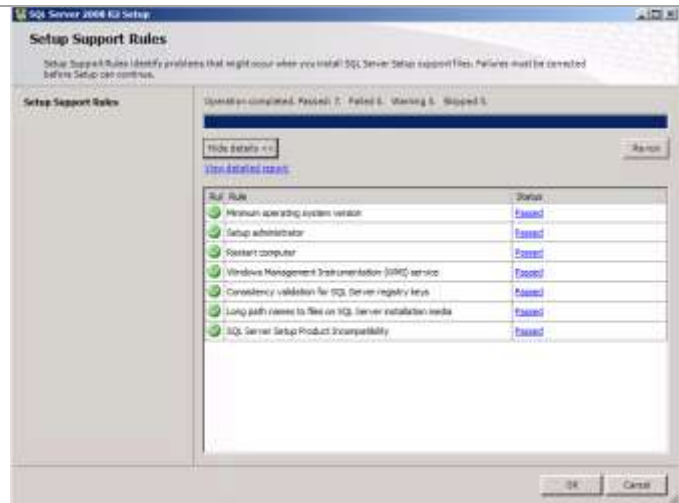
From the SQL Server Installation Center click the Add node to a SQL Server failover cluster link.



Add node to a SQL Server failover cluster

Launch a wizard to add a node to an existing SQL Server 2008 R2 failover cluster.

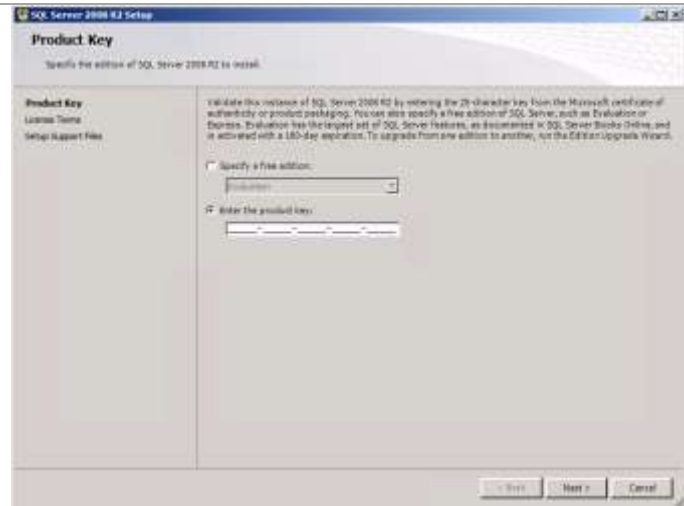
The **SQL Server 2008 R2 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.



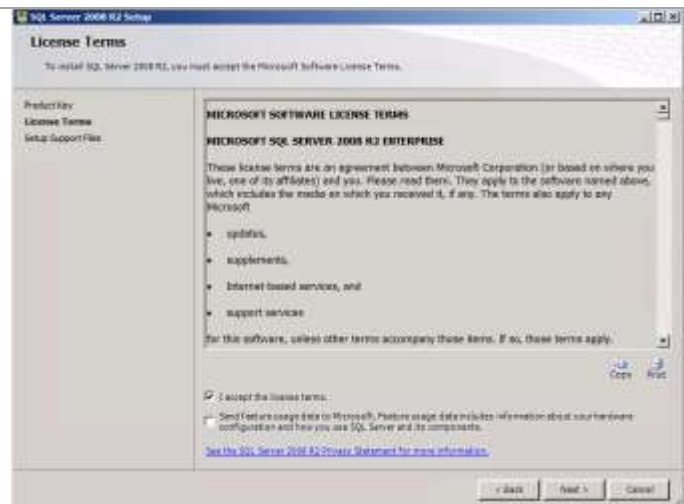


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

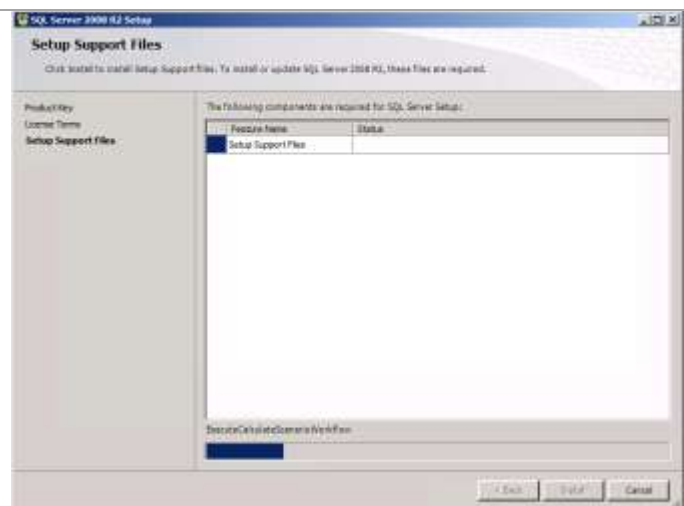
Note: if you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop-down menu for a 180-day evaluation period.



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

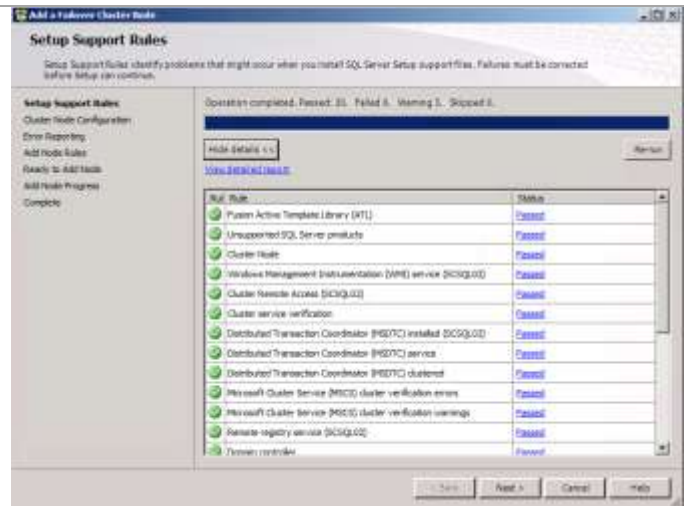


In the **Setup Support Files** dialog, click **Install** and allow the support files to install.

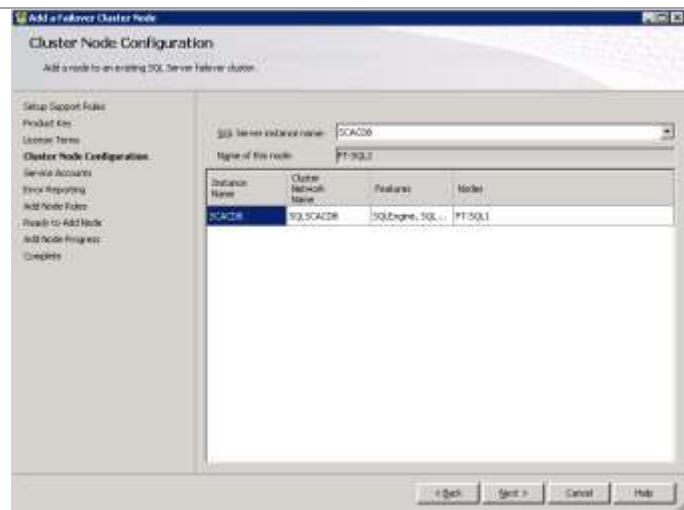




In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

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

Add a Follow-on Cluster Node

Service Accounts

Specify the service accounts and startup configuration.

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

Service	Account Name	Password	Startup Type
SQL Full-text Filter Daemon Launcher	NT AUTHORITY\LOCALSER...		Manual
SQL Server Database Engine	FASTTRACK\FT-SQL-SVC	*****	Manual
SQL Server Browser	NT AUTHORITY\LOCAL SER...		Automatic
SQL Server Agent	FASTTRACK\FT-SQL-SVC	*****	Manual

[Get the service account for SQL Server services](#)

[Back](#) [Next >](#) [Cancel](#) [Help](#)

Add a Follow-on Cluster Node

Service Accounts

Specify the service accounts and startup configuration.

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

Service	Account Name	Password	Startup Type
SQL Full-text Filter Daemon Launcher	NT AUTHORITY\LOCALSER...		Manual
SQL Server Analysis Services	FASTTRACK\FT-SQL-SVC	*****	Automatic
SQL Server Database Engine	FASTTRACK\FT-SQL-SVC	*****	Manual
SQL Server Browser	NT AUTHORITY\LOCALSER...		Automatic
SQL Server Agent	FASTTRACK\FT-SQL-SVC	*****	Manual

[Get the service account for SQL Server services](#)

[Back](#) [Next >](#) [Cancel](#) [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.

Add a Follow-on Cluster Node

Error Reporting

Help Microsoft improve SQL Server features and services.

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 Updates to modify feature usage data. These updates might be downloaded and installed on your machine automatically, depending on your automatic update settings.

[See the SQL Server 2008 R2 Privacy Statement for more information.](#)

[Read more about Microsoft updates and automatic updates.](#)

☐ 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.

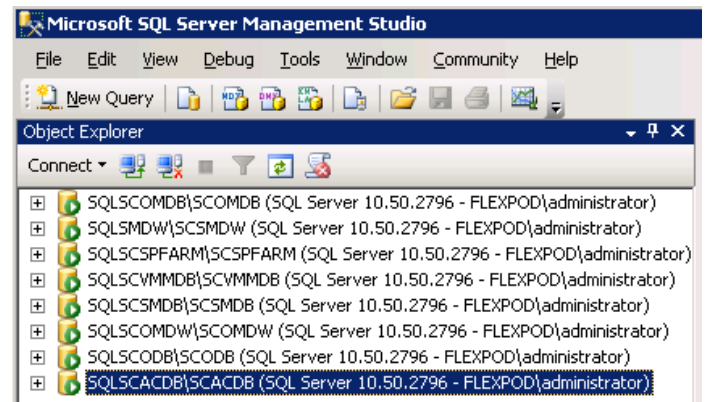
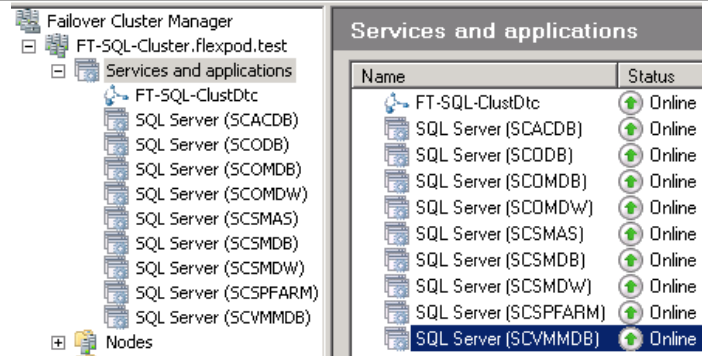
[Back](#) [Next >](#) [Cancel](#) [Help](#)

[illegible]



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

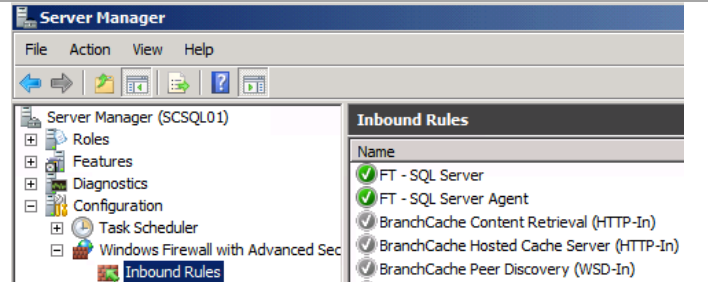
Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server Management Studio prior to moving to the next step of installation.



Configure Windows Firewall for SQL Server:

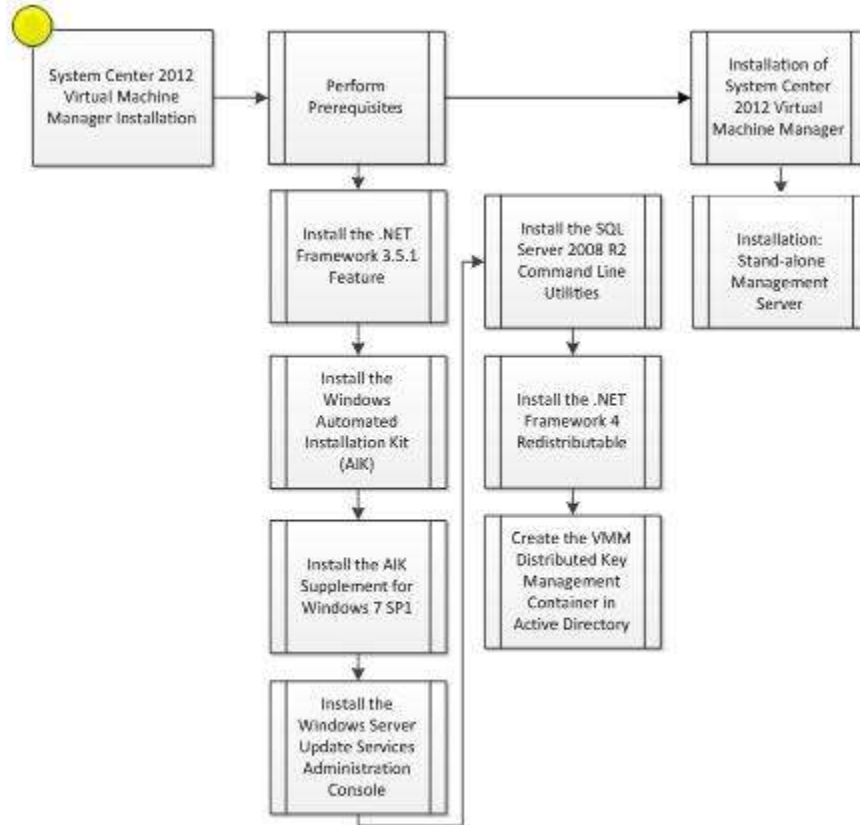
By default, named SQL Server instances will use a unique dynamic port for each instance. If you wish to leave the Windows Firewall enabled, you must set each SQL Server instance to a static port and open the corresponding port in the Windows Firewall. In addition to each instance port, you will need to open the standard SQL Server ports of 1433 and 1434 for SQL Server to function.

Note: the process for setting SQL Server named instances to use static ports is documented at <http://support.microsoft.com/kb/823938>.



Virtual Machine Manager

The System Center 2012 Virtual Machine Manager installation process includes the following high-level steps:



Overview

This section provides high-level walkthrough on how to setup and run the task sequence and scripts for deploying Virtual Machine Manager into the Fast Track fabric management architecture. The following assumptions are made prior to the installation:

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for Virtual Machine Manager.
- The selected installation type during install must be Full Installation.
- The startup RAM must be at least 2 GB for a virtual machine with Dynamic memory.
- For high-availability (HA) Virtual Machine Manager management server you must use the Enterprise or Datacenter editions of Windows Server 2008 R2.
- Requires two iSCSI shared storage LUNs.
- Requires a dedicated virtual network adapter for cluster communication.
- Requires at least two dedicated virtual network adapter for iSCSI.
- The selected installation type during install must be Full Installation.
- The Microsoft .NET Framework 4 Redistributable is installed.



- The target virtual machines must have the Windows Automated Installation Kit 3.0⁶ and Windows Automated Installation Kit 3.0 supplement for SP1⁷ installed.
- The target virtual machine must have the WSUS 3.0 console installed.
- A four-node, SQL Server 2008 R2 cluster with dedicated instance has been established in previous steps for Virtual Machine Manager.

The Virtual Machine Manager SQL Server instance has two drives configured in SQL Server for the instance devoted for Virtual Machine Manager:

- Data
- Logs
- The Virtual Machine Manager SQL Server instance must be case-insensitive (default on SQL Server 2008 R2).
- 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 “VMMDKM” container in Active Directory or this container must already exist prior to running Virtual Machine Manager setup.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User Name	Purpose	Permissions
<DOMAIN>\FT-VMM-SVC	Virtual Machine Manager Service Account	This account will need full admin permissions on all target systems to be managed and the Virtual Machine Manager virtual machine.
<DOMAIN>\FT-SQL-SVC	SQL Server Service Account	This account will need full admin permissions on the Virtual Machine Manager virtual machine.

Note: The user account that initiates the installation process must have dbowner permissions in the SQL Server instance dedicated to Virtual Machine Manager. This can be achieved by adding this account to the FT-SQL-ADMINS group.

⁶ The Windows Automated Installation Kit for Windows 7 - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5753>.

⁷ The Windows Automated Installation Kit Supplement for Windows 7 SP1 - <http://www.microsoft.com/download/en/details.aspx?id=5188>.



Groups

Verify that the following security groups have been created:

Security Group Name	Group Scope	Members
<DOMAIN>\FT-VMM-Admins	Global	FT-VMM-SVC
<DOMAIN>\FT-VMM-DelegatedAdmins	Global	Virtual Machine Manager Delegated Admins
<DOMAIN>\FT-VMM-SSUsers	Global	Virtual Machine Manager Self-Service Users
<DOMAIN>\FT-VMM-ROAdmins	Global	Virtual Machine Manager Read Only Admins

Enabling iSCSI SAN

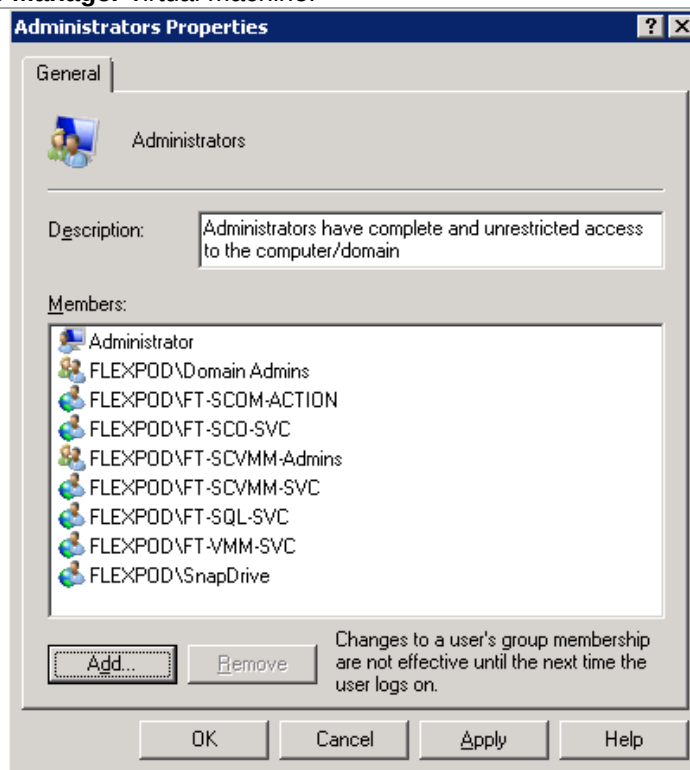
The VMM installation requires at least one iSCSI LUN to house the VMM library share.

Perform the following steps on the **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:

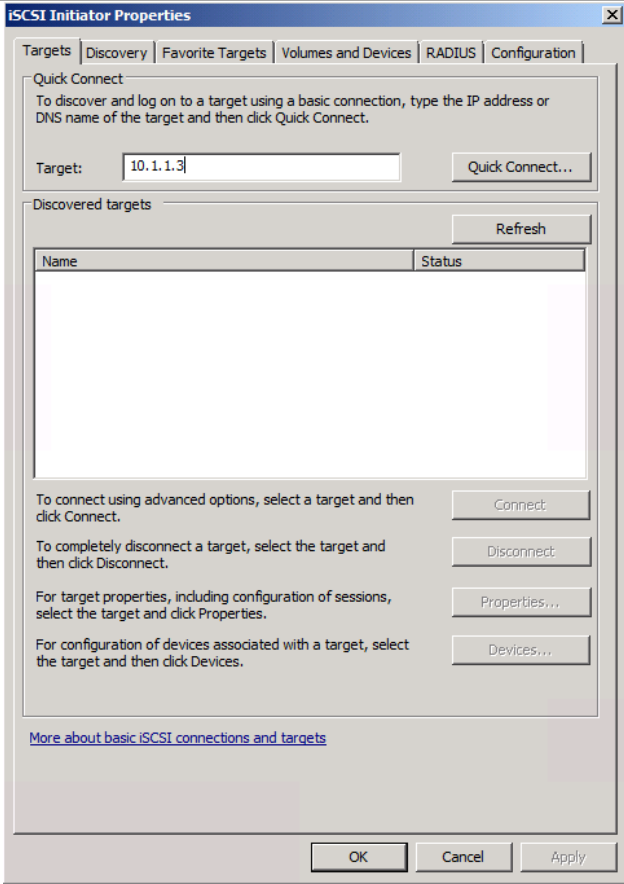
- Orchestrator service account
- Operations Manager Action account
- Virtual Machine Manager Admins group
- Virtual Machine Manager service account
- SQL Server Service Account
- SnapDrive Service Account



Enable the iSCSI Initiator by clicking Start > Administrative Tools > iSCSI initiator. Click yes to start the Microsoft iSCSI service.



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



The image shows the 'iSCSI Initiator Properties' dialog box with the 'Targets' tab selected. The 'Quick Connect' section contains a 'Target' text box with '10.1.1.3' entered and a 'Quick Connect...' button. Below this is a 'Discovered targets' section with a 'Refresh' button and a table with columns 'Name' and 'Status'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

iSCSI Initiator Properties

Targets | Discovery | Favorite Targets | Volumes and Devices | RADIUS | Configuration

Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

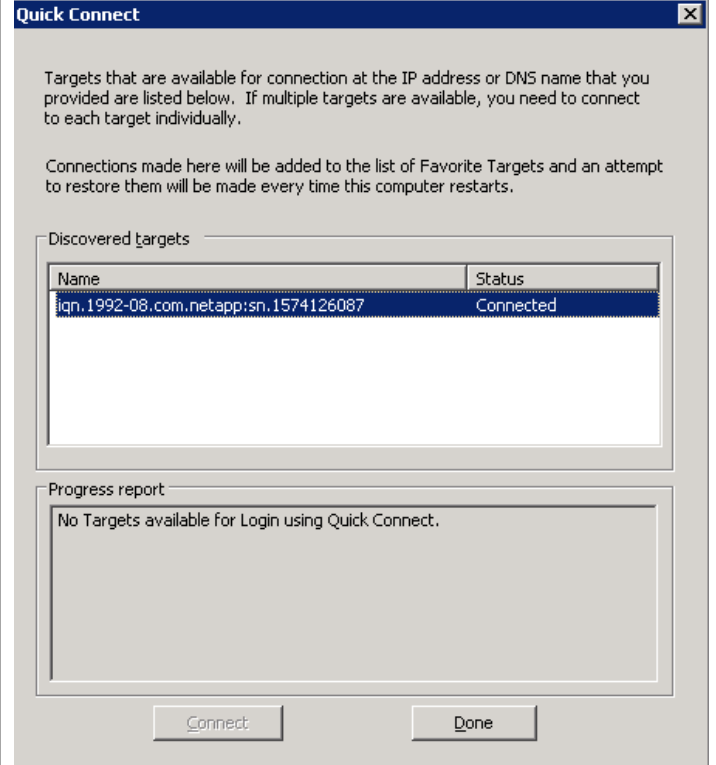
For target properties, including configuration of sessions, select the target and click Properties...

For configuration of devices associated with a target, select the target and then click Devices...

[More about basic iSCSI connections and targets](#)



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



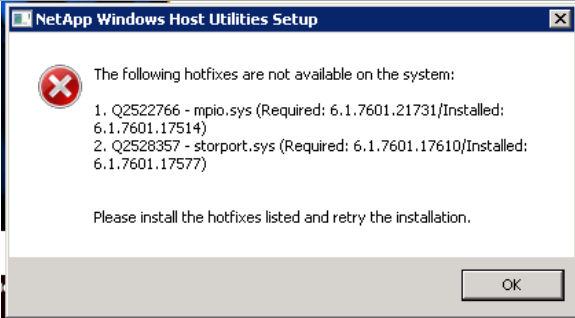
- **Windows Features**

Open Server Manager and select Features. Click the Add Features link launching the Add Features wizard.

Expand .NET Framework 3.5.1 Features. Select the .NET Framework 3.5.1 Feature. Click Next > Install.





• NetApp Windows Host Utilities Kit 1. Download and NetApp Windows Host Utilities Kit from the NOW.netapp.com Site. 2. Launch the Installer, click next, Accept the EULA, and click Next. 3. Select Yes, Install support for Multipath I/O, and click Next. 4. Click Next > Finish. Ignore the HBA error. There is no HBA support in Hyper-V.	
If you receive an error stating that you do not have correct versions of MPIO.SYS and/or STORPORT.SYS, this is because your system is not fully patched. Install the requested HotFixes and repeat this step.	
• NetApp DSM MPIO Download and NetApp DSM MPIO package from the NOW site. Launch the Installer. Click Next then click OK to acknowledge the ALUA requirement. Accept the EULA and click Next. Enter the DSM License Key and click Next. Leave the system account selected and click Next. Click Next > Next > Install and when complete restart the system. Ignore the HBA error. There is no HBA support for Hyper-V.	



- **NetApp SnapDrive**
 1. Download and NetApp SnapDrive.
 2. Launch the Installer, click Next, Accept the EULA, and click Next.
 3. Select the Storage based Licensing method and click Next.
 4. Enter your User Name, and Organization information, and click Next.
 5. Enter the Account information for the <SnapDrive > account created earlier.
 6. Click Next and the select the “Enable Transport Protocol Settings Option.
 7. Select HTTPS.
 8. Enter the UserName: <domain>\<snapdrive> and enter the service account password.
 9. Click Next > Next > Next > Install > Finish.

SnapDrive® - Installation Wizard

Transport Protocol Default Setting
Specify Default Transport Setting for Storage System(s)

☒ Enable Transport Protocol Settings

☐ RPC
☐ HTTP
☒ HTTPS

Specify the user name and password for the HTTP/HTTPS Protocol selection.
User Name: netapp\SnapDrive
Password:
Port ID: 443

InstallShield

< Back Next > Cancel

10. Set Firewall exceptions:
Open Windows Firewall with Advanced Security, by clicking Start > Administrative Tools > Windows Firewall with Advanced Security.
- **SnapDrive**
 1. Highlight Inbound Rules and click New Rule.
 2. Select Program and click Next.
 3. Enter the program path for the SnapDrive Service i.e. %ProgramFiles%\NetApp\SnapDrive\SWSvc.exe.
 4. Click Next, then select the Allow the Connection options and click Next > Next.
 5. Enter the rule Name <SnapDrive>, Description, and click Finish.



- **Create NetApp Flexible Volume for VMM Library LUN**

1. Open a PowerShell console and type in the command

```
import-module dataontap.
```

If the module is not found, download the NetApp PowerShell Toolkit 2.0 and install it on the VMM server. Please refer to the NetApp PowerShell Toolkit download page for installation instructions.

2. After successfully importing the NetApp PowerShell Toolkit module, type in the command

```
connect-nacontroller Controller-A  
-Credential root
```

to connect and authenticate to Controller A.

3. From the PowerShell console, type in the command

```
new-navol VMM_Library aggr0 1200g
```

to create the flexible volume.

Type in the following commands to configure the volume to contain the VMM Library LUN:

```
set-navoloption VMM_Library  
fractional_reserve 0
```

```
set-navoloption VMM_Library  
create_ucose on
```

```
set-navoloption VMM_Library  
convert_ucose on
```

```
set-navoloption VMM_Library nosnap  
on
```

```
set-nasnapshotreserve VMM_Library 0
```

```
set-nasnapshotschedule VMM_Library -  
Weeks 0 -Days 0 -Hours 0 - Minutes 0
```




- **Create VMM Library LUN with SnapDrive**
 1. Click Start > All Programs > NetApp > SnapDrive to open the SnapDrive Management Console.
 2. Expand the SnapDrive instance by clicking on the hostname of the VMM server
 3. Select the Disks object and right click and select the Create Disk task to start the Create Disk Wizard.
 4. In the Welcome screen, click Next.
 5. Enter the hostname of Controller A and click Add.
 6. When NetApp flexible volume enumeration has completed, select the target volume where you intend to add the LUN.
 7. Add a LUN Name, LUN Description and click Next.
 8. Select Dedicated for the LUN type and click Next.
 9. Select Assign a Drive Letter and assign the V: drive letter.
 10. Set the LUN Size to 1TB, click Next.
 11. Select the iSCSI initiators to map the new LUN to the VMM virtual machine
 12. Click Next, then Select Automatic and click Next.
 13. Review the Properties of the LUN to be created and click Next.
- Click Finish to create the LUN.

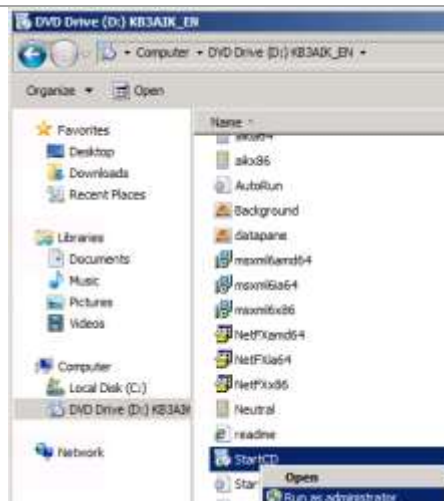
Installing the Windows Automated Installation Kit

The Virtual Machine Manager installation requires that the Windows Automated Installation Kit (AIK) be installed on the Virtual Machine Manager management server. The following steps show how to install the Windows AIK on the Virtual Machine Manager management server.

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



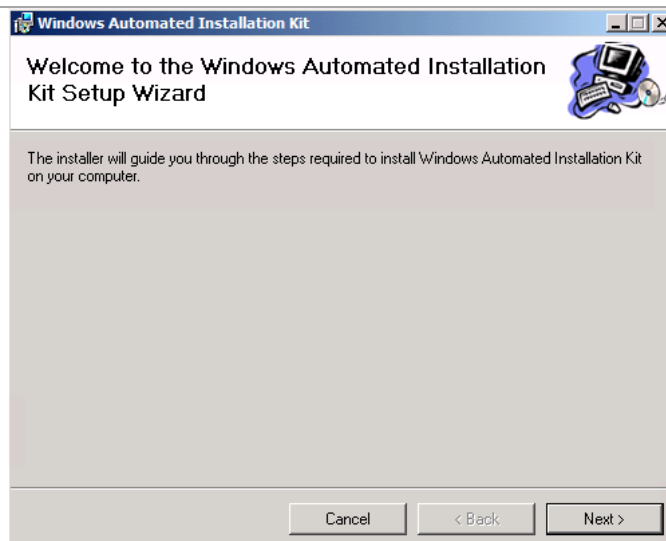
From the Windows AIK installation media source right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



The **Welcome** splash screen will appear. Click the **Windows AIK Setup** option from the sidebar to begin installation.

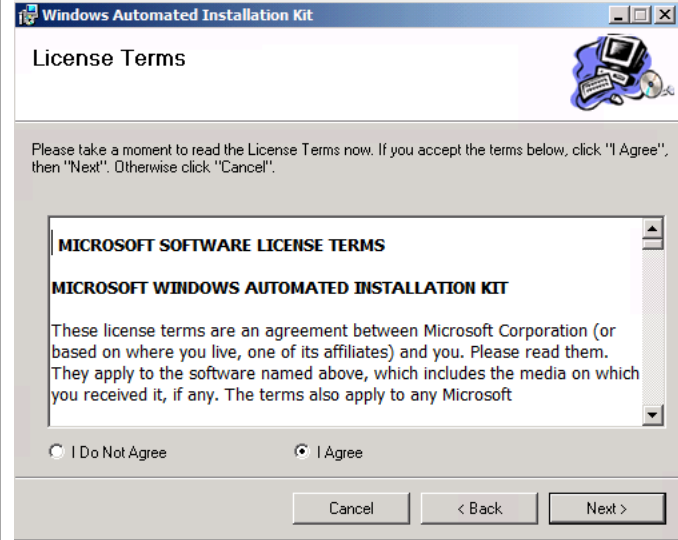


The **Windows Automated Installation Kit** wizard will appear. Click **Next** to continue.

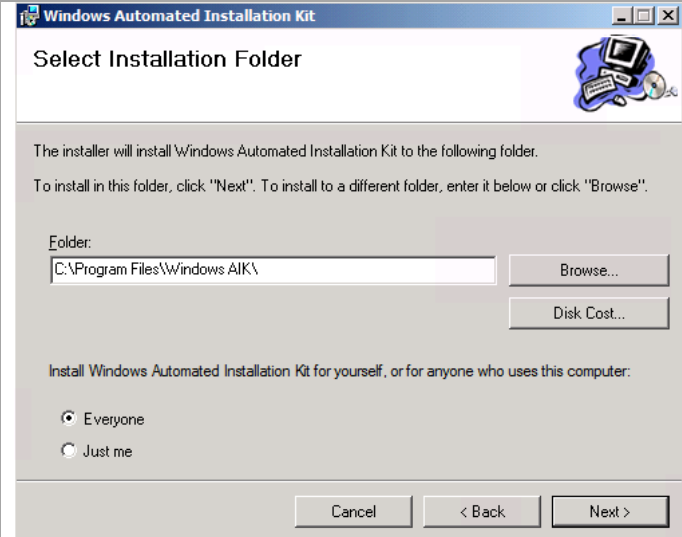




In the **License Terms** dialog, select the **I Agree** option. Click **Next** to continue.

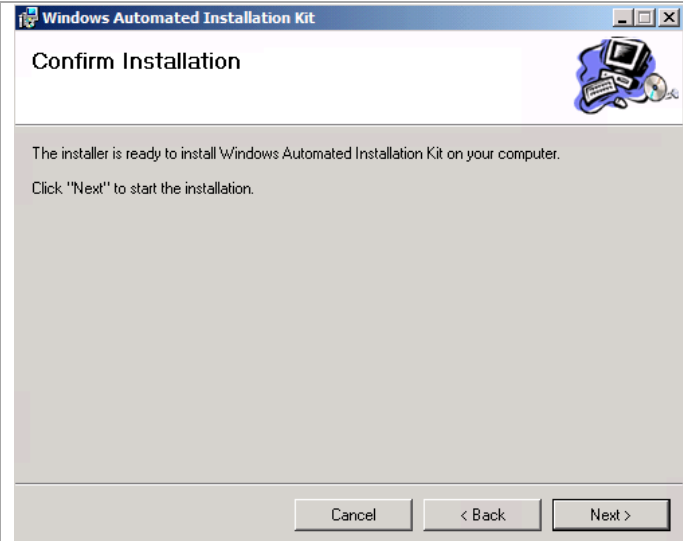


In the **Select Installation Folder** dialog, accept the default folder location of *%ProgramFiles%\Windows AIK*. Select the **Everyone** option and click **Next** to continue.

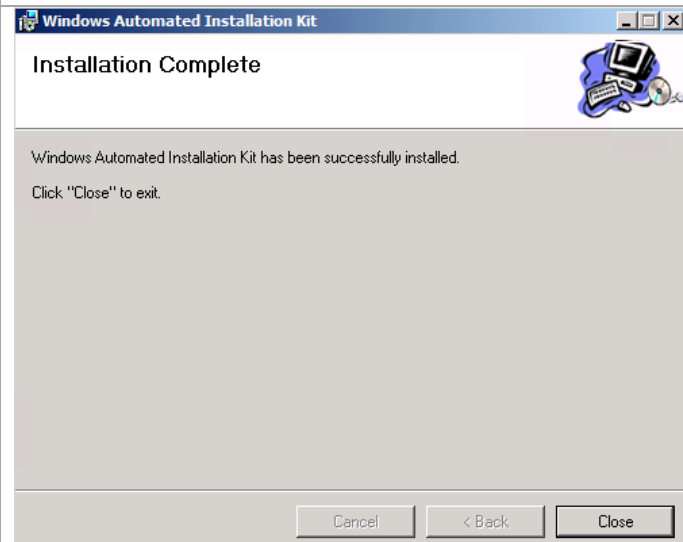




In the **Confirm Installation** dialog, click **Next** to continue.



In the **Installation Complete** dialog, click **Close** to exit the installation wizard.





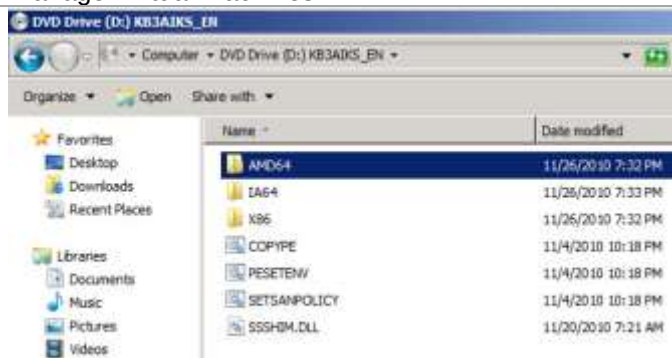
Install the Windows Automated Installation Kit Supplement for Windows 7 SP1

The Windows Automated Installation Kit (AIK) Supplement should be installed in addition to the core AIK binaries. The following steps show how to install the AIK Supplement.

Perform the following steps on the **Virtual Machine Manager** virtual machine. For clustered Virtual Machine Manager, perform this step on both Virtual Machine Manager virtual machines.

Mount the supplement ISO to the virtual machine and browse to the contents. Note the drive letter of the ISO when it is mounted to the virtual machine.

Note: the Windows AIK Supplement for Windows 7 SP1 can be downloaded from <http://www.microsoft.com/download/en/details.aspx?id=5188>.



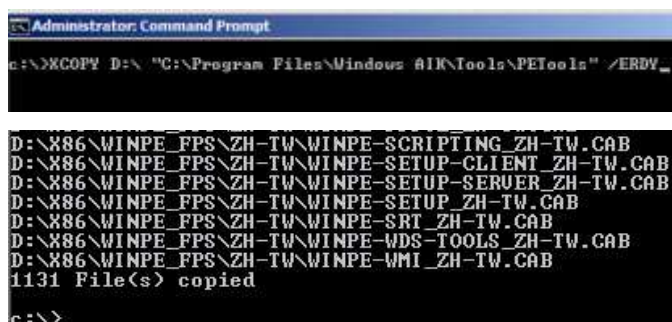
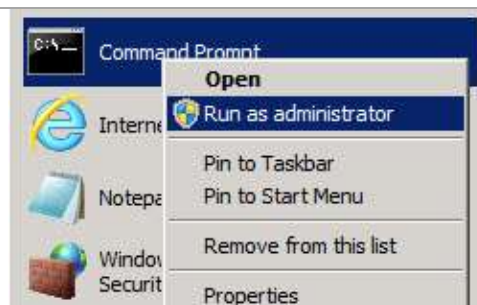
Open an elevated command prompt.

Replace the installed Microsoft Windows Preinstallation Environment (PE) 3.0 files with the corresponding Microsoft Windows PE 3.1 files from the ISO. To do this, run the following command:

```
xcopy D:\ "C:\Program Files\Windows AIK\Tools\PETools" /ERDY
```

In this example "D:\\" is the root directory of the ISO image.

Note: C:\Program Files\Windows AIK\ is the default installation location. If you installed the AIK Supplement to a different location, modify the command accordingly.



For full details on the AIK and the AIK Supplement, refer to the readme file located at [http://technet.microsoft.com/en-us/library/dd349350\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd349350(Ws.10).aspx).



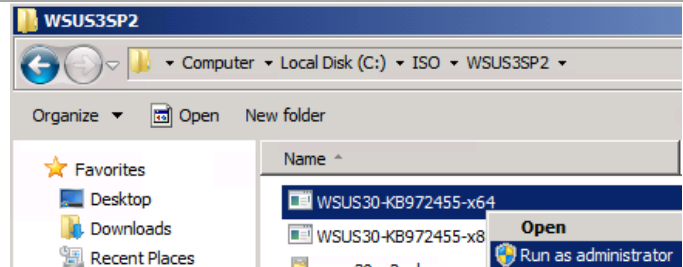
Install the Windows Server Update Services Administration Console

The Virtual Machine Manager installation requires that the WSUS Administration be installed on the Virtual Machine Manager management server. Follow the steps below to install the WSUS Administration on the Virtual Machine Manager management server.

Perform the following steps on the **Virtual Machine Manager** virtual machine. For clustered SCVMM perform this step on both SCVMM virtual machines.

From the WSUS 3.0 Service Pack (SP2) installation media source right-click **WSUS30-KB972455-x64.exe** and select **Run as administrator** from the context menu to begin setup.

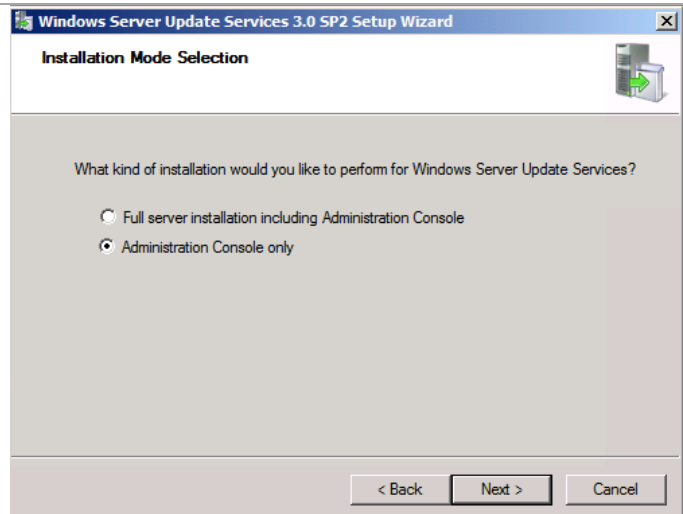
Note: WSUS can be downloaded from <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5216>.



The Windows Server Update Services 3.0 SP2 Setup Wizard will appear. Click the Next button.



In the Installation Mode Selection dialog, select Administration Console only option and click the Next button.

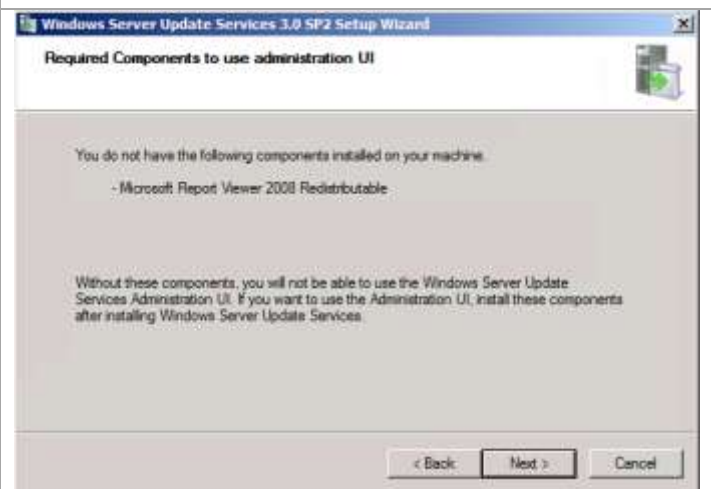




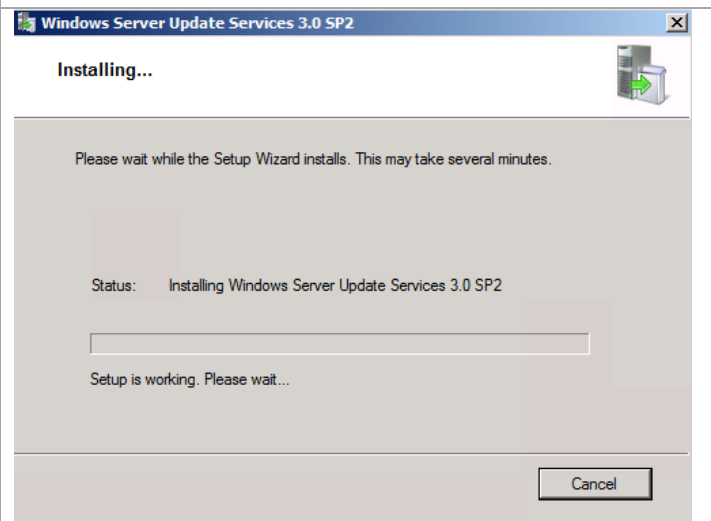
In the License Agreement dialog, select the I accept the terms of the License agreement option. Click **Next** to continue.



In the **Required Components to use administration UI** dialog, accept the installation of the Microsoft Report Viewer 2008 Redistributable and click **Next** to continue.



The **Installing...** dialog will show the installation progress.





The wizard will complete when the installation is finished. Click **Finish** to complete the installation and exit the wizard.

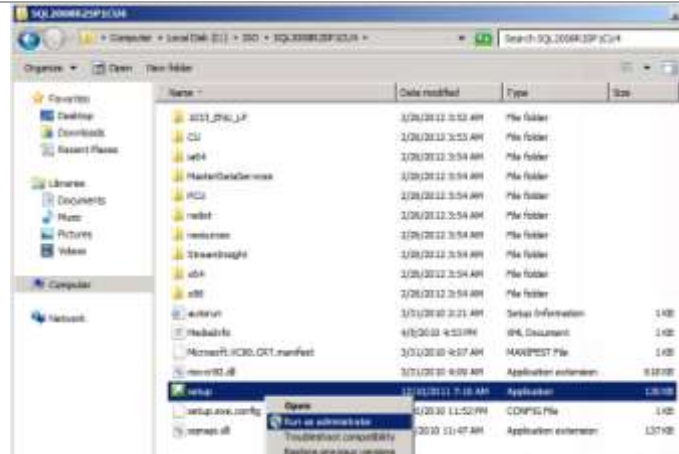


Installing the SQL Server 2008 R2 Command Line Utilities

The Virtual Machine Manager installation requires that the SQL Server 2008 R2 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 the **Virtual Machine Manager** virtual machine.

From the SQL Server 2008 R2 slipstreamed installation media source right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.





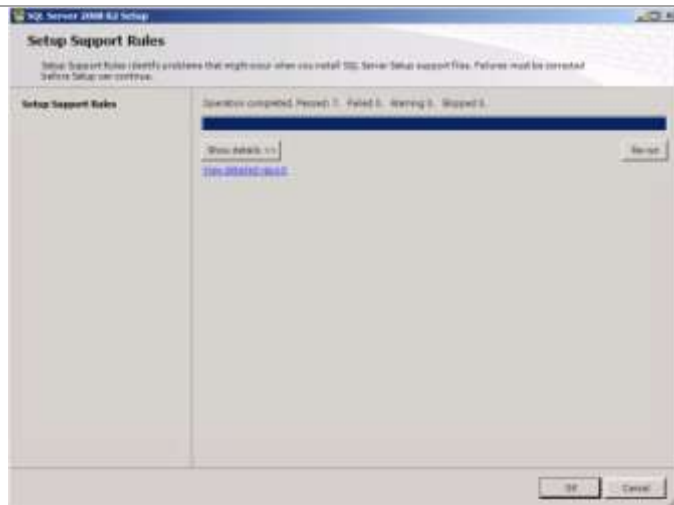
The SQL Server Installation Center will appear.



From the SQL Server Installation Center click the New installation or add features to an existing installation link.



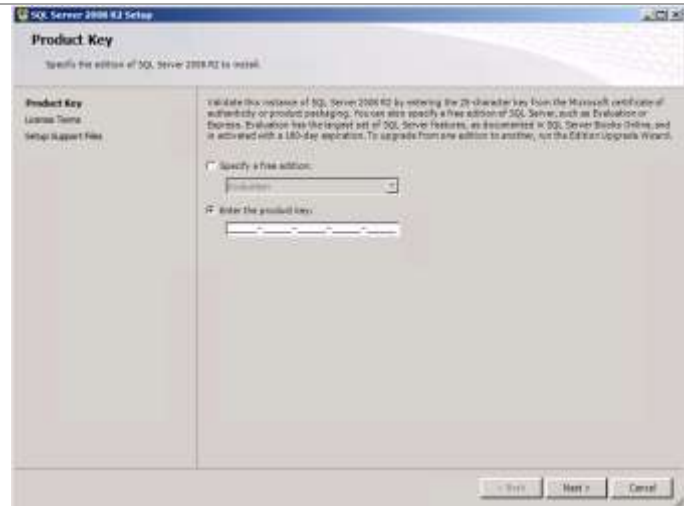
The **SQL Server 2008 R2 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.





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.

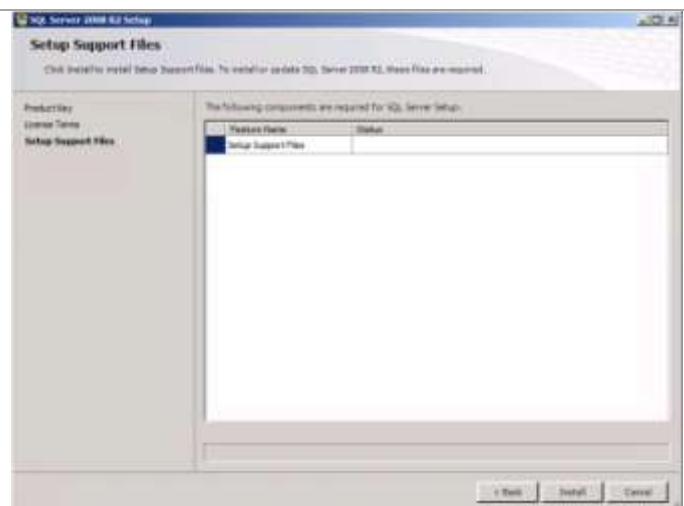
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop down menu for a 180-day evaluation period.



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.

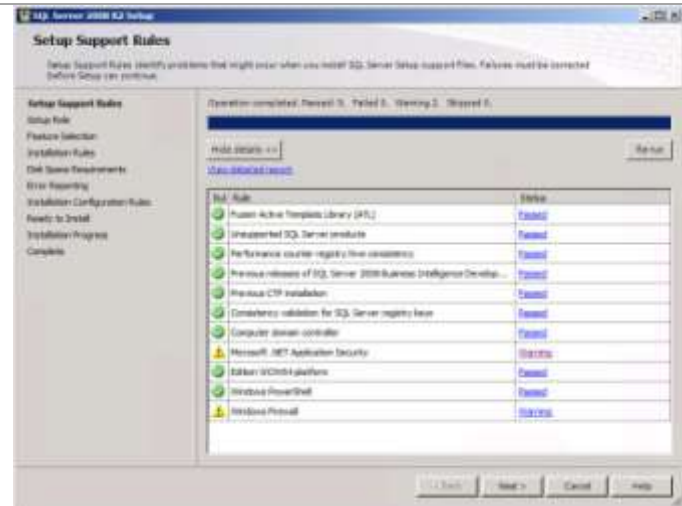


In the **Setup Support Files** dialog, click **install** and allow the support files to install.

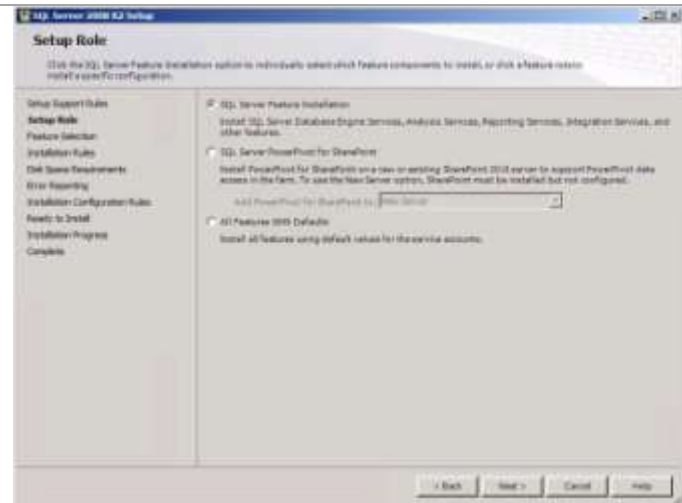




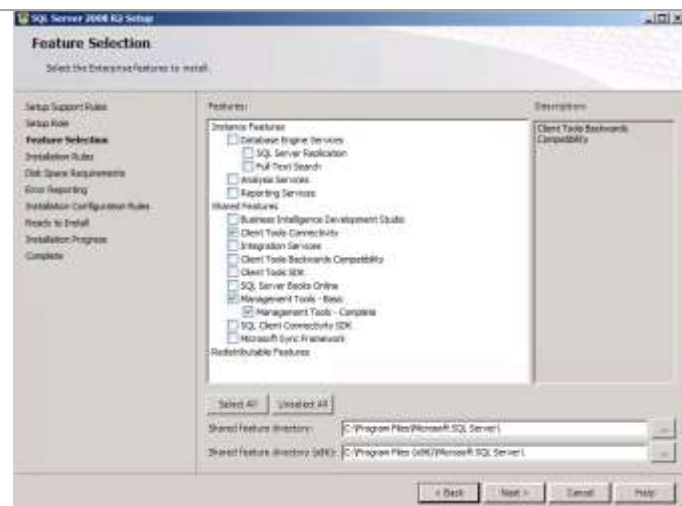
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

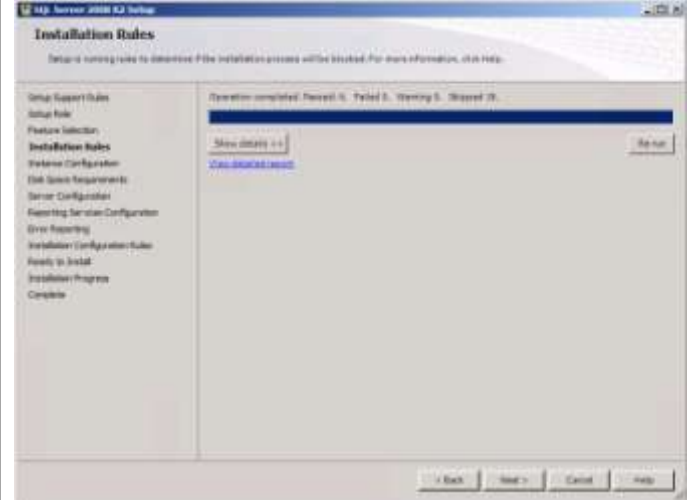


In the **Feature Selection** dialog, Select the **Client Tools Connectivity, Management Tools – Basic** and **Management Tools – Complete** checkboxes. When all selections are made, click **Next** to continue.

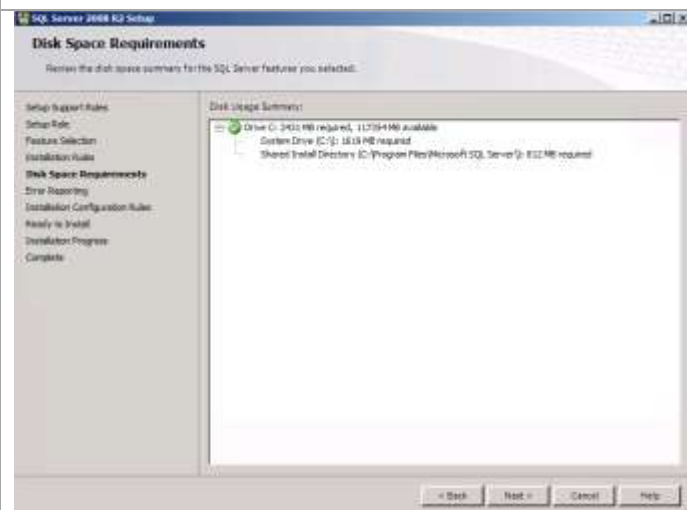




In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

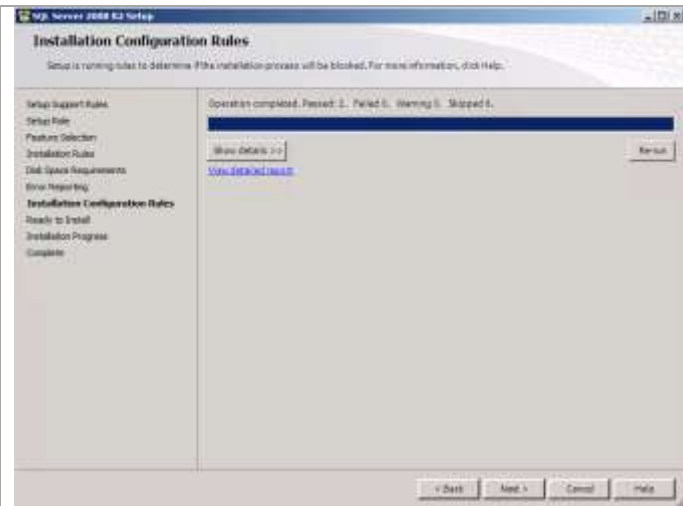


In the **Error Reporting** dialog, select or clear the **Send Windows and SQL Server Error Reports to Microsoft** or your corporate report server based on your organization's policies and click **Next** to continue.





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



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



When complete the **Complete** dialog will appear. Click Close to complete the installation of SQL Server tools.



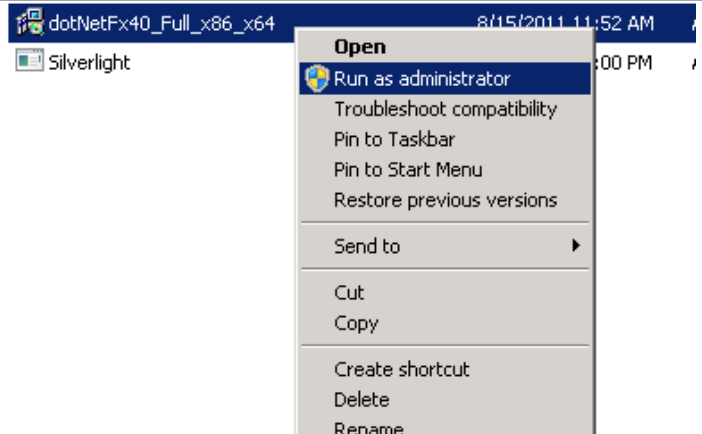


Installing .NET Framework 4

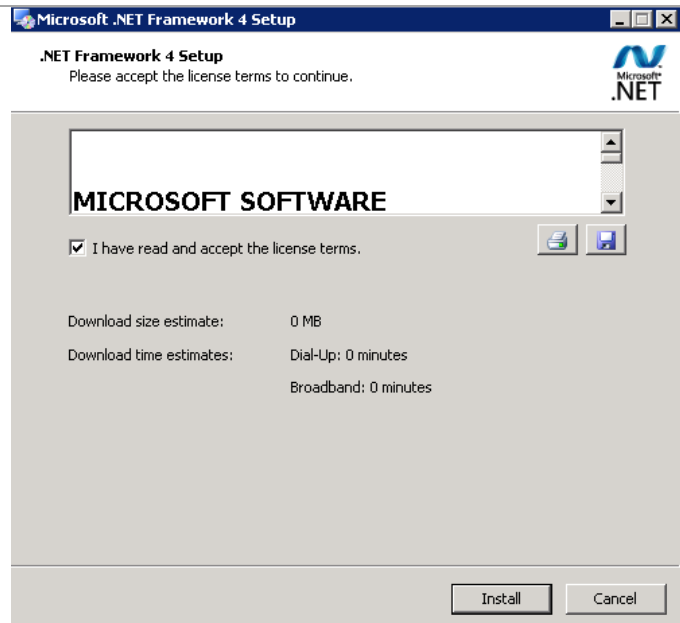
Additionally, Virtual Machine Manager also requires the .NET Framework 4 package be installed prior to installation. Perform the steps described below to install the .NET Framework 4 package.

Perform the following steps on the **Virtual Maching Manager** 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.

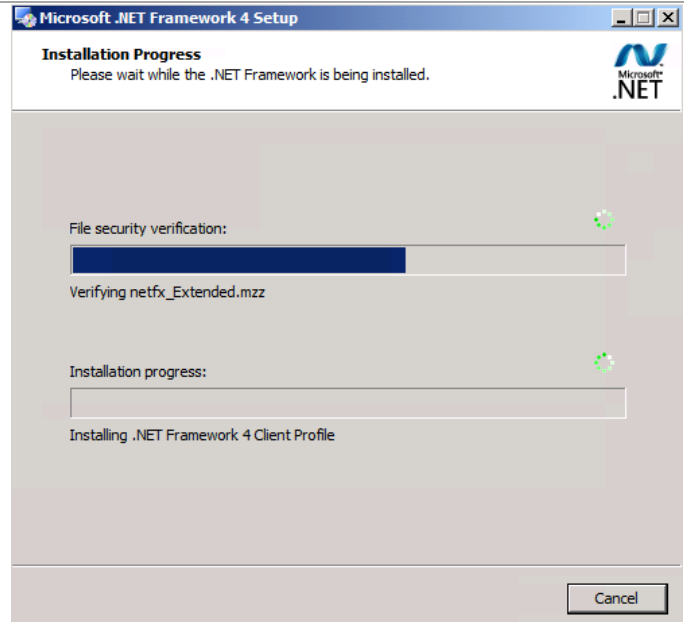


Within the Microsoft .NET Framework 4 Setup dialog, select the I have read and accept the license terms checkbox and click Install to begin the installation.

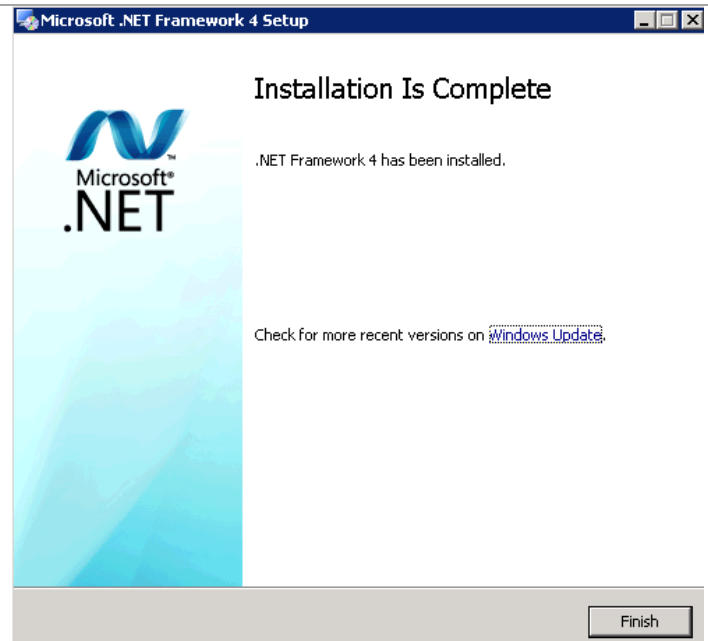




The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.



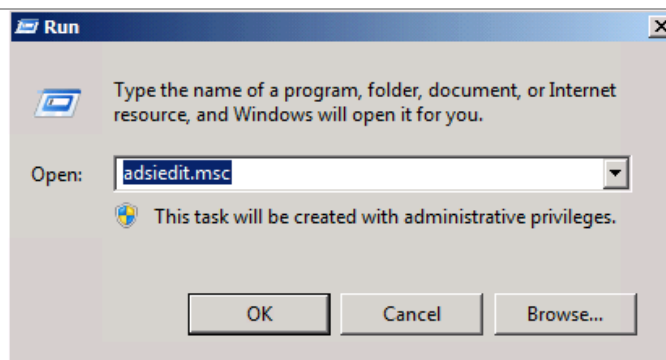


Creating the Virtual Machine Manager Distributed Key Management Container in Active Directory Domain Services

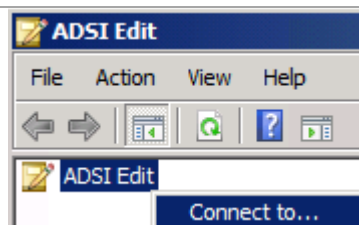
The VMM installation requires that an Active Directory container be created to house the distributed key information for Virtual Machine Manager⁸. The following steps are provided:

Perform the following steps on a **Domain Controller** in the domain where Virtual Machine Manager is to be installed.

Log on to a Domain Controller with a user that has Domain Admin privileges and run **adsiedit.msc**.



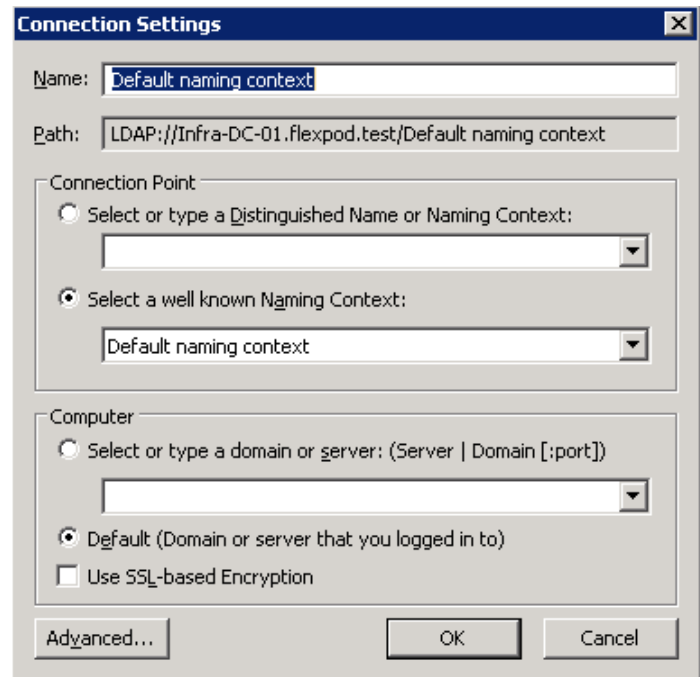
Right-click the **ADSI Edit** node and select **Connect to...** from the context menu.



⁸ Configuring Distributed Key Management in VMM - <http://technet.microsoft.com/library/gg697604.aspx>

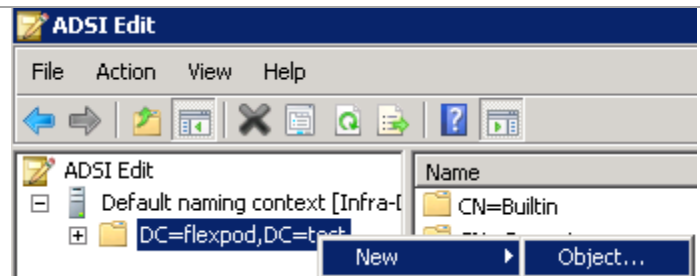


In the Connections Settings dialog in the Connection Point section select the Select a well known Naming Context option. Select Default naming context from the drop-down menu and click OK.



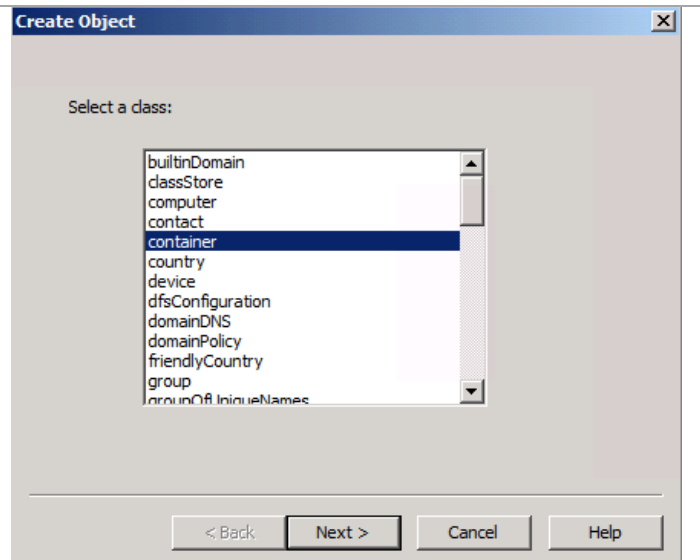
The Connection Settings dialog box is shown. The Name field is set to "Default naming context". The Path field is set to "LDAP://Infra-DC-01.flexpod.test/Default naming context". In the Connection Point section, the radio button "Select a well known Naming Context:" is selected, and the drop-down menu below it shows "Default naming context". In the Computer section, the radio button "Default (Domain or server that you logged in to)" is selected. The "Use SSL-based Encryption" checkbox is unchecked. The "Advanced..." button is visible on the left, and "OK" and "Cancel" buttons are on the right.

Expand Domain Default naming context [<computer fully qualified domain name>], expand <distinguished name of domain>, right-click the root node and select **New – Object...** from the context menu.



The ADSI Edit window is shown. The left pane shows the tree structure: "Default naming context [Infra-DC-01.flexpod.test]" expanded, and "DC=flexpod,DC=test" selected. The right pane shows the "Name" field with "CN=Builtin". The context menu is open, showing "New" and "Object..." options.

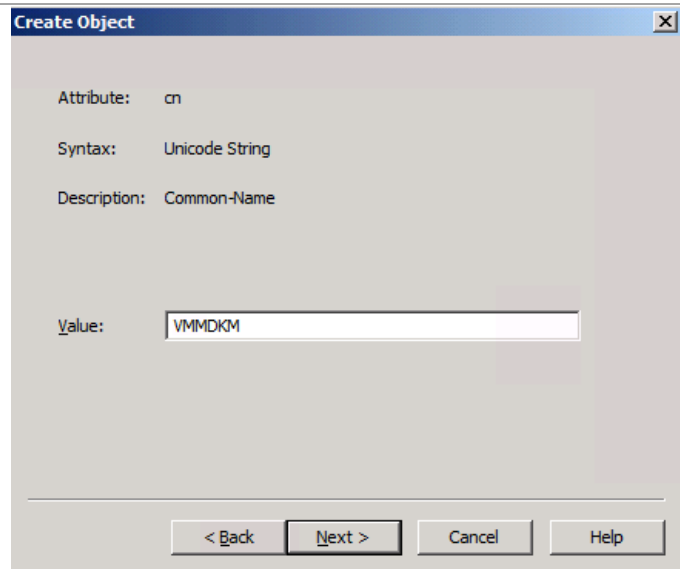
In the **Create Object** dialog box, select **Container**, and then click **Next**.



The Create Object dialog box is shown. The "Select a class:" list box contains the following classes: "builtinDomain", "classStore", "computer", "contact", "container", "country", "device", "dfsConfiguration", "domainDNS", "domainPolicy", "friendlyCountry", "group", and "groupOfUniqueNames". The "container" class is selected. The "Next >" button is highlighted.



In the **Value** text box, type *VMMDKM*, and then click **Next**.

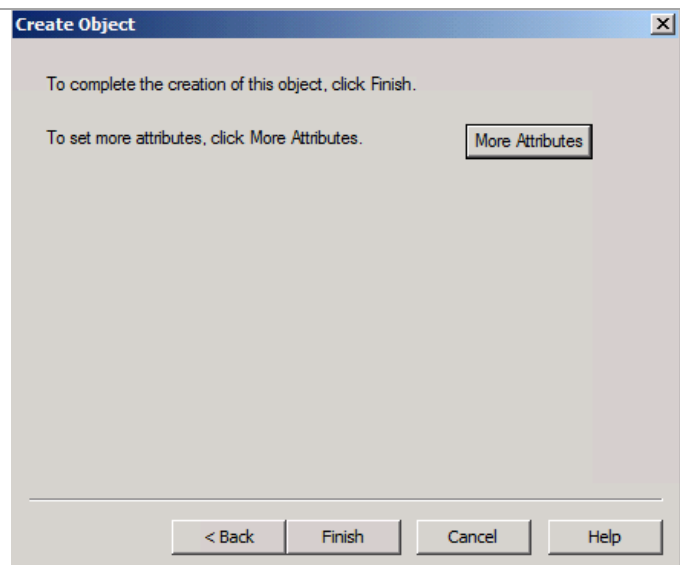


The 'Create Object' dialog box shows the following information:

- Attribute: cn
- Syntax: Unicode String
- Description: Common-Name
- Value: VMMDKM

At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Click **Finish** to create the container object.



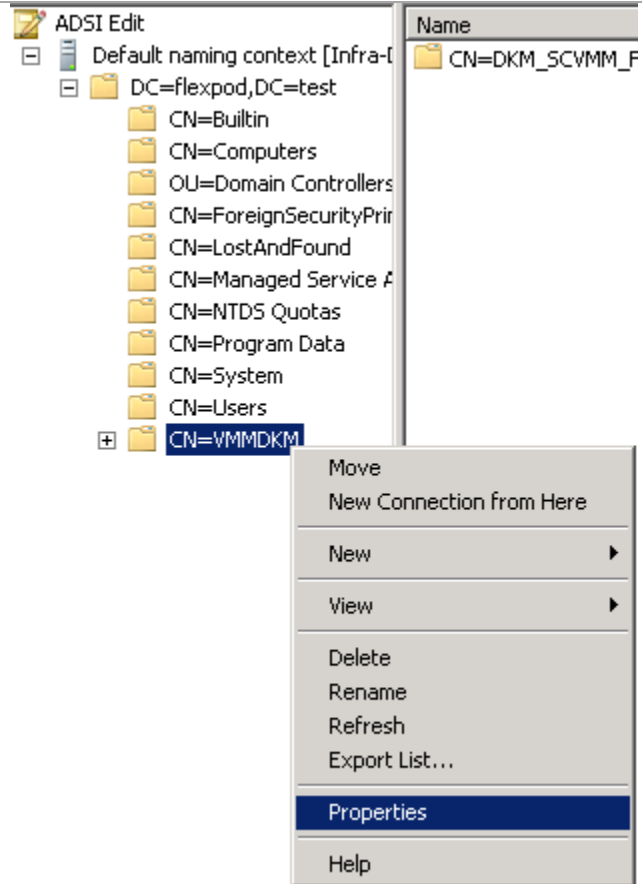
The 'Create Object' dialog box shows the following information:

- To complete the creation of this object, click Finish.
- To set more attributes, click More Attributes.

At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.



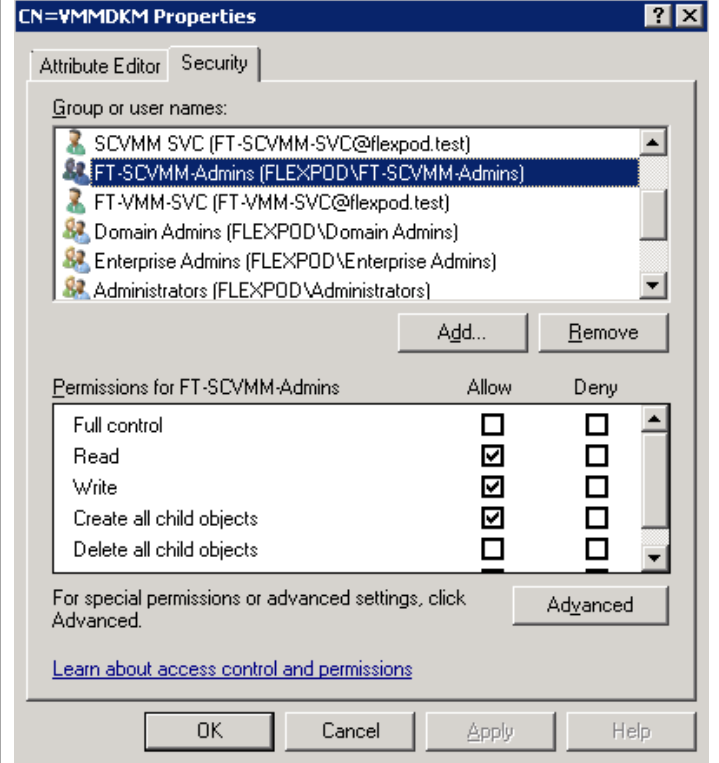
Within ADSI Edit, right-click the new **VMMDKM** object and then click **Properties**.





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 **Read**, **Write** and **Create all child objects** permissions.

Click **OK** three times and close ADSI Edit.

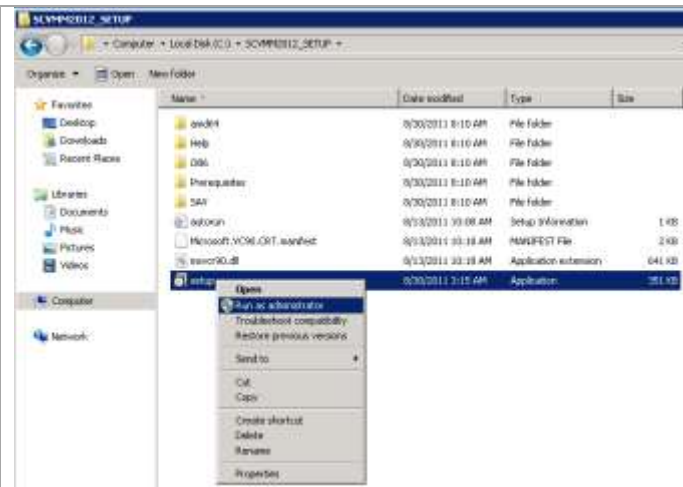


Installing Stand-Alone Virtual Machine Management Server

The following steps need to be completed in order to install VMM into the target virtual machine.

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

From the Virtual Machine Manager (VMM) installation media source right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

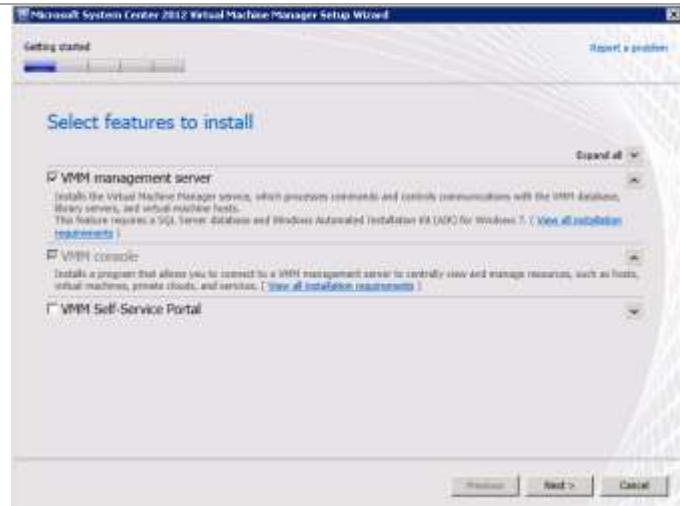




The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



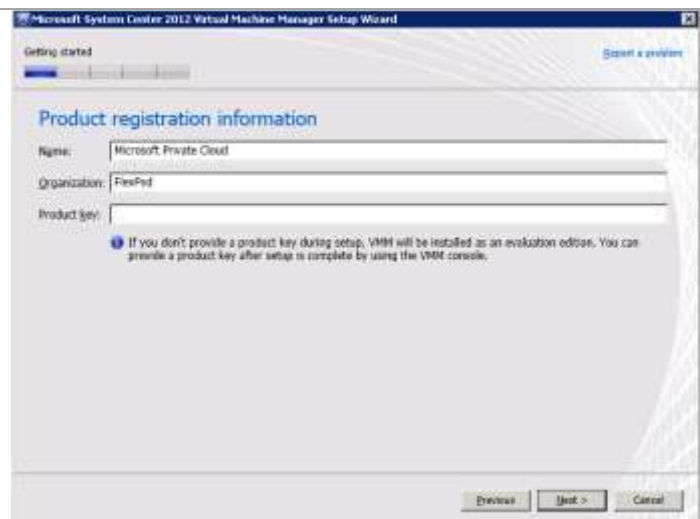
In the **Select features to install** dialog, verify the **VMM management server** installation option checkbox is selected. After selecting it the **VMM console** installation option checkbox will be selected by default. Click **Next** to continue.



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

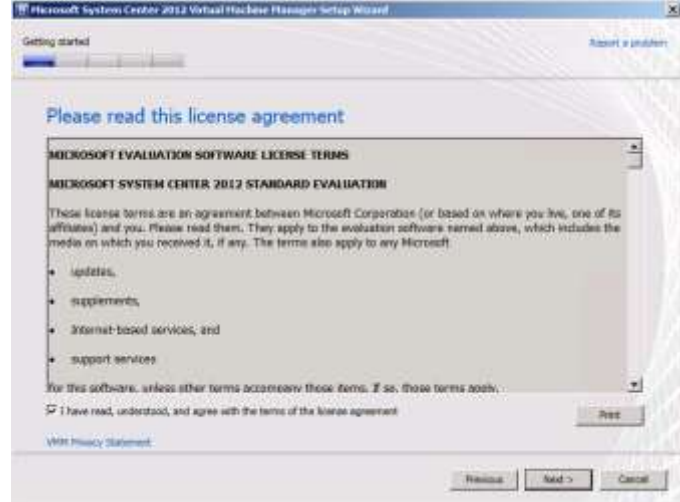
- **Name** – specify the name of primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.
- **Product key** – provide a valid product key for installation of Virtual Machine Manager. If no key is provided, Virtual Machine Manager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

Click **Next** to continue.

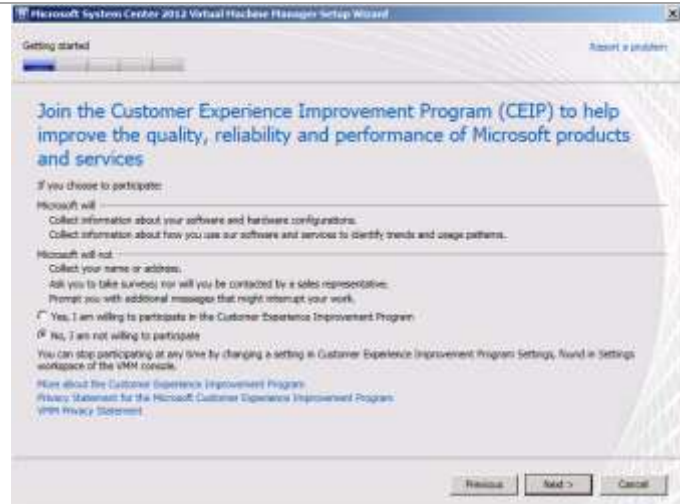




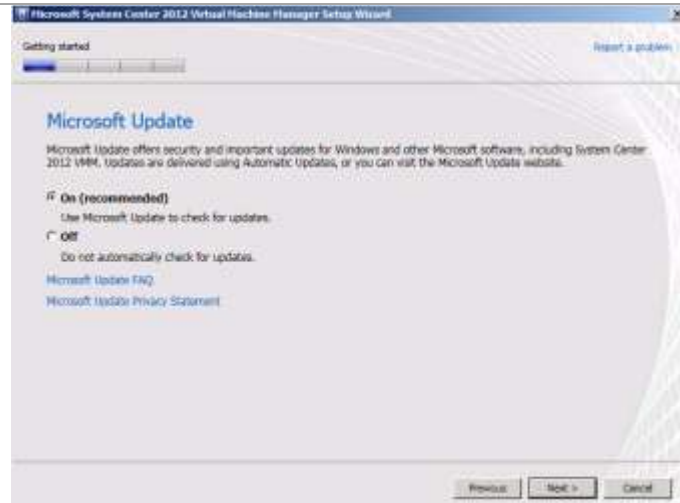
In the Please read this license agreement dialog, verify the I have read, understood and agree with the terms of the license agreement installation option checkbox is selected and click Next to continue.



In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue..

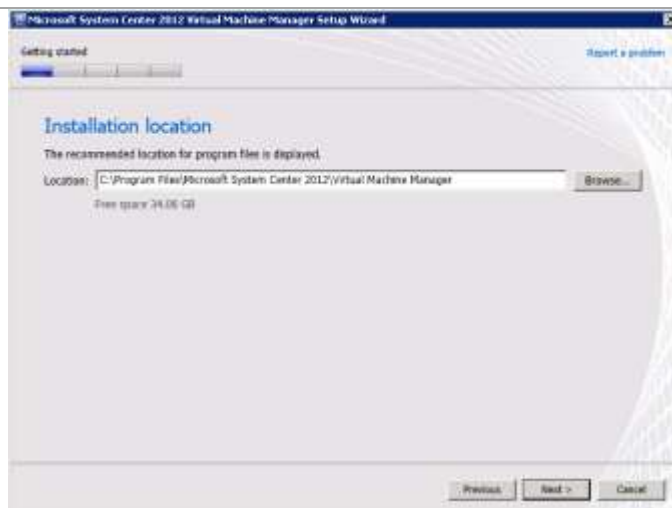


In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.



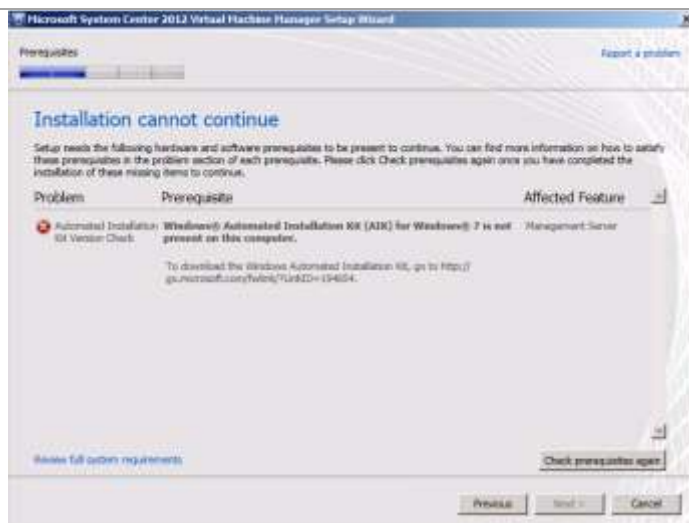


In the **Select installation location** dialog, specify a specific location or accept the default location of %ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager for the installation. Click **Next** to continue.



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.





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

- **Server Name** – Specify the name of SQL Server cluster created in the steps above.
- **Port** - Specify the TCP port used for the SQL Server if not the default

Verify the **Use the following credentials** checkbox is cleared. In the **Instance name** drop-down menu, select the SCVMM database instance deployed earlier in the SQL cluster.

In the **Select an existing database or create a new database** option, select the **New database** option and accept the default database name of *VirtualManagerDB*.

Click **Next** to continue.

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

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

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

Click **Next** to continue.



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

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

Click **Next** to continue.

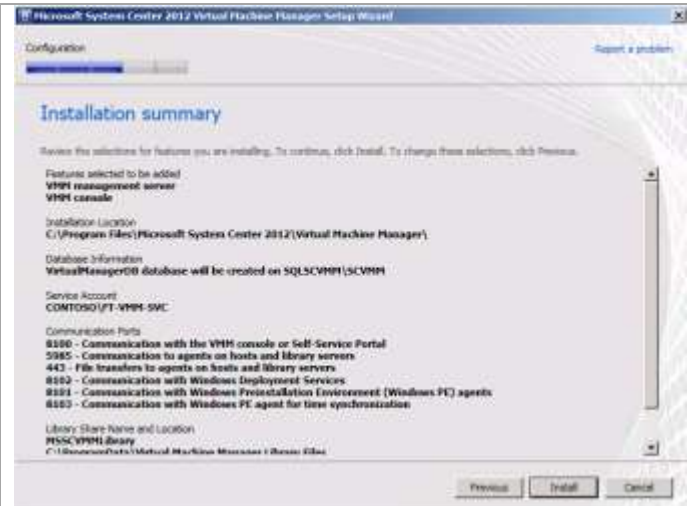
In the **Library configuration** dialog, in the **Specify a share for the Virtual Machine Manager library** section, select the **Create a new library share** option. Accept the defaults or specify the following in the provided text boxes:

- **Share name** – specify the Virtual Machine Manager Library share name. Default value: MSSCVMMLibrary.
- **Share location** – specify the physical location where the Virtual Machine Manager Library share will reside. Note that in some installations, additional LUNs can be provisioned for storing Virtual Machine Manager Library content. Default value: %ProgramData%\Virtual Machine Manager Library Files.
- **Share Description** – A short descriptive name for the library share. Default value: VMM Library Share.

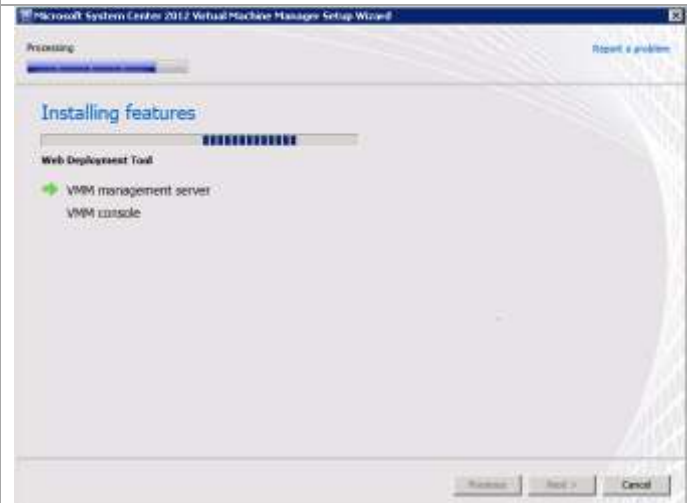
Click **Next** to continue.



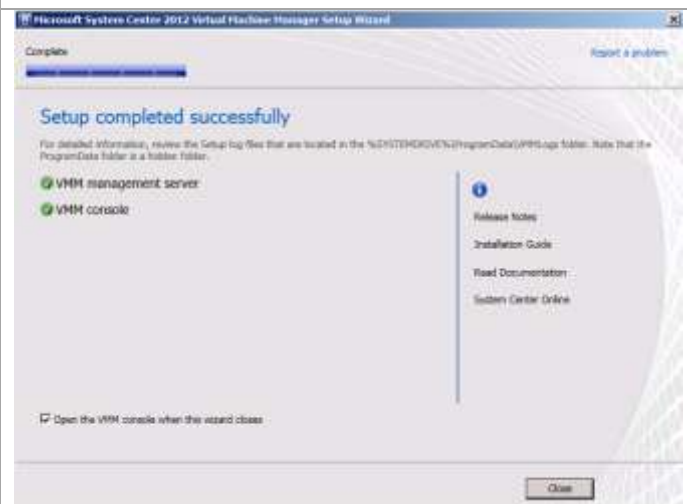
The **Installation summary** dialog will appear and displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.

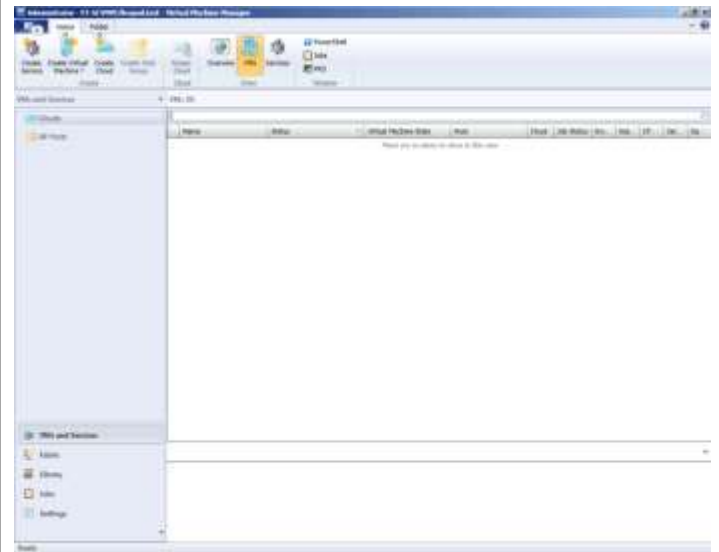


The wizard will display the progress while installing features.



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

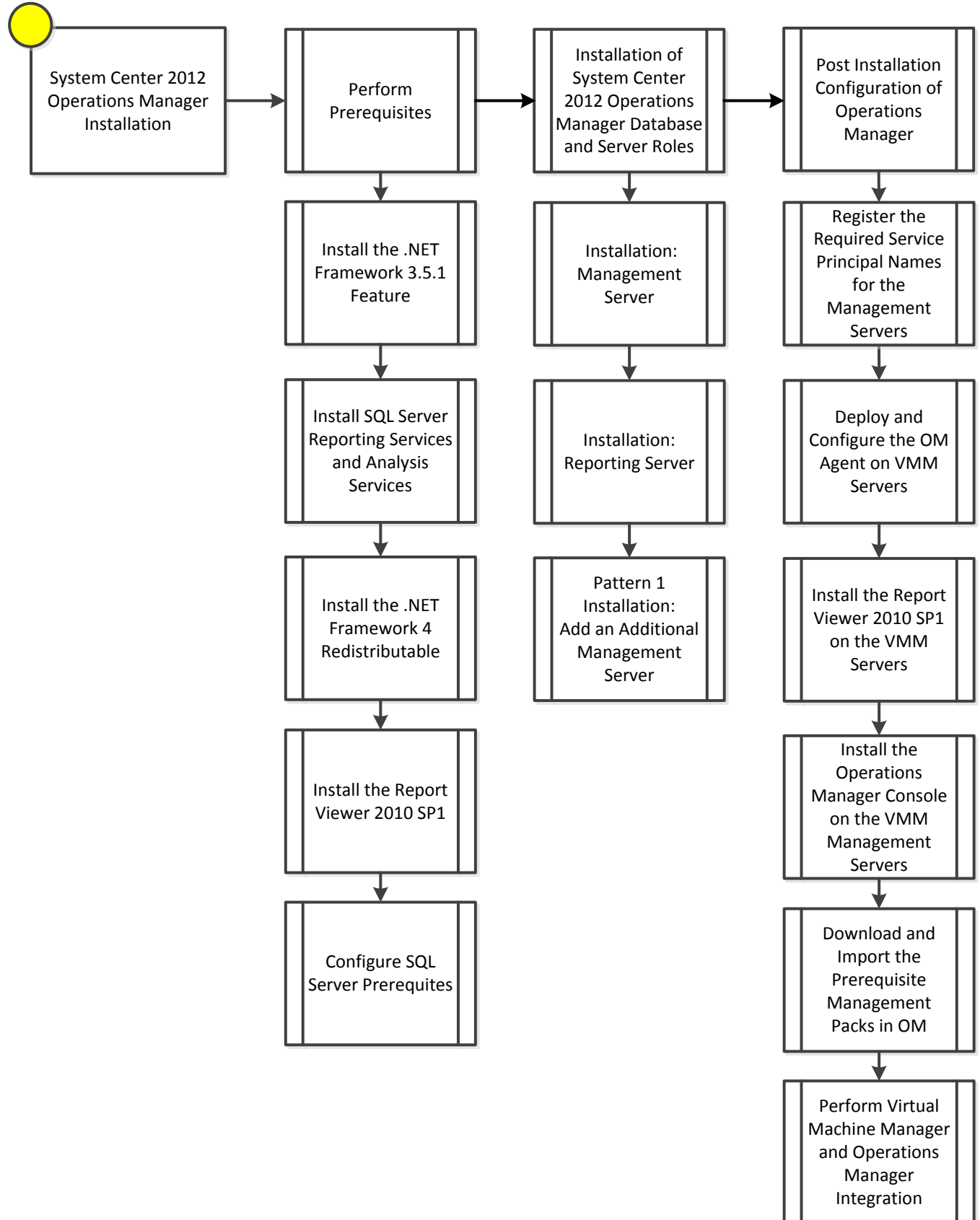




The Operations Manager installation process is comprised of the following high-level steps:



Microsoft





Overview

This section provides high-level walkthrough on how to setup and run the task sequence and scripts for deploying Operations Manager into the Fast Track fabric management architecture. The following assumptions are made:

A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for Operations Manager:

- Both .NET Framework 3.5 SP1 and .NET Framework 4 are required.
- A SQL Server 2008 R2 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 SQL Server cluster instances supporting the Operations Manager databases have two drives each already configured:

- Data
- Logs
- 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 server.
- The Operations Manager databases will run on a separate SQL Server instance on the cluster.

Pre-requisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created⁹:

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-	Operations Manager action	This account will need full admin permissions on all target systems

⁹ Specific rights for Operations Manager are outlined in http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin



User Name	Purpose	Permissions
Action	account	that will be managed using the action account.
<DOMAIN>\FT-SCOM-DR	Operations Manager data reader account	Domain account with local admin permissions on all Operations Manager management servers local admin rights on all SQL Server nodes.
<DOMAIN>\FT-SCOM-DW	Operations Manager, Data Warehouse write account	Domain account with local admin permissions on all Operations Manager management servers and local admin rights on all SQL Server nodes.



Groups

Verify that the following security groups have been created:

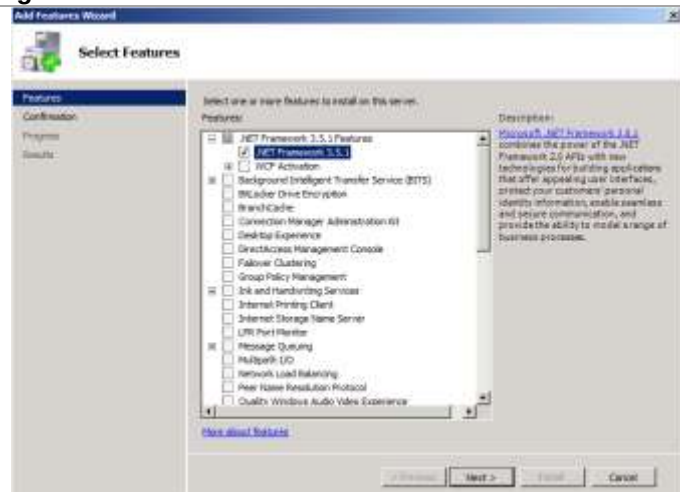
Security Group Name	Group Scope	Members
<DOMAIN>\FT-SCOM-ADMINS	Global	<DOMAIN>\FT-SCOM-Action <DOMAIN>\FT-SCOM-SVC <DOMAIN>\FT-SCOM-DR <DOMAIN>\FT-SCOM-DW Operations Manager Administrators' privileged admin account Operations Manager computer account <DOMAIN>\FT-VMM-SVC
<DOMAIN>\FT-OM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>\FT-OM-AdvOperators	Global	OpsMgr Advanced Operators privileged admin accounts

Add the .NET Framework 3.5.1 Feature

The Operations Manager installation requires the .NET Framework 3.5.1 Feature be enabled to support installation. Follow the steps below to enable the .NET Framework 3.5.1 Feature.

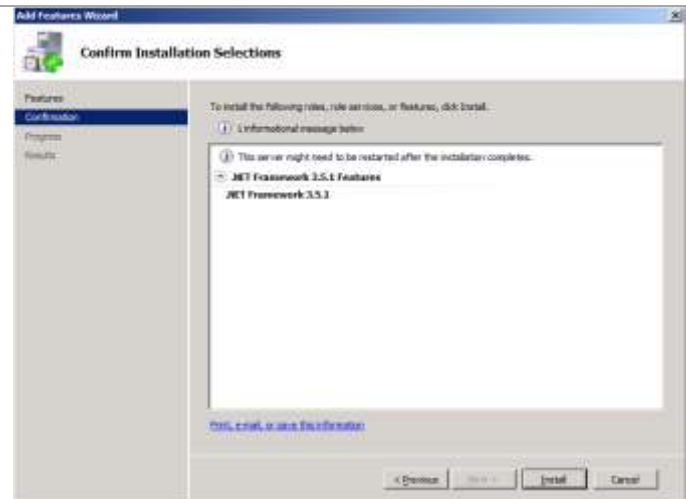
Perform the following steps on all **Operations Manager** virtual machines.

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**, **.NET Framework 3.5.1** check box only. Leave **WCF Activation** clear.

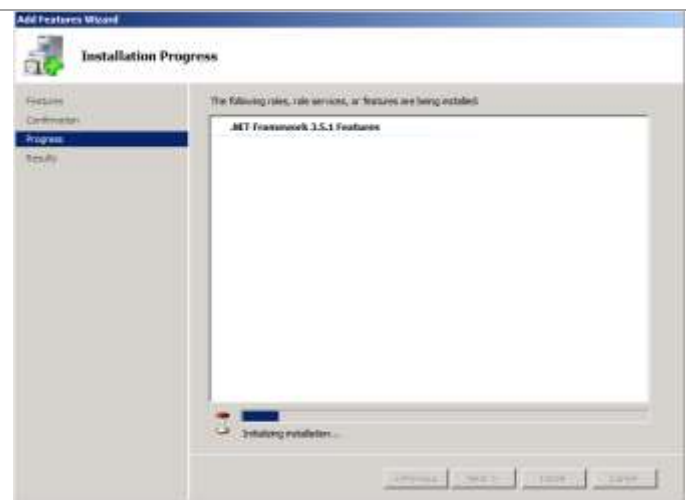




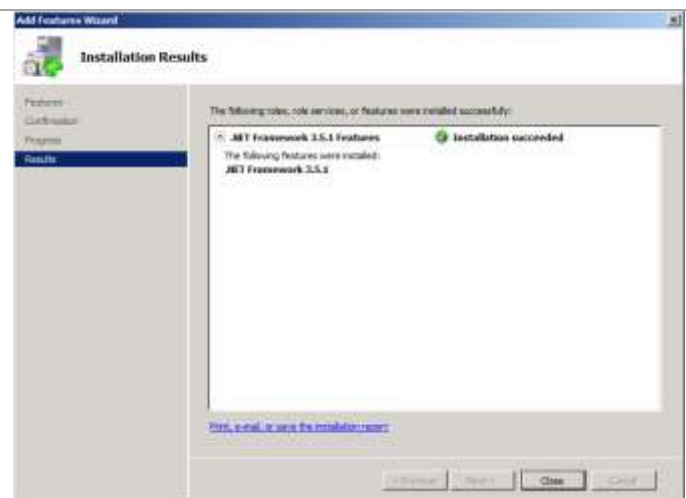
In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.



The **Installation Progress** dialog will show the progress of the feature install.



When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.





Installing SQL Server Reporting Services and Analysis Services (Split Configuration)

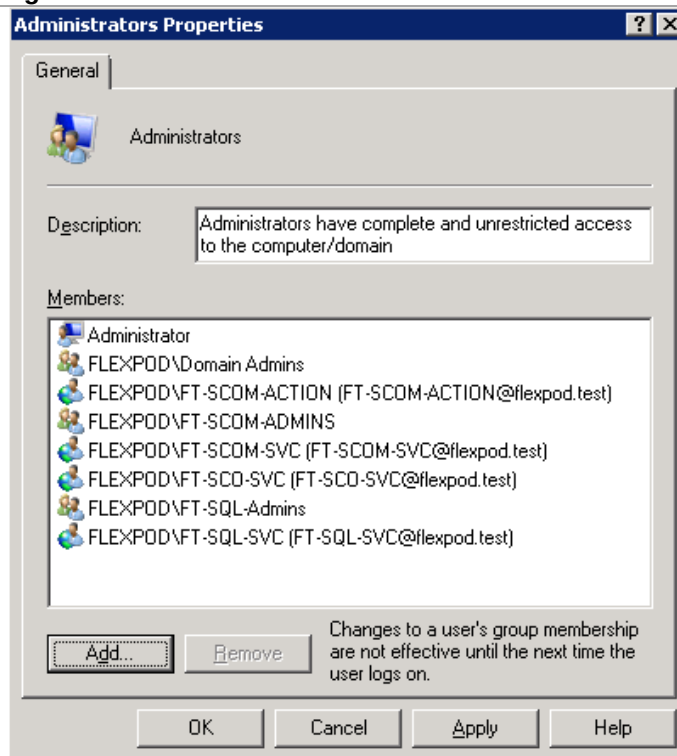
The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the provided steps to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

Perform the following steps on the **Operations Manager** virtual machine.

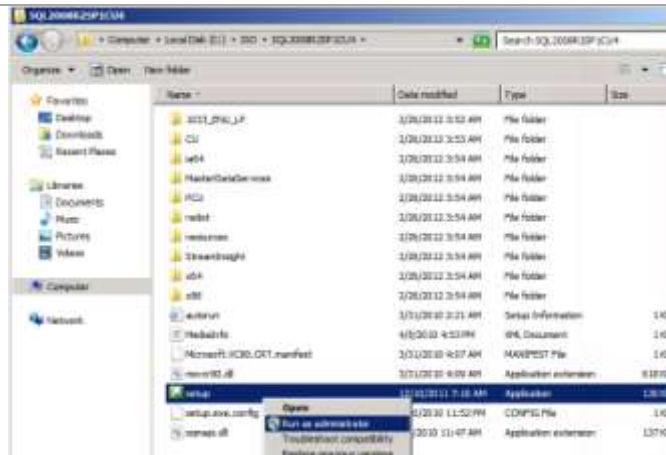
Log on to the Operations Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the 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 2008 R2 slipstreamed installation media source right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.





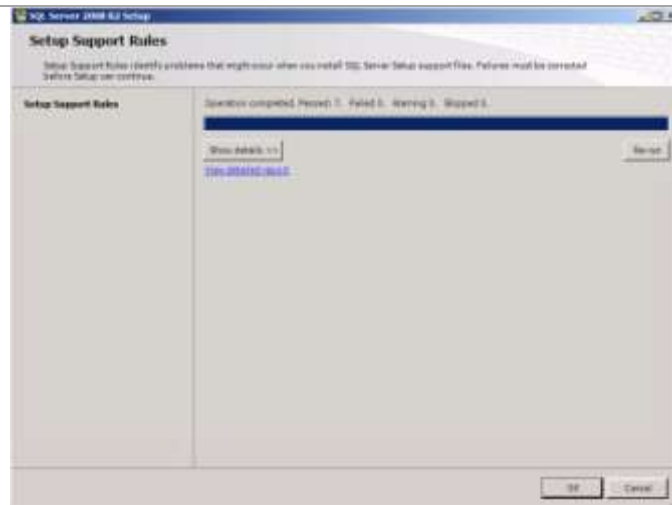
The SQL Server Installation Center will appear.



From the SQL Server Installation Center click the New installation or add features to an existing installation link.



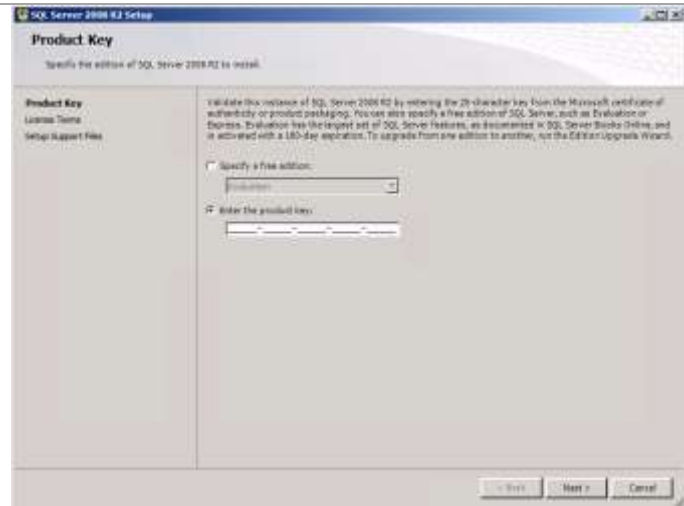
The **SQL Server 2008 R2 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.





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.

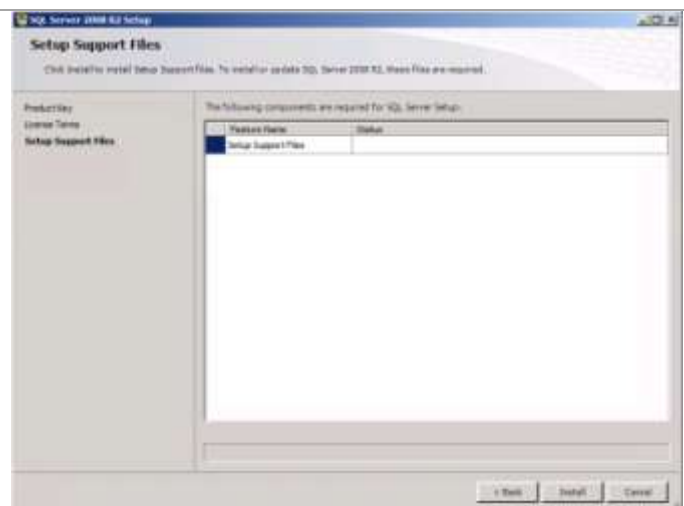
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop down menu for a 180-day evaluation period.



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

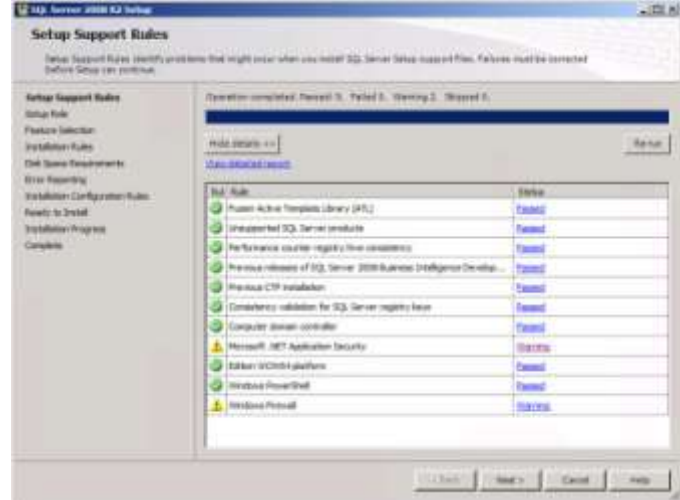


In the **Setup Support Files** dialog, click **Install** and allow the support files to install.

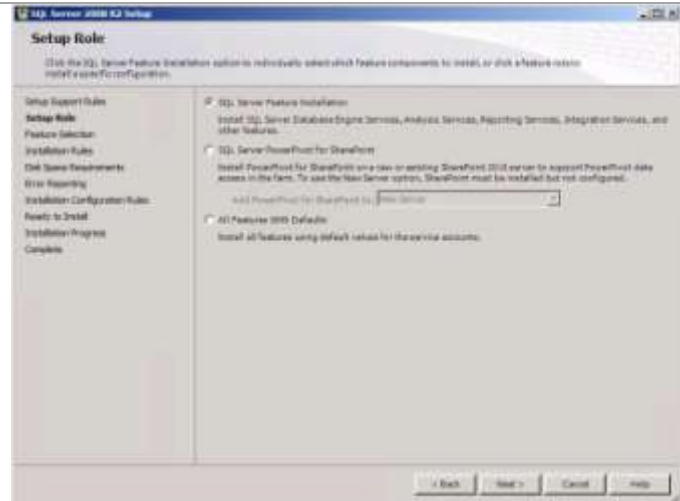




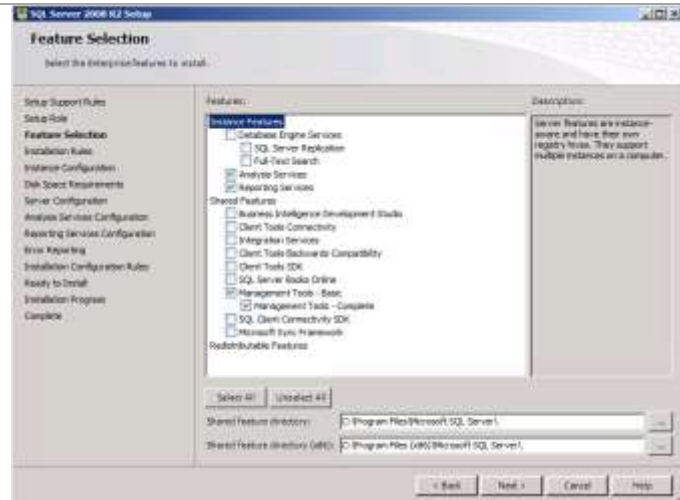
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

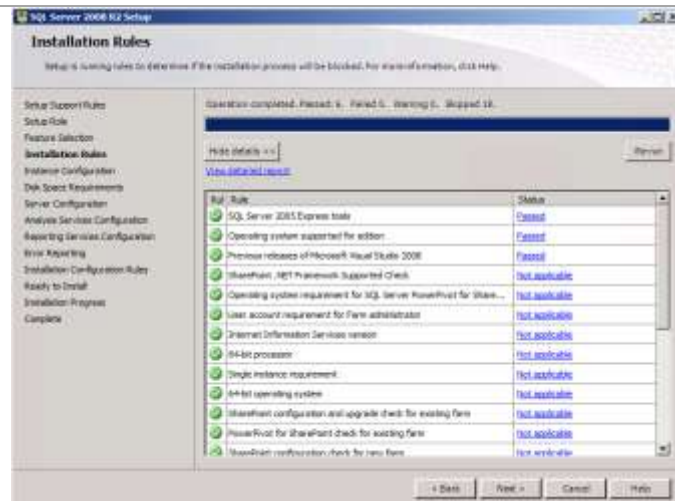


In the **Feature Selection** dialog, Select the **Analysis Services, Reporting Services, Management Tools – Basic and Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.

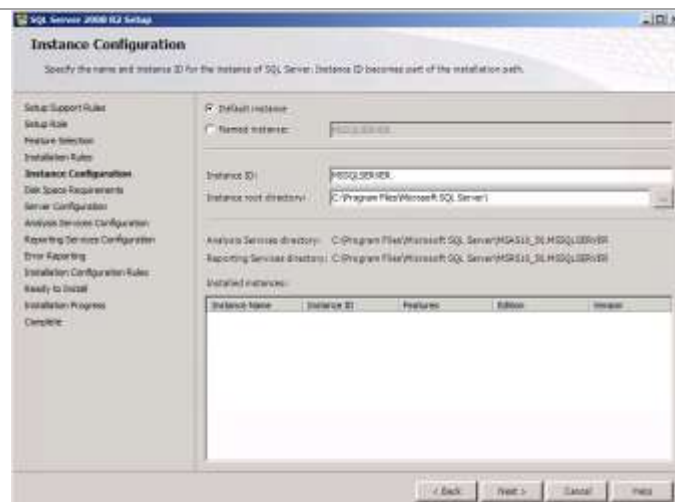




In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

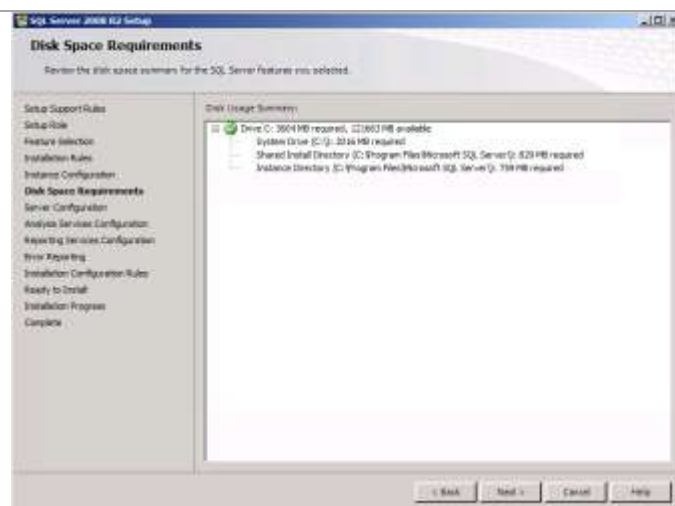


In the **Instance Configuration** dialog, select the **Named instance** option and specify **SCOMASRS** in the provided text box. Verify the **Instance ID** is listed as **SCOMASRS** in the provided text box. Keep the default **Instance root directory** values and click **Next** to continue.



Note: a post-installation configuration process will occur to configure the reporting server database within the Operations Manager SQL Server instance.

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

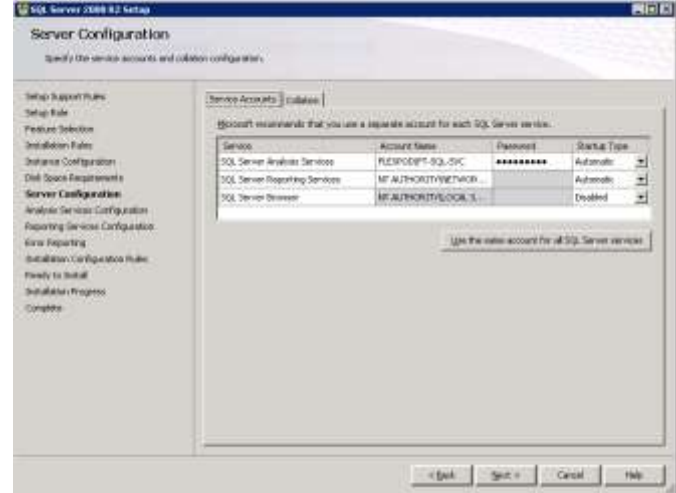




In the Server Configuration dialog, select the Service Accounts tab.

- Specify the NETWORK SERVICE account for the SQL Server Reporting Services service.
- Specify the Fast Track SQL Server Service account for the SQL Server Analysis Services service.

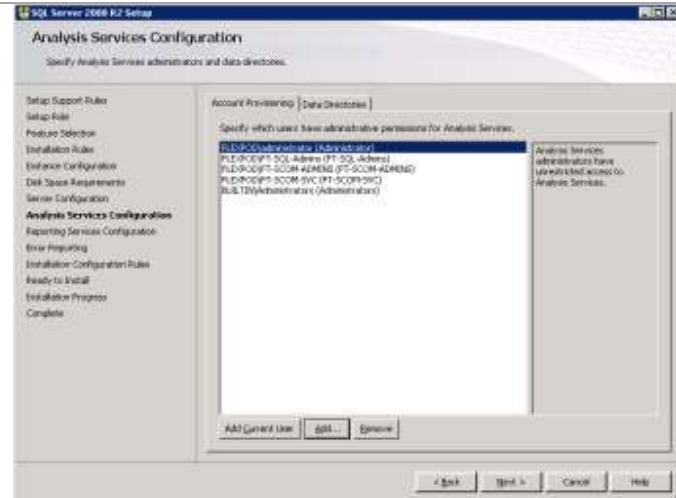
Click **Next** to continue.



In the Analysis Services Configuration dialog, select the Account Provisioning tab. In the Specify which users have administrative permissions for Analysis Services section, click the Add Current User button to add the current installation user. Click the Add... button to select the following groups:

- Operations Manager Admins group.
- Operations configuration service and data access service account.
- SQL Server service account.
- SQL Server Admins group.
- BUILTIN\Administrators.SQL Server Admins group.

Click **Next** to continue.

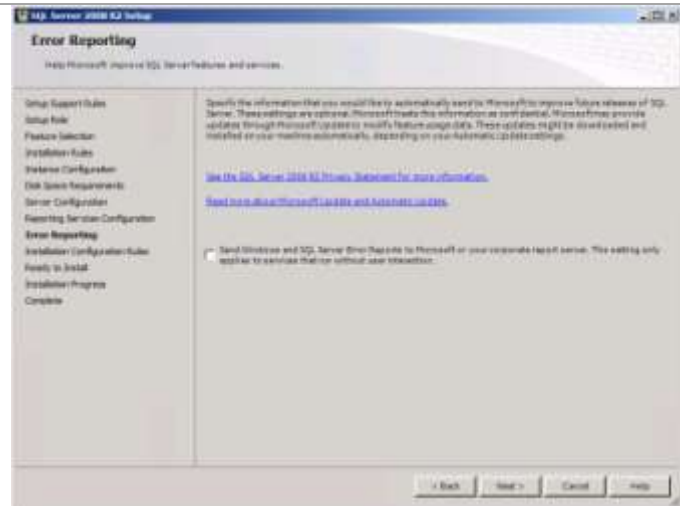


In the **Reporting Services Configuration** dialog, select the **Install, but do not configure the report server** radio button. Note that other options should not be available since the database engine was not selected as a feature for installation. Click **Next** to continue.

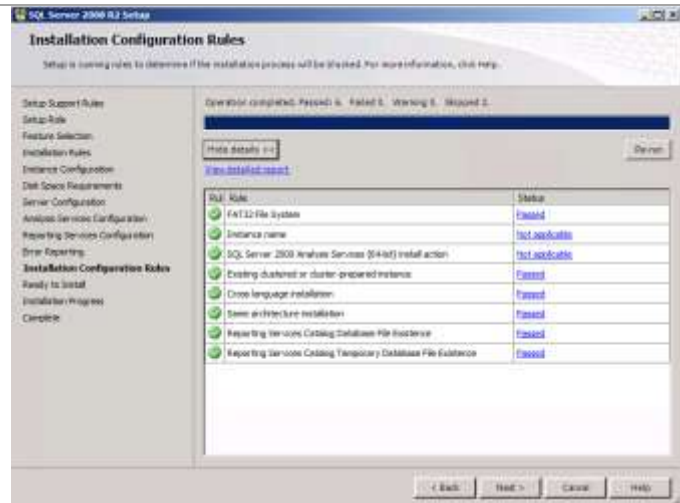




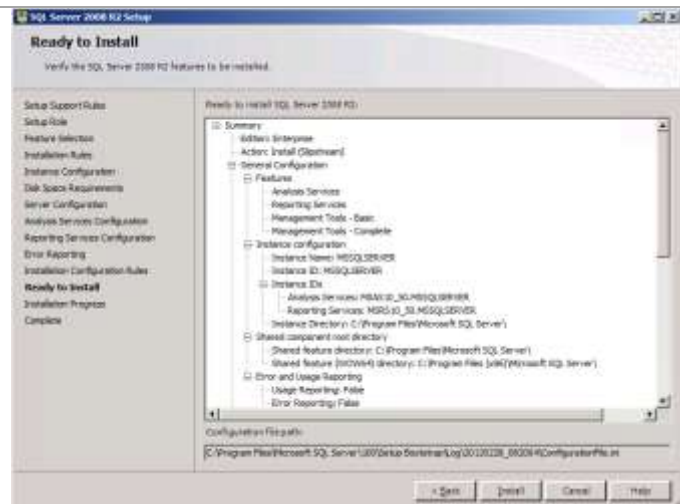
In the Error Reporting dialog, select or deselect the Send Windows and SQL Server Error Reports to Microsoft or your corporate report server based on your organization's policies and click Next to continue.



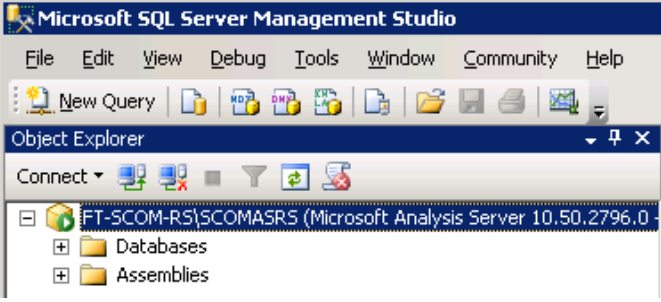
In the **Installation Configuration Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

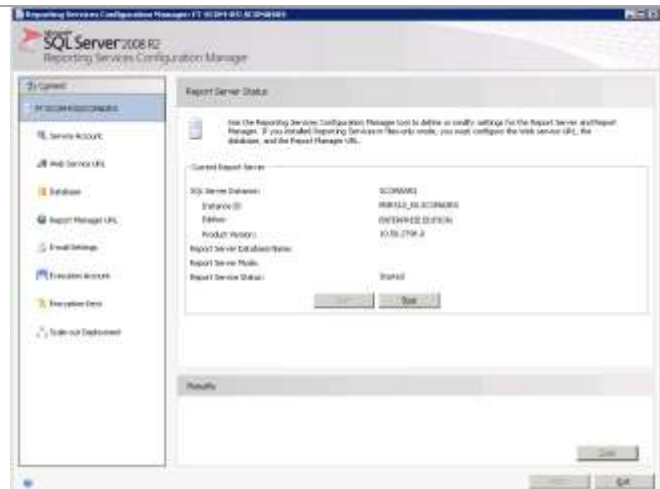




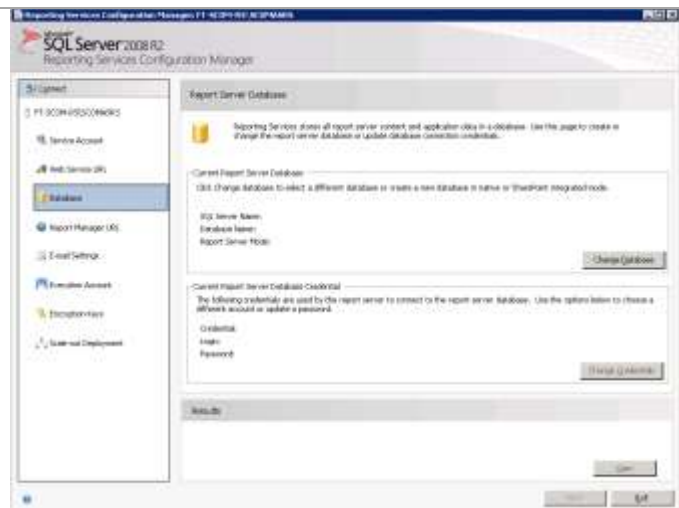
When complete the Complete dialog will appear. Click Close to complete the installation of this SQL database instance.	
Verify the installation in SQL Server Management Studio prior to moving to the next step of installation.	
When installed, verify that the Service Manager Management Server installed properly by opening the console. From the Start Menu, navigate to the Microsoft SQL Server 2008 R2 folder and click the Reporting Services Configuration Manager shortcut.	
The Reporting Services Configuration Connection dialog will appear. In the Server Name text box, specify the name of the Operations Manager server. In the Report Server Instance text box, use the default SCOMASRS drop-down menu value. Click Connect.	



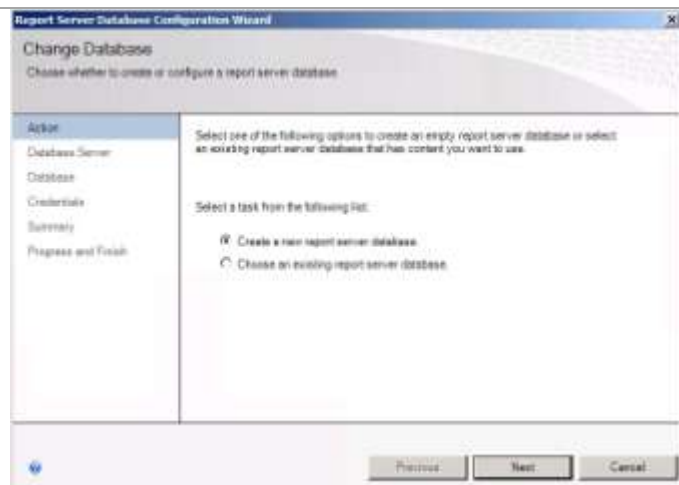
The Reporting Services Configuration Manager tool will appear.



In the Reporting Services Configuration Manager tool, click the Database option from the toolbar. Within the Current Report Server Database section, click the Change Database button.



The Reporting Services Database Configuration Wizard will appear. In the Action section, choose the Create a new report server database option. Click Next to continue.





In the **Database Server** section, specify the following values:

- **Server Name** – specify the name of the SQL Server CNO and the database instance created for the Operations Manager installation.
- **Authentication Type** – specify **Current User – Integrated Security** from the drop-down menu.

Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.

The screenshot shows the 'Report Server Database Configuration Wizard' window. The 'Change Database' section is active, with the 'Database Server' tab selected in the left-hand navigation pane. The main area contains the following fields and options:

- Server Name:** SQLSCOMBVISCOMDB
- Authentication Type:** Current User - Integrated Security (selected from a dropdown menu)
- Username:** PLEEFOD\administrator
- Password:** (empty field)
- Test Connection:** button

At the bottom of the window, there are 'Previous', 'Next', and 'Cancel' buttons.

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.

The screenshot shows the 'Report Server Database Configuration Wizard' window. The 'Change Database' section is active, with the 'Database' tab selected in the left-hand navigation pane. The main area contains the following fields and options:

- Database Name:** ReportServer
- Temp Database Name:** ReportServerTemp
- Language:** English (United States) (selected from a dropdown menu)
- Report Server Mode:** Native Mode (selected with a radio button)
- SharePoint Integrated Mode:** (unselected with a radio button)

At the bottom of the window, there are 'Previous', 'Next', and 'Cancel' buttons.

In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.

The screenshot shows the 'Report Server Database Configuration Wizard' window. The 'Change Database' section is active, with the 'Credentials' tab selected in the left-hand navigation pane. The main area contains the following fields and options:

- Authentication Type:** Service Credentials (selected from a dropdown menu)
- Username:** PLEEFOD\administrator
- Password:** (empty field)

At the bottom of the window, there are 'Previous', 'Next', and 'Cancel' buttons.



In the **Summary** section, review the selections made and click **Next** to create the SQL Server Reporting Services database.

The following information will be used to create a new report server database. Verify this information is correct before you continue.	
SQL Server Instance:	SQLSCMDENSCOMDB
Report Server Database:	ReportServer
Temp Database:	ReportServerTempDB
Report Server Language:	English (United States)
Report Server Mode:	Native
Authentication Type:	Service Account
Username:	NT AUTHORITY\NETWORKSERVICE
Password:	*****

Buttons: 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**.

Step	Status
Verifying database info	Success
Generating database script	Success
Flushing database script	Success
Generating rights scripts	Success
Applying connection rights	Success
Setting DSN	Success

Buttons: 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.

Report Server Database

Reporting services stores all report server content and application data in a database. Use this page to create a new 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:	SQLSCMDENSCOMDB
Database Name:	ReportServer
Report Server Mode:	Native

Current Report Server Database Credential

The following credentials are used by the report server to connect to the report server database. Use the options to request or update a password.

Credential:	Service Account
Logon:	NT AUTHORITY\NETWORKSERVICE
Password:	*****

Buttons: Previous, Next, Cancel



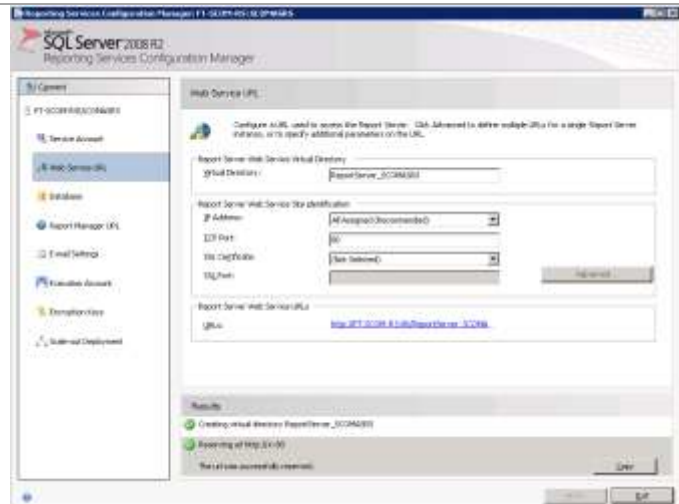
In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

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).

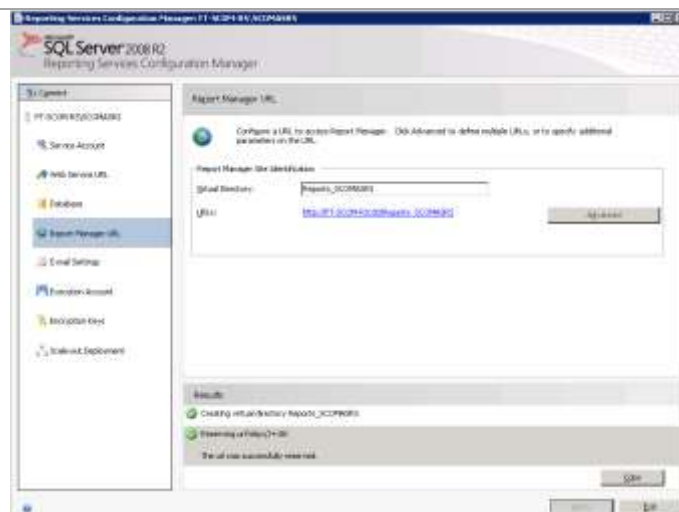
Click the **Apply** button to save the settings and create the Web Service URL.



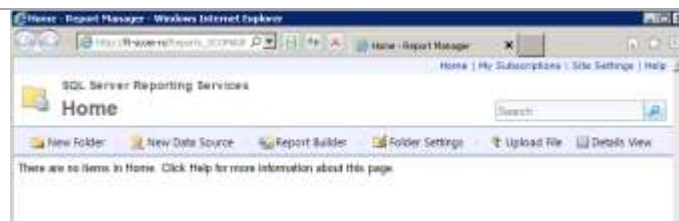
In the **Reporting Services Configuration Manager** tool, click the **Report Manager URL** option from the toolbar. Specify the following value:

In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports** in the provided text box.

Click the **Apply** button to save the settings and create the Report Manager URL.



Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.





Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.

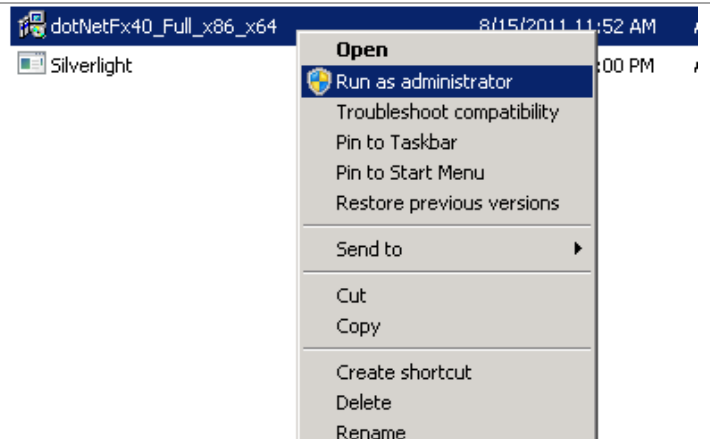


Installing .NET Framework 4

Additionally, the Operations Manager installation also requires the .NET Framework 4 package be installed prior to installation. Follow the provided steps to install the .NET Framework 4 package.

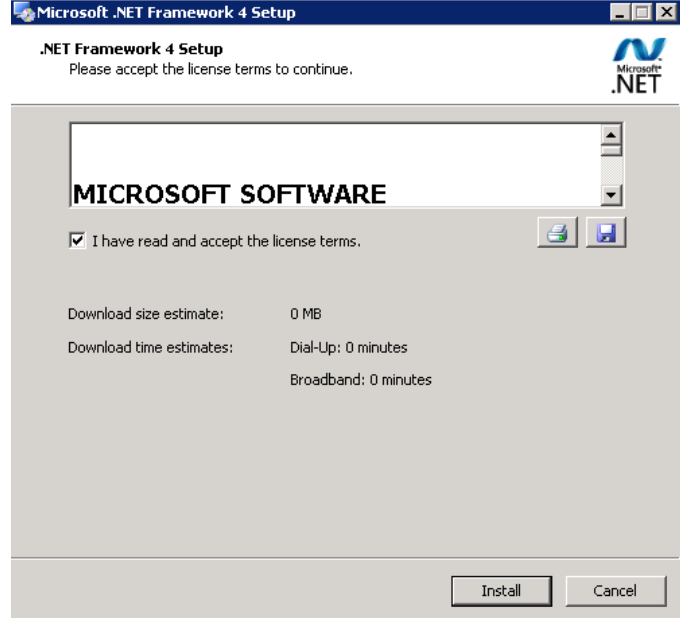
Perform the following steps on the **Operations Manager** virtual machine.

From the installation media source right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** from the context menu to begin setup.

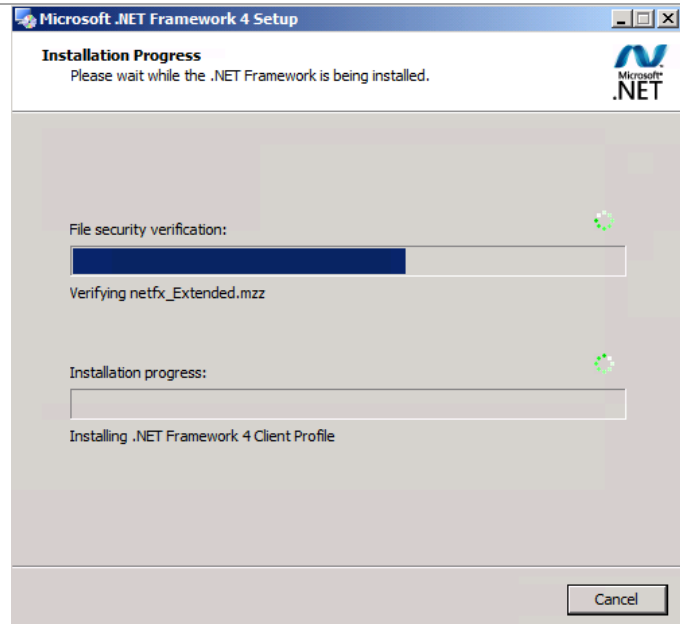




Within the Microsoft .NET Framework 4 Setup dialog, select the I have read and accept the license terms check box and click Install to begin the installation.

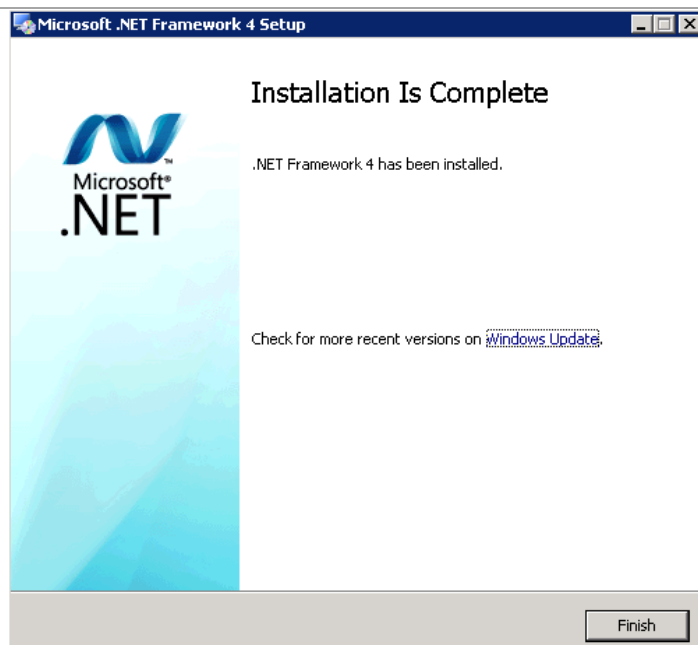


The installation progress will be displayed in the setup wizard.





When completed, click **Finish** to exit the installation.

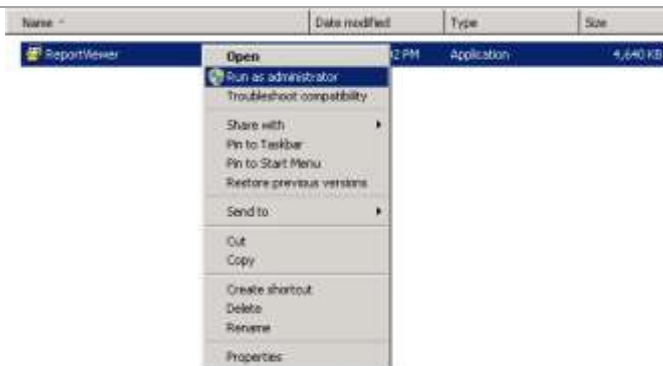


Install Microsoft Report Viewer 2010 SP1

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.¹⁰ Follow the provided steps to install the Microsoft Report Viewer 2010 SP1.

Perform the following steps on both **Operations Manager management server** virtual machines.

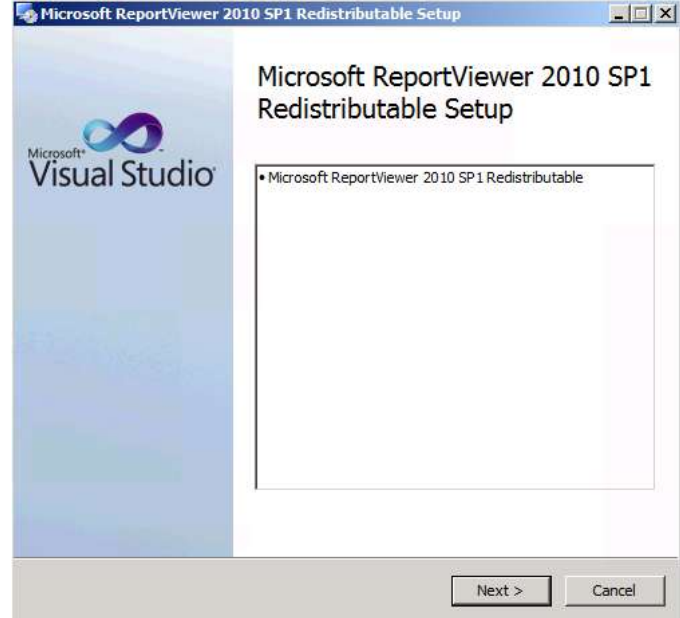
From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



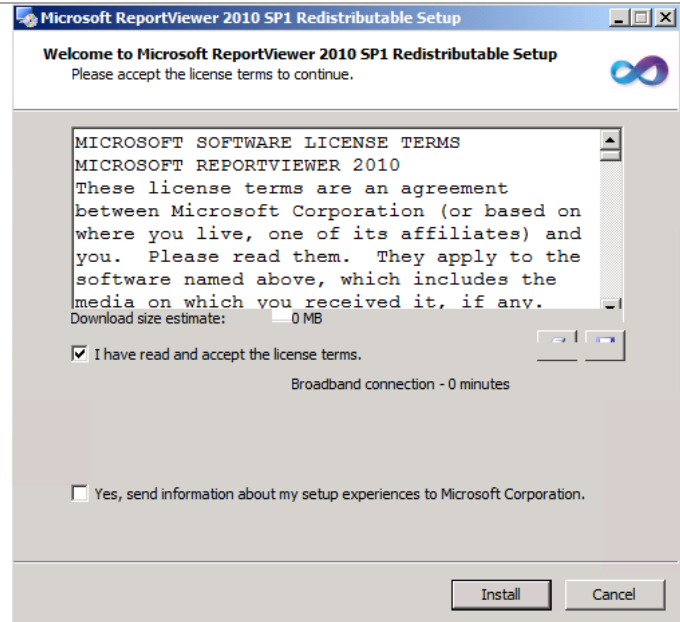
¹⁰ Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en>.



Within the Microsoft ReportViewer 2010 SP1 Redistributable Setup dialog, select Next to begin the installation.

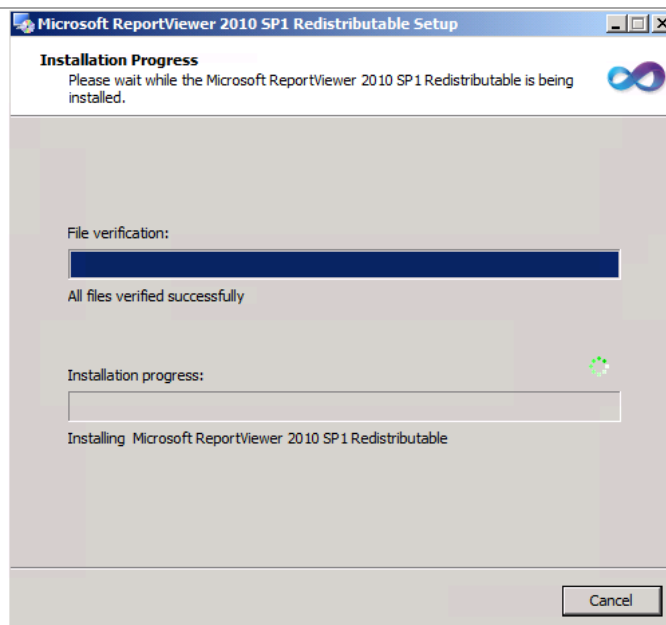


Select the I have read and accept the license terms check box and click Install.





The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.



Configuration of Operations Manager SQL Prerequisites

The following steps must be completed in order to install the required pre-requisites for Operations Manager¹¹.

Perform the following step on the **Operations Manager management server** virtual machine.

¹¹ Deploying System Center 2012 - Operations Manager - http://technet.microsoft.com/en-us/library/d81818d2-534e-475c-98e1-65496357d5a5#BKMK_BeforeYouBegin

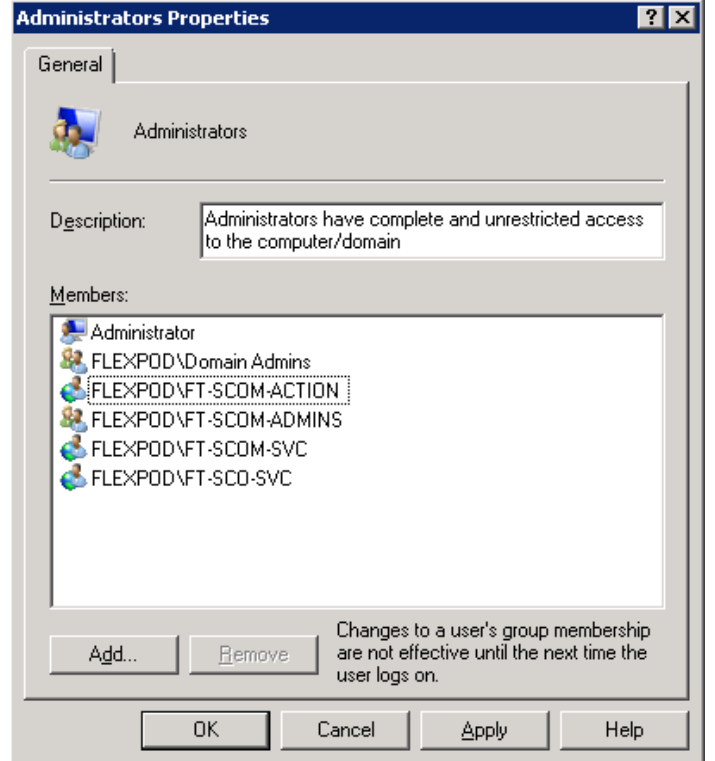


Log on to the Operations Manager virtual machine with a user with local admin rights.

Verify that the following accounts and/or groups are members of the Local Administrators group on the Operations Manager virtual machine:

- Orchestrator service account.
- Operations Manager action account.
- Operations Manager Admins group.

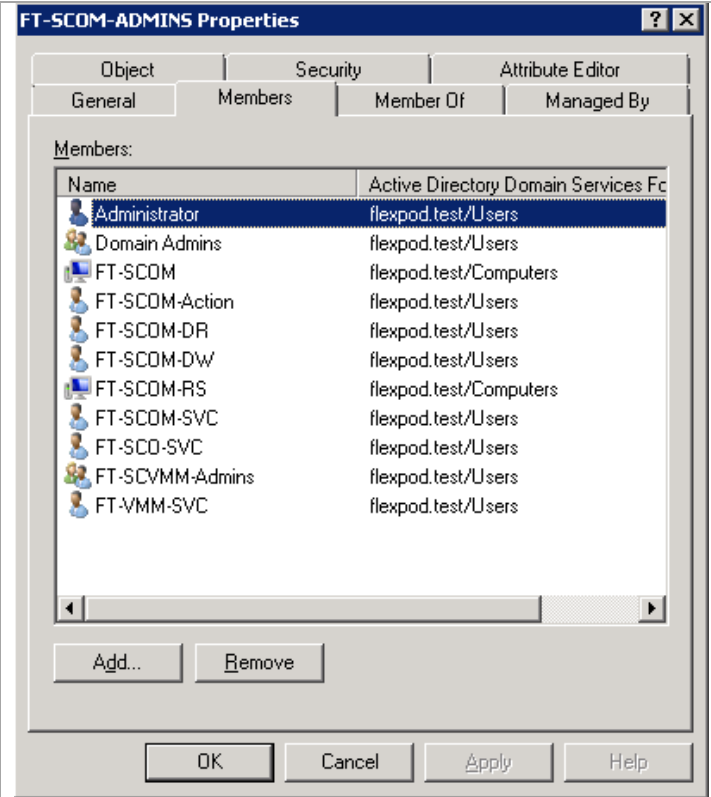
Operations configuration service and data access service account.



Perform the following step on an **Active Directory Domain Controller** in the target environment.



In the domain where Operations Manager will be installed, verify that the Operations Manager computer account and the groups outlined in the table above are members of the OM Admins group created earlier.

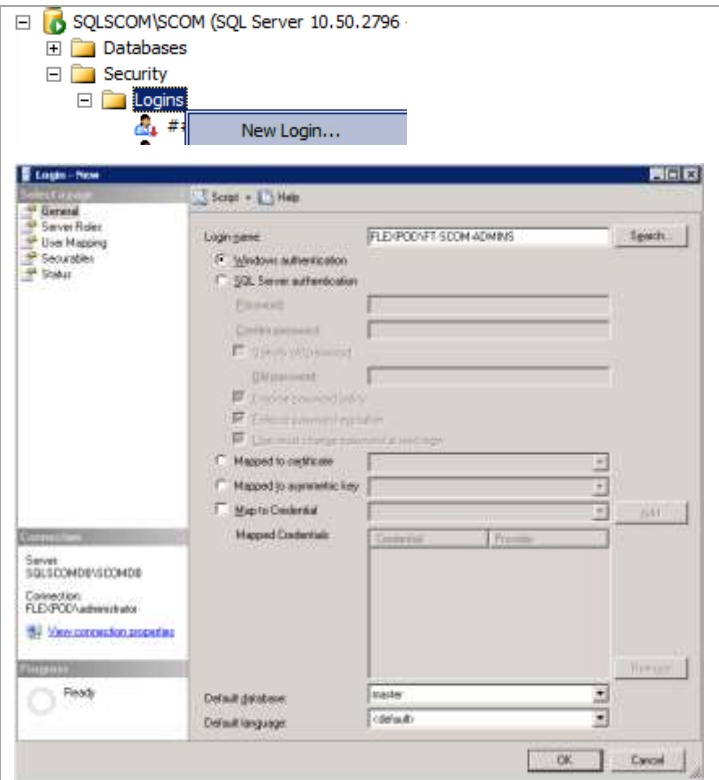


Perform the following steps on the **First SQL Server** virtual machine.



Using Administrative credentials, log into the first SQL server and open SQL Management Studio. Connect to the Operations Manager SQL 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.

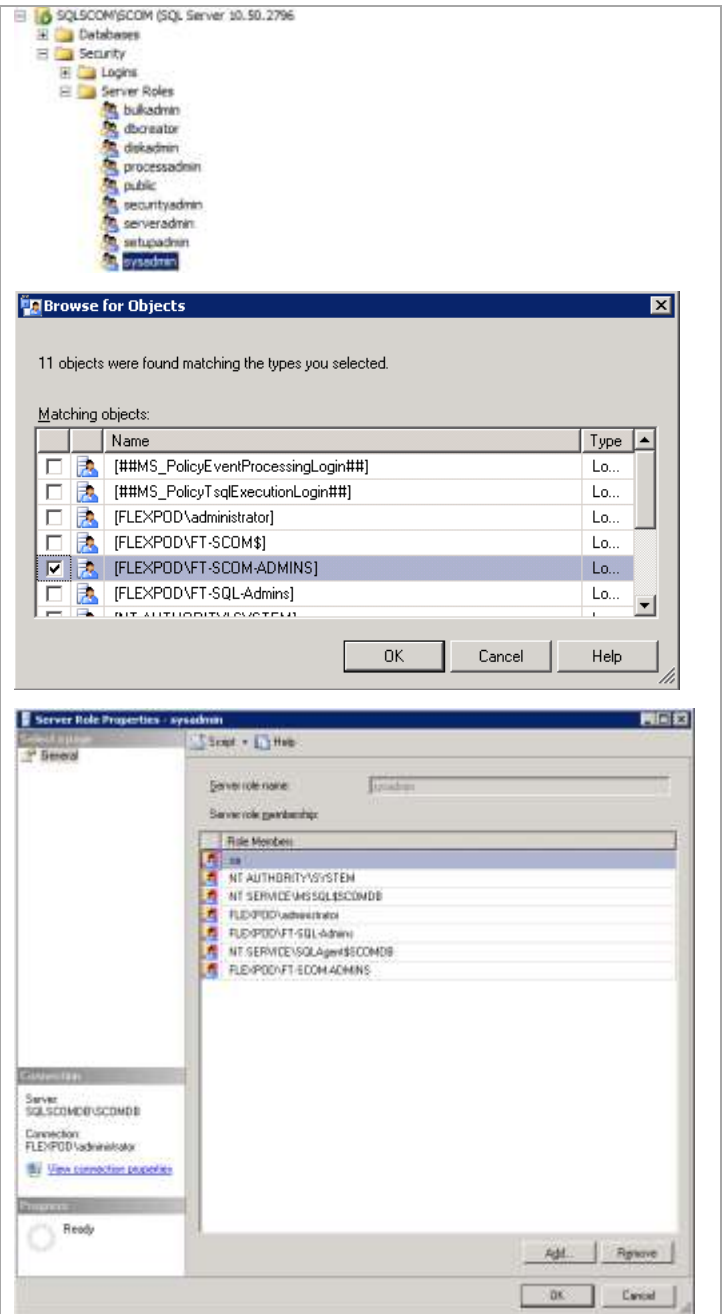
In the **Login – New** dialog, specify the OM Admins group created earlier as the new **Login name** and click **OK** to create the new login.





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** and click **OK** to create the new login.



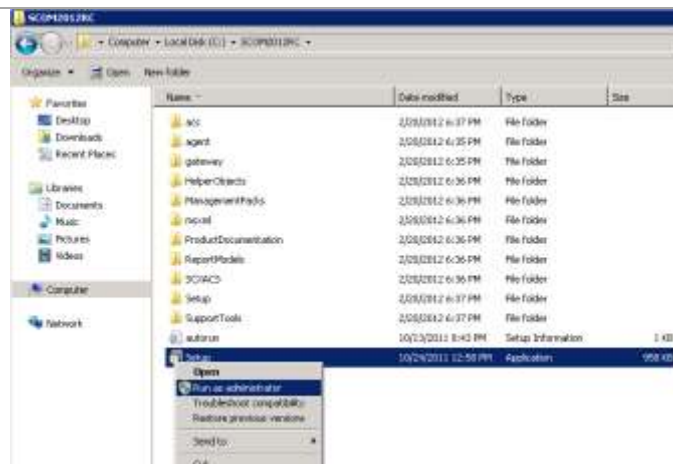


Installing the Management Server

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 **Operations Manager** management server virtual machine.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup

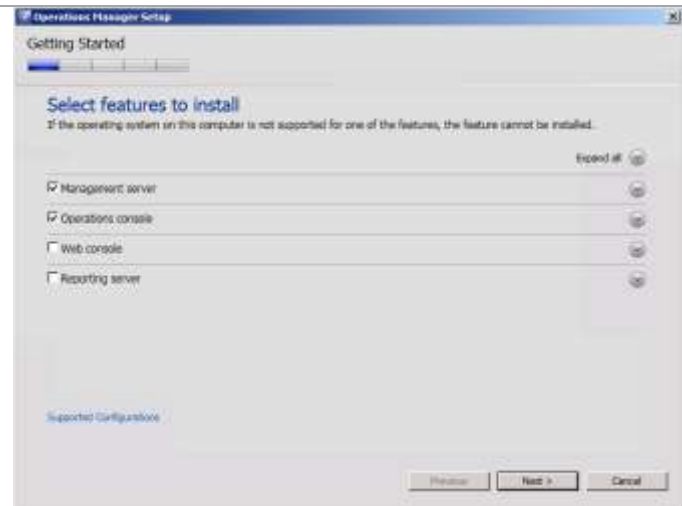


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation..





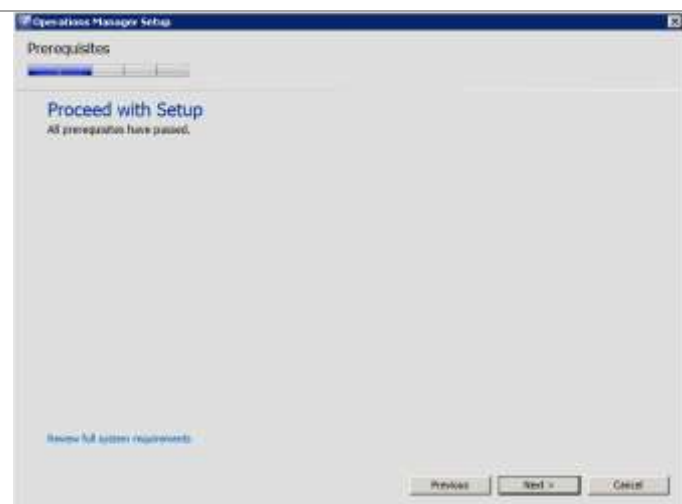
In the **Select features to install** dialog, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of `%ProgramFiles%\System Center Operations Manager 2012` for the installation. Click **Next** to continue.



The setup will verify that all system pre-requisites are met in the **Proceed with Setup** dialog. If any pre-requisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





In the **Specify an installation option** dialog, two installation options are provided:

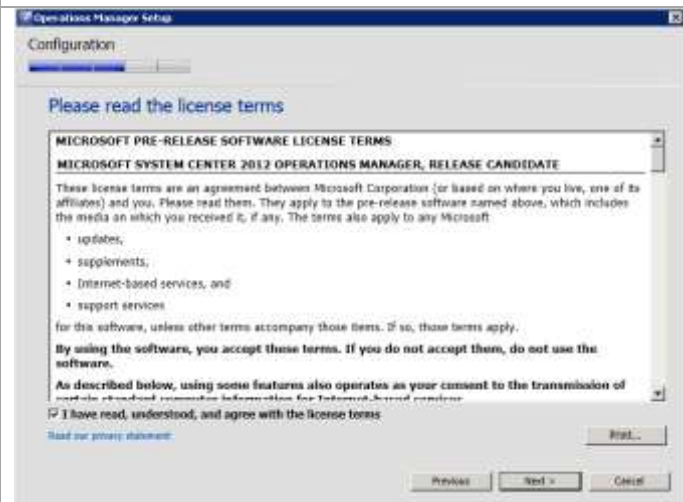
- Create the first management server in a new management group.
- Add a Management server to an existing management group.

Select the **Create the first Management server in a new management group** option and supply a unique name in the **Management group name** text box. Note that this name must be unique across System Center products.

Click **Next** to continue.



In the Please read this license agreement dialog, verify 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 textboxes:

- **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, may be different based on instance).
- **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.¹² The following values can be used as a general guideline:
 - Up to 500 agents: 12 GB.
 - Up to 1000 agents: 24 GB.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the log files for the Operations Manager database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

¹² Supported Configurations for System Center 2012 are located here: <http://technet.microsoft.com/en-us/library/hh205990.aspx#4> which contains the Operations Manager Sizing Helper <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23016>. This helper is being updated for System Center 2012 Operations Manager, but provided general guidance for database sizing.



In the **Configure the data warehouse database** dialog, Specify the following information in the provided textboxes:

- 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, may be different based on instance).
- **Database name** – specify the name of the Operations Manager Data Warehouse database. In most cases the default value of OperationsManagerDWH 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: 356 GB.
 - Up to 1000 agents: 720 GB.
- **Data file folder** – specify the drive letter associated in the SQL Service cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the database log files for the Operations Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

¹³ Supported Configurations for System Center 2012 are located here: <http://technet.microsoft.com/en-us/library/hh205990.aspx#4> which contains the Operations Manager Sizing Helper <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23016>. This helper is being updated for System Center 2012 Operations Manager, but provided general guidance for database sizing.



In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- Management server action account.
- System Center Configuration service and System Center Data Access service.
- Data Reader account.
- Data Writer account.

If the use of a Domain Account is specified, enter the user account information as **<DOMAIN>\<USERNAME>** and enter the appropriate password.

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

The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- Customer Experience Improvement Program.
- Error Reporting.

Select the appropriate option based on your organization's policies and click **Next** to continue.

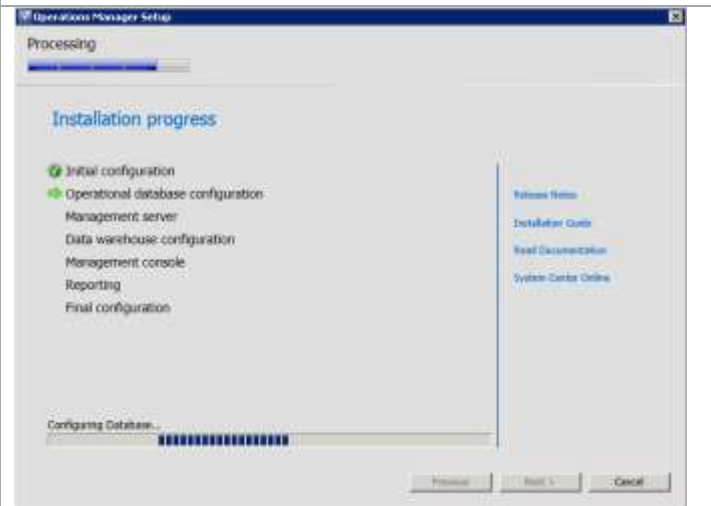
In the **Microsoft Update** dialog, select the option that best matches your organization's policies and click **Next** to continue.



The **Installation Summary** dialog will appear and displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.



The wizard will display the progress while installing features.

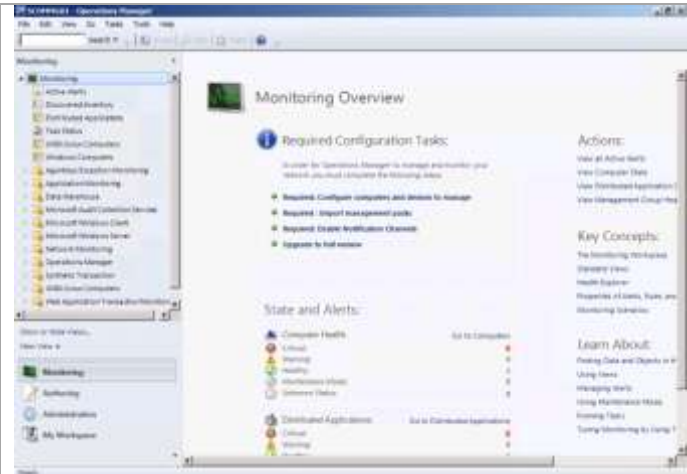


When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.





When completed, the **Operations Manager** console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.

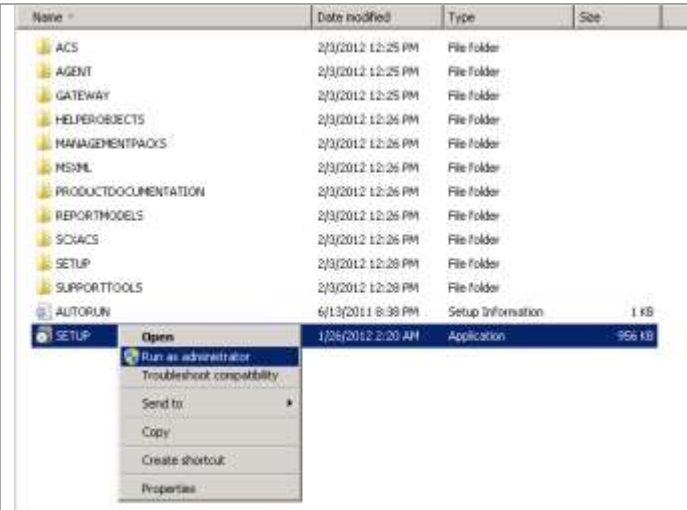


Installing the Reporting Server

The following steps must be completed in order to install and configure the Operations Manager reporting server role.

Perform the following steps on the **Operations Manager reporting server** virtual machine.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

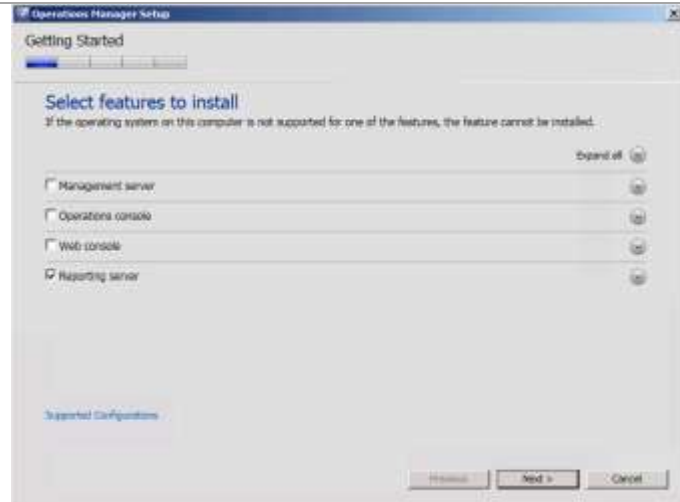




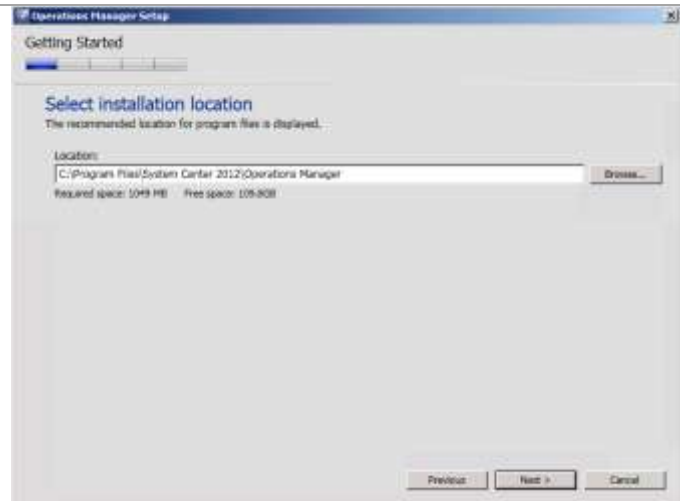
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager management server installation.



In the **Select features to install** dialog, verify that the **Reporting server** check boxes are selected. Click **Next** to continue.

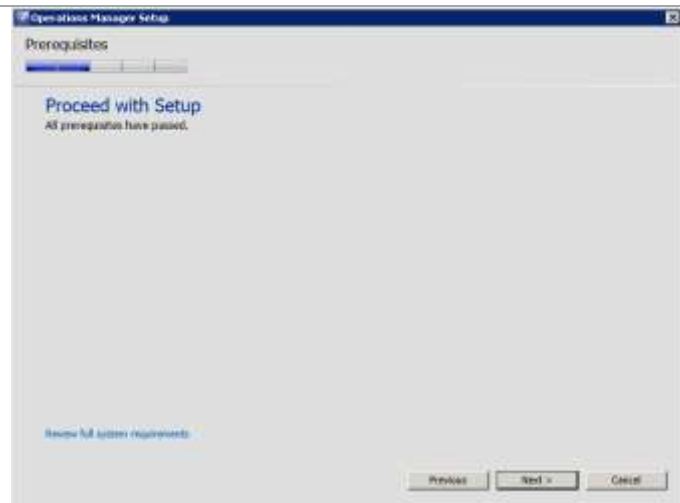


In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.

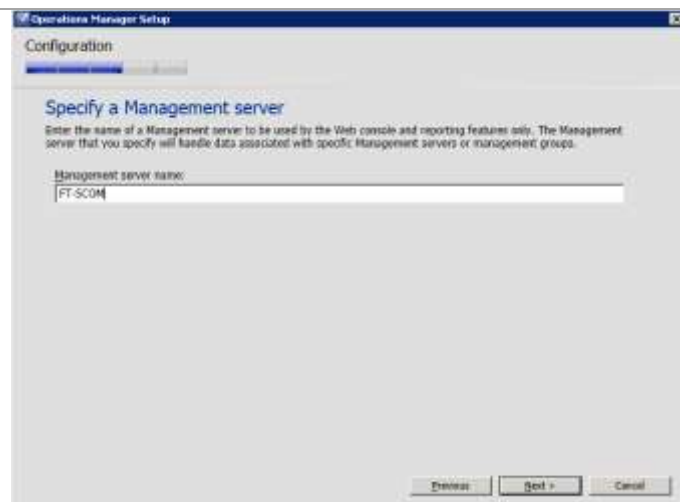




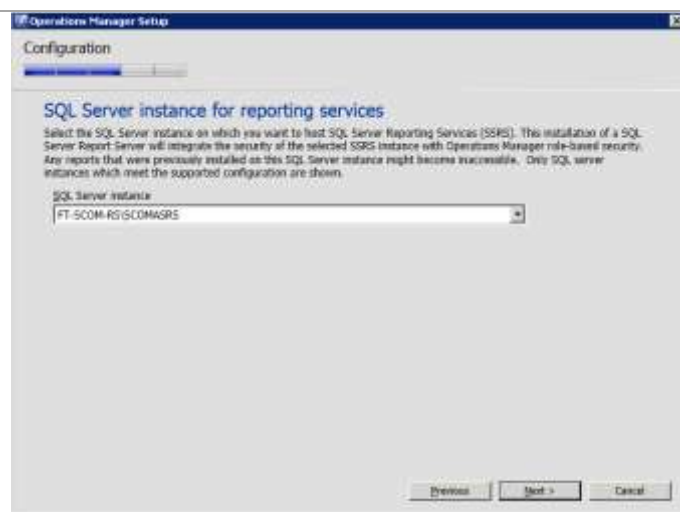
The setup will verify that all system prerequisites are met in the **Proceed with Setup** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



In the **Specify a Management server** dialog, type the name of the previously installed management server in the **Management server name** text box. Click **Next** to continue.



In the **SQL Server instance for reporting services** dialog, select the SQL Server instance hosting the local SQL Server Reporting Services and SQL Server Analysis Services from the drop-down menu created during earlier steps. Click **Next** to continue.





In the **Configure Operations Manager accounts** dialog. For each of the following accounts, specify whether the account is a **Local System** or **Domain Account** using the available options:

- Data Reader account.

If the use of a Domain Account is specified, enter the user account information as **<DOMAIN>\<USERNAME>** and enter the appropriate password.

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

The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. This includes:

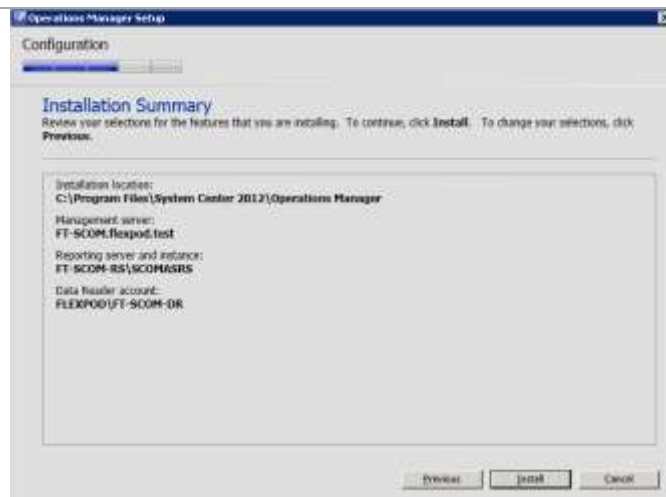
- Operational Data Reporting (ODR).

Select the appropriate option based on your organization's policies and click **Next** to continue.

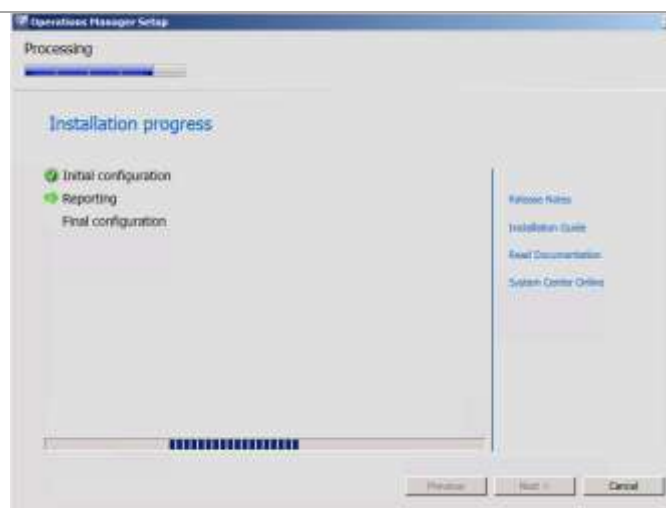
In the **Microsoft Update** dialog, select the option that best matches your organization's policies and click **Next** to continue.



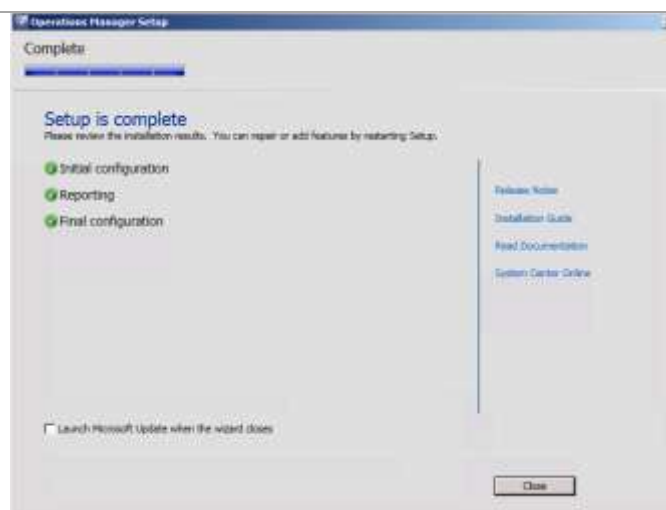
The **Installation Summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



The wizard will display the progress while installing features.

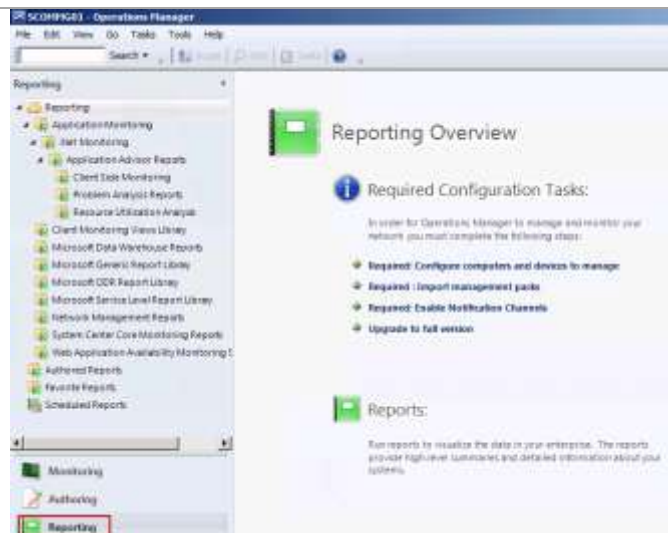


When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch Microsoft Update when the wizard closes** check box is selected and click **Close** to complete the installation.





When completed, open the Operations Manager console from the first management server. From this console, the installation can be validated by noting that the **Reporting** node is now visible in the console.



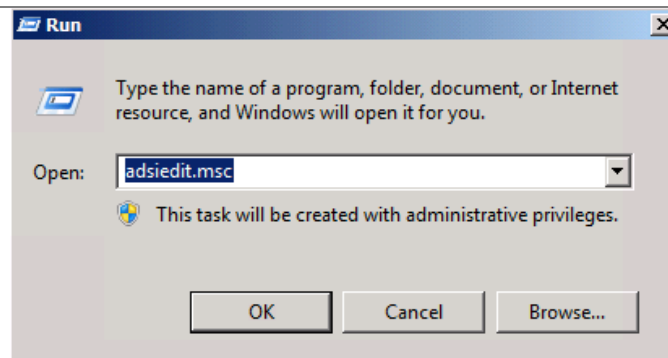
Post Installation Tasks

When the installation is complete, the following tasks must be performed to complete Operations Manager and Virtual Machine Manager integration.

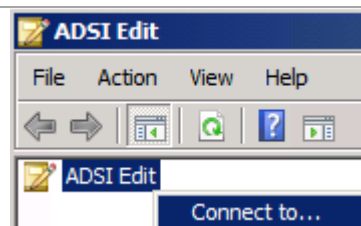
Register the Required Service Principal Names for the Operations Manager Management Servers

Perform the following steps on a **Domain Controller** in the domain where Operations Manager is installed.

Log on to a Domain Controller with a user that has Domain Admin privileges and run **adsiedit.msc**.



Right-click the **ADSI Edit** node and select **Connect to...** from the context menu.





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.

Connection Settings

Name: Default naming context

Path: LDAP://DC1.contoso.com/Default naming context

Connection Point

☐ Select or type a Distinguished Name or Naming Context:

☒ Select a well known Naming Context:

Default naming context

Computer

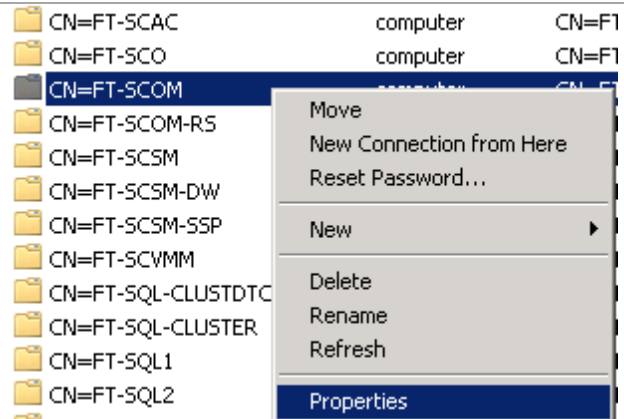
☐ Select or type a domain or server: (Server | Domain [:port])

☒ Default (Domain or server that you logged in to)

☐ Use SSL-based Encryption

Advanced... OK Cancel

Navigate to the container where the Operations Manager management server computer objects reside. Right-click the object and select **Properties** from the context menu.





In the **Properties** dialog, select the Attribute Editor tab, locate the servicePrincipalName attribute and click **Edit**.

CN=FT-SCOM Properties

Attribute Editor | Security

Attributes:

Attribute	Value
rid	<not set>
ridSetReferences	<not set>
roomNumber	<not set>
sAMAccountName	FT-SCOM\$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	MSOMHsvc/FT-SCOM; MSOMHsvc/FT-SCOM
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>

Edit Filter

OK Cancel Apply Help

In the **Multi-valued String Editor** dialog, verify the following SPNs are registered:

MSOMSdkSvc/<servername>
MSOMSdkSvc/<server FQDN>

Click **OK** to save the changes. Repeat these steps for each management server.

Multi-valued String Editor

Attribute: servicePrincipalName

Value to add:

Add

Values:

- HOST/FT-SCOM
- HOST/FT-SCOM.flexpod.test
- MSOMHsvc/FT-SCOM
- MSOMHsvc/FT-SCOM.flexpod.test
- MSOMSdkSvc/FT-SCOM**
- MSOMSdkSvc/FT-SCOM.flexpod.test**
- RestrictedKrbHost/FT-SCOM
- RestrictedKrbHost/FT-SCOM.flexpod.test
- TERMSRV/FT-SCOM
- TERMSRV/FT-SCOM.flexpod.test
- WSMAN/FT-SCOM
- WSMAN/FT-SCOM.flexpod.test

Remove

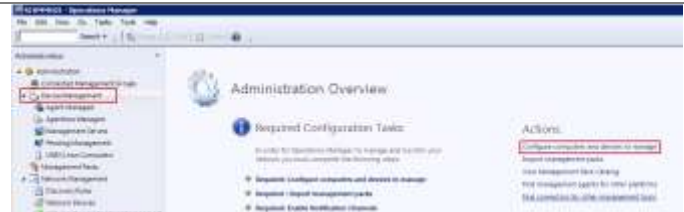
OK Cancel



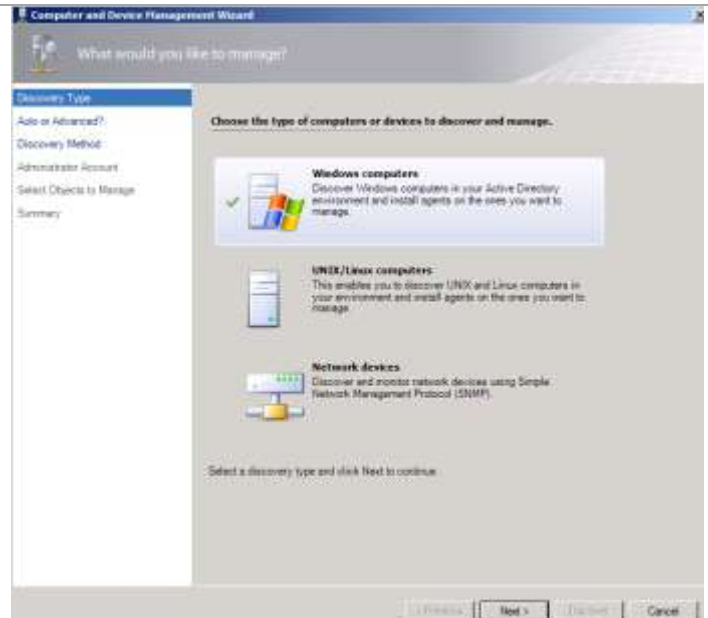
Deploying and Configuring the Operations Manager Agent on the Virtual Machine Manager Management Server

Perform the following steps on the **Operations Manager** 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.

Computer and Device Management Wizard

Auto or Advanced?

Discovery Type

Auto or Advanced?

Administrator Account

Select Objects to Manage

Summary

Choose automatic or advanced discovery.

☒ **Automatic computer discovery**
Scan the "RD" domain for all Windows-based computers.

☐ **Advanced discovery**
Allow you to specify advanced discovery options and settings:

Computer and Device Classes

Discovery and Clients

Notes: This setting applies only when scanning Active Directory. You can configure how these clients will be discovered, on the next screen(s).

Management Server

Management Server

☐ Verify all discovered computers are in the context.

< Previous Next > 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 **Next** to continue.

Computer and Device Management Wizard

Administrator Account

Discovery Type

Auto or Advanced?

Administrator Account

Select Objects to Manage

Summary

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.

☐ Use selected Management Server Admin Account.

☒ **Other user account**

User name

administrator

Password

Domain

PLDPOD

☐ **This is a local computer account, not a domain account**

Notes: 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 Admin Account.

< Previous Next > Done Cancel

[illegible]

The screenshot shows the 'Summary' page of the 'Computer and Device Management Wizard'. On the left is a navigation pane with the following items: 'Discovery Type', 'Autos or Advanced?', 'Administrative Account', 'Select Objects to Manage', and 'Summary' (which is highlighted in blue). The main area is titled 'Summary' and contains the following information:

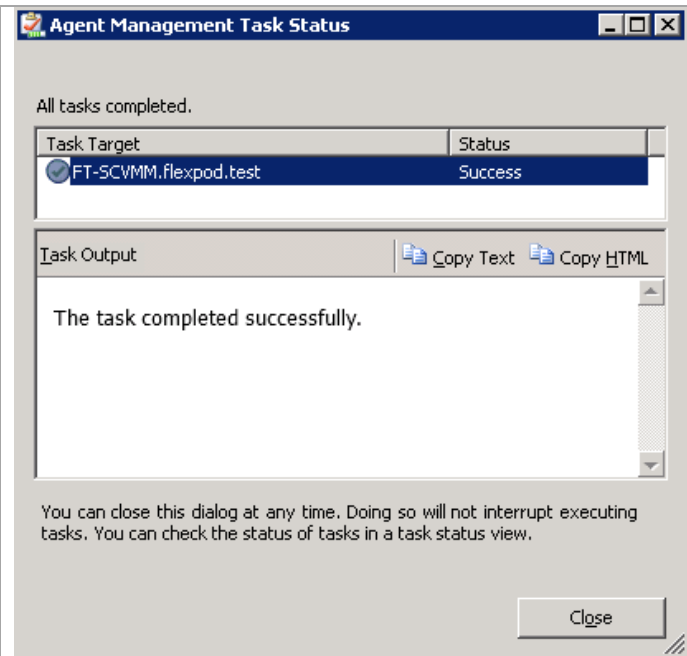
- Agents to be installed:** 1
- Agent installation directory:** `\\ProgramFiles\Symantec\Operations Manager`
- Agent Action Account:**
 - ☒ **Local System**
 - ☐ **Other**
 - User name: [text box]
 - Password: [text box]
 - Domain: [text box]
 - [button]

At the bottom, it says: 'To close the wizard and deploy the agents, click Finish.'

At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.



In the **Agent Management Task Status** dialog, verify that the agent installation completes successfully. When successful, click **Close** to complete the operation.

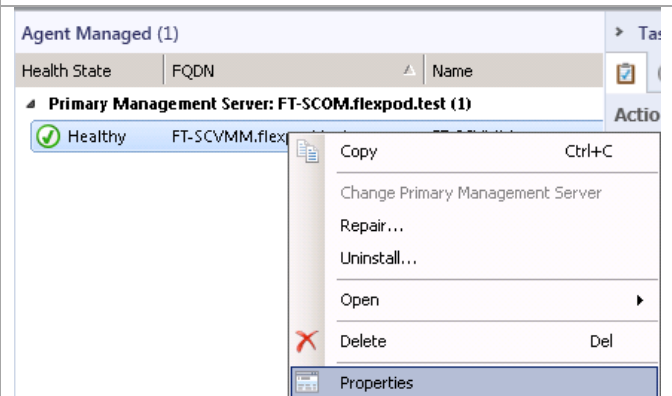


The next step is to enable the Operations Manager agent deployed to the Virtual Machine Manager management server to be a proxy agent.

In **Operations Manager** console, navigate to the **Administration** workspace, expand the **Device Management** node and select the **Agent Managed** view.



In the **Agent Managed** pane, select the agent associated with the VMM Management Server and click **Properties** in the task pane.



In the Agent Properties dialog, select the Security tab. Verify that the Allow this agent to act as a proxy and discover managed objects on other computers check box is selected then click OK to save the changes.



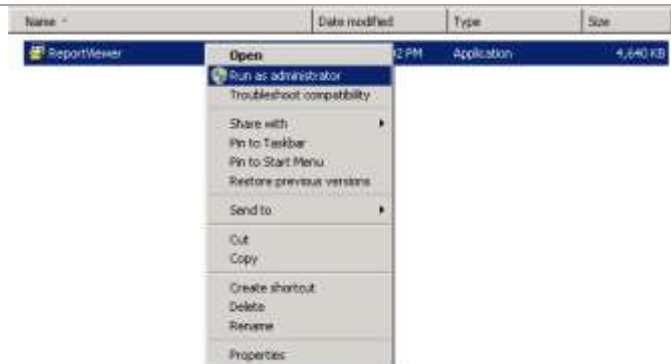


Installing Microsoft Report Viewer 2010 SP1 on the Virtual Machine Manager Management Server

Additionally, the Operations Manager installation also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.¹⁴ Follow the provided steps to install the Microsoft Report Viewer 2010 SP1 package.

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

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



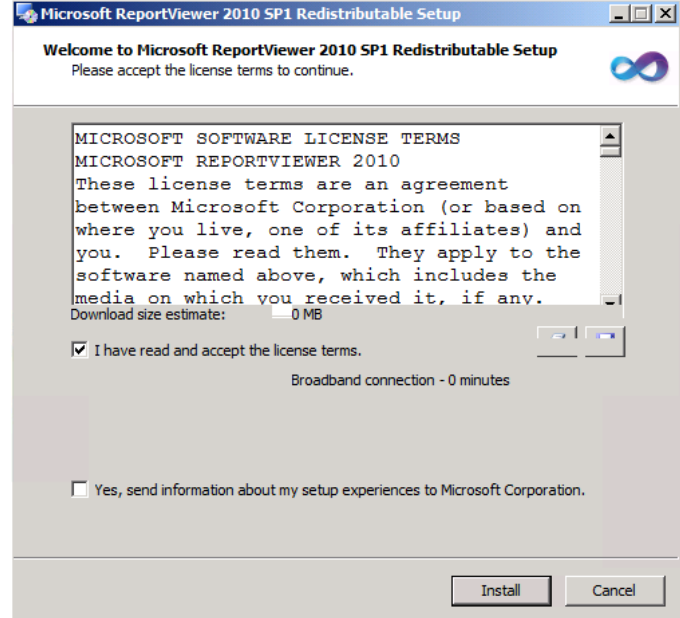
Within the Microsoft ReportViewer 2010 SP1 Redistributable Setup dialog, select **Next** to begin the installation.



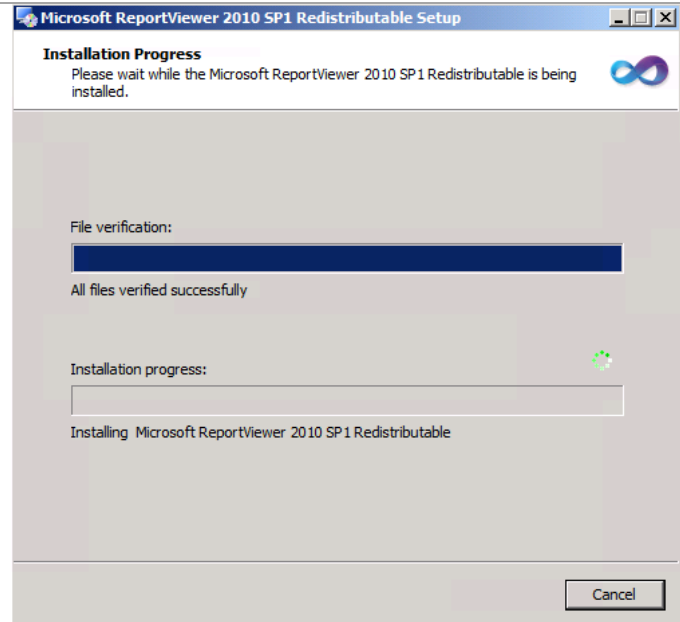
¹⁴ Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en>.



Select the I have read and accept the license terms check box and click Install.

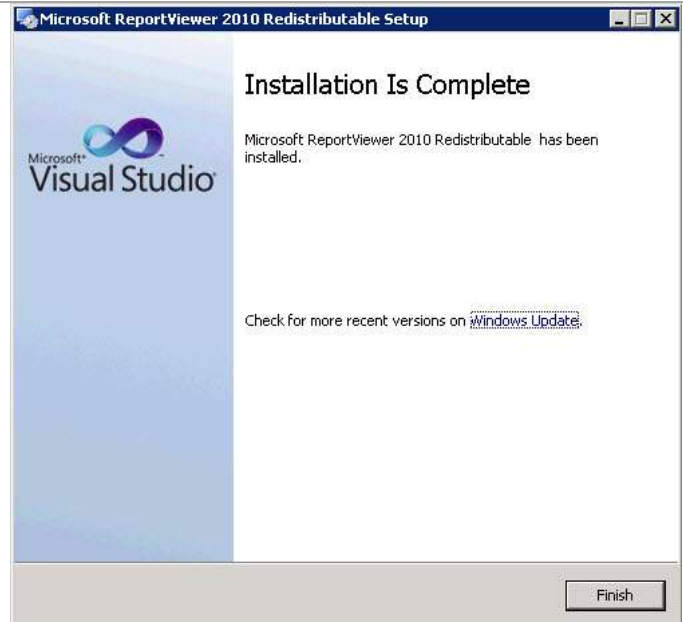


The installation progress will be displayed in the setup wizard.





When completed, click **Finish** to exit the installation.

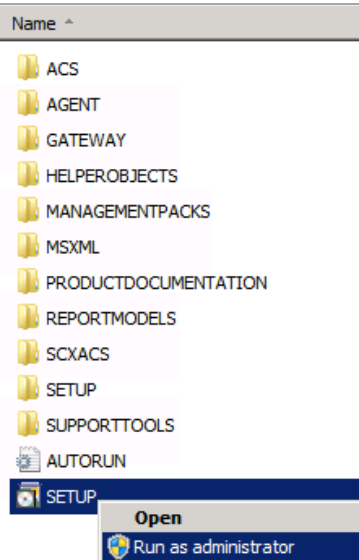




Installing the Operations Manager Console on the Virtual Machine Manager Management Server

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

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

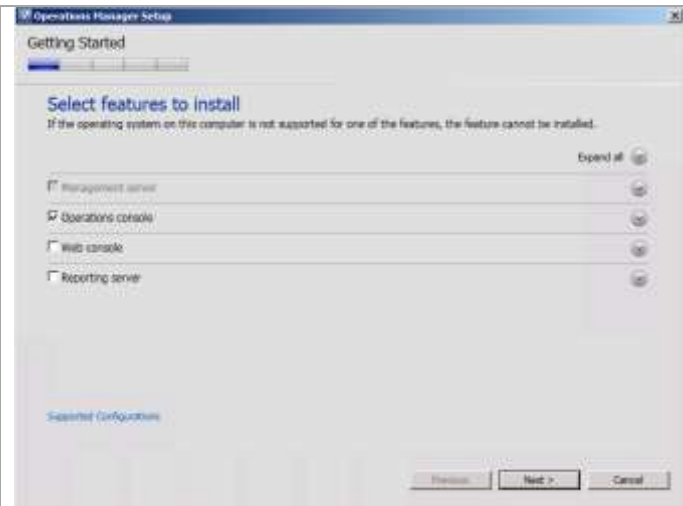


The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.





In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. 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.

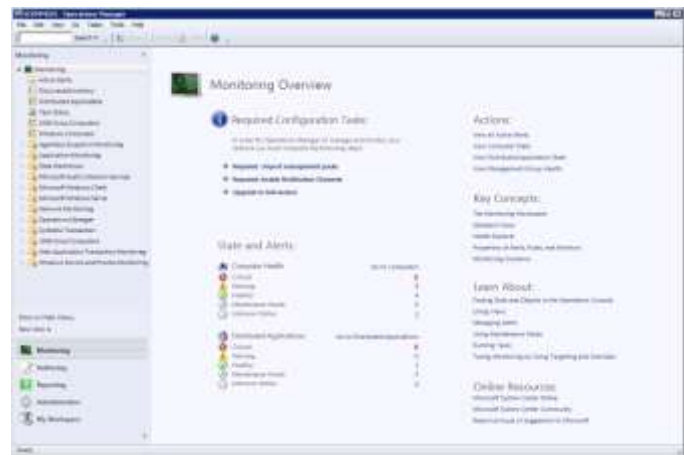
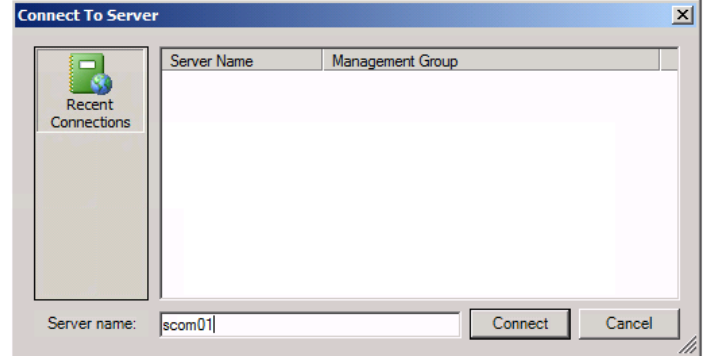


When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **start the Management console when the wizard closes** check box is selected and click **Close** to complete the installation.





When completed, the Operations Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



Downloading and Importing the Required Prerequisite Management Packs in Operations Manager

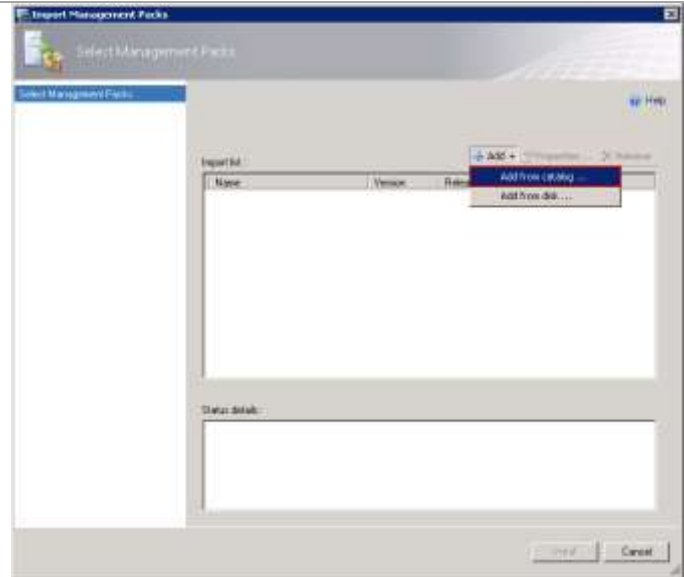
Perform the following steps on the **Operations Manager** virtual machine.

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.

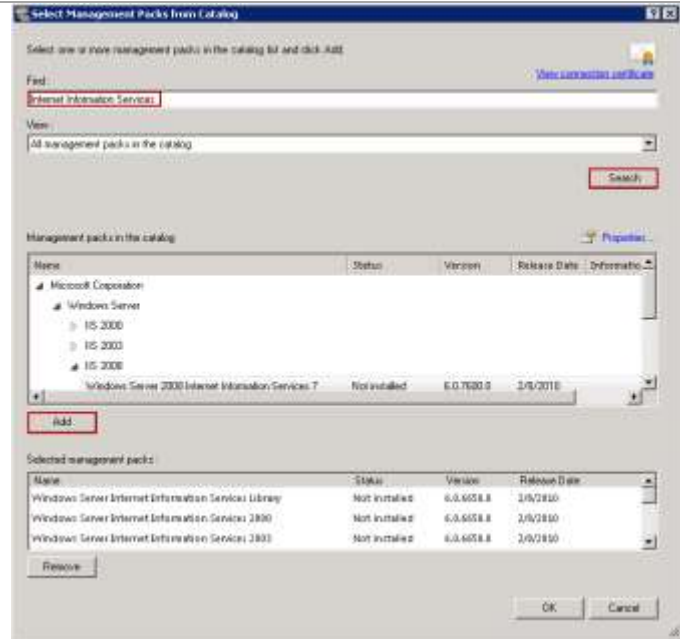




In the **Select Management Packs from Catalog** dialog, find and add the following management packs:

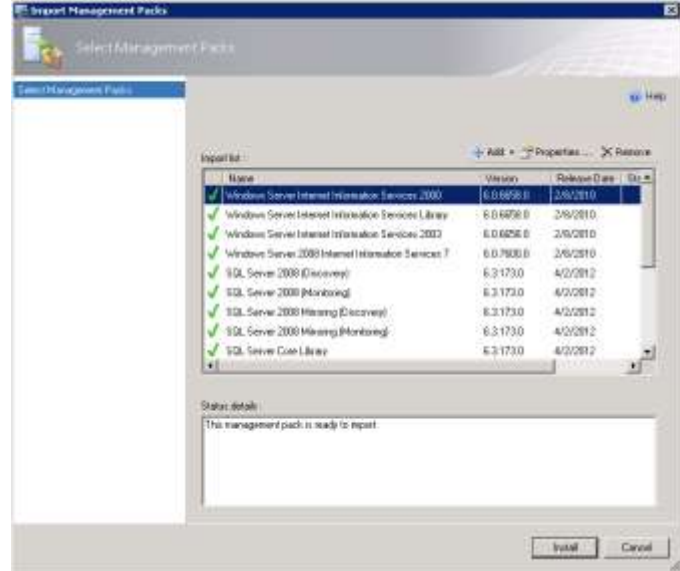
- Windows Server Internet Information Services Library.
- Windows Server Internet Information Services 2000.
- Windows Server Internet Information Services 2003.
- Windows Server 2008 Internet Information Services 7.
- SQL Server 2008 (Discovery).
- SQL Server 2008 (Monitoring).
- SQL Server 2008 Mirroring (Discovery).
- SQL Server 2008 Mirroring (Monitoring).
- SQL Server Core Library.
- Windows Server 2008 R2 Best Practice Analyzer Monitoring.
- Microsoft Windows Server® 2000 Operating System.
- Windows Server® 2003 Operating System.
- Windows Server 2008 Operating System (Discovery).
- Windows Server 2008 Operating System (Monitoring).
- Windows Server Operating System Library.
- Windows Server Operating System Reports.
- Windows Server Cluster Shared Volume Monitoring.

When added, click **OK** to continue.

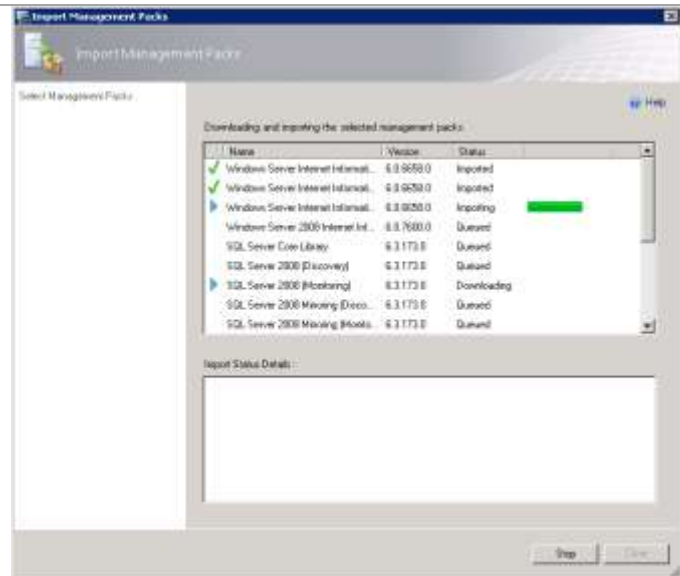




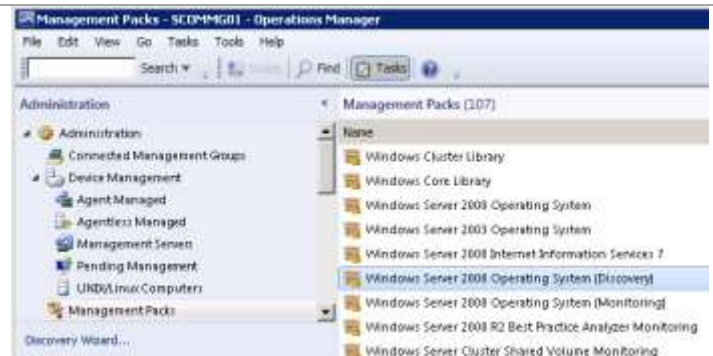
At the **Select Management Packs** dialog, click **Install** to import the selected management packs.



The management packs will download and import into Operations Manager. When complete, verify that the imports were successful and click **Close** to exit the Import Management Packs wizard.



In the **Operations Manager** console, go to the **Administration** workspace and verify the previously selected management packs are now installed.





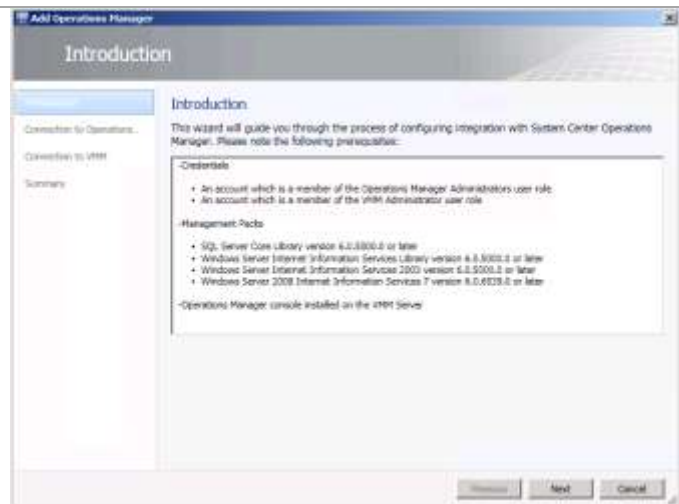
Perform Virtual Machine Manager and Operations Manager Integration

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 from the context menu.

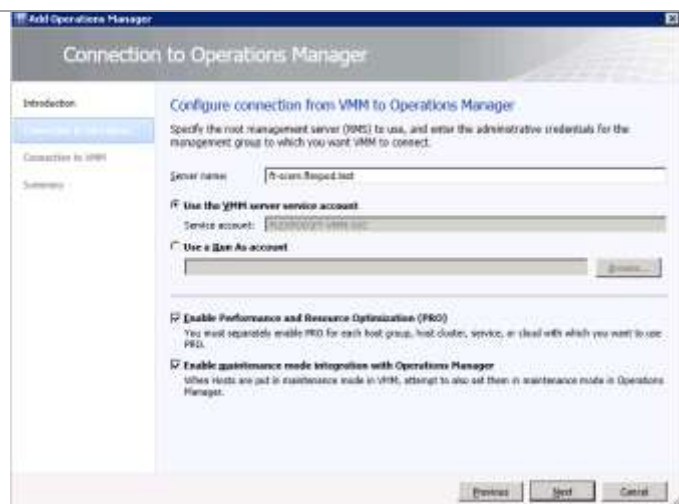


The **Add Operations Manager** dialog will appear. In the **Introduction** dialog, verify the prerequisites have been met and click **Next** to continue.



In the **Connection to Operations Manager** dialog, type the FQDN of the Operations Manager server in the Server name text box. Select the **Use the VMM server service account** option. Select the **Enable Performance and Resource Optimization (PRO)** and **Enable maintenance mode integration with Operations Manager** check boxes.

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





In the **Connection to VMM** dialog, specify the VMM service account credentials in the **User name** and **Password** text boxes and click **Next** to continue.

The screenshot shows the 'Add Operations Manager' dialog box with the 'Connection to VMM' tab selected. The 'Introduction' pane on the left lists 'Introduction', 'Connection to Operations...', 'Connection to VMM', and 'Summary'. The main area is titled 'Configure connection from Operations Manager to VMM' and contains the instruction: '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 'PLEXP001-VM-SVC' 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 Operations...', 'Connection to VMM', and 'Summary'. The main area is titled 'Confirm the settings' and contains a table of configuration details. At the bottom right are 'Previous', 'Next', and 'Cancel' buttons.

Confirm the settings	
RPO name:	Return Period Test
Operations Manager credentials:	PLEXP001-VM-SVC
VMM credentials:	PLEXP001-VM-SVC
Enable RPO:	Yes
Maintenance mode integration:	Yes



The **Jobs** pane will appear. Before moving forward, wait for the job to complete successfully.

Note: If any management pack is missing on the Operations Manager server the following error will be logged.

Error (10218)

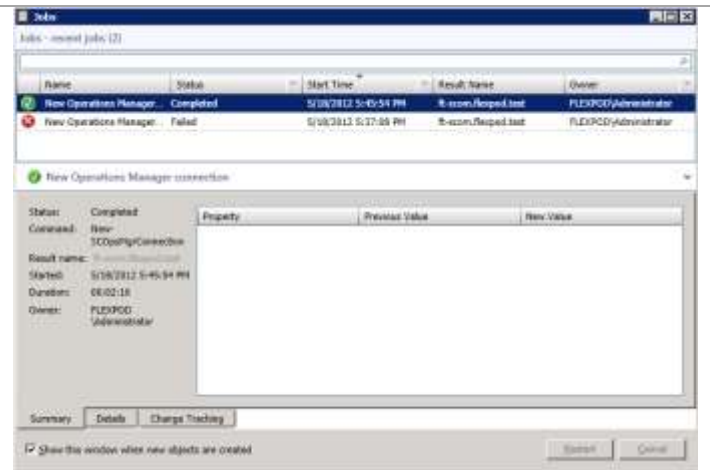
Setup could not import the System Center Virtual Machine Manager Management Pack into Operations Manager server because one or more required management packs are missing. The VMM Management Packs cannot be deployed unless the following component management packs are present in Operations Manager 2007:

- Windows Server Internet Information Services 2003
- Windows Server 2008 Internet Information Services 7
- Windows Server Internet Information Services Library,
- SQL Server Core Library

Recommended Action

To provide the missing component management packs, ensure that the following management packs have been imported into Operations Manager server:

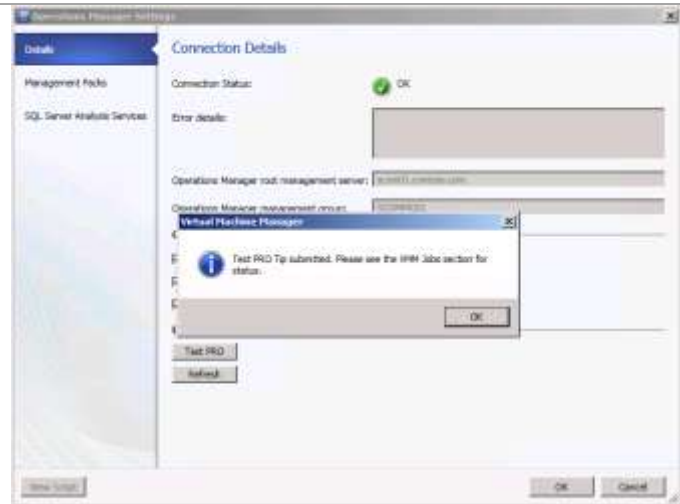
- Microsoft Windows Server 2000/2003 Internet Information Services Management Pack for OpsMgr 2007 (version 6.0.6278.0 or later)
- Microsoft SQL Server 2000/2005 Management Pack
- You can download the management packs from the System Center Operations Manager 2007 Catalog at <http://go.microsoft.com/fwlink/?LinkId=86411>



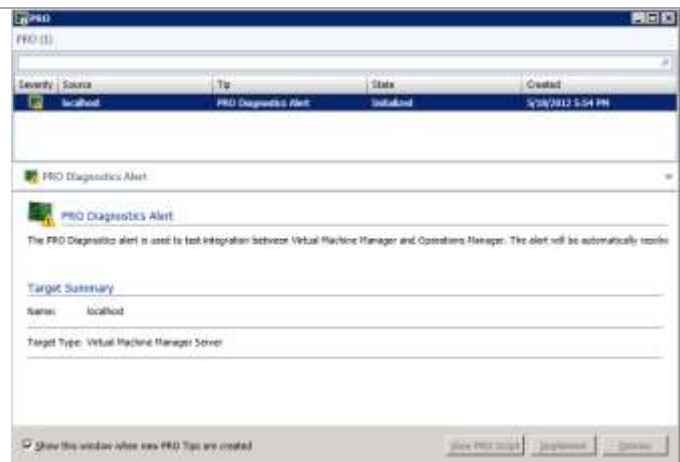


In the Virtual Machine Manager console, navigate back to **Settings** then select **System Center Settings** and double-click **Operations Manager Server**. The Operations Manager Settings dialog will appear.

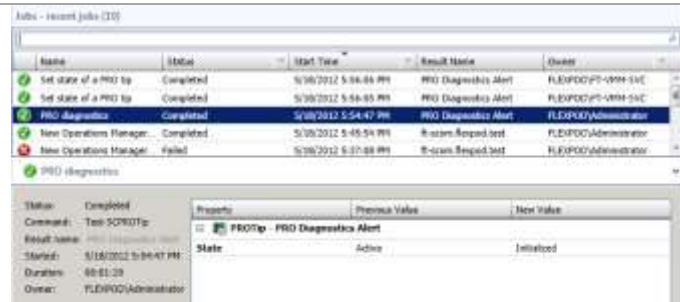
In the **Details** pane, click **Test PRO**.



As part of the test, PRO will generate a diagnostics alert.

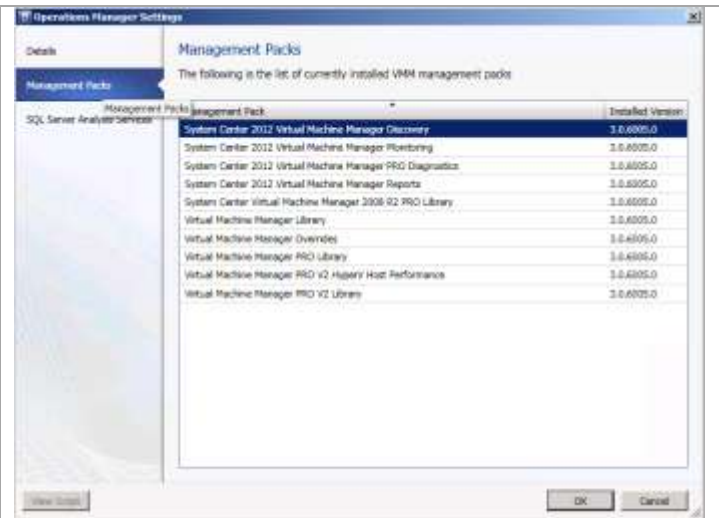


After a few minutes, verify that the PRO test is successful. Navigate to the Jobs pane and verify the PRO jobs completed successfully.





In the **Management Packs** dialog, verify all Virtual Machine Manager Management Packs were successfully installed.

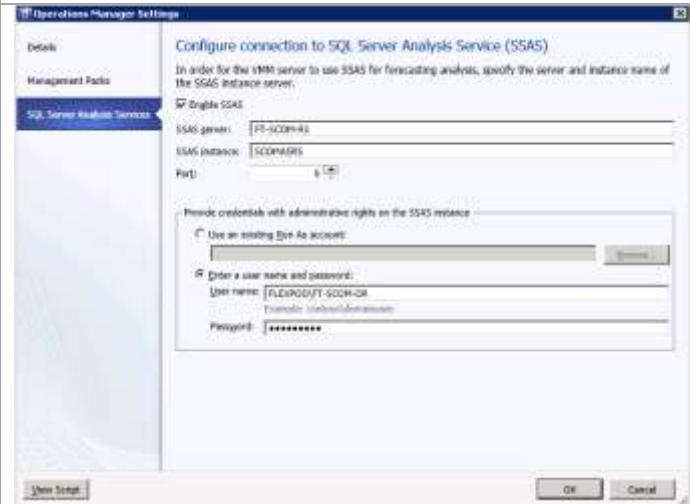


In the **Configure connection to SQL Server Analysis Services (SSAS)** dialog, provide the following information.

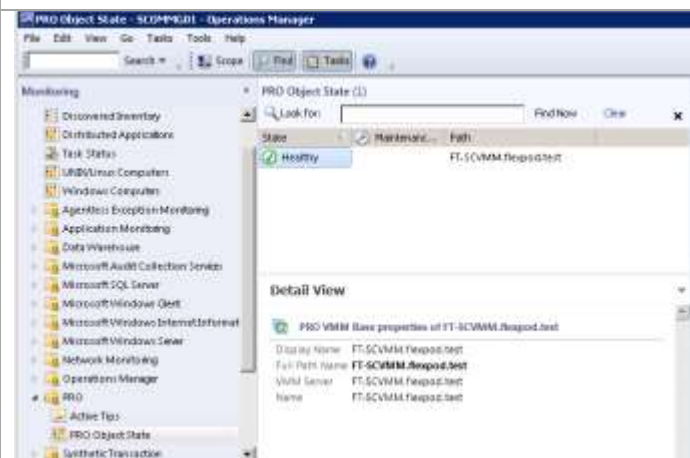
Select the **Enable SSAS** check box. Provide the following information on the text boxes provided:

- **SSAS server**—Specify the Operations Manager database server instance.
- **SSAS Instance**—Specify the SSAS instance name created earlier.

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.

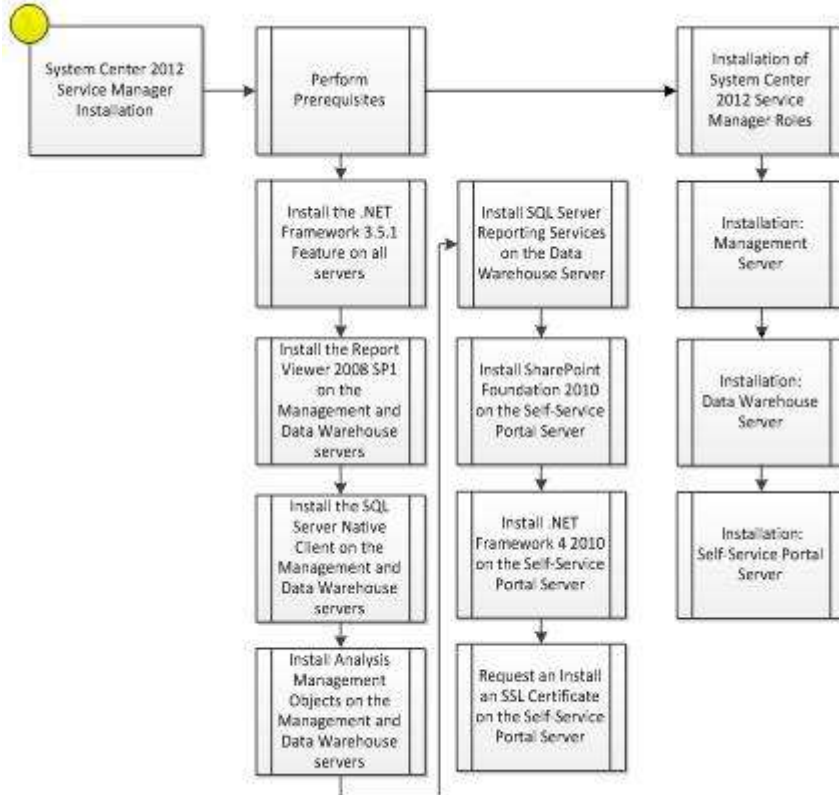


On the **Operations Manager** console, go to **Monitoring** workspace, navigate to the **PRO** node and select **PRO Object State**. Verify the VMM server is listed with a health state other than **“Not Monitored.”**



Service Manager

The Service Manager installation process includes the following high-level steps:



Overview

This section provides a high-level walkthrough on how to setup and complete the task sequence and scripts for deploying Service Manager into the Fast Track fabric management architecture. The following assumptions are made:

Management Server

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role.
- A two-node, SQL Server 2008 R2 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 3.5.1 Feature is installed.
- The Microsoft Report Viewer 2008 Redistributable (KB971119) is installed - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3203>.
- The Microsoft SQL Server 2008 R2 Native Client is installed- <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.



- The Microsoft SQL Server R2 Analysis Management Objects is installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.

Data Warehouse Server

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role.
- A two-node, SQL Server 2008 R2 cluster with dedicated instance that has been established in previous steps for Service Manager.
- SCSMAS – instance for SQL Server 2008 R2 Analysis Services and SQL Server Reporting Services databases.
- SCSMDW – instance for Service Manager Data Warehouse databases.
- The .NET Framework 3.5.1 Feature is installed.
- The Microsoft Report Viewer 2008 Redistributable (KB971119) is installed - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3203>.
- The Microsoft SQL Server 2008 R2 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.
- The Microsoft SQL Server R2 Analysis Management Objects are installed- <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.
- The Microsoft SQL Server R2 Reporting Services (split configuration) is installed.
- The Microsoft SQL Server R2 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 two-node, SQL Server 2008 R2 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 3.5.1 Feature is installed.
- The Microsoft Report Viewer 2008 Redistributable (KB971119) is installed - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3203>.
- The Microsoft SQL Server 2008 R2 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.
- The Microsoft SQL Server R2 Analysis Management Objects is installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.
- SharePoint Foundation 2010 is installed.
- The .NET Framework 4 Redistributable is installed.

Additional Management Server for this Design Pattern Deployment

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role.



- A two-node, SQL Server 2008 R2 cluster with dedicated Service Manager instances that has been established in previous steps for Service Manager.
- SCSMDB – instance for Service Manager management database.
- The .NET Framework 3.5.1 Feature is installed.
- The Microsoft Report Viewer 2008 Redistributable (KB971119) is installed - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3203>.
- The Microsoft SQL Server 2008 R2 Native Client is installed - <http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409>.
- The Microsoft SQL Server R2 Analysis Management Objects is installed - <http://go.microsoft.com/fwlink/?LinkID=188448&clcid=0x409>.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User name	Purpose	Permissions
<DOMAIN>\ FT-SCSM-SVC	SCSM services account	Add the account to the local Administrators group on the all SCSM servers. Must be a local admin on all SQL Server nodes.
<DOMAIN>\ FT-SCSM-WF	SCSM workflow account	Must have permissions to send e-mail and must have a mailbox on the SMTP server (required for the E-mail Incident feature). Must be member of Users local security group on all SCSM servers. Must be made a member of the Service Manager Administrators user role in order for e-mail 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	Must be a member of the Users local security group on all



User name	Purpose	Permissions
	account	SCSM servers. Must be an Operations Manager Operator.
<DOMAIN>\ FT-SCSM-ADCI	SCSM Active Directory CI connector account	Must be a member of the Users local security group on the Service Manager management server. Must have permissions to bind to the domain controller that the connector will read data from. Needs generic read rights on the objects that are being synchronized into the Service Manager database from Active Directory.
<DOMAIN>\ FT-SCSM-OMAlert	SCSM Operations Manager alert connector account	Must be a member of the Users local security group on the Service Manager management server. Must be a member of FT-SCSM-Admins
DOMAIN>\ FT-SCSM-VMMCI	Virtual Machine Manager CI connector account	Member of the VMM Admin domain group. The account must also be in the Service Manager Advanced Operator role
DOMAIN>\ FT-SCSM-OCI	Orchestrator CI connector	Member of SCO Operators (Users) domain group. The account must also be in the Service Manager Advanced Operator role
<DOMAIN>\ FT-SCSM-OLAP	Service Manager Analysis Services account	Must be a local admin on all SQL Server nodes.

Groups

Verify that the following security groups have been created:

Security group name	Group scope	Members	Member of
<DOMAIN>\ FT-SCSM-ADMINS	Global	DOMAIN\ FT-SCSM-SVC	Must be added to the Service Manager Administrators user role and added to the Operations



Security group name	Group scope	Members	Member of
			Manager Administrators role in Operations Manager and a member of the Administrators group on each SQL Server.

Adding the .NET Framework 3.5.1 Feature on all Server Manager Servers

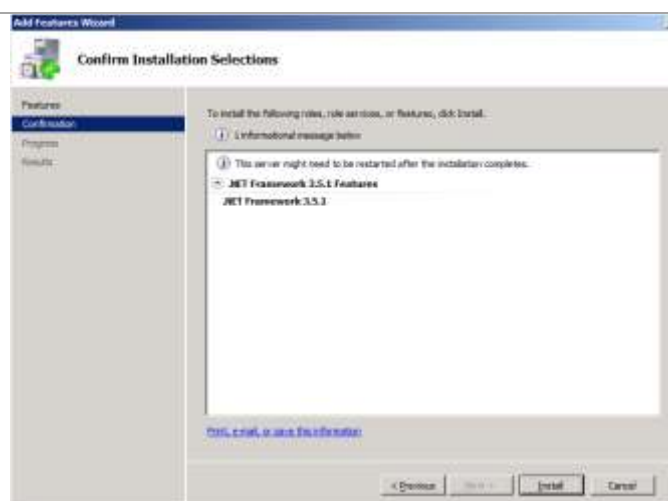
The Service Manager installation requires the .NET Framework 3.5.1 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5.1 Feature.

Perform the following steps on all **Service Manager** virtual machines.

To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features**, and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.

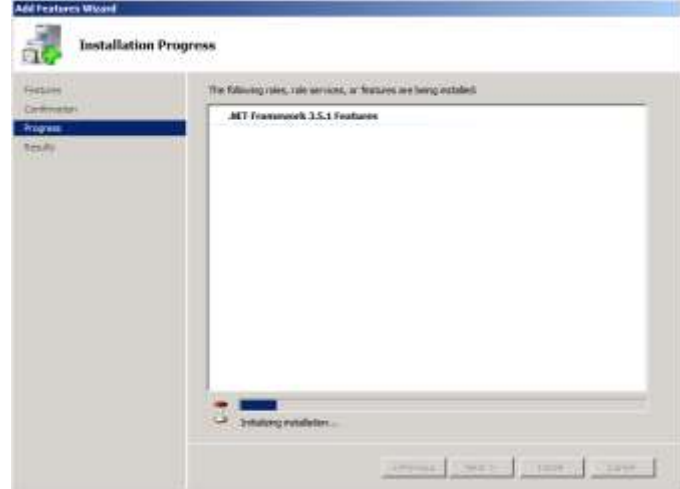


In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.

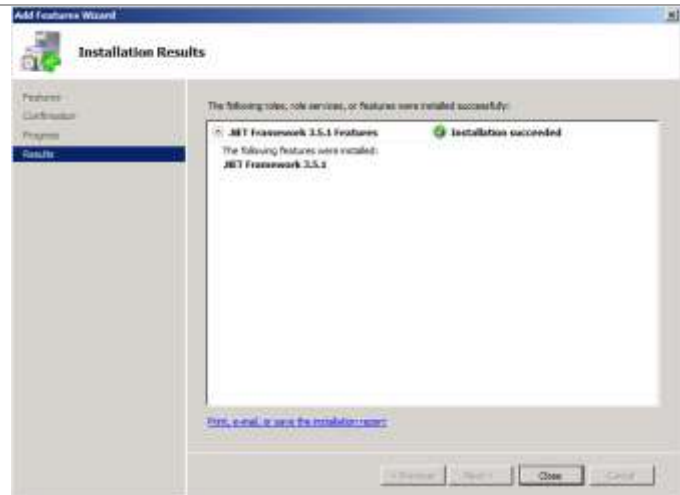




The **Installation Progress** dialog will show the progress of the feature install.



When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.



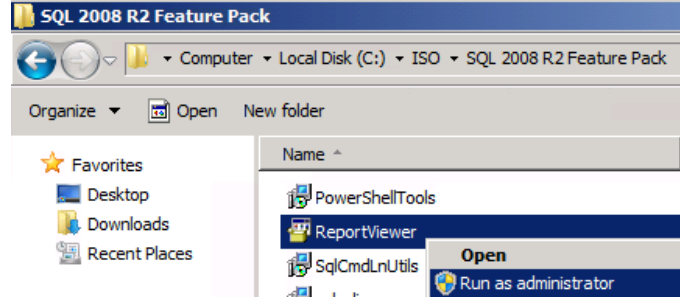
Installing Microsoft Report Viewer 2008 Redistributable on the Management and Data Warehouse Servers

The Server Manager management and Data Warehouse server installations also require the Microsoft Report Viewer 2008 Redistributable be installed prior to installation. The following steps are provided to help install the Microsoft Report Viewer 2008 Redistributable.

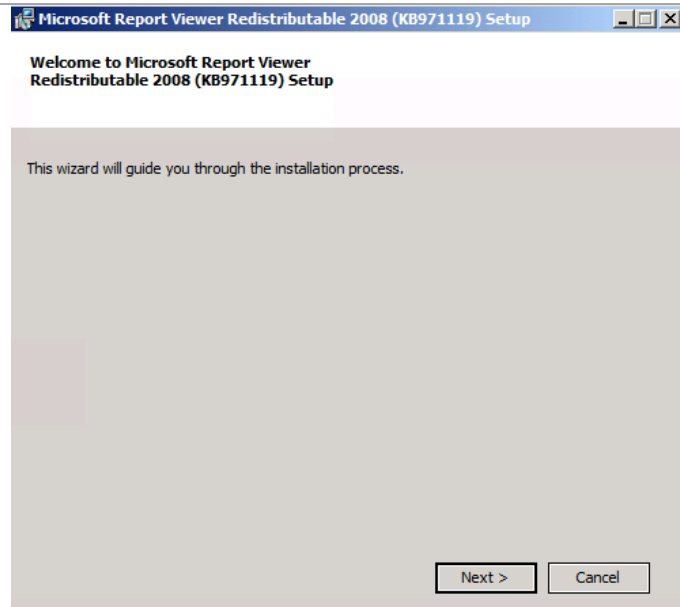
Perform the following steps on the Server Manager Management and Data Warehouse Servers virtual machines.



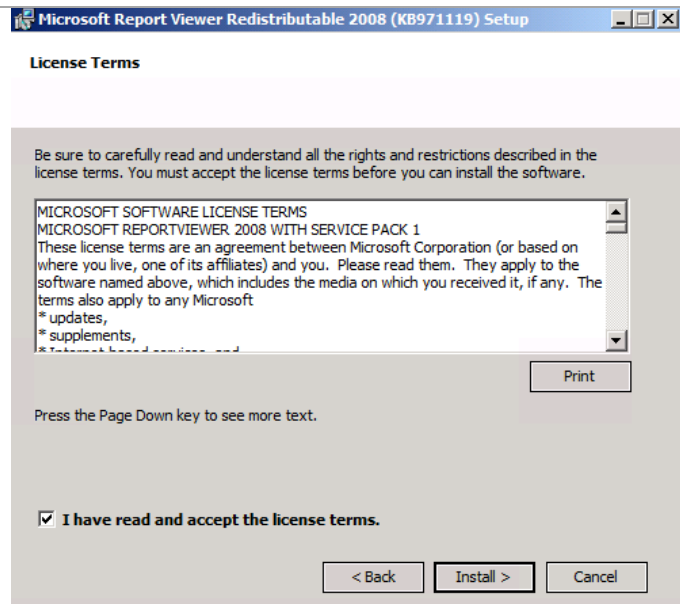
From the installation media source right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



The setup wizard will appear. Click **Next** to continue.

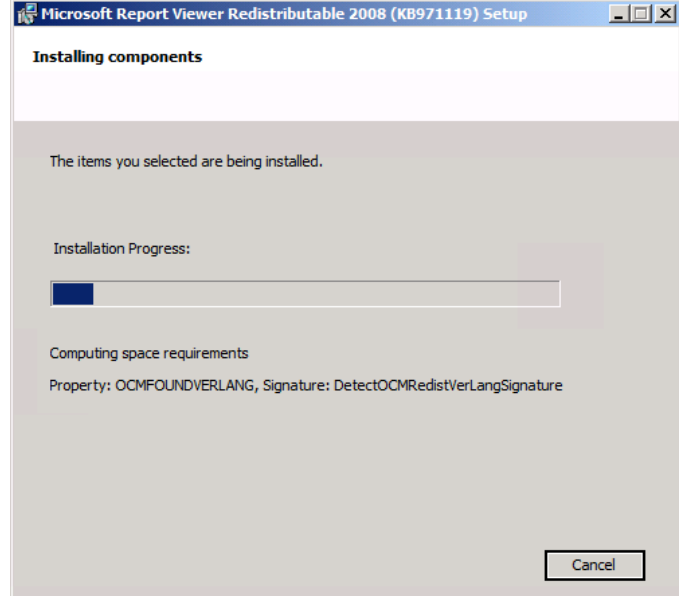


Within the **License Terms** dialog, select the **I have read and accept the license terms** check box. Click **Install** to begin the installation.

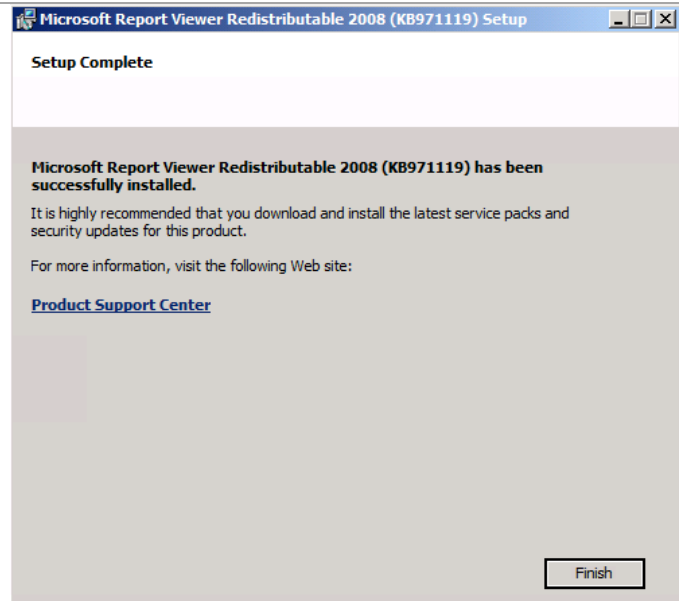




The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.



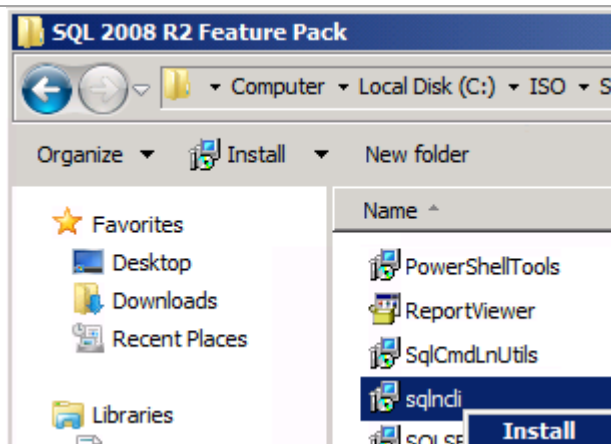


Installing SQL Server 2008 R2 Native Client on the on the Management and Data Warehouse Servers

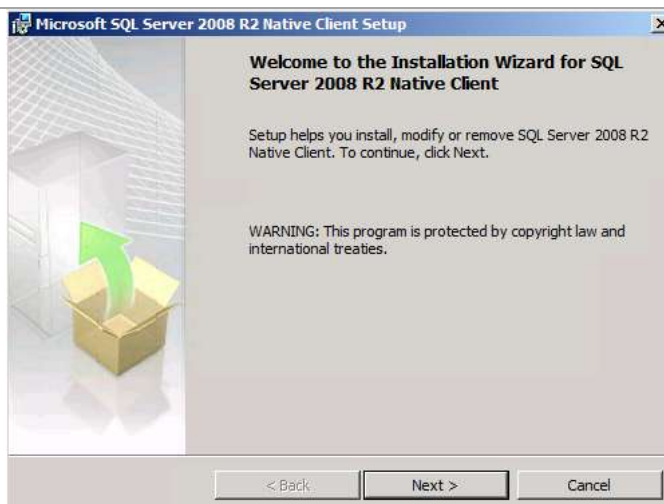
The Server Manager Management and Data Warehouse Server installations also require the SQL Server 2008 R2 Native Client be installed prior to installation. The following steps are provided:

Perform the following steps on the Server Manager Management and Data Warehouse Servers virtual machines.

From the installation media source right-click **SQLNCLI.MSI** and select **Install** from the context menu to begin setup.

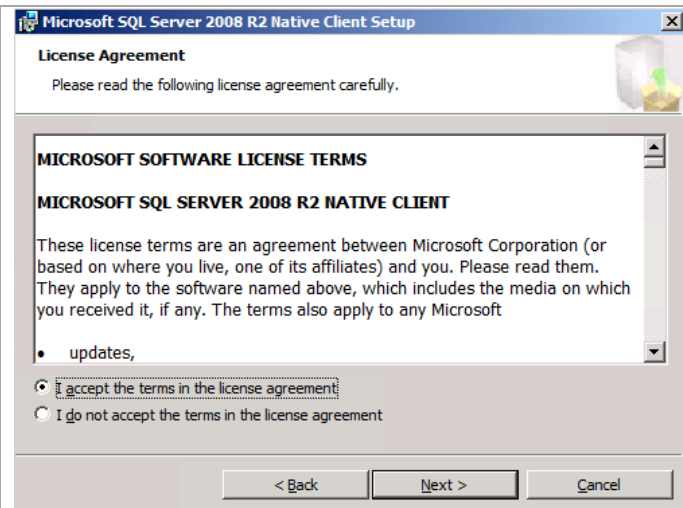


The Setup wizard will appear. Click **Next** to continue.

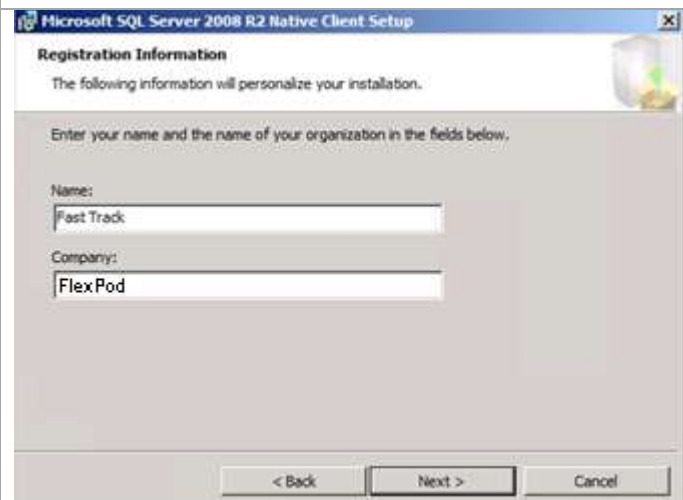




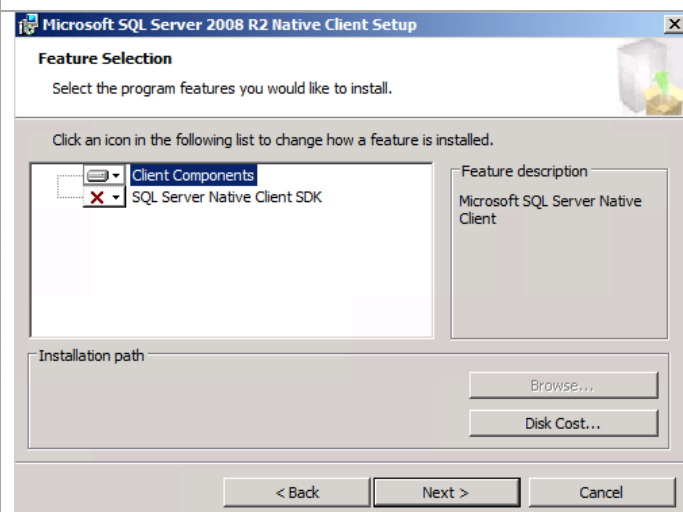
Within the **License Terms** dialog, select the **I accept the terms in the license agreement** check box. Click **Next** to continue.



In the **Registration Information** dialog, enter values for your organization in the **Name** and **Company** textboxes. Click **Next** to continue.

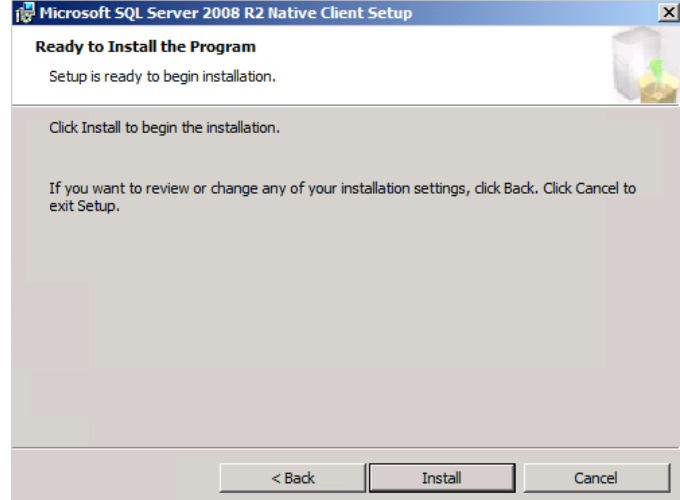


In the **Feature Selection** dialog, verify that the **Client Components** feature is selected for installation. Click **Next** to continue.

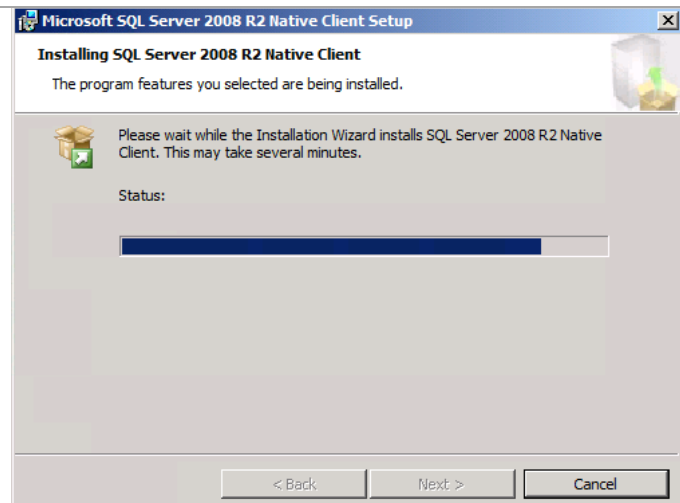




In the **Ready to Install the Program** dialog, click **Install** to begin the installation.



The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.





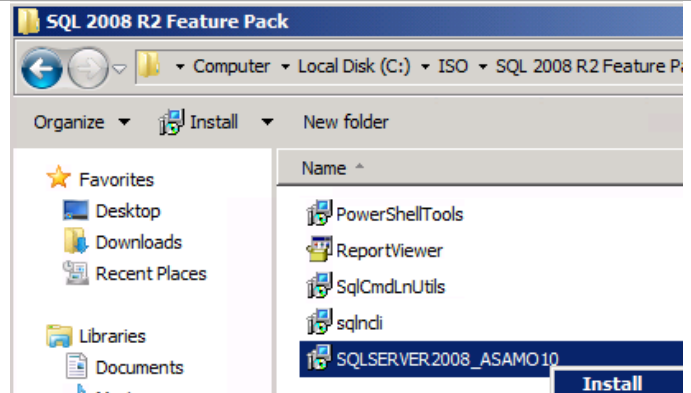
Installing SQL Server 2008 R2 Analysis Management Objects on the Management and Data Warehouse Servers

Server Manager management and Data Warehouse server installations also require the SQL Server 2008 R2 Analysis Management Object be installed prior to installation. Follow the provided steps to install the SQL Server 2008 R2 Analysis Management Object.

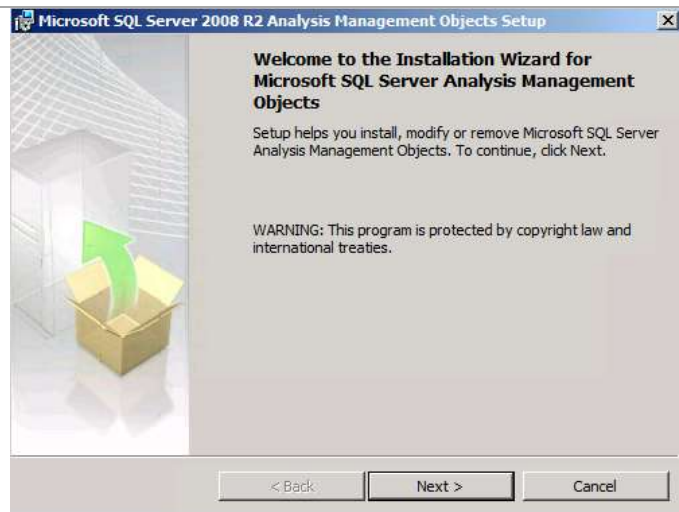
Perform the following steps on the Server Manager management and Data Warehouse Servers virtual machines.

From the installation media source, right-click **SQLSERVER2008_ASAMO10.MSI** and select **Run as administrator** from the context menu to begin setup.

Note: the Analysis Management Objects installer, **1033x64\SQLSERVER2008_ASAMO10.msi**, can be downloaded from <http://www.microsoft.com/download/en/details.aspx?id=26728>.

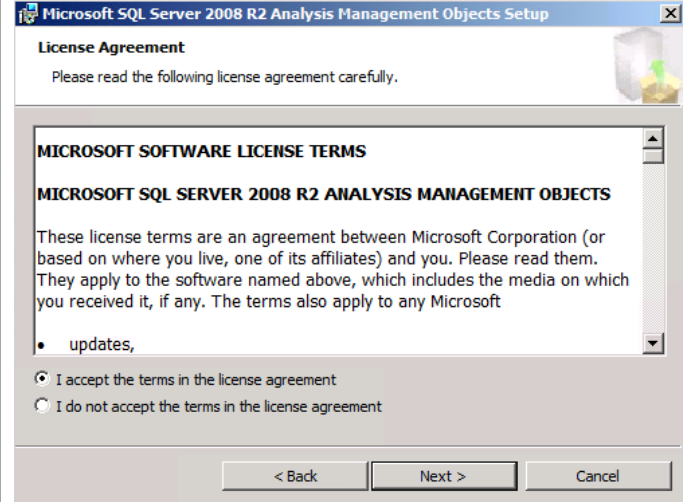


The Setup wizard will appear. Click **Next** to continue.

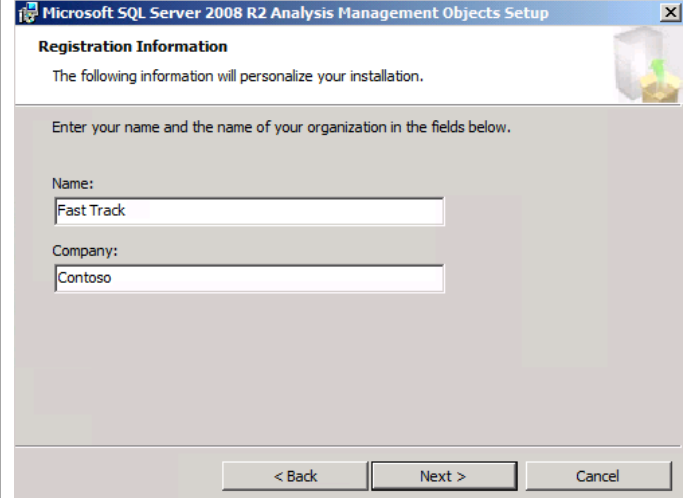




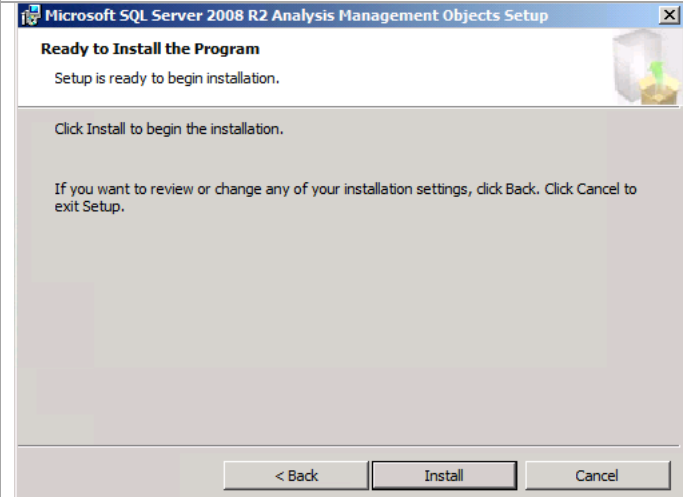
Within the License Terms dialog, select the I accept the terms in the license agreement check box. Click Next to continue.



In the **Registration Information** dialog, enter values for your organization in the **Name** and **Company** textboxes. Click **Next** to continue.

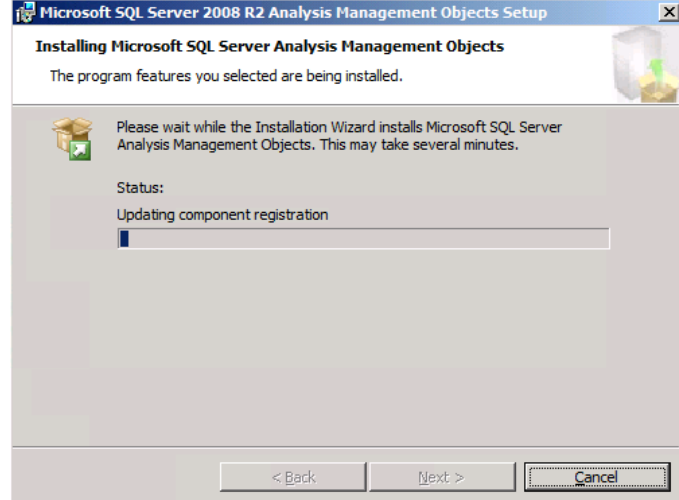


In the **Ready to Install the Program** dialog, click **Install** to begin the installation.





The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.



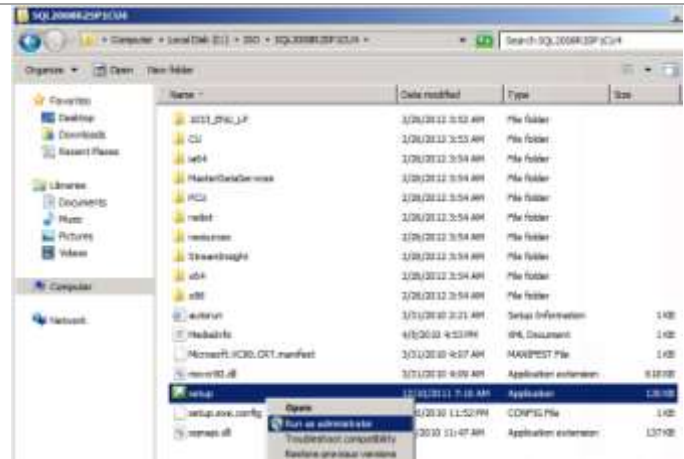
Installing SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

The SM Data Warehouse installation requires SQL Server Reporting Services (SSRS) to be installed to support the SM reporting features. The following steps are provided:

Perform the following steps on the **Service Manager Data Warehouse** virtual machine.



From the SQL Server 2008 R2 slipstreamed installation media source right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



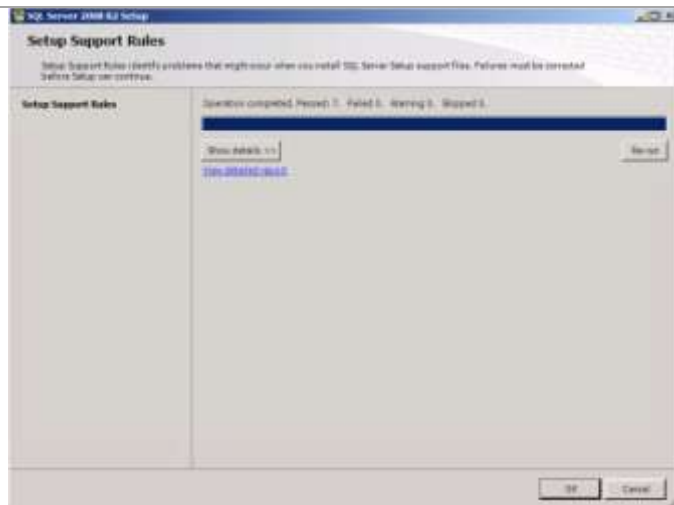
The SQL Server Installation Center will appear.



From the SQL Server Installation Center click the New installation or add features to an existing installation link.



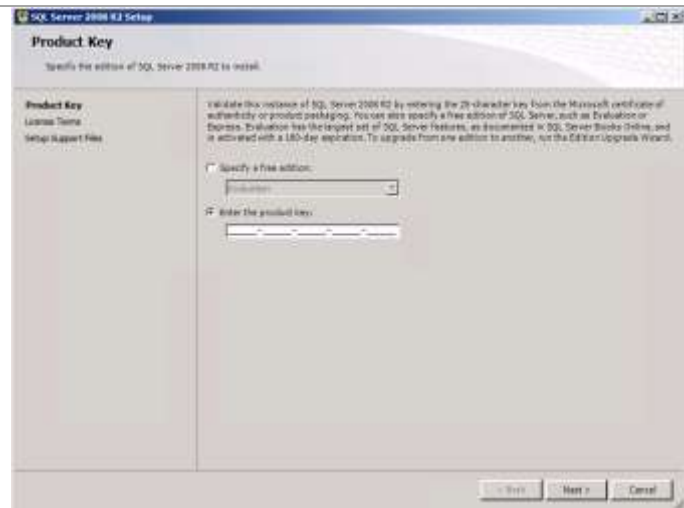
The **SQL Server 2008 R2 Setup** wizard will appear. In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **OK** to continue.



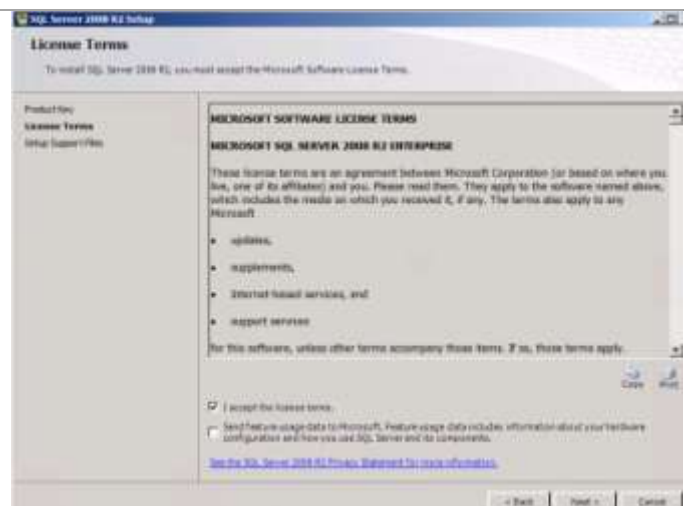


In the **Product Key** dialog, select the **Enter the product key** option and enter the associated product key in the provided textbox. Click **Next** to continue.

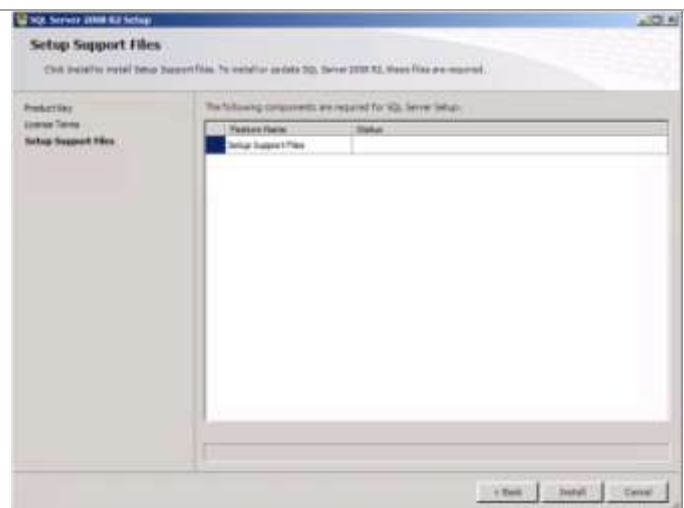
Note: If you do not have a product key, select the **Specify a free edition** option and select **Evaluation** from the drop down menu for a 180-day evaluation period.



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

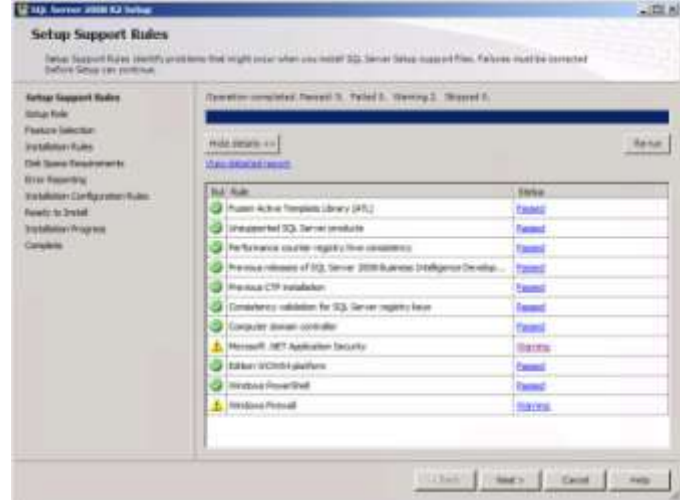


In the **Setup Support Files** dialog, click **install** and allow the Support Files to install.

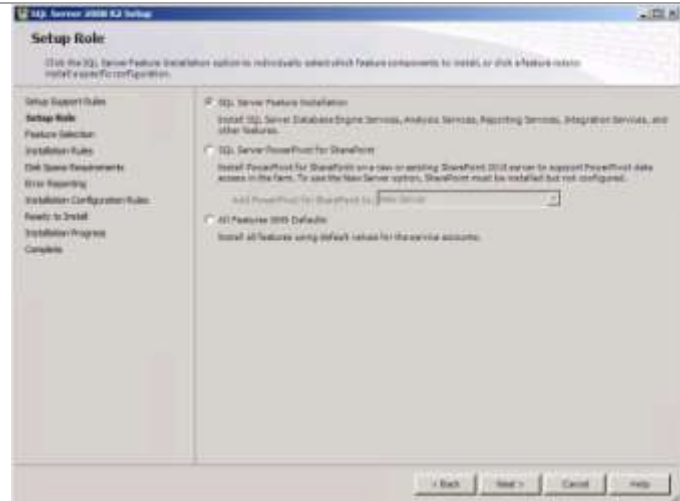




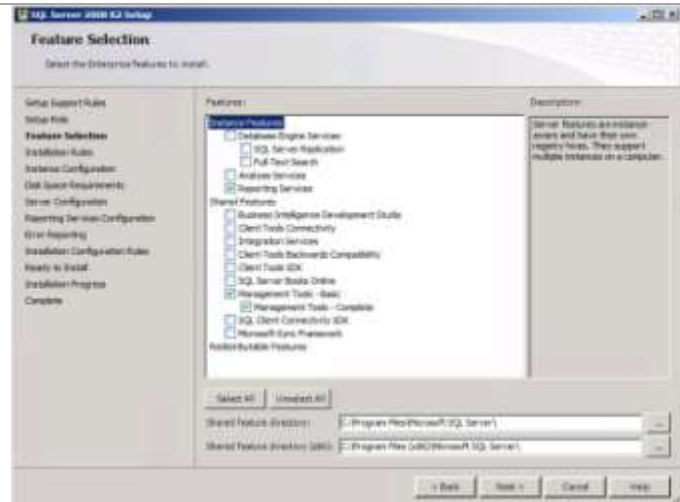
In the **Setup Support Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.



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

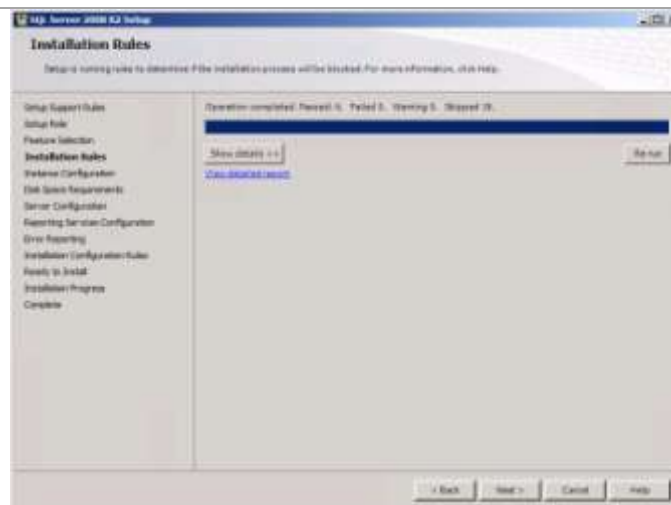


In the **Feature Selection** dialog, select the **Reporting Services, Management Tools – Basic** and **Management Tools – Complete** check boxes. When all selections are made, click **Next** to continue.



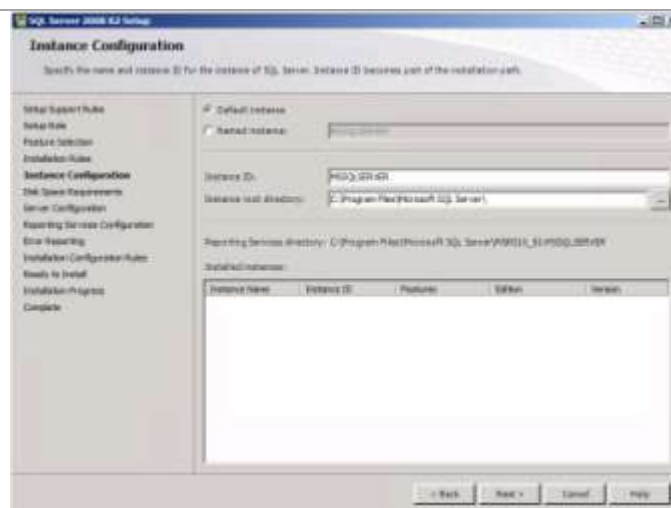


In the **Installation Rules** dialog, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and re-run the validation check. Click **Next** to continue.

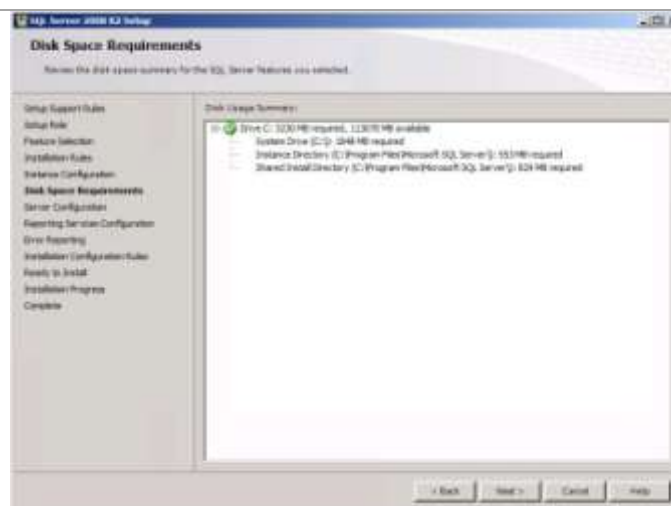


In the **Instance Configuration** dialog, select the **Default instance** option. Keep the default **Instance ID** and **Instance root directory** values and click **Next** to continue.

Note: A post installation configuration process will occur to configure the database within the SCOM SQL Instance.

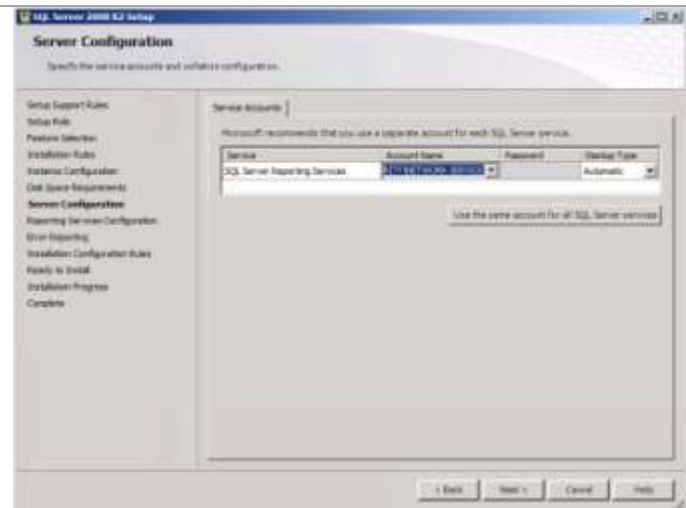


In the **Disk Space Requirements** dialog, verify that you have sufficient disk space and click **Next** to continue.

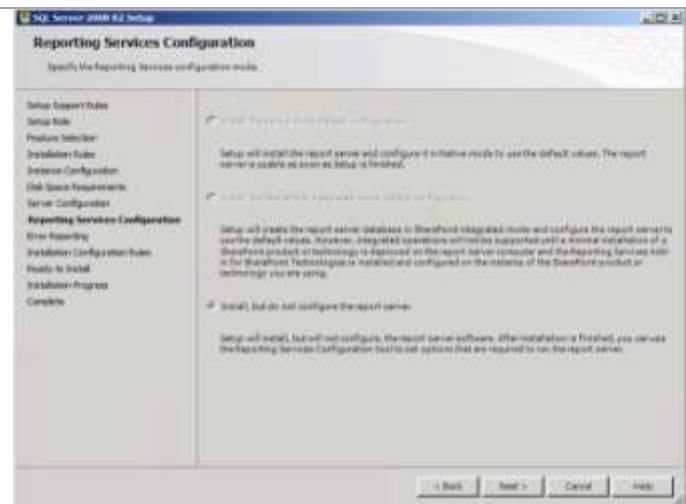




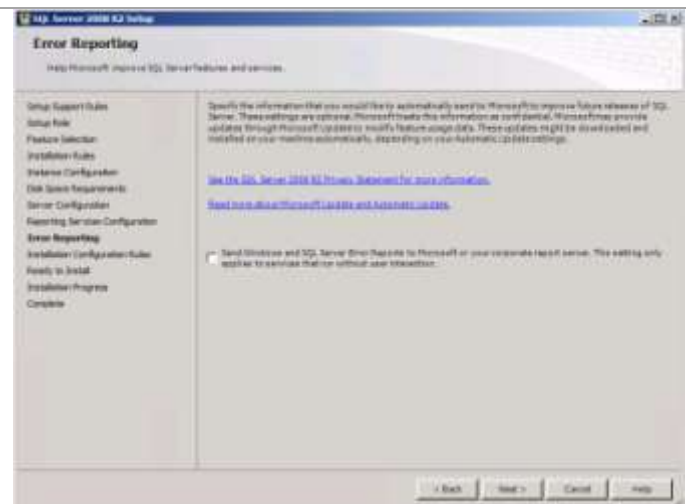
In the **Server Configuration** dialog, select the **Service Accounts** tab. Specify the **NETWORK SERVICE** account for the **SQL Server Reporting Services** service. Click **Next** to continue.



In the **Reporting Services Configuration** dialog, select the **Install, but do not configure the report server** 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.

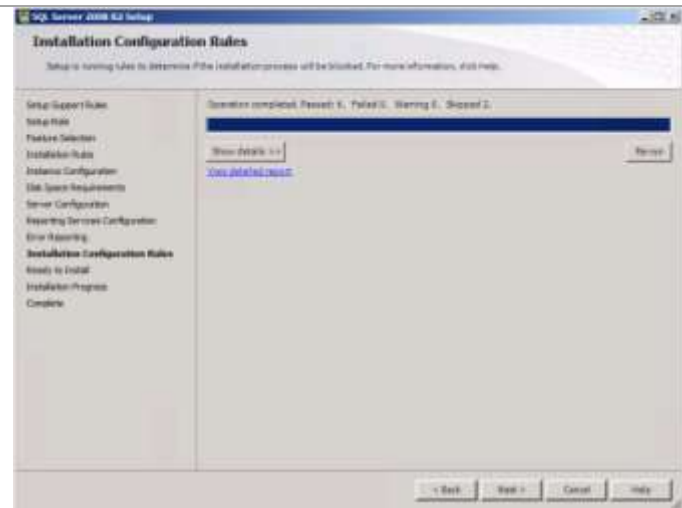


In the **Error Reporting** dialog, select or deselect the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server based on your organization's policies** and click **Next** to continue.





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 instance.



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

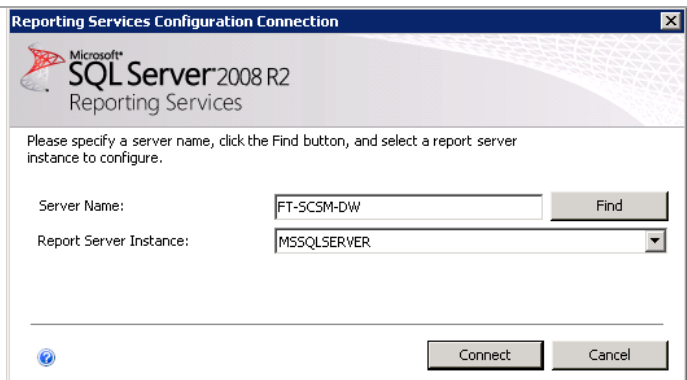




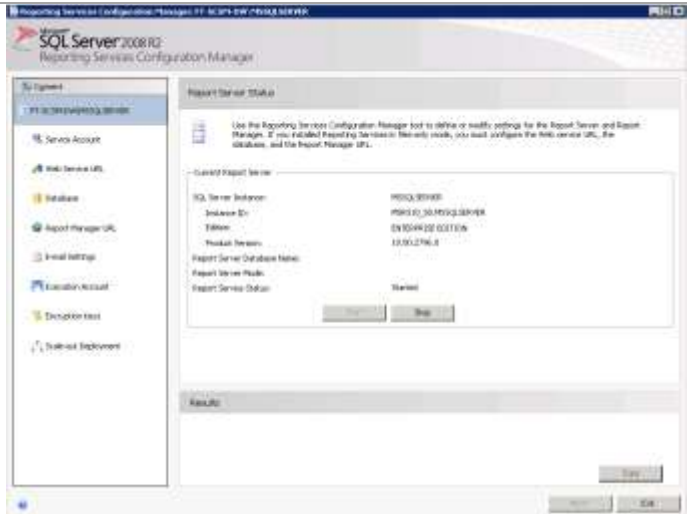
When installed, verify that the Service Manager management server installed properly by opening the console. From the **Start Menu**, navigate to the **Microsoft SQL Server 2008 R2** folder and click the **Reporting Services Configuration Manager** shortcut.



The **Reporting Services Configuration Connection** dialog will appear. In the **Server Name** textbox specify the name of the SCSM server. In the **Report Server Instance** textbox, use the default **MSSQLSERVER** drop-down menu value. Click **Connect**.

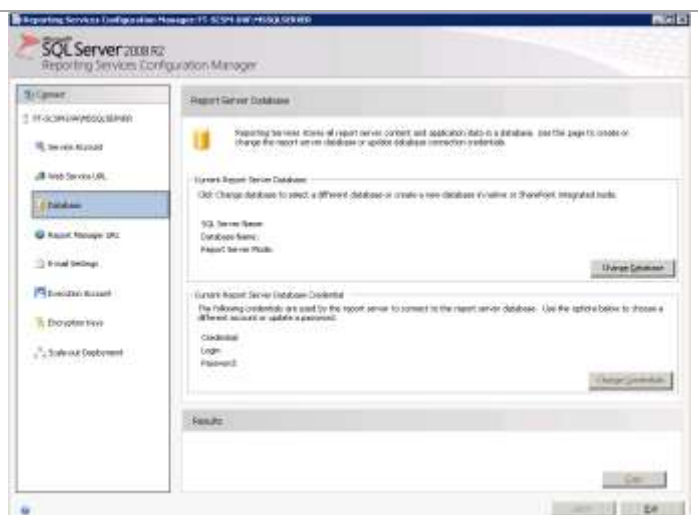


The Reporting Services Configuration Manager tool will appear.

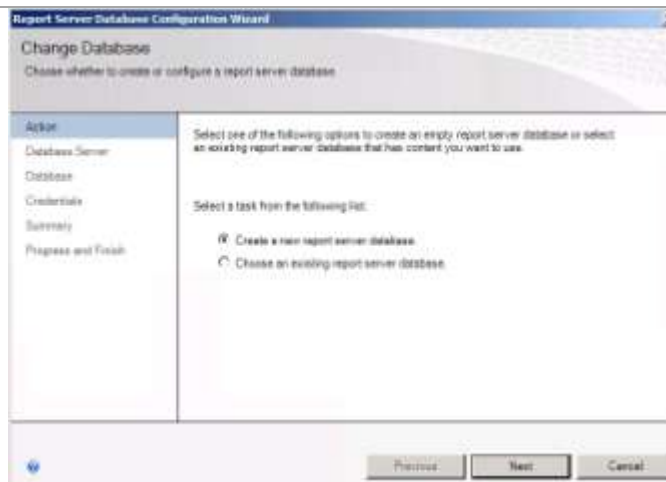




In the Reporting Services Configuration Manager tool, click the Database option from the toolbar. Within the Current Report Server Database section, click the Change Database button.



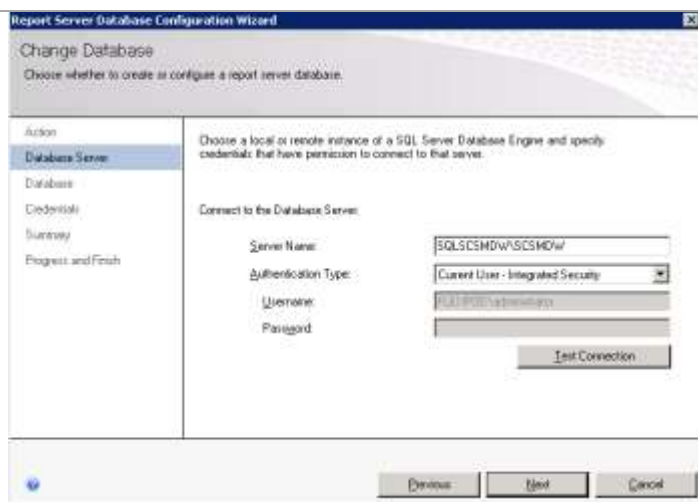
The Reporting Services Configuration Wizard will appear. In the Action section, choose the Create a new report server database option. Click Next to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – specify the name of the SQL Server cluster network name (CNO) and the database instance created for the SM installation.
- **Authentication Type** – specify Current User – Integrated Security from the drop-down menu.

Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.





In the **Database** section, specify the following values:

- **Database Name** – Accept the default value of ReportServer.
- **Language** – specify the desired language option from the drop-down menu.
- **Report Server Mode** – select the Native Mode option.

Click **Next** to continue.

Report Server Database Configuration Wizard

Change Database

Choose whether to create or configure a report server database.

Action: Database Server, Database, Credentials, Summary, Progress and Finish

Enter a database name, select the language to use for running SQL scripts, and specify whether to create the database in native or SharePoint mode.

Database Name: ReportServer

Temp Database Name: ReportServerTemp

Language: English (United States)

Report Server Mode: ☒ Native Mode ☐ SharePoint Integrated Mode

Previous Next Cancel

In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down menu and click **Next** to continue.

Report Server Database Configuration Wizard

Change Database

Choose whether to create or configure a report server database.

Action: Database Server, Database, Credentials, Summary, Progress and Finish

Specify the credentials of an existing account that the report server will use to connect to the report server database. Permission to access the report server database will be automatically granted to the account you specify.

Credentials:

Authentication Type: Service Credentials

User name: NT AUTHORITY\NETWORKSERVICE

Password:

Previous Next Cancel

In the **Summary** section, review the selections made **Next** to create the SQL Server Reporting Service 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

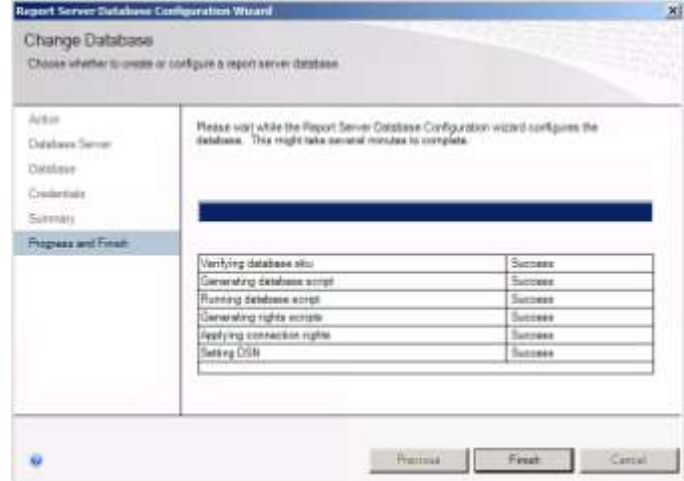
The following information will be used to create a new report server database. Verify this information is correct before you continue.

SQL Server Instance:	SQLSCRM\rf\SCRM\rf
Report Server Database:	ReportServer
Temp Database:	ReportServerTempDB
Report Server Language:	English (United States)
Report Server Mode:	Native
Authentication Type:	Service Account
User name:	NT AUTHORITY\NETWORKSERVICE
Password:	*****

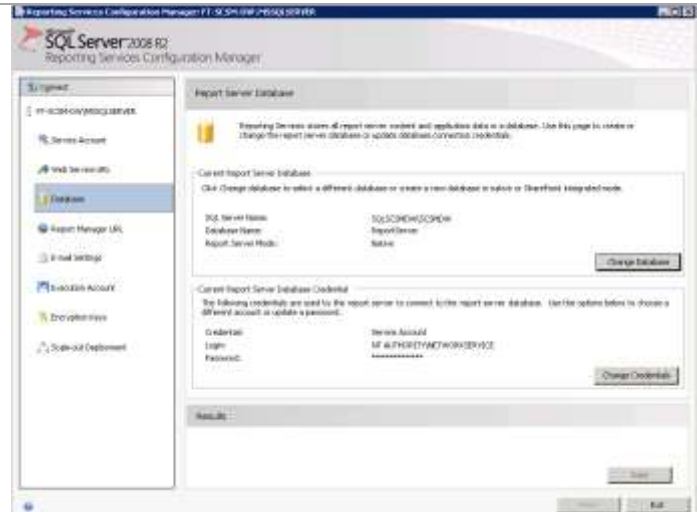
Previous Next Cancel



The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.



In the **Reporting Services Configuration Manager** tool, the **Database** option will now display the database and Report Server Database credentials specified in the wizard.

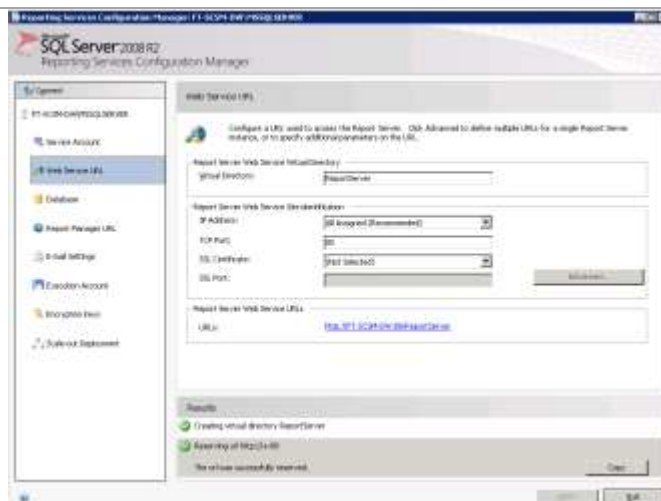




In the **Reporting Services Configuration Manager** tool, click the **Web Service URL** option from the toolbar. Specify the following values:

- In the Report Server Web Service Virtual Directory section, set the Virtual Directory value to ReportServer in the provided textbox.
- 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).

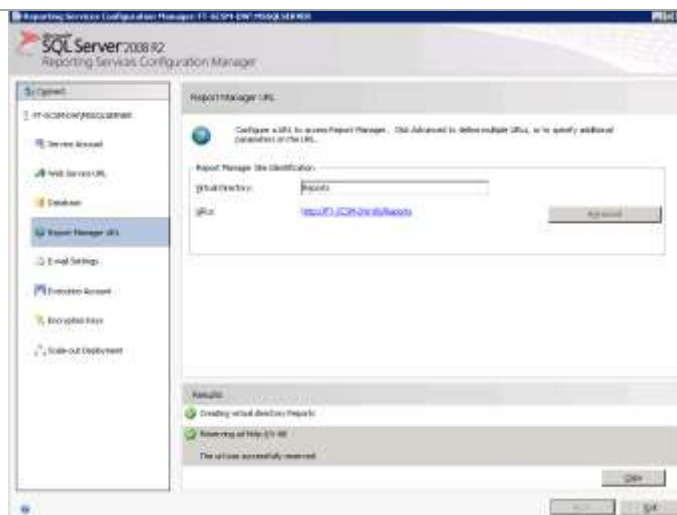
Click the **Apply** button to save the settings and create the Web Service URL.



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** in the provided textbox.

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.

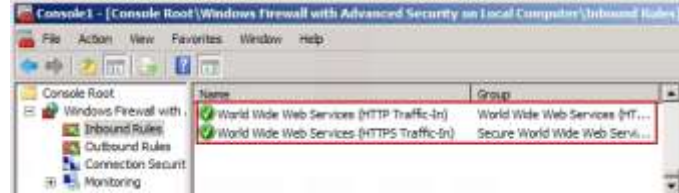




If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall:

- World Wide Web Services (HTTP Traffic-In).
- World Wide Web Services (HTTPS Traffic-In).

Right-click each rule and select **Enable Rule** from the context menu.



Installing SharePoint Foundation 2010 on the Self-Service Portal Server

The following steps must be completed in order to install SharePoint Foundation 2010 on the Service Manager self-service portal server only.

Perform the following steps on the **Service Manager Self-Service Portal** virtual machine.

Log on to Service Manager self-service portal server (**NOT** a Service Manager management server or the Data Warehouse server). Locate the SharePoint Foundation 2010 installation file. Right-click **SharePointFoundation.exe** and select **Run as administrator** from the context menu to begin setup.¹⁵



¹⁵ 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.

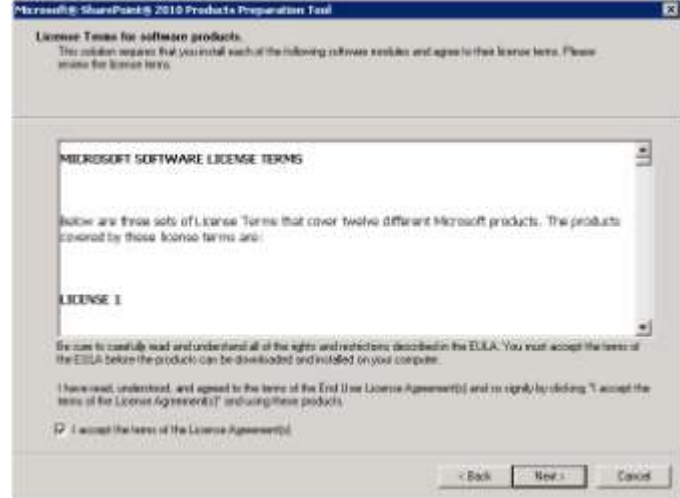


The Microsoft SharePoint 2010 Products Preparation Tool will open. Click Next to continue.





In the **License Terms** for software products dialog, verify 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.





If you have not already done so, you must install a valid SSL certificate. The Subject of the certificate (SN) must match the server name of your SSP VM.

If you have AD Certificate Services installed in your domain, you can request a new certificate via IIS manager.

Open IIS manager, select your web server and double click on the “Server Certificates” icon.

Right-click in the center pane and select “Create Domain Certificate.” Fill out the server name in the common name field along with all the other fields and click next. Select your AD Certificate server by clicking on “Select” and choosing from the list. Give the server a friendly name and click Finish.



After the system restart, log back in 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, select **Install SharePoint Foundation**.

If the wizard reports you have missing pre-requisites, you may need to run the pre-requisite installer again. Because this installer downloads products from the Internet, non-Internet connected systems will fail to install correctly. You will need to manually download and install these files. See the SharePoint foundation documentation for instructions on manual installation.





In the Read the Microsoft Software License Terms dialog, verify the I accept the terms of this Agreement installation option check box is selected and click Continue.



In the Choose the installation you want dialog, click the Server Farm button.





In the **Server Type** dialog, select the **Complete** option and click **Install Now**.



After installation, the **Run Configuration Wizard** dialog will appear. Verify the **Run the SharePoint Products Configuration Wizard now** check box is selected and click **Close**.





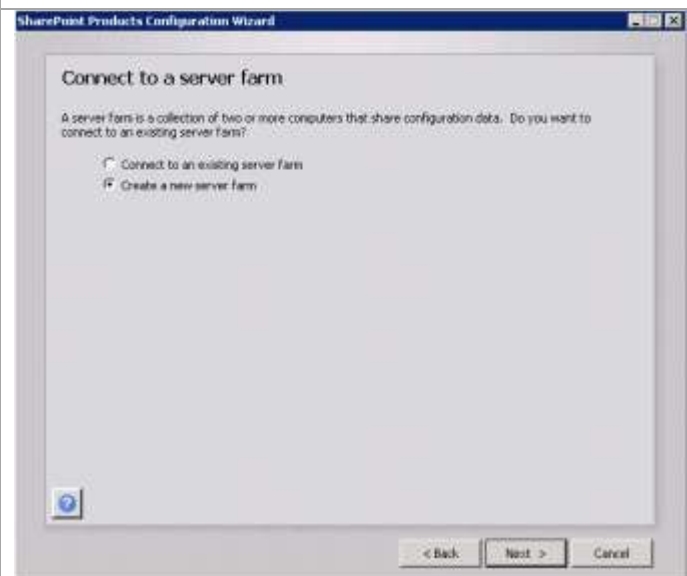
The **SharePoint Products Configuration Wizard** will appear. Click **Next** to continue with the wizard.



A dialog will appear stating 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 is selected 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. When complete, click **Next** to continue.

The screenshot shows the 'Specify Configuration Database Settings' dialog box. It contains two text input fields: 'Database server' with the value 'SQLSCSPFarm\SCSPFarm' and 'Database name' with the value 'SharePoint_Config'. Below these is the 'Specify Database Access Account' section, which includes a 'Username' field with the value 'testpod#1-SCSM-Svc' and a 'Password' field with masked characters. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

In the **Specify Farm Security Settings** dialog enter an unique passphrase in the Passphrase textbox. Re-type the passphrase in the Confirm passphrase textbox and click **Next** to continue.

The screenshot shows the 'Specify Farm Security Settings' dialog box. It contains two text input fields for a passphrase: 'Passphrase' and 'Confirm passphrase', both filled with masked characters. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.



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 textbox.

In the **Configure Security Settings** section, select the **NTLM** option.

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

The screenshot shows the 'SharePoint Products Configuration Wizard' window. The title bar reads 'SharePoint Products Configuration Wizard'. The main heading is 'Configure SharePoint Central Administration Web Application'. Below this, a paragraph explains that the web application allows managing configuration settings for a server farm and that the first server added must host this application. It prompts the user to specify a port number between 1 and 65535. There is a checkbox labeled 'Specify port number:' which is checked, and a text box next to it containing '1309'. Below this is the 'Configure Security Settings' section. It states that Kerberos is the recommended security configuration but requires special configuration by the domain administrator, while NTLM authentication will work with any application pool account and the default domain configuration. A link 'Show me more information.' is provided. The user is asked to choose an authentication provider, with 'NTLM' selected (indicated by a radio button) and 'Negotiate (Kerberos)' unselected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

The **Completing the SharePoint Products Configuration Wizard** dialog will appear and displaying 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 with the title 'Configuration Successful'. It states 'The following configuration settings were successfully applied:'. Below this is a list of settings with their corresponding values in text boxes: 'Configuration Database Server' is 'SQLSRVMS\SQLSRVMS', 'Configuration Database Name' is 'SharePoint_Config', 'Host the Central Administration Web Application' is 'Yes', 'Central Administration URL' is 'http://f5-scvm-sap:1309/', and 'Authentication provider' is 'NTLM'. A paragraph at the bottom instructs the user to click 'Finish' to close the wizard and launch the SharePoint Central Administration website to continue configuring the SharePoint installation, noting that users may be prompted for credentials in the form 'DOMAIN\user_name' and password. At the bottom right, there is a 'Finish' button.



The wizard will display the progress while performing the SharePoint configuration.



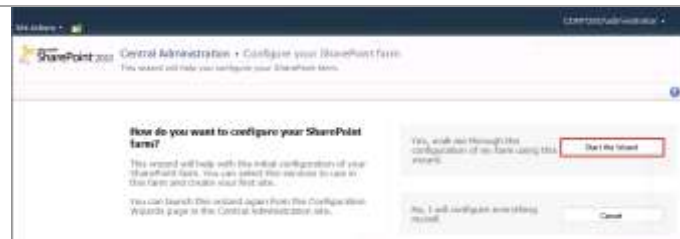
When successful the **Configuration Successful** dialog will appear. Click **Finish** to complete the configuration of SharePoint Foundation 2010.



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.

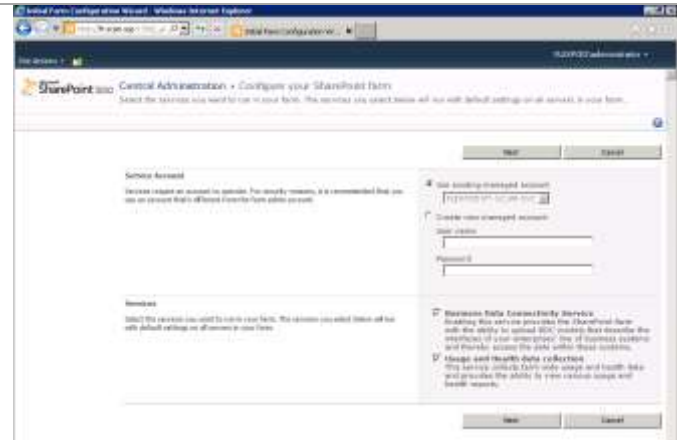




In the **Service Account** section, select the **Use existing managed account** and select the SM service account from the drop-down menu.

In the Services section, select the Business Data Connectivity Services and Usage and Health data collection check boxes.

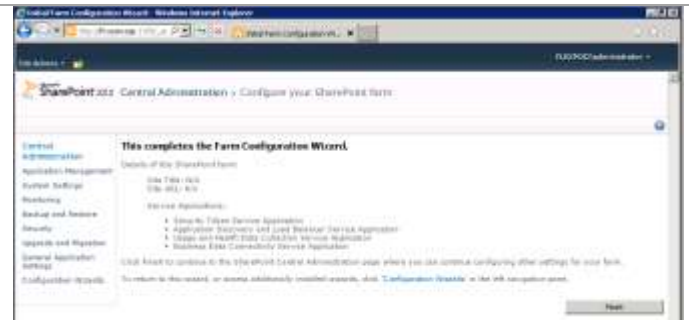
Click **Next** to continue.



In the Web Site configuration page, click the **Skip** button to continue without configuring these settings.



The SharePoint farm configuration is now complete. Click the **Finish** button to exit.



The **SharePoint Central Administration** portal will open. Verify that SharePoint is operating properly on the system prior to proceeding to the SM Self-Service Portal installation.



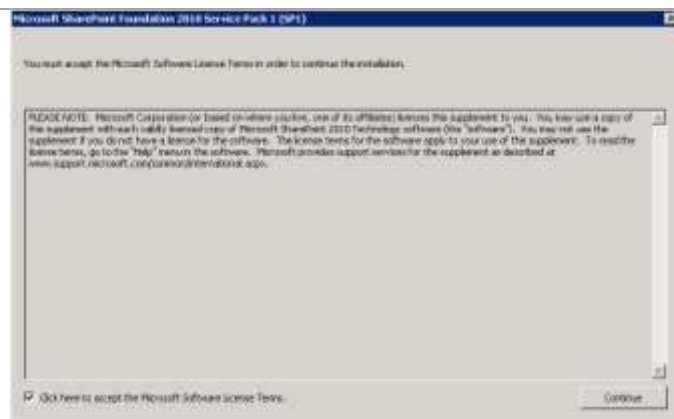


Note: The latest service pack should be applied to SharePoint Foundation Server after this installation¹⁶.

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.



The Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1) wizard will appear. Verify that the Click here to accept the Microsoft Software License Terms installation option check box is selected and click Continue.



The installation will continue without interaction until it completes. When prompted, click **OK** to complete the installation. You must restart the system after the Service Pack installation.



Installing .NET Framework 4 on the Self-Service Portal Server

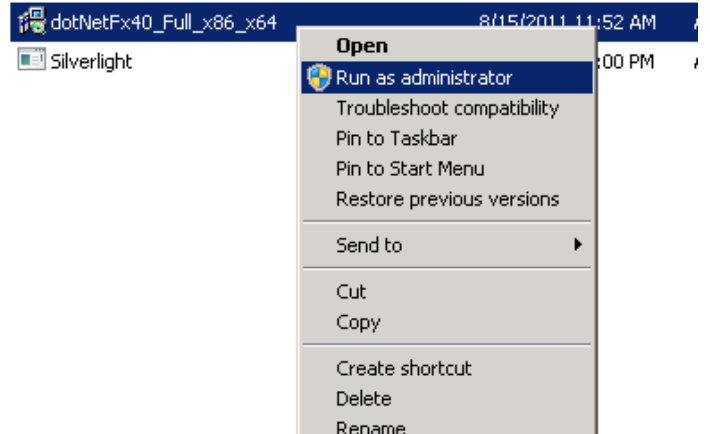
Additionally, the SM Self-Service portal installation also requires the .NET Framework 4 package be installed prior to installation. The following steps are provided:

Perform the following steps on the **Service Manager Self-Service Portal** virtual machine.

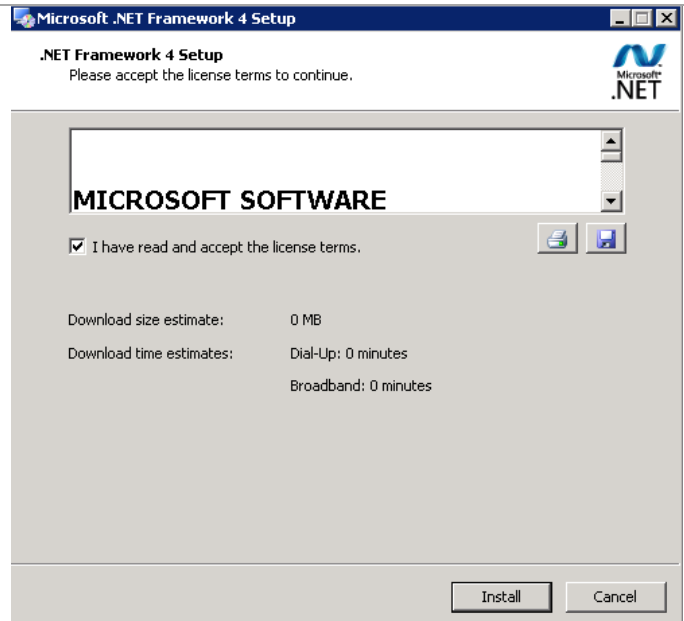
¹⁶ Service Pack 1 (SP1) for Microsoft SharePoint Foundation 2010 - <http://www.microsoft.com/download/en/details.aspx?id=26640>



From the installation media source right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** from the context menu to begin setup.

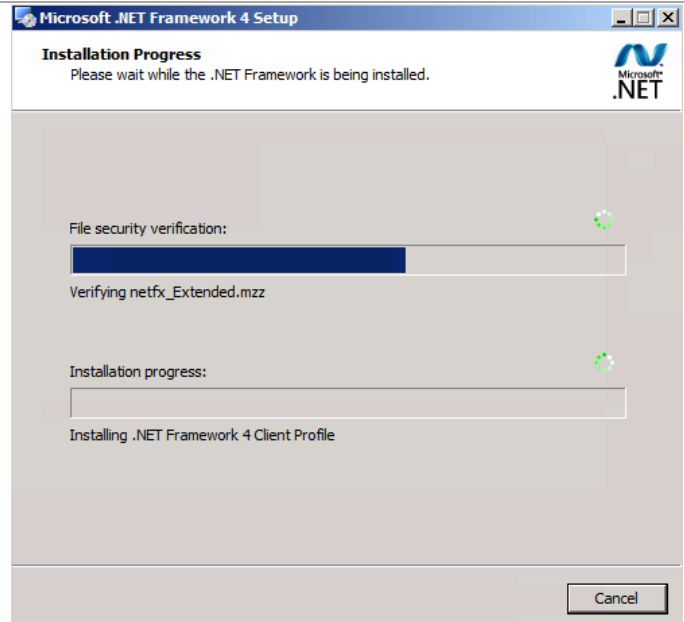


Within the Microsoft .NET Framework 4 Setup dialog, select the I have read and accept the license terms check box and click Install to begin the installation.

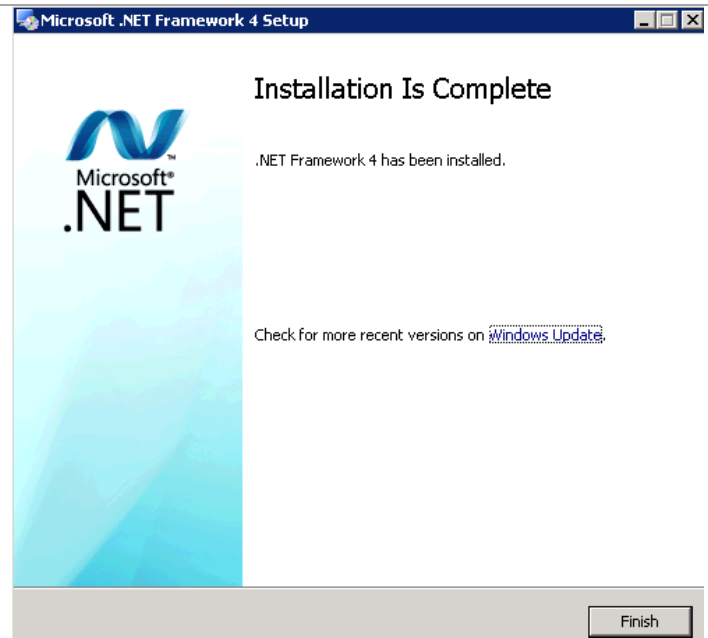




The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.



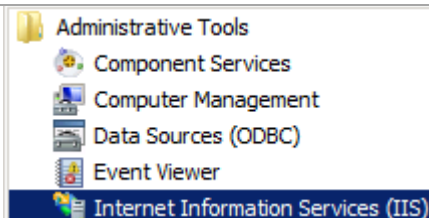


Requesting and Installing an SSL Certificate on the Self-Service Portal Server

Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate in order to enable SSL on the portal website.¹⁷ If the self-service portal is to be installed without SSL this section can be skipped. There are several ways to request an SSL Certificate. One method, through the IIS Manager console, is outlined below.

Perform the following steps on the **Service Manager self-service portal** 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...



¹⁷ SSL Certificates for the self-service portal - <http://technet.microsoft.com/en-us/library/hh667343.aspx>.



The **Request Certificate** dialog will appear. In the **Distinguished Name Properties** dialog, complete the information as prompted. Note the **Common Name** field must equal the exact name that the server will be accessed in the web browser. Click **Next** to continue.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: FT-SCSM-SSP

Organization: FlexPod

Organizational unit: FastTrack

City/locality: San Jose

State/province: CA

Country/region: US

Previous Next Finish Cancel

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.

Request Certificate

Cryptographic Service Provider Properties

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.

Cryptographic service provider: Microsoft RSA Schannel Cryptographic Provider

Bit length: 1024

Previous Next Finish Cancel

In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

When completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.

Request Certificate

File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request: C:\FT-SCSM-SSP.req

Previous Next Finish Cancel



After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** when again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Click **OK** to complete the operation.



In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.



Installing the Service Manager Roles

The following steps must to be completed in order to install the Service Manager roles correctly.

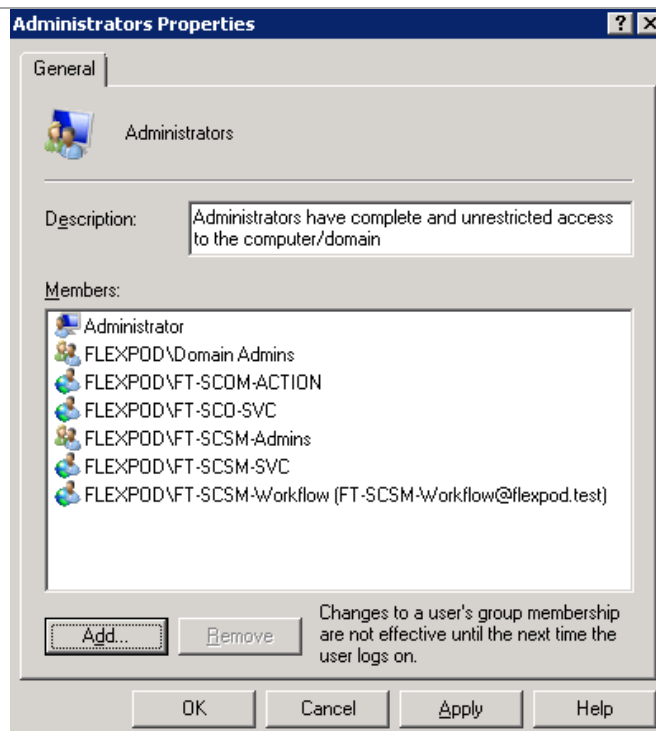
Perform the following steps on **all Service Manager Servers** virtual machines.



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:

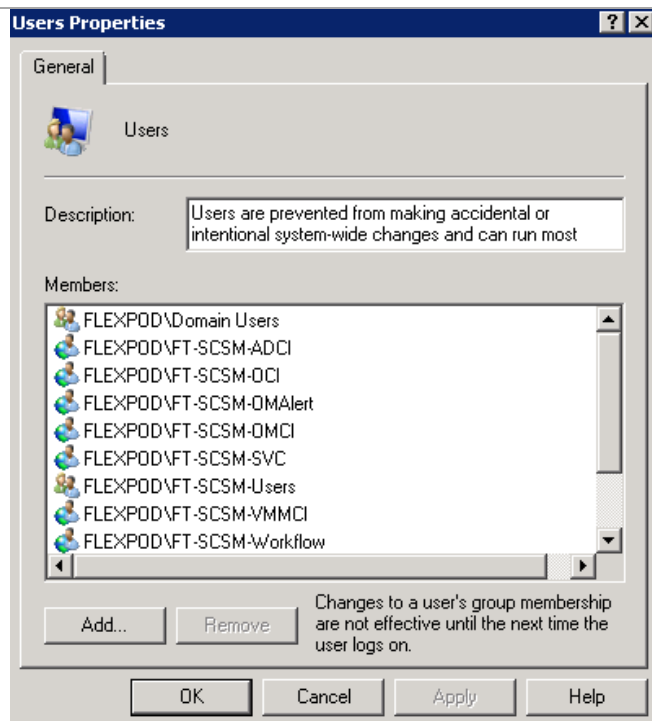
- Operations Manager action account.
- Service Manager workflow account.
- Service Manager service account.
- Service Manager Admins group.
- Orchestrator service account.



Verify that the following accounts and/or groups are members of the Local Users group on each Service Manager virtual machine:

- Service Manager Active Directory CI connection account.
- Service Manager Orchestrator CI connection account.
- Service Manager Operations Manager alert connection account.
- Service Manager Operations Manager CI connection account.
- Service Manager service account.
- Service Manager users group.
- Service Manager Virtual Machine Manager CI connection account.

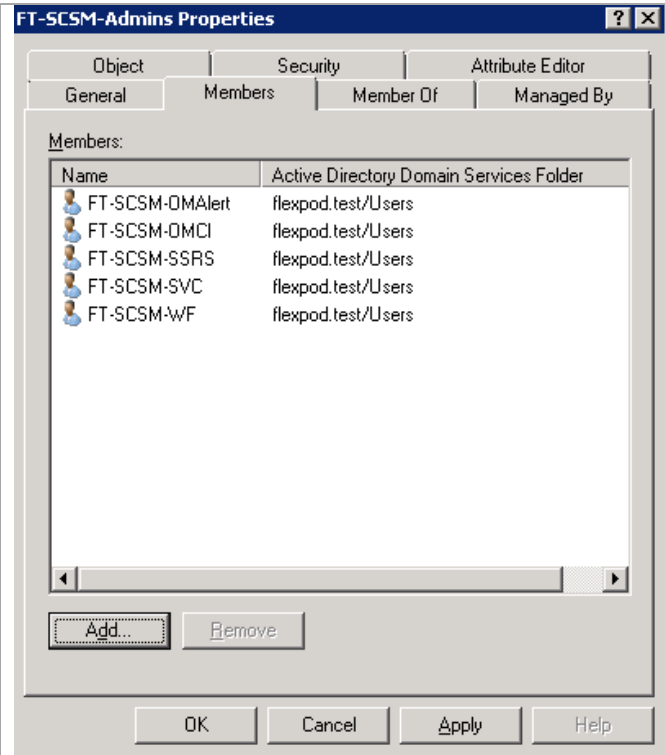
Service Manager workflow account.



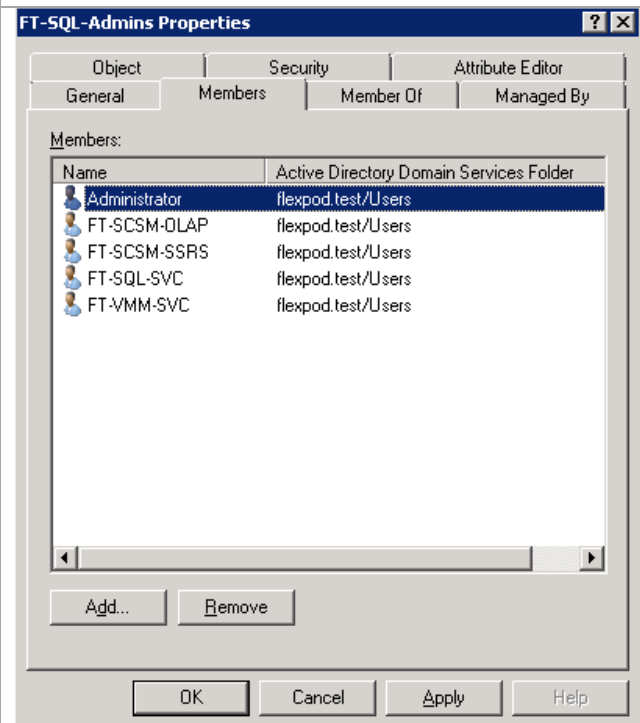


Perform the following step on an **Active Directory Domain Controller** in the target environment.

In the domain where Service Manager will be installed, verify that the SM Operations Manager alert connectors and the Service Manager service accounts are members of the SM Admins group created earlier.



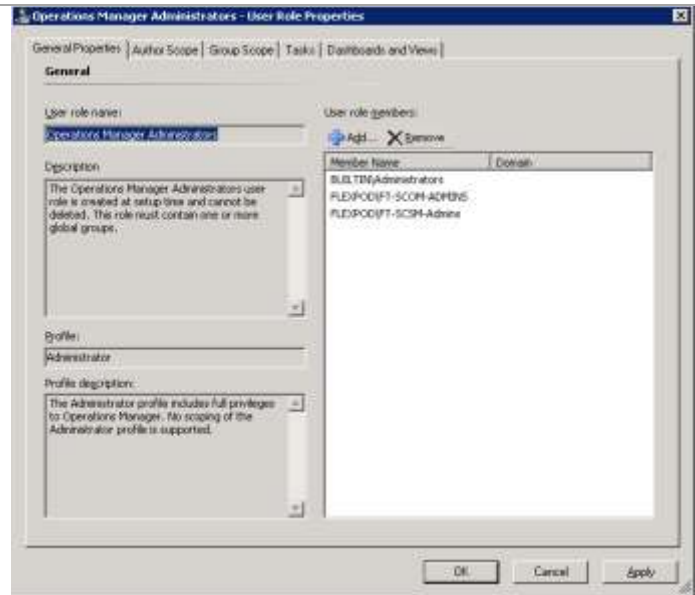
In the domain where Service Manager will be installed, verify that the SM OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group created earlier.



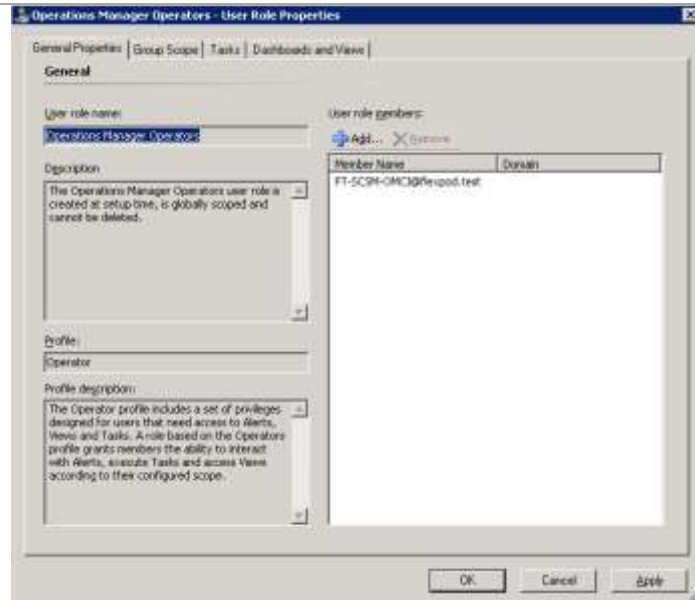


Perform the following steps on the **Operations Manager** virtual machine.

Log on to the Operations Manager server as an Administrator. In the **Operations Manager console**, navigate to Administration pane. In the **Security** node under **User Roles**, locate the **Operations Manager Administrators** role and add the **SCSM Admins** group to the role. Click **OK** to save the changes.



While still in the **Security** node under **User Roles**, locate the **Operations Manager Operators** role and add the **SCSM OMCI** user to the role. Click **OK** to save the changes.





Installing the Management Server

The following steps must be completed in order to install the Service Manager Management Server role.

Perform the following steps on the **System Center Service Manager management server** virtual machine.

Log on to Service Manager management server (**NOT** the Service Manager Data Warehouse server or the self-service portal server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager management server** to begin the Service Manager server installation.

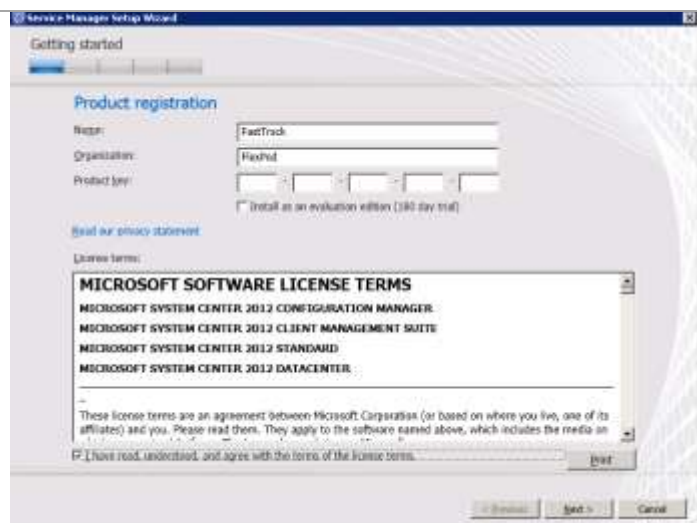




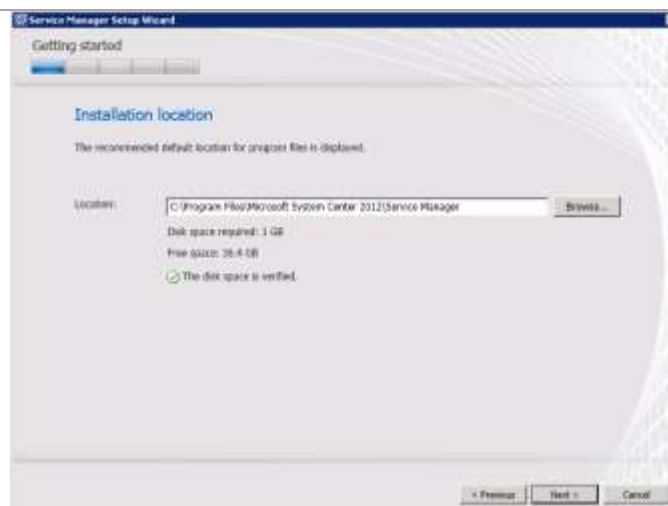
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name**—specify the name of primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.
- **Product key**—provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.

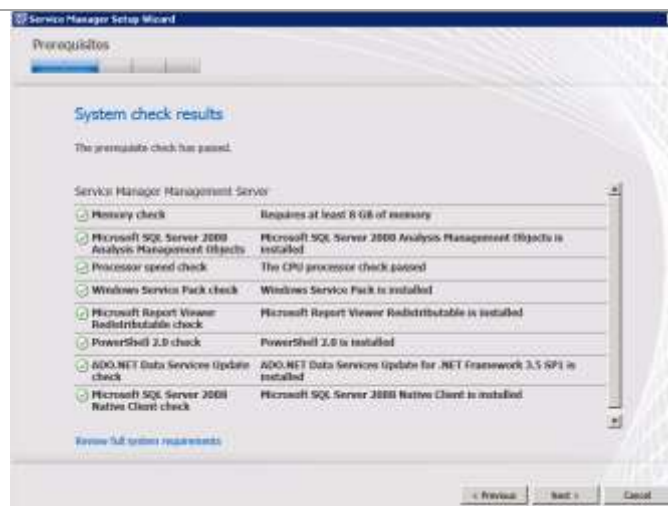
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a specific location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





In the **Configure the Service Manager database** dialog, specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation.
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation.

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the Service Manager database. In most cases the default value of ServiceManager should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

A warning message will appear due to the use of the default SQL collation (SQL_Latin1_General_CP1_CI_AS). Support for multiple languages in Service Manager is not possible when you are using the default collation. If the installation requires support for multiple languages using a different collation, the SQL Server instance will be required to be reinstalled.



In the **Configure the Service Manager management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager Data Warehouse and Operations Manager installations.

Specify the Service Manager Administrators group in the **Management group administrators** object picker section.

Click **Next** to continue.

In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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

In the **Configure the account for Service Manager workflow account** dialog, verify that the **Domain account** option is selected and specify the Service Manager service account in the **User name** text box. Enter the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



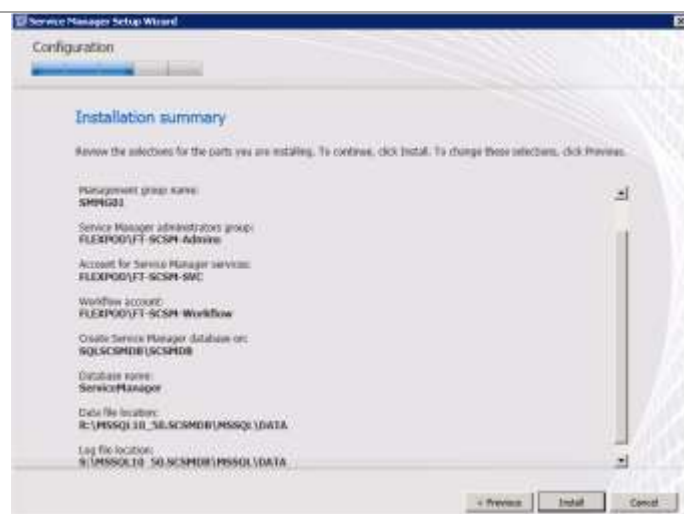
In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



In the **Use Microsoft Update to help keep your computer secure and up-to-date** dialog, select the appropriate option to either participate or not participate in the automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.

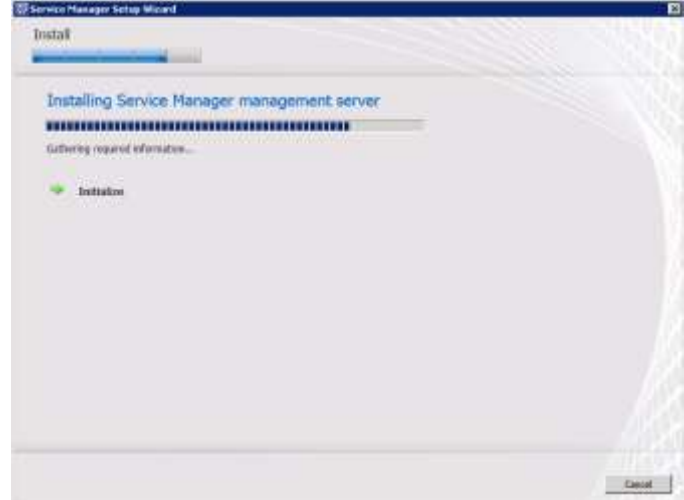


The **Installation summary** dialog will appear displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.





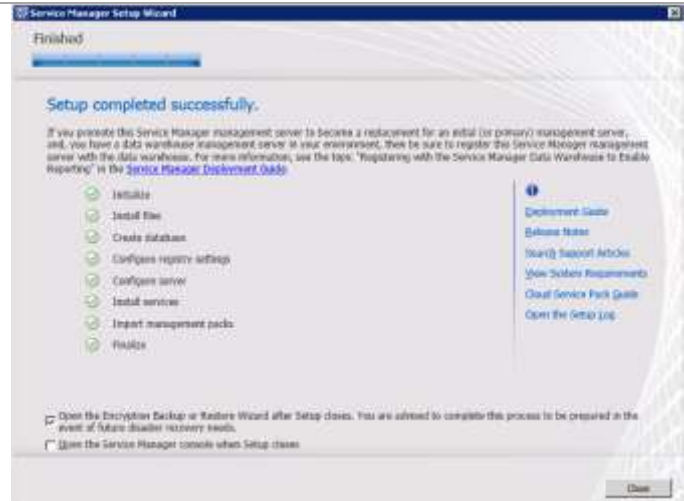
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** dialog.

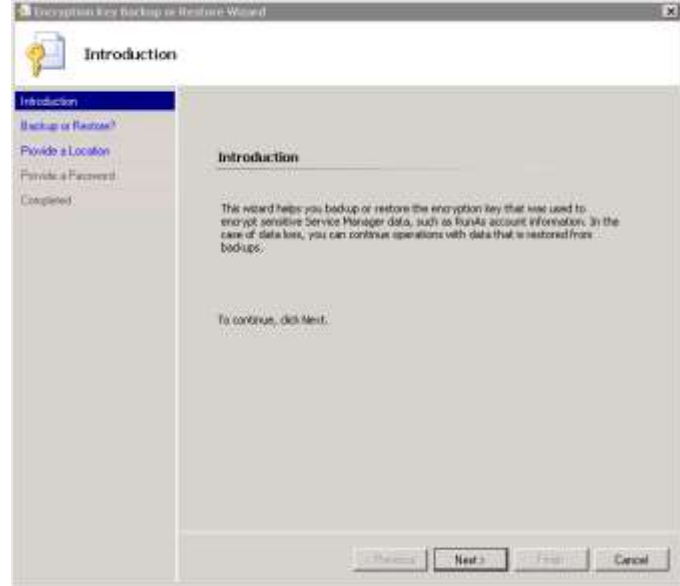
When each step shows successful installation, select the **Open the Encryption Backup or Restore Wizard after Setup closes** is selected to launch the wizard after setup.

Click **Close** to complete the installation.

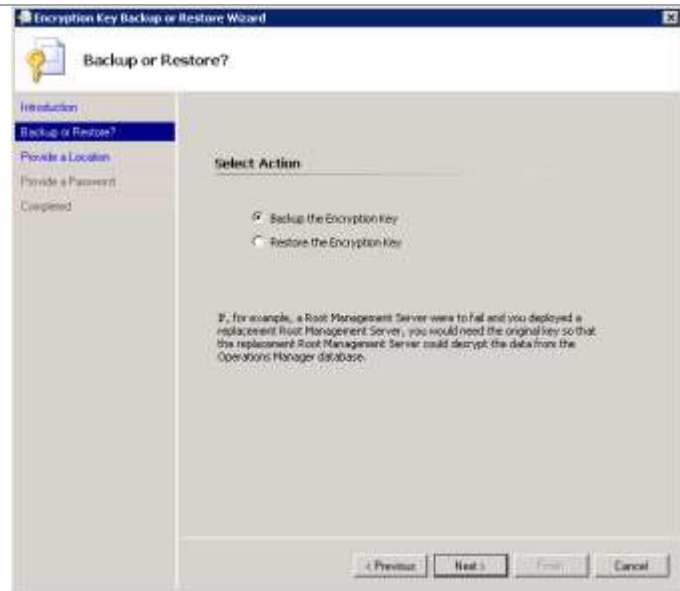




When the installation completes, the **Encryption Key Backup or Restore wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



In the **Select Action** dialog, select the **Backup the Encryption Key** option and click **Next** to continue.





In the **Specify the Location of the Backup File** dialog, specify the desired backup file name and path in the **Path** textbox and object picker. Click **Next** to continue.

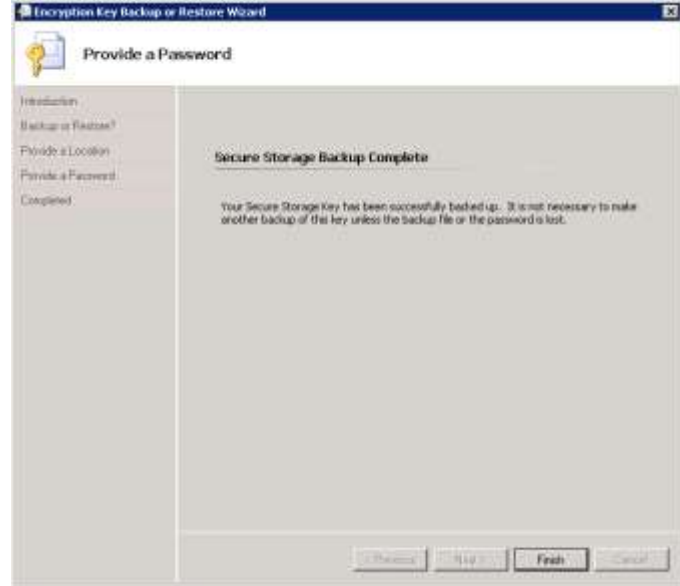
The screenshot shows the 'Encryption Key Backup or Restore Wizard' window. The 'Provide a Location' step is selected in the left sidebar. The main area is titled 'Specify the Location of the Backup File'. It contains instructions: 'Please provide a location to which you want the encryption key backed up, or from which you want the encryption key restored. 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.' Below this is a 'Path:' label followed by a text box containing the path '\\FH-eq11-y-f\\SCSM_Key_Backup\\F1-SCSM_Backupkey.bin' and a 'Browse...' button. An example path is shown below: 'Example: \\FH-Server01\\Backup\\RM3Server01\\Backupkey.bin'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

In the **Provide a Password** dialog, specify a desired password in the **Password** textbox. Re-type the password in the **Confirm Password** textbox and click **Next** to begin the backup process.

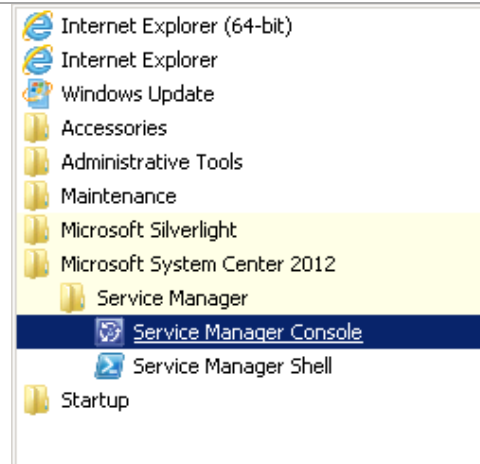
The screenshot shows the 'Encryption Key Backup or Restore Wizard' window. The 'Provide a Password' step is selected in the left sidebar. The main area is titled 'Specify the Password That Will Authorize the Backup or Restore'. It contains instructions: 'The minimum password length is 8 characters. This password is used to secure the data in the backup file.' Below this are two text boxes: 'Password:' and 'Confirm Password:', both containing eight asterisks. A note at the bottom says 'Click Next to run the operation.' At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.



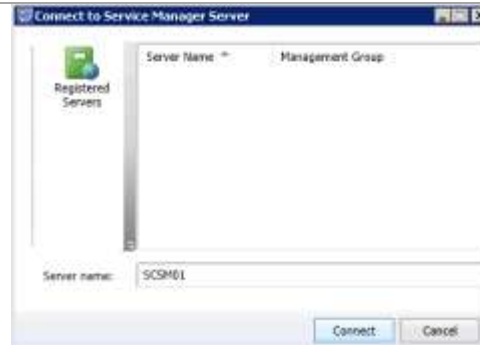
When complete, click **Finish** to exit the wizard.



When installed, verify that the Service Manager Management Server installed properly by opening the console. From the **Start Menu**, navigate to the **Microsoft System Center 2012\Service Manager** folder and click the **Service Manager Console** shortcut.

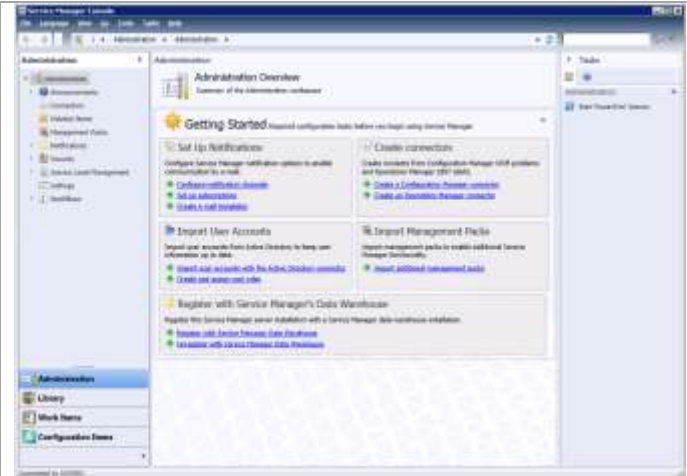


In the **Connect to Service Manager Server** dialog, specify the Service Manager management server name in the **Server name** textbox and click **Connect** to start the console.





The Service Manager console will open. From this console, the installation can be validated by reviewing the configuration and proper operation of the console.



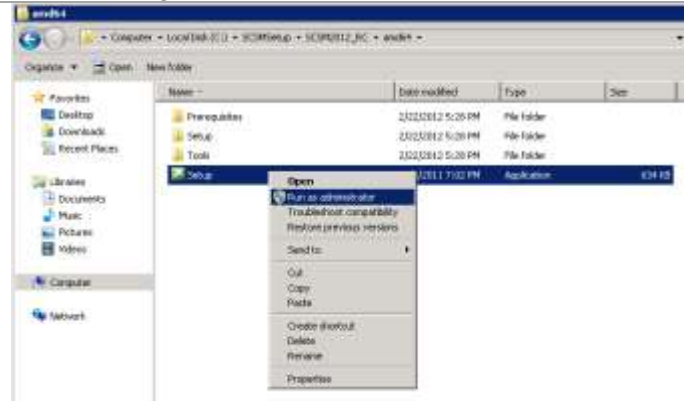


Installing the Data Warehouse Server

The following steps must be completed in order to install the Service Manager Data Warehouse server role.

Perform the following steps on the System Center Service Manager Data Warehouse Server virtual machine.

Logon on to Service Manager Data Warehouse Server (**NOT** the Service Manager Management Server or the Self-service portal server). From the System Center Service Manager (SM) 2012 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.





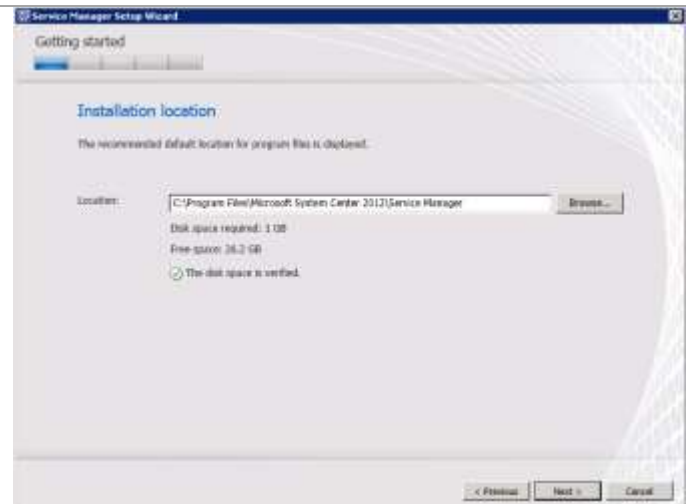
In the **Product registration** dialog, provide the following information in the provided text boxes:

- **Name**—specify the name of primary user or responsible party within your organization.
- **Organization**—specify the name of the licensed organization.
- **Product key**—provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.

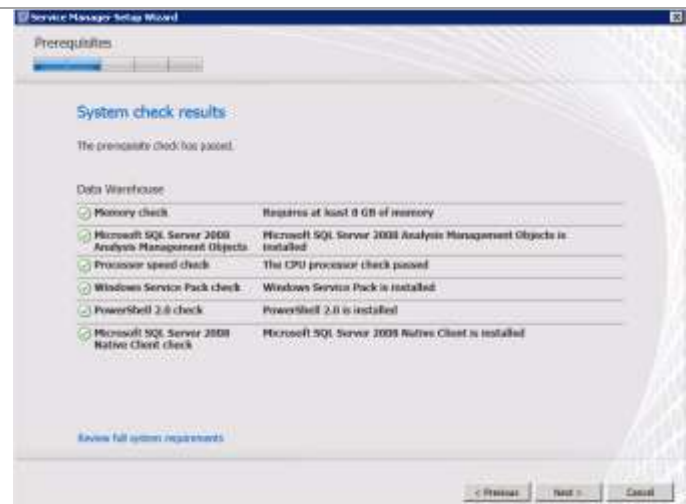
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.



In the **Installation location** dialog, specify a specific location or accept the default location of *%ProgramFiles%\Microsoft System Center 2012\Service Manager* for the installation. Click **Next** to continue.



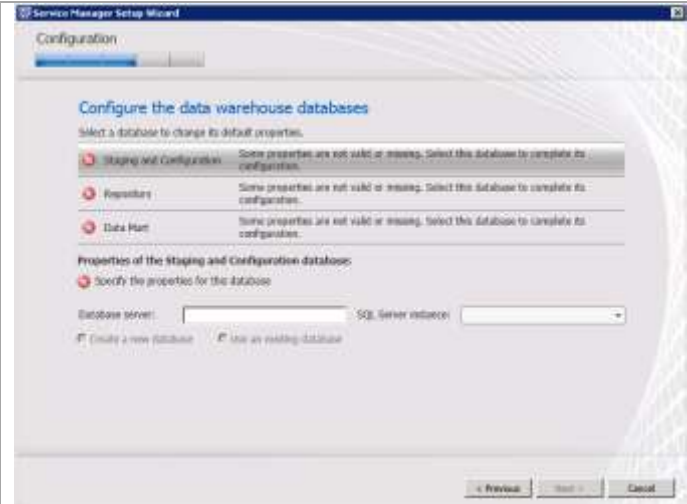
The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





When the **Configure the data warehouse databases** dialog launches each subcategory will appear with an error message until each of the following sections are configured:

- Staging and Configuration
- Repository
- Data Mart





In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

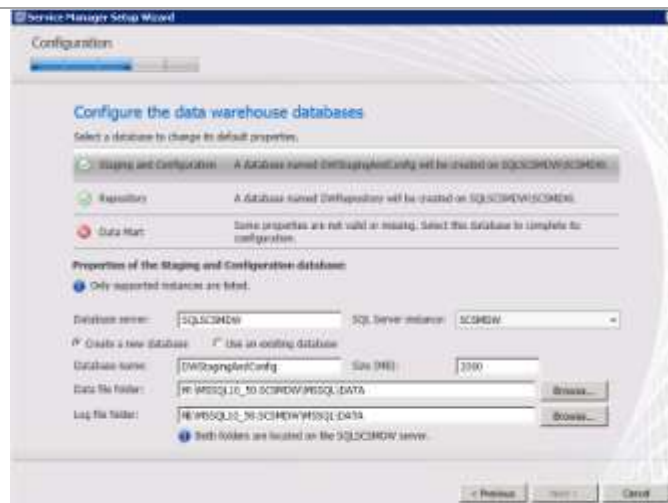
- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation Data Warehouse.

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – specify the name of the SM Data Warehouse database. In most cases the default value of DWStagingAndConfig should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the drive letter associated in the SQL Server cluster for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

A warning message will appear due to the use of the default SQL collation (SQL_Latin1_General_CP1_CI_AS). Support for multiple languages in Service Manager is not possible when you are using the default collation. If the installation requires support for multiple languages using a different collation, the SQL Server instance will be required to be reinstalled.





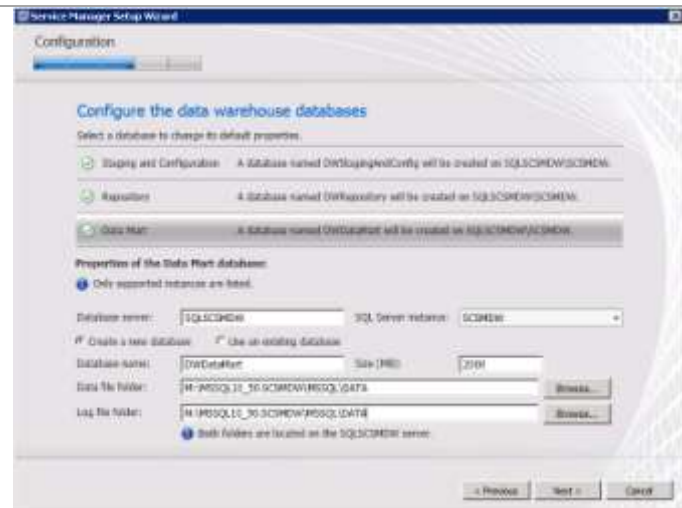
In the **Configure the data warehouse databases** dialog, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **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 Service Manager Data Warehouse database. In most cases the default value of DWDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the same drive letter associated above for the database log files for the Service Manager Data Warehouse database. This should be cross-checked with the worksheet identified earlier.

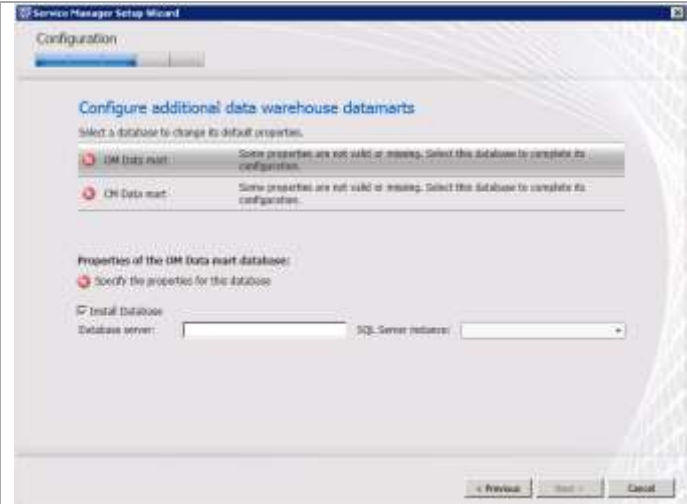
Click **Next** to continue.





When the **Configure additional data warehouse datamarts** dialog launches each subcategory will appear with an error message until each of the following sections are configured:

- OM Data mart
- CM Data mart





In the **Configure additional data warehouse datamarts** dialog, supply the following information in the provided text boxes to configure the **OM Data Mart** section:

- **Database server** – specify the name of the SQL Server CNO created for the Service Manager installation Data Warehouse.
- **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 Service Manager OM Data mart database. In most cases the default value of OMDWDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager OM Data mart database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the same drive letter associated above for the database log files for the Service Manager OM Data mart database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.





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.
- **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 Service Manager CM Data mart database. In most cases the default value of CMDWDataMart should be used.
- **Size (MB)** – specify the initial database size. The default value can be used for Fast Track validation.
- **Data file folder** – specify the same drive letter associated above for the database data files for the Service Manager CM Data mart database. This should be cross-checked with the worksheet identified earlier.
- **Log file folder** – specify the same drive letter associated above for the database log files for the Service Manager CM Data mart database. This should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.



In the **Configure the data warehouse management group** dialog, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 products such as the Service Manager management server and Service Manager Operations Manager installations.

Specify the SM Administrators group in the **Management group administrators** object picker section.

Click **Next** to continue.

In the **Configure the reporting server for the data warehouse** dialog, specify the data warehouse server in the **Report server** textbox.

In the **Report server instance** drop-down menu, select **Default**.

In the **Web service URL** drop-down menu, select the default reporting server URL.

Click **Next** to continue.

In the **Configure the account for Service Manager services** dialog, verify that the **Domain account** option is selected and specify the Service Manager Service Account in the **User name** textbox. Provide the appropriate **Password** and **Domain** in the provided textbox and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



In the **Configure the reporting account** dialog, specify the SM Reporting Account in the **User name** textbox. Provide the appropriate **Password** and **Domain** in the provided textbox and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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

In the **Configure Analysis Services for OLAP cubes** dialog, select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database server** – specify the name of the SQL Server cluster CNO created for the Service Manager installation SQL Server Analysis Services.
- **SQL Server instance** – specify the name of the SQL Server database instance created for the Service Manager installation SQL Server Analysis Services..
- **Database name** – specify the name of the SQL Server Analysis Services database. In most cases the default value of DWASDataBase should be used.

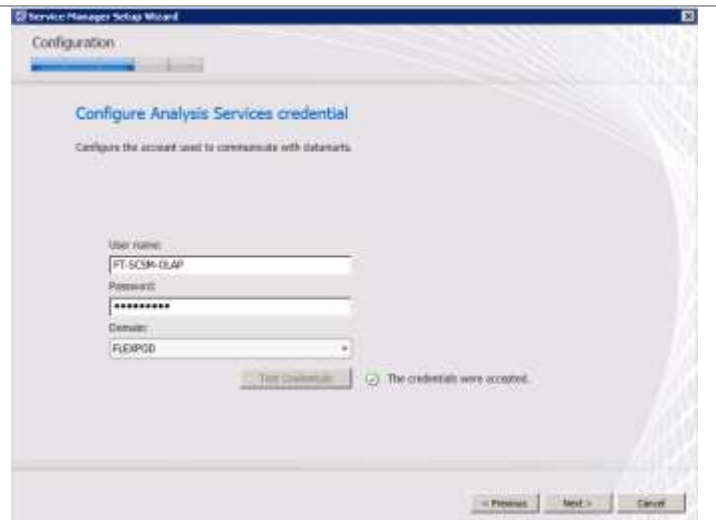
Confirm that the **Change database storage directory** check box is clear and click **Next** to continue.



In the **Configure Analysis Services Credential** dialog, specify the SM OLAP Account in the **User name** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

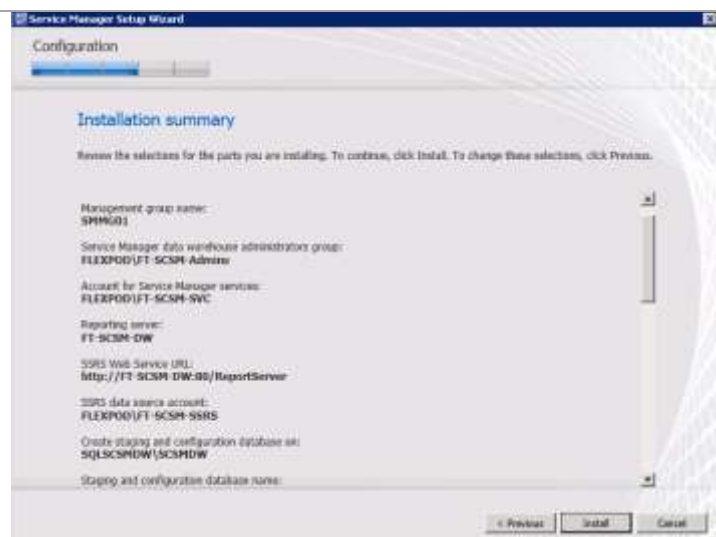
When successful, click **Next** to continue.



In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the Customer Experience Improvement Program (CEIP) by providing selected system information to Microsoft. Click **Next** to continue.

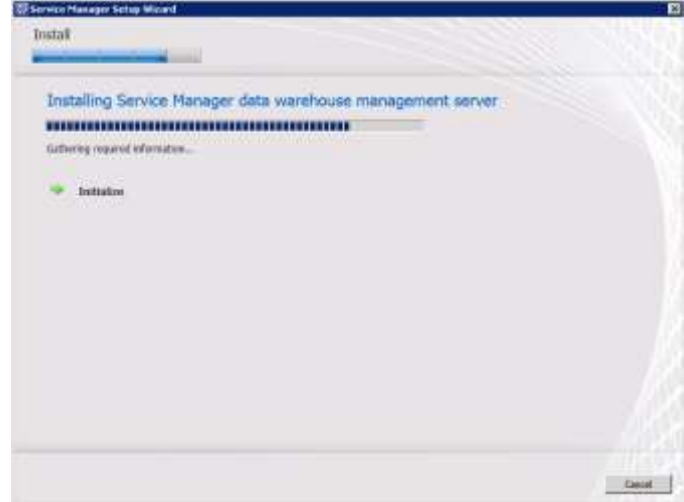


The **Installation summary** dialog will appear displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.

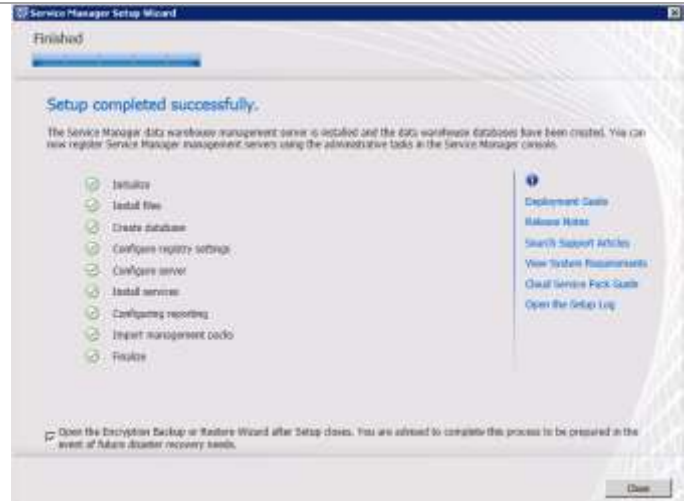




The wizard will display the progress while installing features.

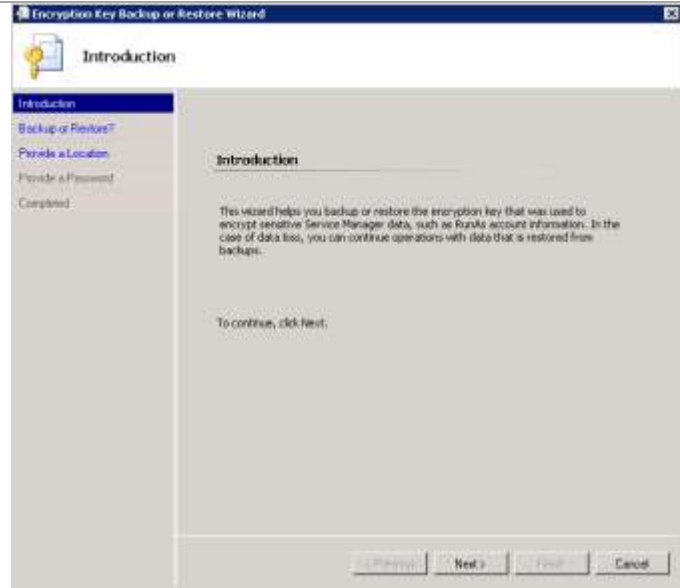


When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.

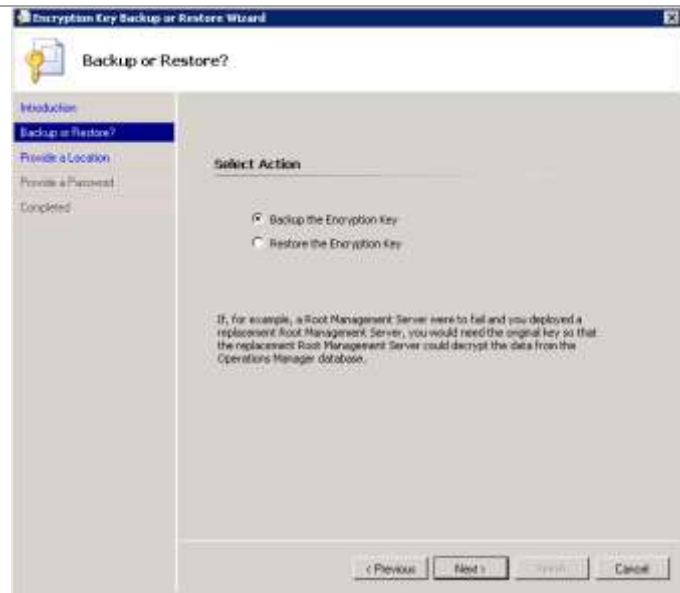




When the installation completes, the **Encryption Key Backup or Restore wizard** will appear. At the **Introduction** dialog, click **Next** to continue.



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** textbox and object picker. Click **Next** to continue.

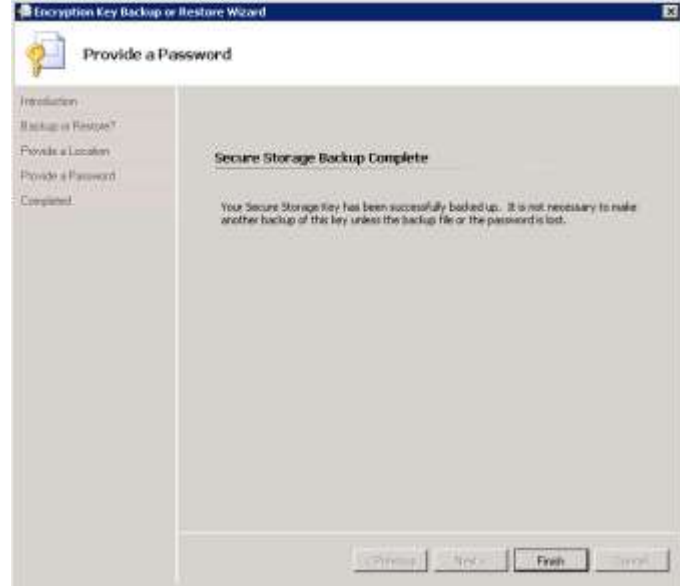
The screenshot shows the 'Encryption Key Backup or Restore Wizard' window, specifically the 'Provide a Location' step. The left sidebar contains a list of steps: Introduction, Backup or Restore?, Provide a Location (highlighted), Provide a Password, and Completed. The main area is titled 'Specify the Location of the Backup File'. It contains instructions: 'Please provide a location to which you want the encryption key backed up, or from which you want the encryption key restored.' and 'This location should not be on the same computer as the Host Management Server. Ideally, the location should be accessible in case of disaster. Examples: a shared folder on an offsite network, or a USB drive.' Below this is a 'Path' label and a text box containing the path '\\R-sql11-c:\SCSM_Key_Backup\PT-SCSM-OW_Backupkey.bin'. A 'Browse...' button is to the right of the text box. Below the text box is an example: 'Example: \\MyServer01\Backup\PT-SCSM-OW_Backupkey.bin'. At the bottom are buttons for '< Previous', 'Next >', '>>> Finish', and 'Cancel'.

In the **Provide a Password** dialog, specify a desired password in the **Password** textbox. Re-type the password in the **Confirm Password** textbox and click **Next** to begin the backup process.

The screenshot shows the 'Encryption Key Backup or Restore Wizard' window, specifically the 'Provide a Password' step. 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 contains instructions: '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 text boxes contain eight asterisks. Below the text boxes is the instruction 'Click Next to run the operation.' At the bottom are buttons for '< Previous', 'Next >', '>>> Finish', and 'Cancel'.



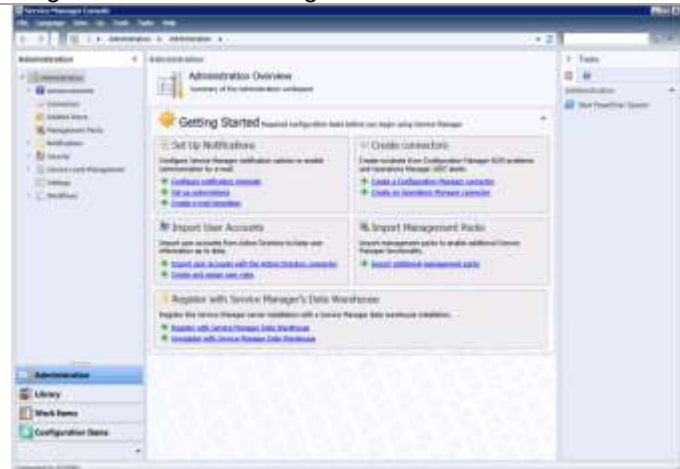
When complete, click **Finish** to exit the wizard.



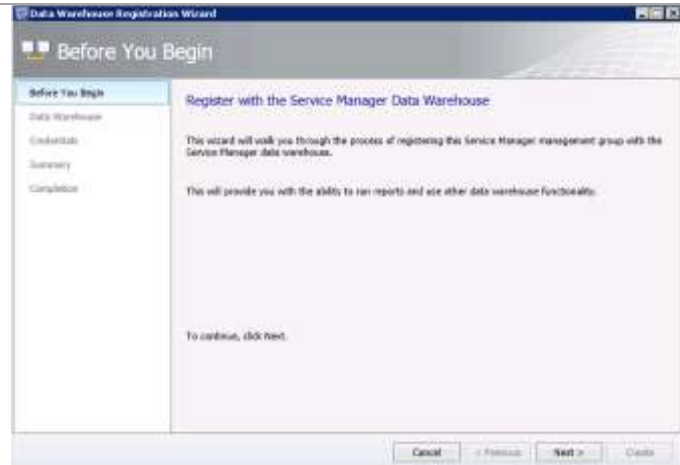
Perform the following steps on the **Service Manager Management Server** virtual machine to register the Service Manager Data Warehouse and enable reporting in the Service Manager instance.

Within the Service Manager Console, 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 in the **Server name** drop-down menu. When selected, click the **Test Connection** button to validate connectivity between the Service Manager management and Data Warehouse servers. Click **Next** to continue.

The screenshot shows the 'Data Warehouse Registration Wizard' window. The 'Data Warehouse' tab is selected in the left sidebar. The main area is titled 'Specify the data warehouse management server name'. It contains a 'Server name:' label and a dropdown menu showing 'FT-SCSM-DW-Flexpod-test'. Below this is a 'Test Connection' button. A green message states: 'Your connection to the data warehouse management server was successful.' A yellow warning icon and text below state: 'The current console user must have administrative privileges on the data warehouse management server.' At the bottom are buttons for 'Cancel', '< Previous', 'Next >', and 'Finish'.

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.

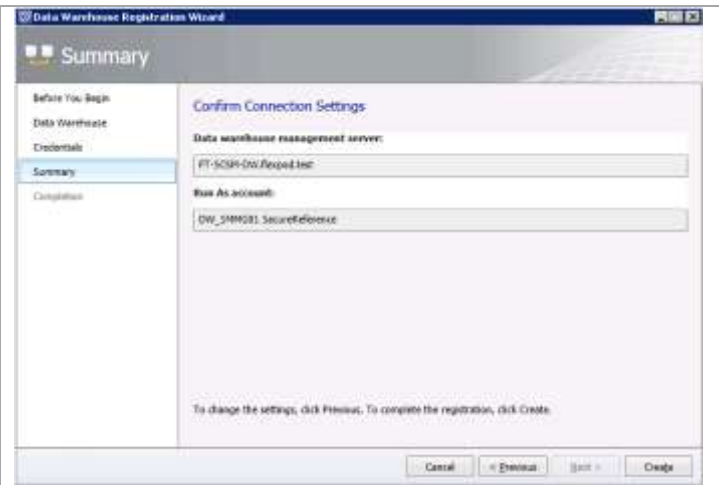
The screenshot shows the 'Data Warehouse Registration Wizard' window, 'Credentials' tab. The main area is titled 'Provide credentials for the data warehouse'. It contains instructions: 'Create or select the Run As account that the data warehouse will use to connect to this Service Manager installation. The account must have administrator privileges on this server.' Below is a 'Run As account:' label and a dropdown menu showing 'DW_SMSG01\ServiceReference'. A 'New...' button is to the right. A yellow warning icon and text below 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 are buttons for 'Cancel', '< Previous', 'Next >', and 'Finish'.

A **Credentials** dialog will appear prompting you for the password for the SM service account. When provided, click **OK** to continue.

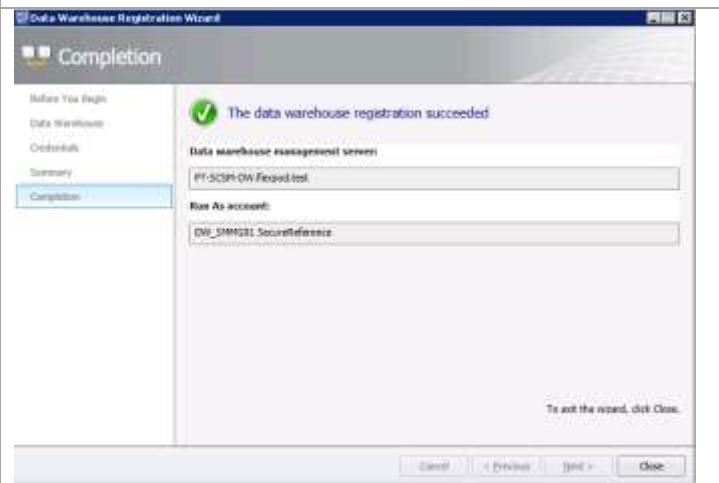
The screenshot shows a 'Credentials' dialog box. It has three input fields: 'User name:' with 'FT-SCSM-SVC', 'Password:' with '*****', and 'Domain:' with 'FLEXP0D'. At the bottom are 'OK' and 'Cancel' buttons.



The **Summary** dialog will appear, review the information that was provided earlier and click **Create** to begin the registration process.



The **Completion** dialog will show the successful registration of the Data Warehouse. Click **Close** to exit the wizard.

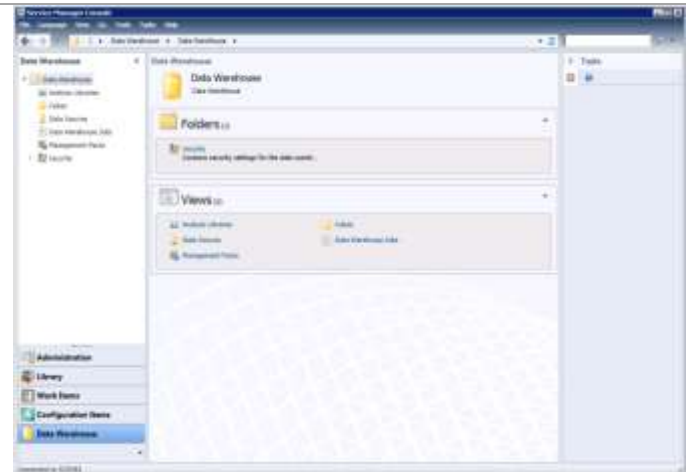


Note: the Data Warehouse registration process can take several hours for the registration process to complete. During this time several management packs are imported into the Data Warehouse server and several Data Warehouse jobs run.





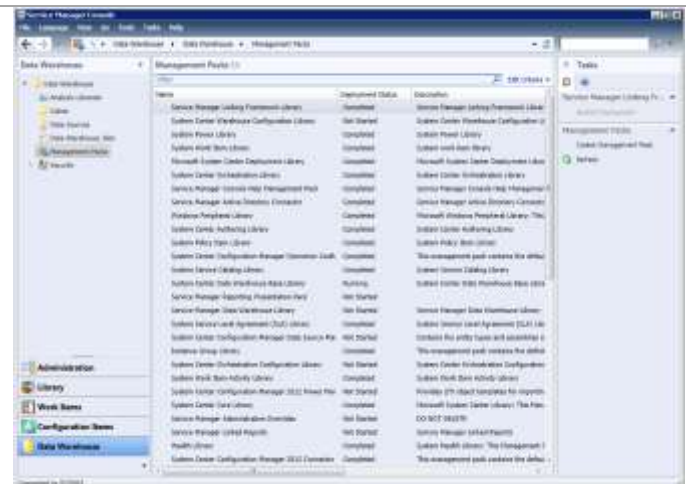
After a few minutes the **Data Warehouse** button will be added to the **Service Manager Console**.



Note: this deployment and association process can take up to two hours to complete.

The status of the management pack imports can be checked by selecting **Management Packs** in the **Data Warehouse** pane.

Deployment is complete when all listed management packs show a deployment status of **Completed**.





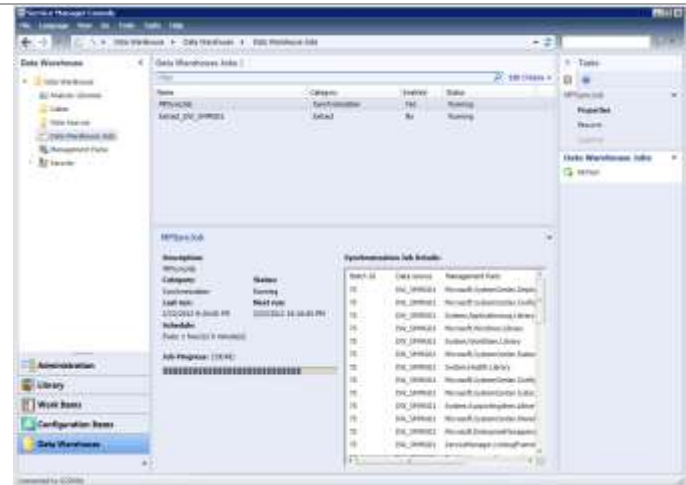
Note: this deployment and association process can take up to two hours to complete.

In the Data Warehouse pane, select Data Warehouse Jobs.

In the Data Warehouse Jobs pane, click MPSyncJob.

In the **MPSyncJob** details pane, in the **Synchronization Job Details** list, scroll to the right to view the **Status** column, and then click **Status** to alphabetically sort the status column.

Scroll through the **Status** list. The management pack deployment process is complete when the status for all of the management packs is **Associated** or **Imported**. Confirm that there is no status of either **Pending Association** or **Failed** in the status list. In the **Data Warehouse Jobs** pane, the status of the **MPSyncJob** will have changed from **Running** to **Not Started** when the registration process is complete.



Installing the Self-Service Portal Server

The following steps must to be completed in order to install the Service Manager Self-Service Portal server role.

Perform the following steps on the **System Center Service Manager Self-Service Portal** virtual machine.

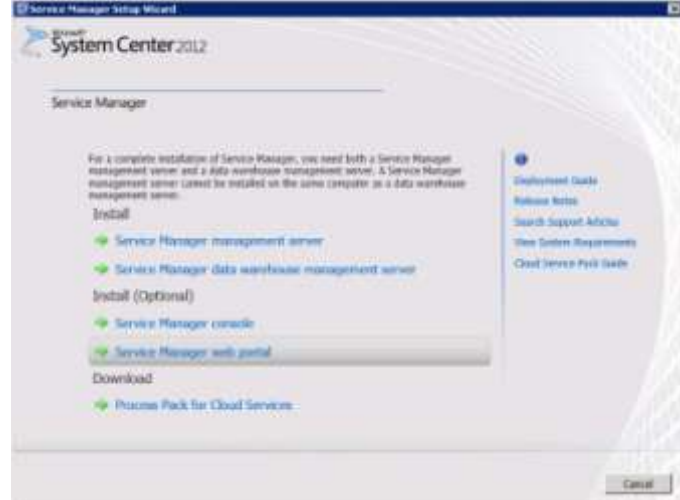
Log on to Service Manager self-service portal server (**NOT** the Service Manager management server or the Data Warehouse server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.



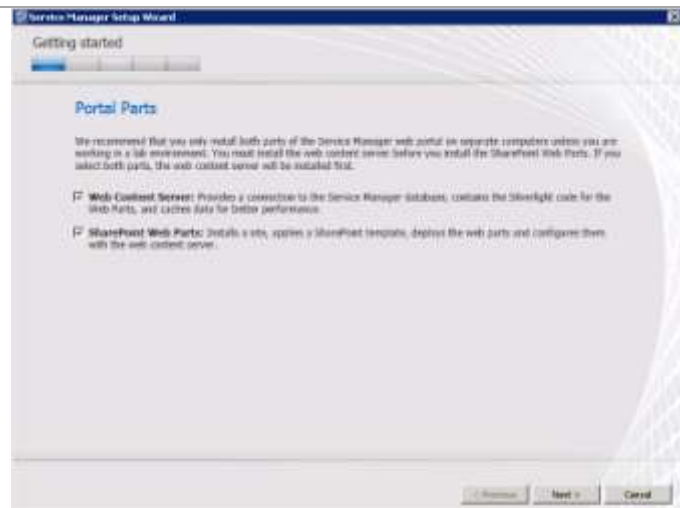


The Service Manager installation wizard will begin. At the splash page, navigate to the **Install** section and click **Service Manager web portal** to begin the Service Manager self-service portal server installation.



The Service Manager Setup Wizard will open. In the Portal Parts dialog, select the Web Content Server and SharePoint Web Parts check boxes and click Next to continue.

Note: the warning about installing both Portal Parts on a single server can be safely ignored. The setup wizard assumes that the SharePoint Farm is using a local SQL Server installation whereas the Fast Track design uses a dedicated SQL Server instance for the SharePoint farm drastically reducing the load on the SharePoint Web Parts installation.



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

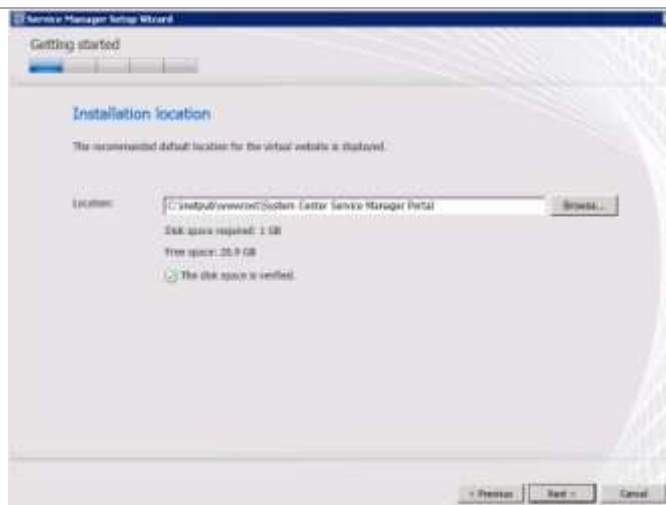
- **Name** – specify the name of primary user or responsible party within your organization.
- **Organization** – specify the name of the licensed organization.

In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.

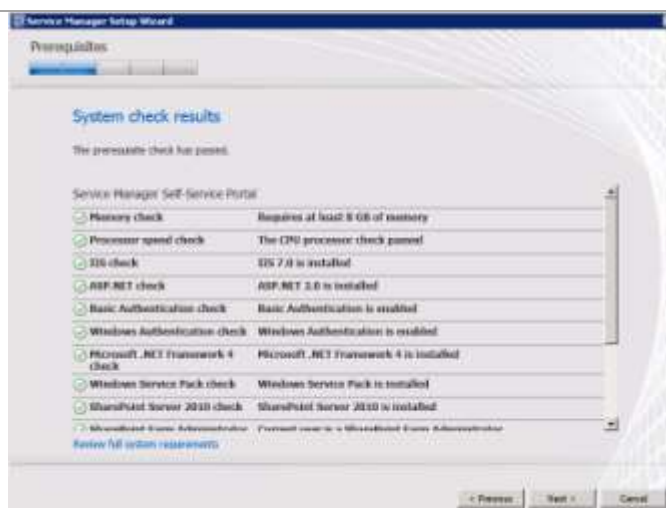




In the **Installation location** dialog, specify a specific location or accept the default location of *C:\inetpub\wwwroot\System Center Service Manager Portal* for the installation. Click **Next** to continue.



The setup will verify that all system pre-requisites are met in the **System check results** dialog. If any pre-requisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





In the **Configure the Service Manager Self-Service Portal name and port** dialog, specify the following information in the provided text boxes:

- **Website name** – specify the name of the website used for the self-service portal. In most cases, the default name of 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.

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 installation management server.
- **SQL Server instance** – specify the SQL Server database instance created for the Service Manager installation management server.
- **Database** – specify the name of the Service Manager database configured earlier. In most cases the default value of ServiceManager should be used.

Click **Next** to continue.



In the **Configure the account for the Self-Service Portal** dialog, verify that the **Domain account** option is selected and specify the SM Service Account in the **User name** textbox. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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

Service Manager Setup Wizard

Configuration

Configure the account for the Self-Service Portal

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 Administrator's user role.

☐ Local System account

☒ Domain account:

User name: FT-GSM-SVC

Password: *****

Domain: RLENPOD

Test Credentials

The credentials were accepted.

< Previous Next > 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.
 - **SQL Server instance** – specify the SQL Server database instance created for the Service Manager installation SharePoint Farm.
 - **Database server** – specify the database name for the portal. In most cases, the default value of SharePoint_SMPortalContent will be used.

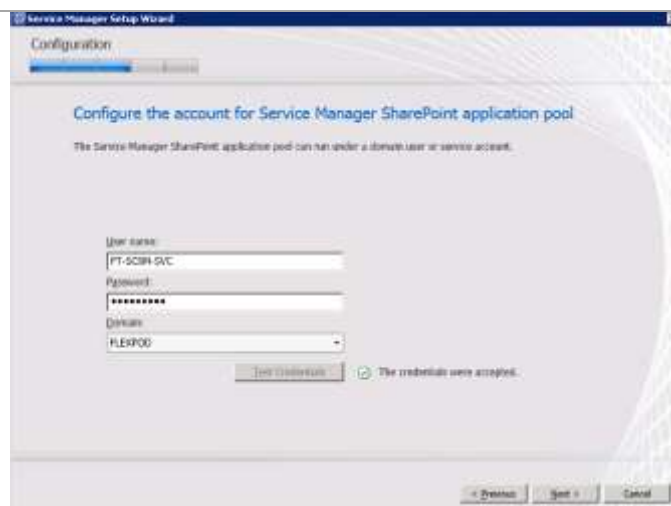
Click **Next** to continue.



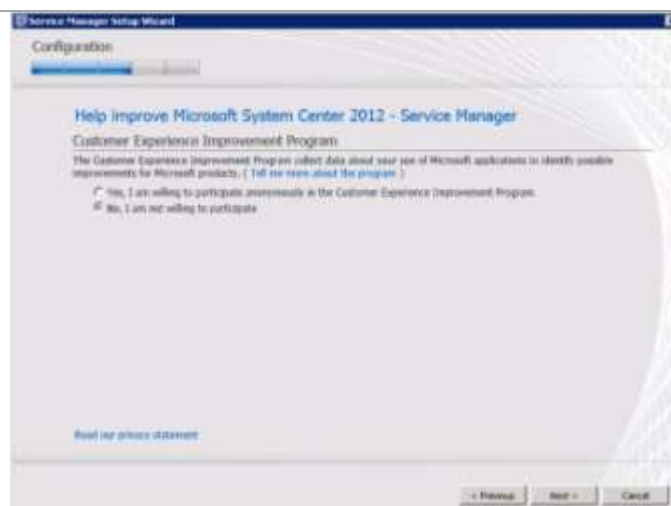
In the **Configure the account for Service Manager SharePoint application pool** dialog, specify the SM Service Account in the **User name** textbox. Provide the appropriate **Password** and **Domain** in the provided textbox and drop-down menu.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

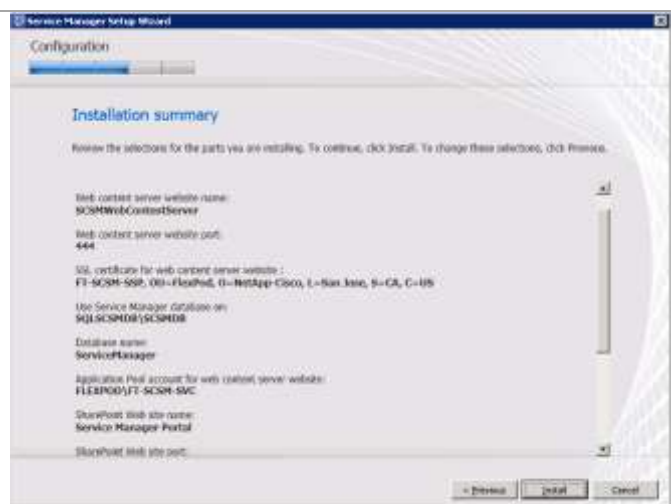
When successful, click **Next** to continue.



In the **Help improve Microsoft System Center 2012** dialog, select the option to either participate or not participate in the Customer Experience Improvement Program (CEIP) by providing selected system information to Microsoft. Click **Next** to continue.

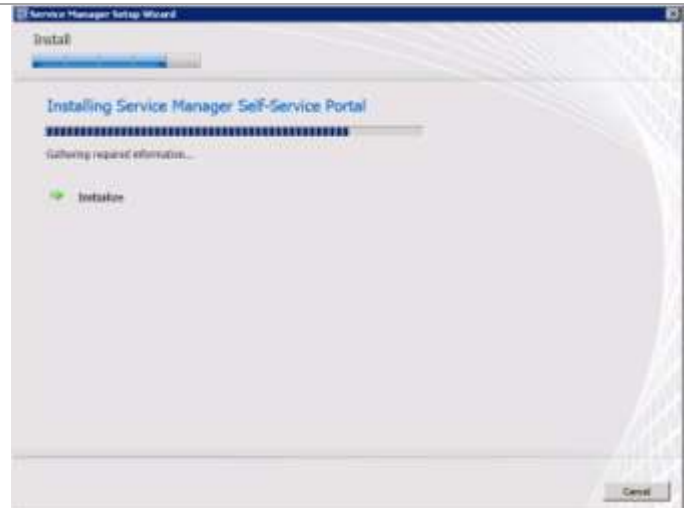


The **Installation summary** dialog will appear displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.



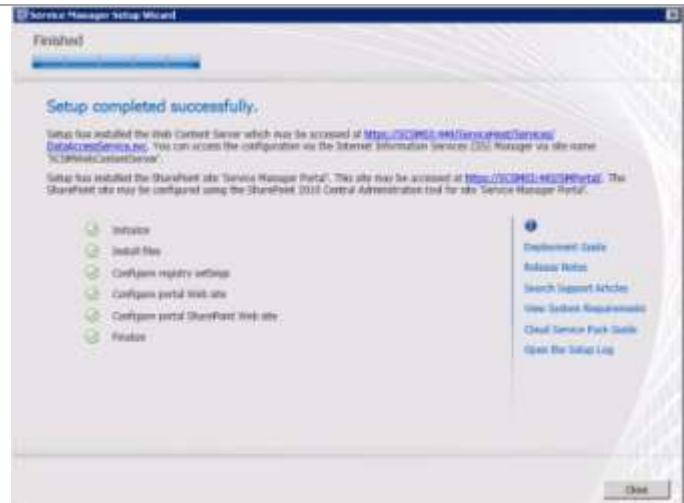


The wizard will display the progress while installing features.



When completed, the Service Manager Setup Wizard will display the **Setup completed successfully** dialog. Click **Close** to finish the installation.

Note the SMPortal link provided in the dialog.



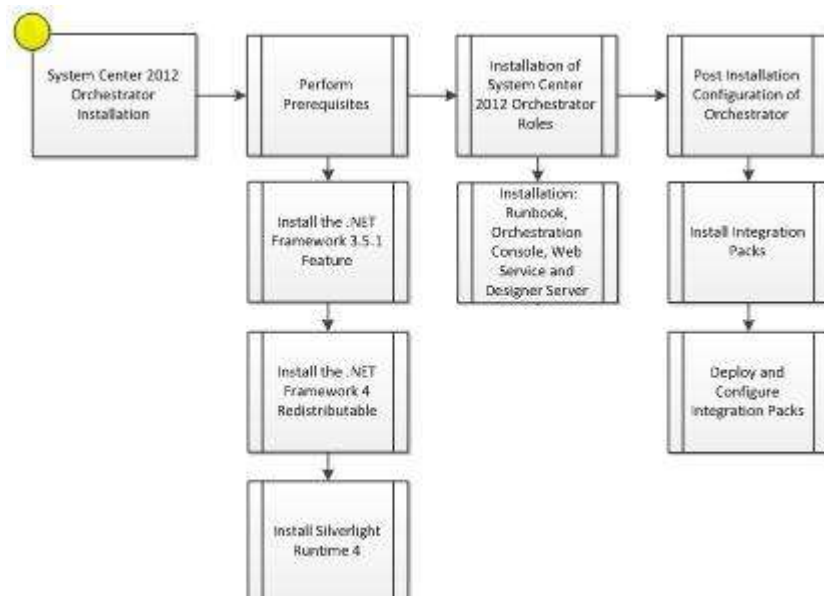
From Internet Explorer, open the Service Manager Self-Service Portal at <https://<servername>/SMPortal>.

Confirm all sections display as expected.



Orchestrator

The Orchestrator installation process is comprised of the following high-level steps:



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 2008 R2 (x64) have been provisioned.
- A two-node, SQL Server 2008 R2 cluster with dedicated instance has been established in previous steps for Orchestrator.
- The .NET Framework 3.5.1 Feature is installed.
- The .NET Framework 4 Redistributable is installed.



Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User Name	Purpose	Permissions
<DOMAIN>\FT-SCORCH-SVC	Orchestrator service account	This account will need: Full admin permissions on all target systems to be managed. Log on As a Service rights (User Rights) <i>Sysadmin</i> on the SQL Server, or dbo rights to the Orchestrator database after its created This account will need to be a member in the following groups: FT-VMM-Admins

Groups

Verify that the following security groups have been created:

Security group name	Group scope	Members	Member of
<DOMAIN>\FT-SCO-Operators	Global	<DOMAIN>\FT-SCO-SVC	
<DOMAIN>\FT-SCO-Admins	Global	<DOMAIN>\FT-SCO-SVC	Local Administrators Target Active Directory domain BUILTIN\Distributed COM Users

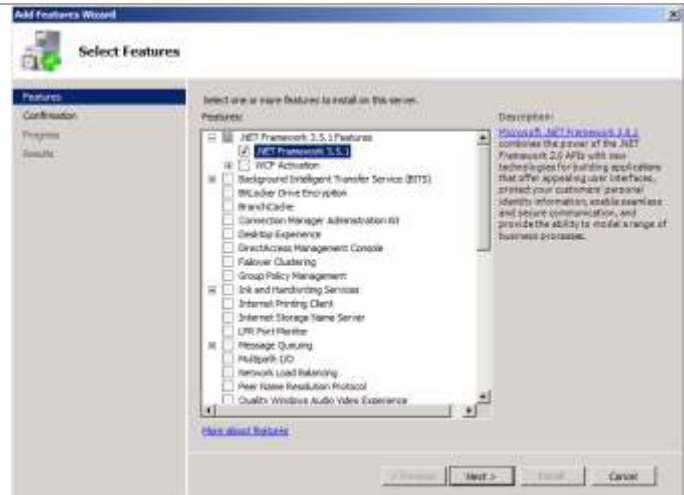
Adding the .NET Framework 3.5.1 Feature

The Orchestrator installation requires the .NET Framework 3.5.1 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5.1 Feature.

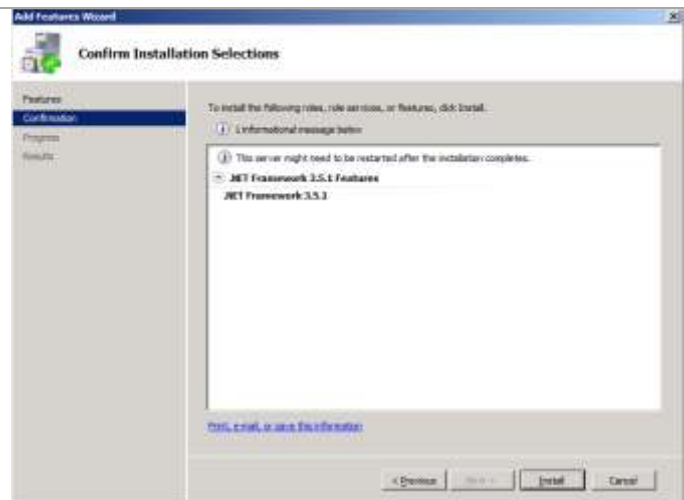
Perform the following steps on the **Orchestrator** virtual machine.



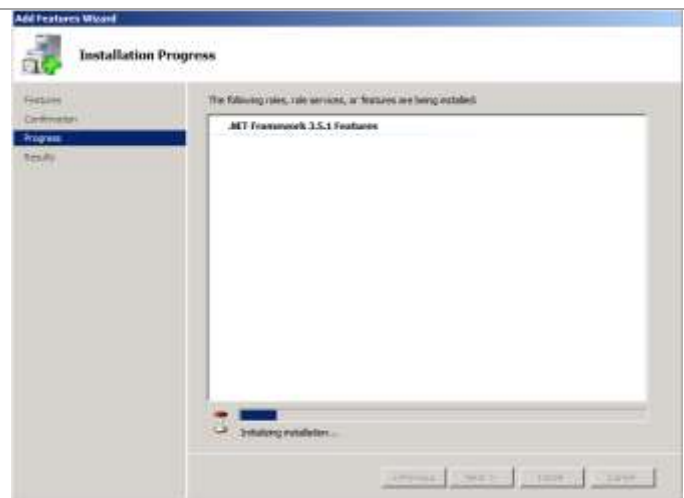
To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features**, and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.



In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.

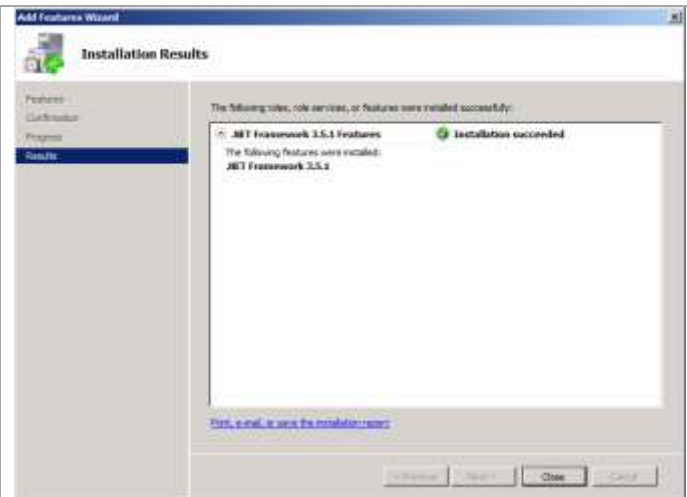


The **Installation Progress** dialog will show the progress of the feature install.





When complete, the **Installation Results** dialog will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.



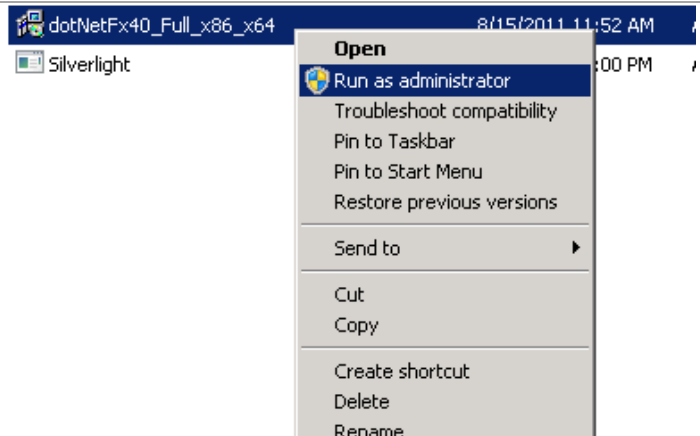


Installing .NET Framework 4

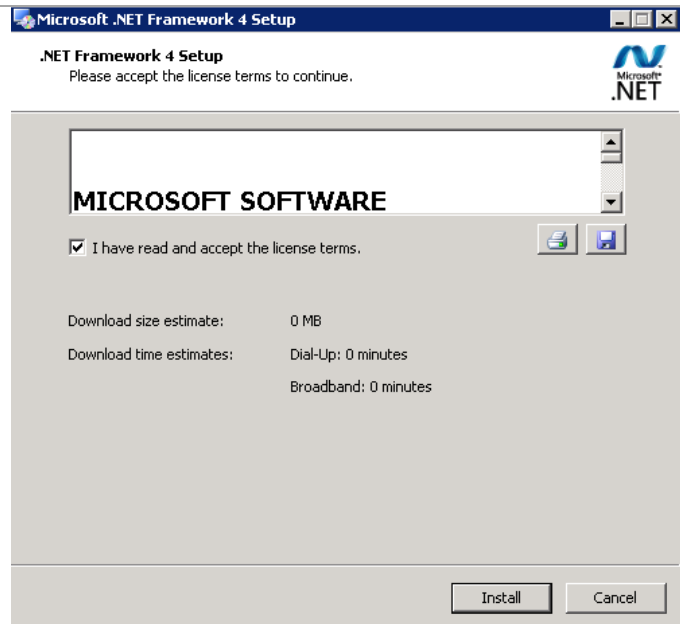
Additionally, the Orchestrator portal installation also requires the .NET Framework 4 package be installed prior to installation. Follow the provided steps to install the .NET Framework 4 package.

Perform the following steps on the **Orchestrator** 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.

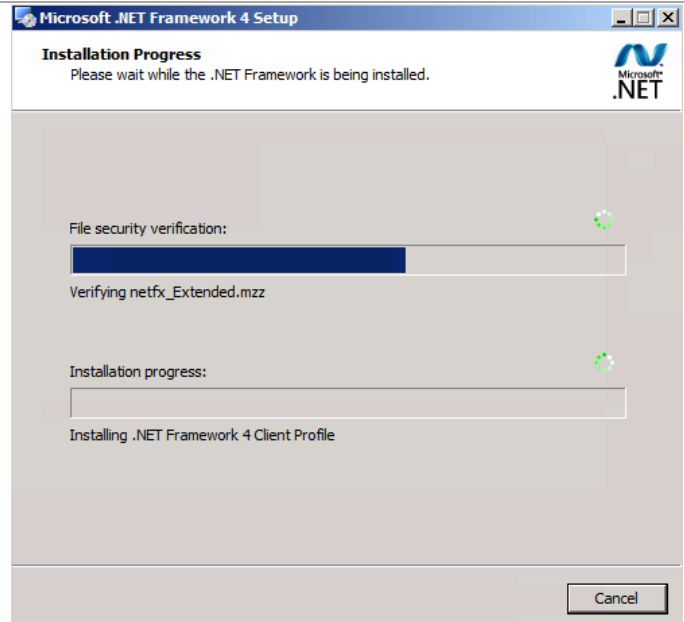


Within the Microsoft .NET Framework 4 Setup dialog, select the I have read and accept the license terms checkbox and click Install to begin the installation.

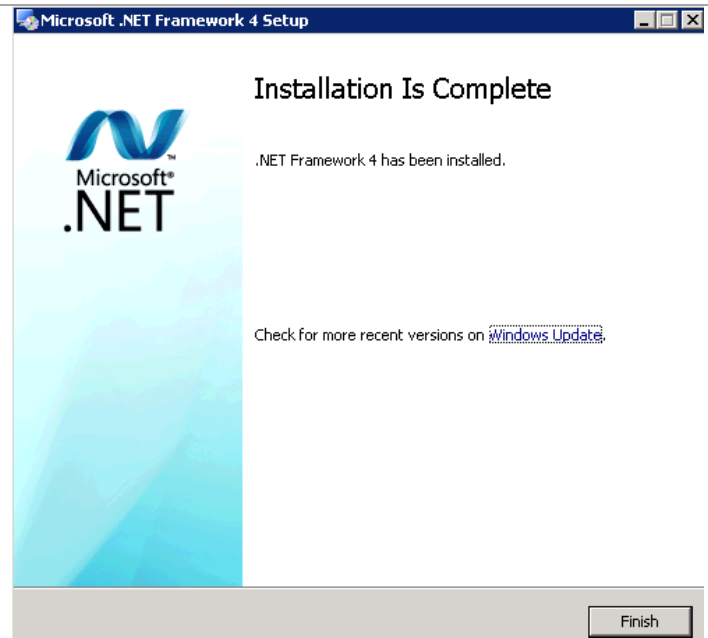




The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.

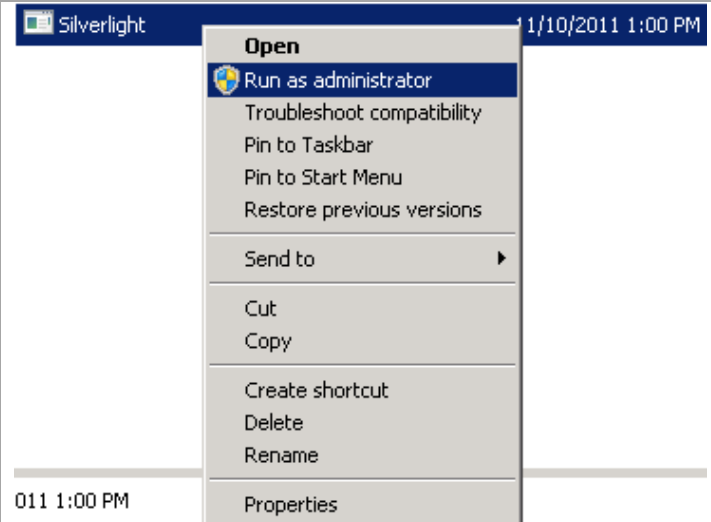




Installing Silverlight Runtime 4

Perform the following steps on the **Orchestrator** virtual machine.

From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** from the context menu to begin setup.



In the Install Silverlight dialog, click Install now.



In the **Enable Microsoft Update** dialog, select or clear the **Enable Microsoft Update** check box based on organizational preferences and click **Next** to continue.





In the **Installation Successful** dialog, click **Close** to exit the installation.



Installing Runbook, Orchestration Console, Web Service, and Designer Server

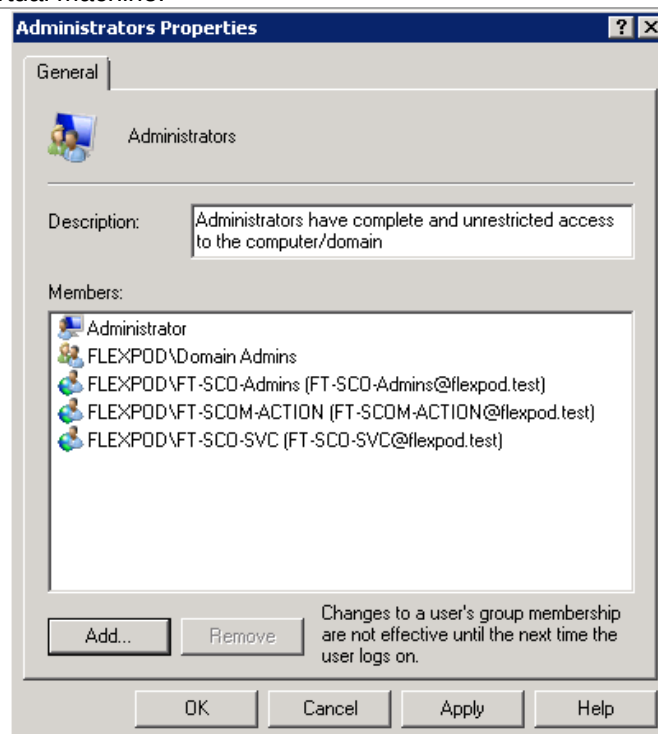
The following steps need to be completed in order to install the Orchestrator Runbook Server component.

Perform the following steps on the **Orchestrator** virtual machine.

Log on to the Orchestrator virtual machine with a user with local admin rights.

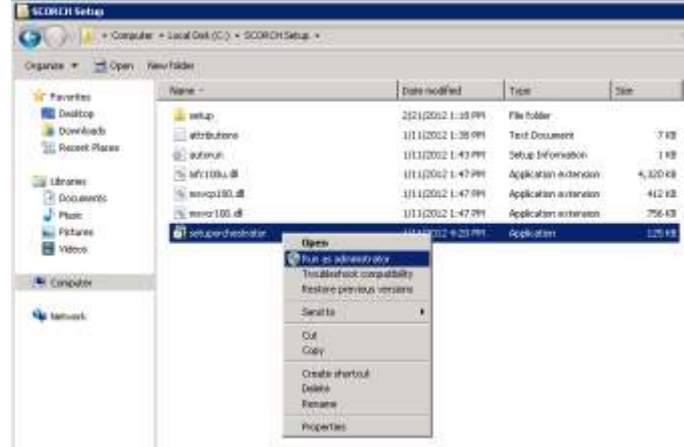
Verify that the following accounts and/or groups are members of the Local Administrators group on the Orchestrator virtual machine:

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

Click **Next** to continue.

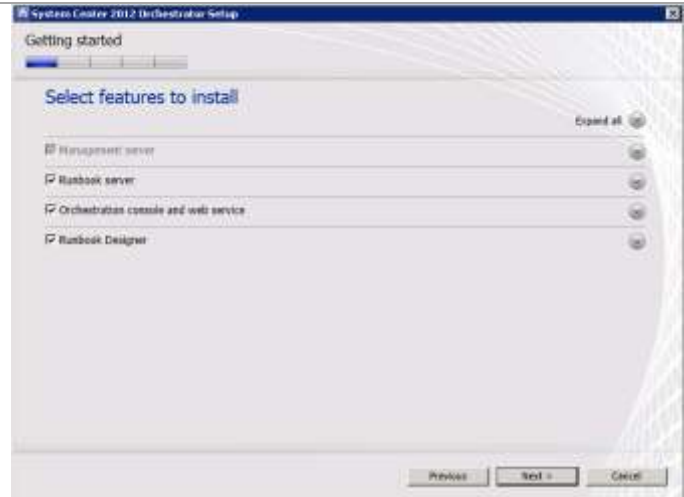




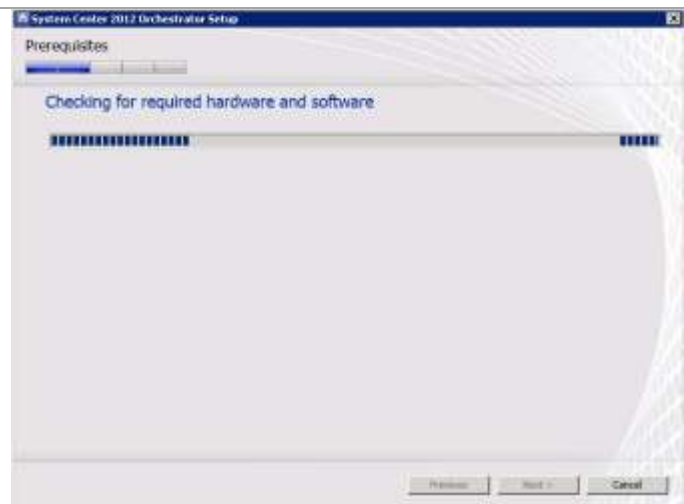
In the **Please read this License Terms** dialog, verify that the **I accept the license terms** installation option check box is selected and click **Next** to continue.



In the Select Features to install dialog, select the Management Server (default selected), Runbook server, Orchestration console and web service, Runbook Designer check boxes and click Next to continue.

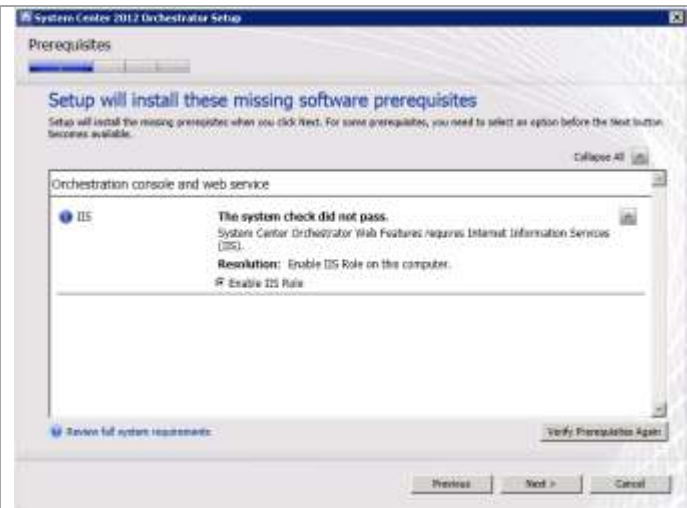


The **Checking for required hardware and software** dialog will appear to verify the installation prerequisites. When validation completes click **Next** to continue.





The Orchestrator setup will identify any prerequisite software required for the installation to complete. The **Setup will install these missing software prerequisites** dialog will attempt to perform the installation of missing prerequisites. When completed, click **Next** to continue.



When the installation of the missing prerequisites is completed, click **Next** to continue.



In the **Configuration the service account** dialog, specify the Orchestrator service account in the **Username** text box. Provide the appropriate **Password** and **Domain** in the provided text box and drop-down menu.

Before proceeding, click the **Test** button to verify the credentials provided.

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





In the **Configure the database server** dialog, enter the following information in the provided text boxes:

- **Server** – specify the SQL Server cluster name and instance name created in the steps above.
- **Port** – specify the TCP port used for the SQL Server if not the default.

In the Authentication Credentials section, select the Windows Authentication option and click the Test Database Connection button.

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

In the **Configure the database** dialog in the **Database** section, select the **New Database** option. Specify the default database name of *Orchestrator*.

Click **Next** to continue.

In the **Configure Orchestrator users group** dialog select the Orchestrator users group created earlier using the object picker by clicking **Browse...** and selecting the associated group.

Verify that that the **Grant remote access to the Runbook Designer** check box is selected and click **Next** to continue.



In the **Configure the ports for the web services** dialog, provide the following information in the provided text boxes:

- **Web Service Port** – Specify the TCP port used for the Orchestrator Web Service. The default value of 81 is recommended.
- **Orchestration console port**- Specify the TCP port used for the Orchestrator console port. The default value of 82 is recommended.

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

System Center 2012 Orchestrator Setup

Configuration

Configure the ports for the web services

Choose an available port on the local computer where the web service is being installed. This port number will be used to create a new website in Internet Information Services (IIS) to host the web service application.

To learn more about how these ports will be used, see the [Orchestrator deployment guide](#).

Web service port:
81

Orchestration console port:
82

Previous Next Cancel

In the **Select the installation location** dialog, specify a specific location or accept the default location of `%ProgramFiles(x86)%\Microsoft System Center 2012\Orchestrator` for the installation. Click **Next** to continue.

System Center 2012 Orchestrator Setup

Configuration

Select the installation location

The recommended location for program files is displayed.

Location: C:\Program Files (x86)\Microsoft System Center 2012\Orchestrator Browse...

Previous Next Cancel

The **Help Improve Microsoft System Center Orchestrator** dialog provides options for participating in various product feedback mechanisms. These include:

- CEIP
- Error Reporting

Select the appropriate option based on your organization's policies and click **Next** to continue.

System Center 2012 Orchestrator Setup

Help with System Center 2012 Orchestrator

Help improve Microsoft System Center Orchestrator

Customer Experience Improvement Program

The Customer Experience Improvement Program collects data about your use of Microsoft applications to identify possible improvements for Microsoft products. [\(Tell me more about the program\)](#)

☒ 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 Orchestrator. [\(Tell me more about the program\)](#)

☒ 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

[Read our privacy statement.](#)

Previous Next Cancel



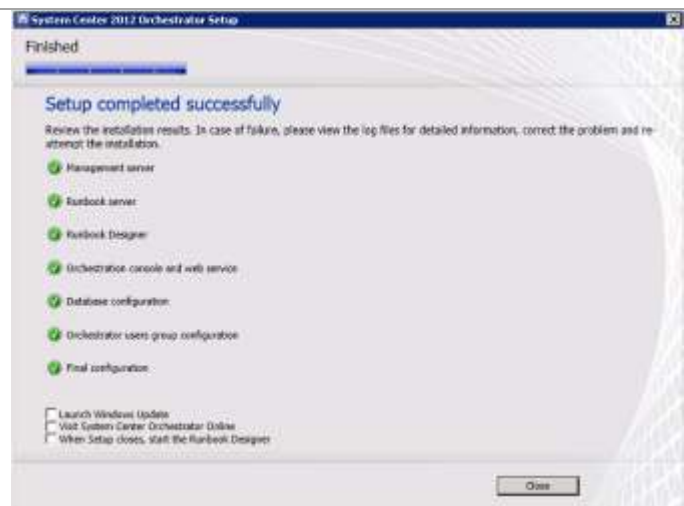
The **Installation summary** dialog will appear displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.



In the **Installing features** dialog, the installation will proceed and show progress.

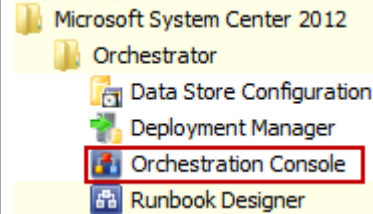


The **Setup completed successfully** dialog will appear when all portions of setup complete successfully. Verify that all check boxes are cleared and click **Close** to finish the installation.

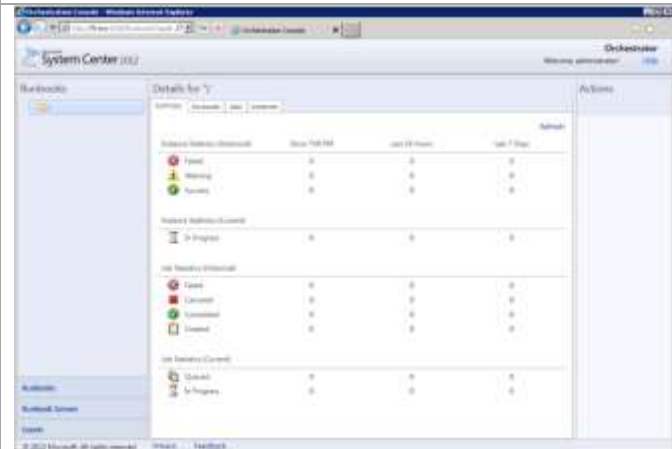




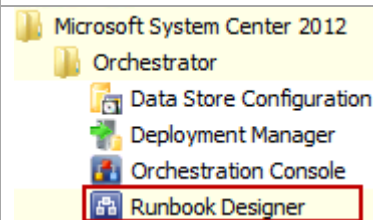
When installed, verify that the Orchestrator roles installed properly by opening the consoles. From the **Start Menu**, navigate to **Microsoft System Center 2012** then select the **Orchestrator** folder and click the **Orchestration Console** shortcut.



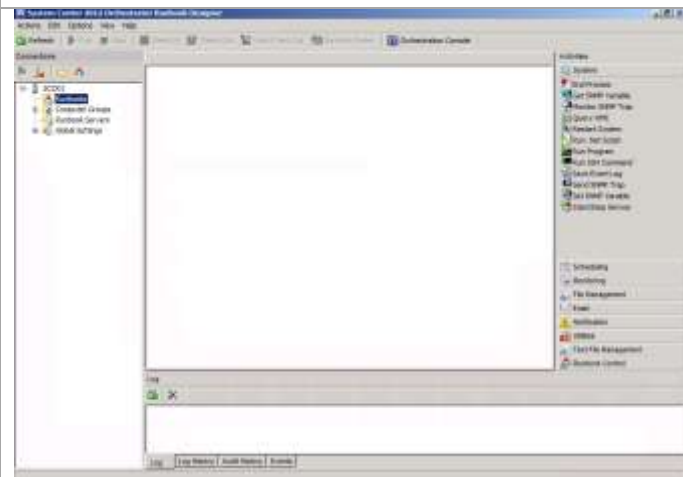
Validate that the **Orchestration console** performs properly in Internet Explorer.



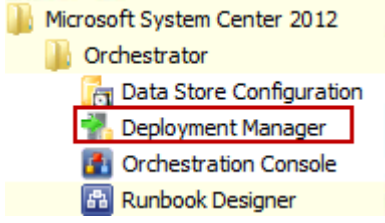
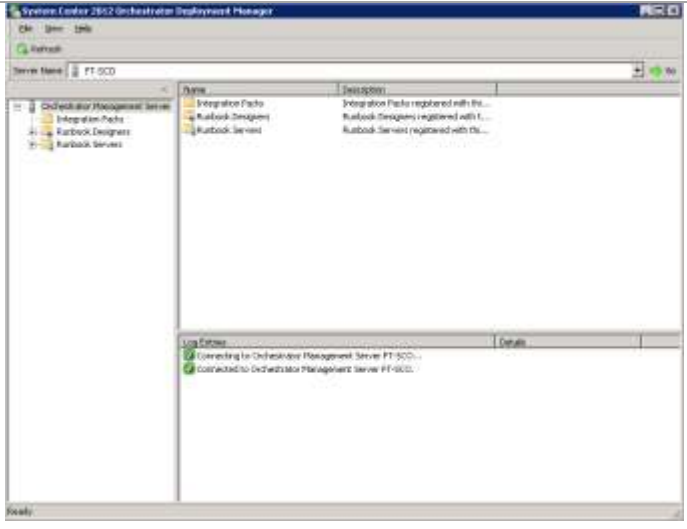
From the **Start Menu**, navigate to the **Microsoft System Center 2012** then select the **Orchestrator** folder and click the **Runbook Designer** shortcut.



Launch the **Runbook Designer** console and verify that it performs properly.





From the Start Menu, navigate to the Microsoft System Center 2012 then select the Orchestrator folder and click the Deployment Manager shortcut.	
Launch the Deployment Manager console and verify that it performs properly.	
Configure Windows Firewall for the first Orchestrator Runbook Server.¹⁸ If you wish to leave the Windows Firewall enabled you must first enable the following rules in Windows Firewall: • Windows Management Instrumentation (WMI-In). • Windows Management Instrumentation (DCOM-In). • Windows Management Instrumentation (ASync-In). Right-click each rule and select Enable Rule from the context menu.	

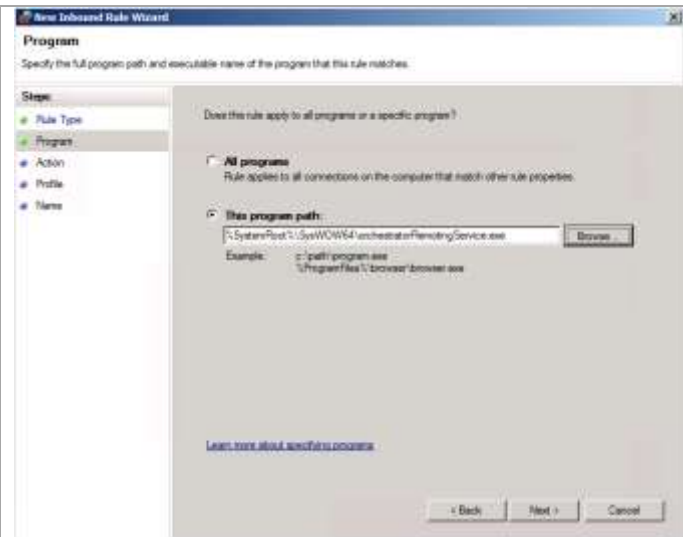
¹⁸ Orchestrator guidance is provided from the following TechNet resources: Using Windows Firewall with Orchestrator - <http://technet.microsoft.com/en-us/library/hh912321.aspx> and TCP Port Requirements <http://technet.microsoft.com/en-us/library/hh420382.aspx>.



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).



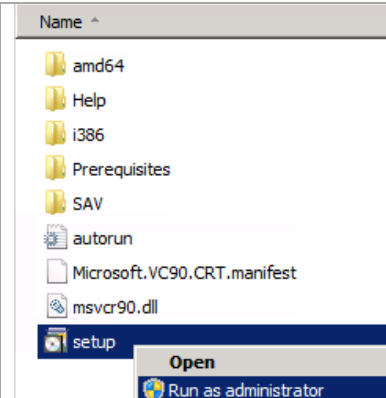
Post Installation Tasks

When the installation is complete, the installation and configuration of Orchestrator Integration Packs on the target Runbook Servers.

Installing the Virtual Machine Manager Console

Perform the following steps on the **Orchestrator** virtual machine.

Log on to the Orchestrator server with a privileged user account that has Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

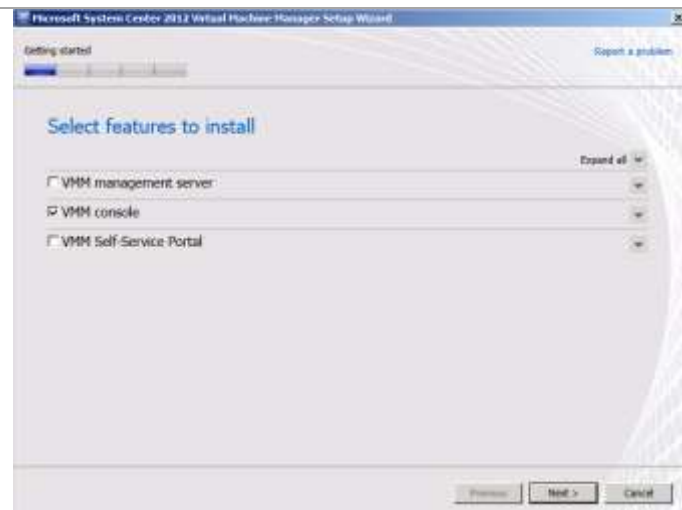




The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.



In the **Select features to install** dialog, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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

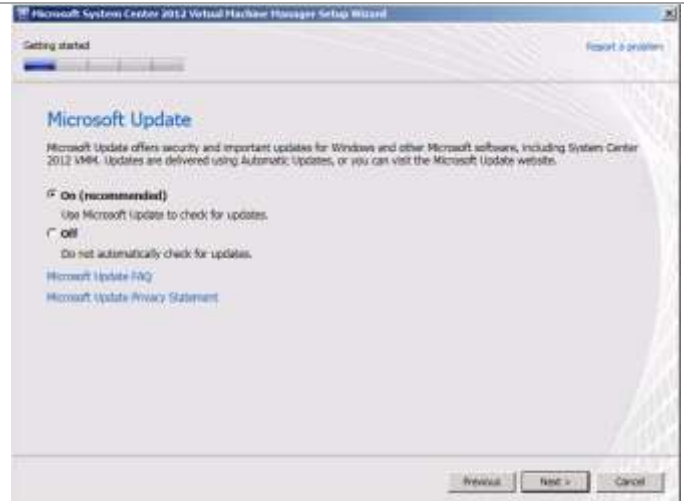




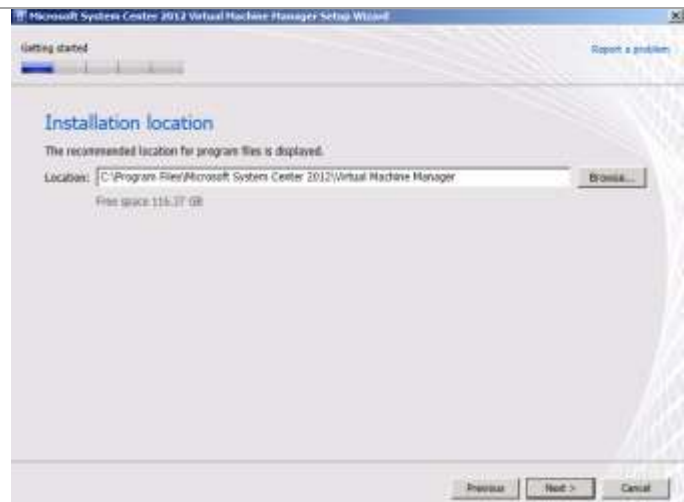
In the Customer Experience Improvement Program dialog, click Next to continue.



In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center Operations Manager 2012* for the installation. Click **Next** to continue.

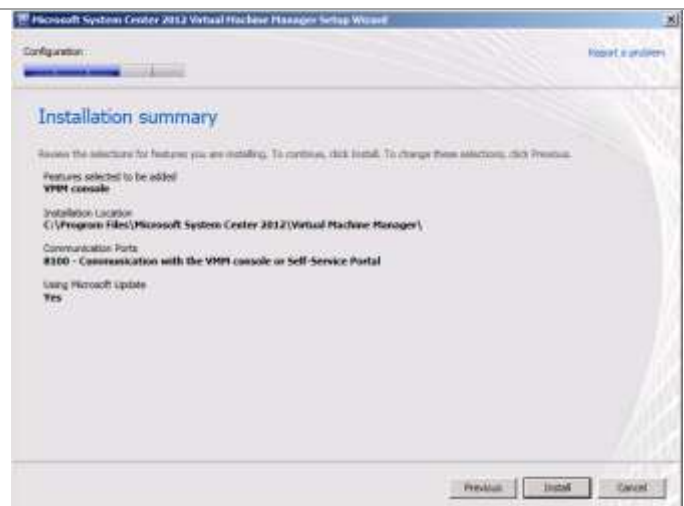




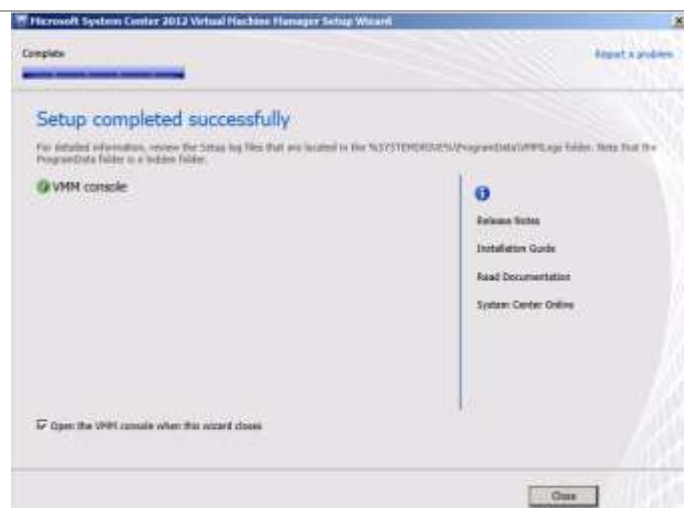
In the **Port Configuration** dialog, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



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



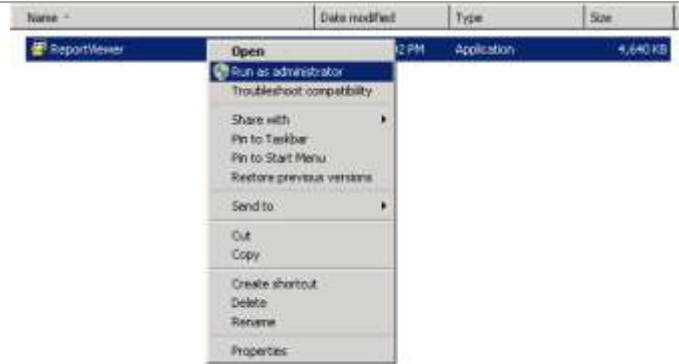


Installing the Microsoft Report Viewer 2010 SP1

Additionally, the Operations Manager console installation also requires the Microsoft Report Viewer 2010 SP1 package be installed prior to installation.¹⁹ Follow the provided steps to install the SP1 package.

Perform the following steps on each **Orchestrator** virtual machine.

From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** from the context menu to begin setup.



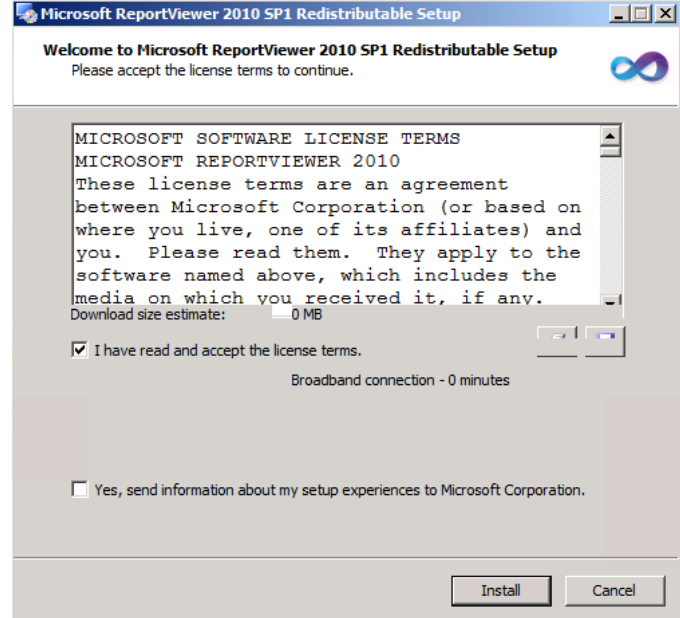
Within the Microsoft ReportViewer 2010 SP1 Redistributable Setup dialog, select Next to begin the installation.



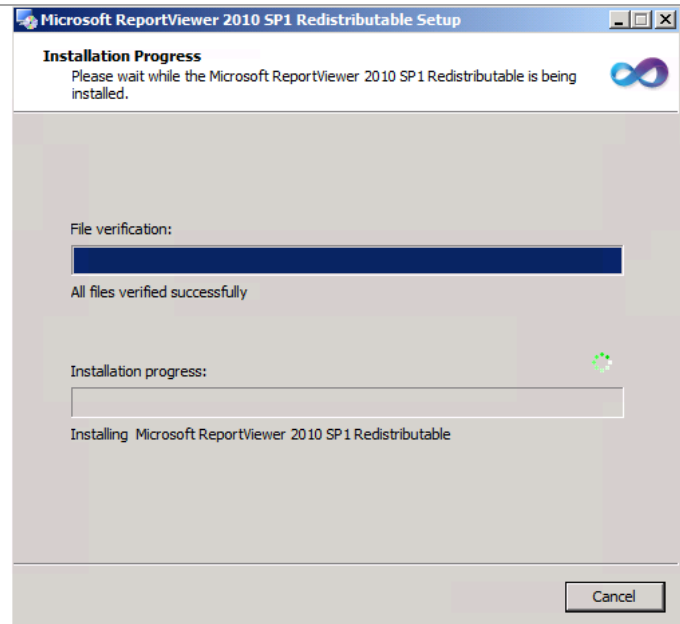
¹⁹ Microsoft Report Viewer 2010 SP1 Redistributable Package - <http://www.microsoft.com/downloads/details.aspx?FamilyID=3EB83C28-A79E-45EE-96D0-41BC42C70D5D&displaylang=r&displaylang=en>.



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.





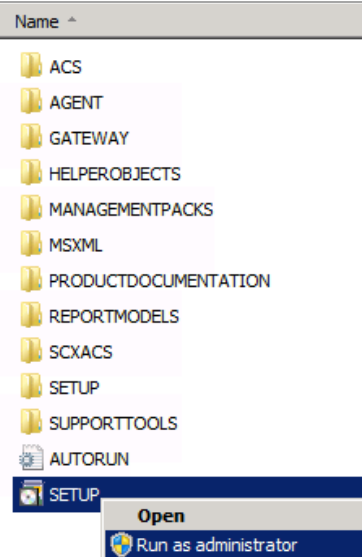
When completed, click **Finish** to exit the installation.



Installing the Operations Manager Console

Perform the following steps on the **Orchestrator** virtual machine. For Pattern 1 installations, perform these steps on **both** servers.

From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

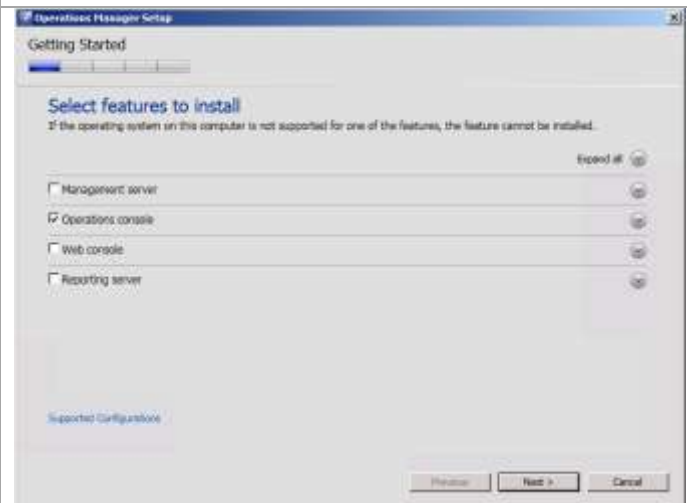




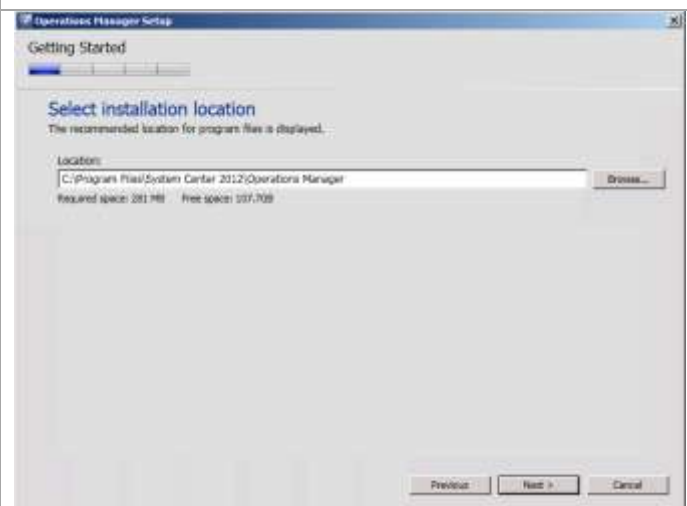
The Operations Manager installation wizard will begin. At the splash page, click **Install** to begin the Operations Manager console installation.



In the **Select features to install** dialog, verify that the **Operations console** check box is selected. Click **Next** to continue.



In the **Select installation location** dialog, specify a location or accept the default location of *%ProgramFiles%\System Center 2012\Operations Manager* for the installation. Click **Next** to continue.

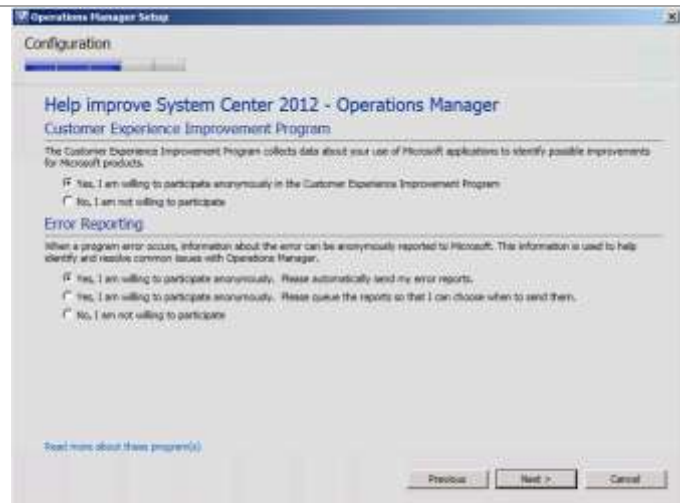




The **Help Improve Operations Manager 2012** dialog provides options for participating in various product feedback mechanisms. These include:

- 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.



When the installation completes, the wizard will display the **Setup is complete** dialog. Verify that the **Launch the Operations console when the wizard closes** check box is selected and click **Close** to complete the installation.

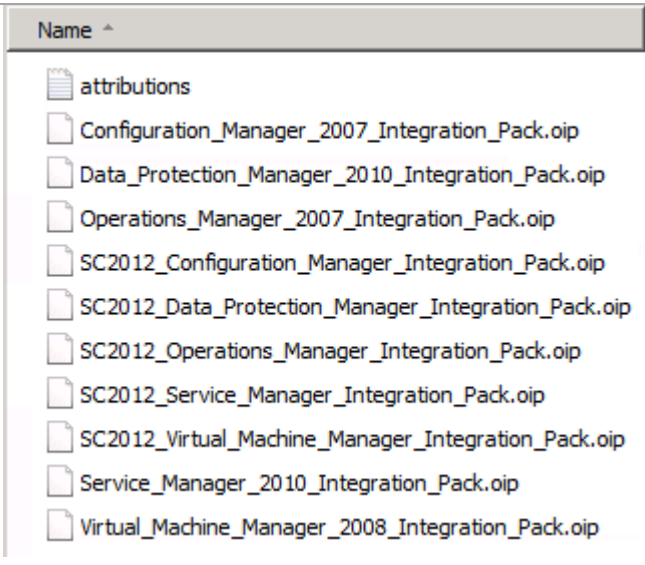
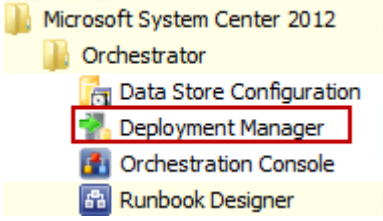


[illegible]



Installing the System Center Integration Packs

The following steps need to be completed in order to install the Orchestrator Integration Packs.²⁰

Perform the following steps on the Orchestrator Runbook Server virtual machine.	
Download the System Center 2012 Integration Packs from http://technet.microsoft.com/en-us/library/hh830706.aspx ²¹ and expand them to a single location so the Orchestrator Integration Pack files are expanded.	
From the Start Menu , navigate to the Microsoft System Center 2012 then select the Orchestrator folder and click the Deployment Manager shortcut.	
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.	

²⁰ System Center 2012 – Orchestrator Component Add-ons and Extensions - <http://www.microsoft.com/download/en/details.aspx?id=28725>.

²¹ The actual download link for the integration packs installed for Fast Track can be found directly at <http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28725>.

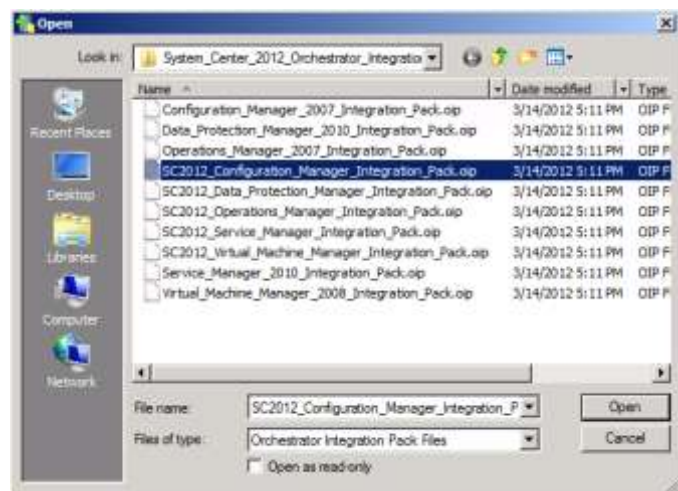
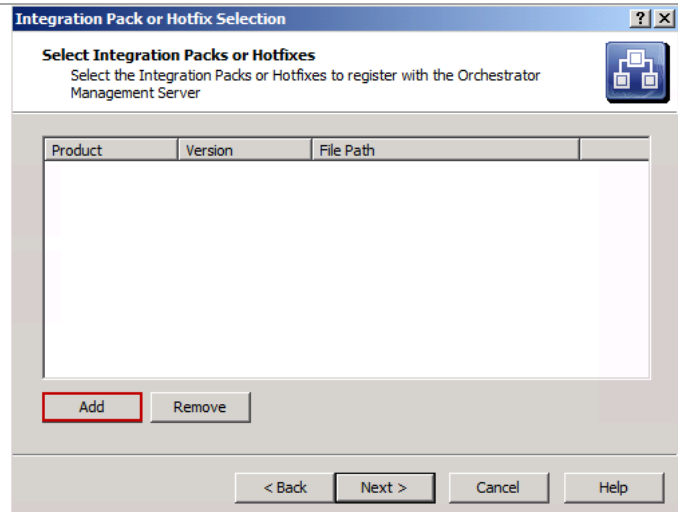


The Integration Pack Registration Wizard will appear. Click Next to continue.



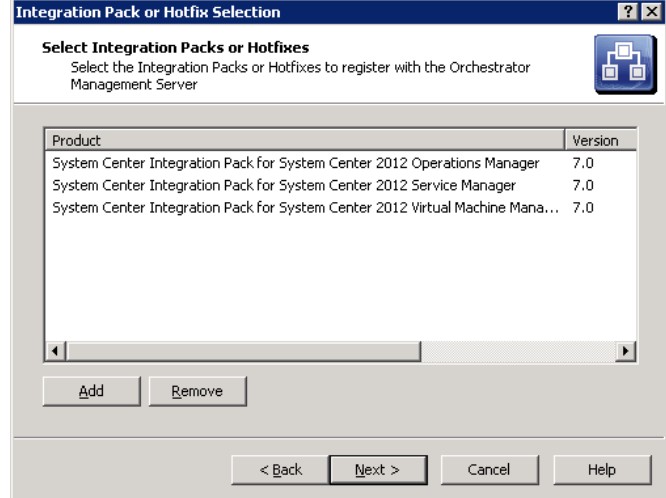
In the **Select Integration Packs or Hotfixes** dialog, click **Add**. Navigate to the expanded integration packs folder created earlier and select the following integration packs and click **Open**:

- System Center 2012 Operations Manager.
- System Center 2012 Service Manager.
- System Center 2012 Virtual Machine Manager.

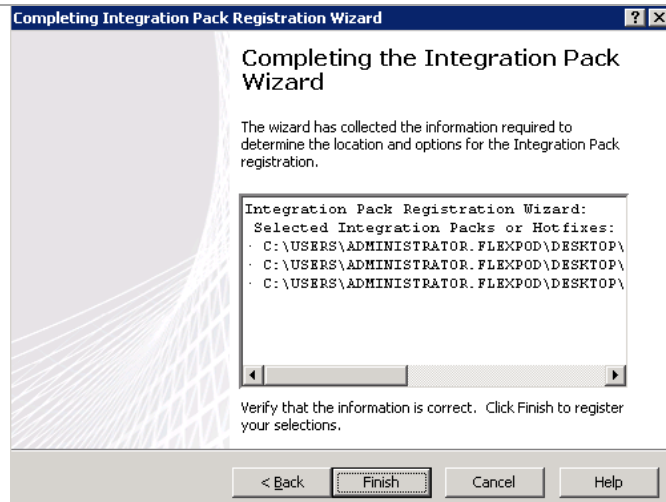




When all integration packs are selected, click **Next** to continue.

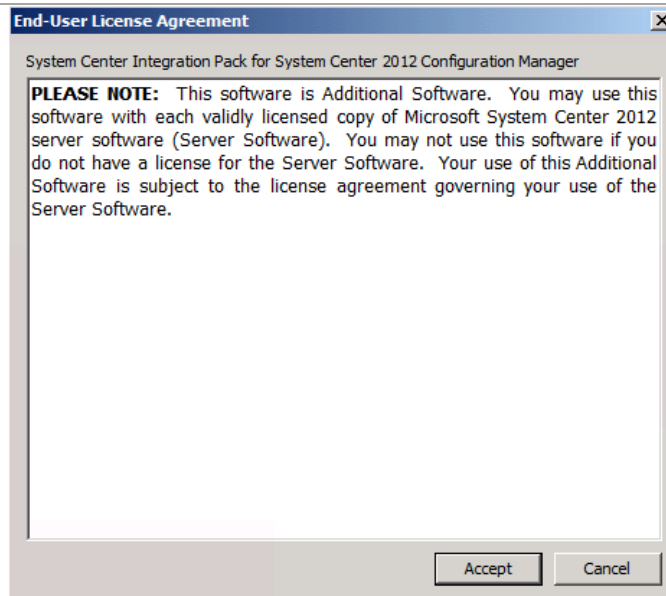


The **Completing the Integration Pack Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.

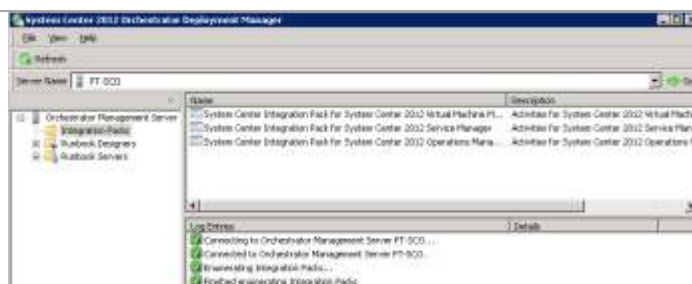




During the installation each integration pack will display Microsoft Software License Terms. Click **Accept** to continue with the installation.



When complete, each integration pack will be displayed in the Deployment Manager interface.

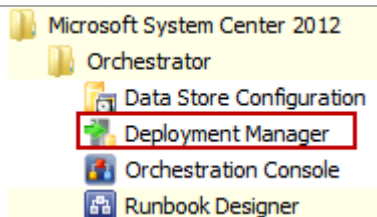


Deploying the System Center Integration Packs

The following steps need to be completed in order to install the Orchestrator Integration Packs.²²

Perform the following steps on the **Orchestrator Runbook Server** virtual machine.

From the **Start Menu**, navigate to the **Microsoft System Center 2012** then select the **Orchestrator** folder and click the **Deployment Manager** shortcut.



²² System Center 2012 – Orchestrator Component Add-ons and Extensions - <http://www.microsoft.com/download/en/details.aspx?id=28725>.



In the **Runbook Designer** console, on the selected Runbook Server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer...** option from the context menu.



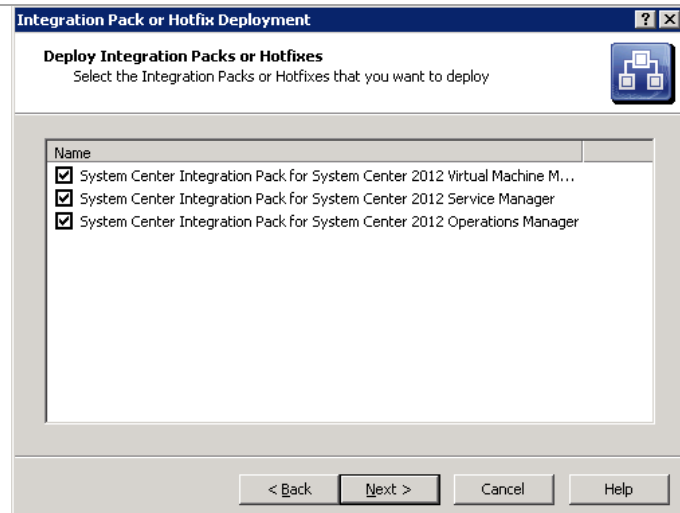
The Integration Pack Deployment Wizard will appear. Click **Next** to continue.



In the **Deploy Integration Packs or Hotfixes** dialog, select the check boxes integration packs folder created earlier and select the following integration packs:

- System Center 2012 Operations Manager.
- System Center 2012 Service Manager.
- System Center 2012 Virtual Machine Manager.

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





In the **Computer Selection Details**, type the name of the Orchestrator management server and click **Add**. When added, click **Next** to continue.

Computer Selection

Computer Selection Details
Select the computers that you want to deploy the Integration Pack or Hotfix on.

Computer: FT-SCO

FT-SCO

Remove

< Back Next > Cancel Help

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.

Installation Options

Installation Configuration
Configure the installation options for the Integration Packs or Hotfixes

You can install the Integration Packs or Hotfixes now, or at a time that you specify.

☐ Schedule installation

Perform installation at: 12:23:39 AM 5/21/2012

Advanced Options

☒ Stop all running Runbooks before installing the Integration Packs or Hotfixes

☐ Install the Integration Packs or Hotfixes without stopping the running Runbooks. You may need to restart the computer to complete the installation.

< Back Next > Cancel Help

The **Completing the Integration Pack Deployment Wizard** dialog will appear with a summary of selections. Click **Finish** to begin the integration pack installation.

Completing Integration Pack Deployment Wizard

Completing the Integration Pack Deployment Wizard

The wizard has collected the information required to determine the location and options for the Integration Pack or Hotfix deployment.

Integration Pack Deployment Wizard:

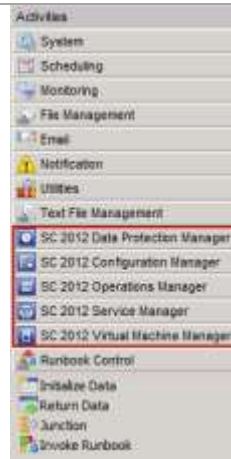
- Target Servers:
 - FT-SCO
- Integration Packs
 - System Center Integration Pack for S1
 - System Center Integration Pack for S1
 - System Center Integration Pack for S1

Verify that the information is correct. Click Finish to deploy your selections.

< Back Finish Cancel Help



When complete, each integration pack will be displayed in the Runbook Designer interface.



To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console** and go to the **Options** drop-down menu and select **SC 2012 Virtual Machine Manager** option.



In the Prerequisite Configuration dialog, click **Add**.





In the **Add Configuration** dialog, fill in the required information for the Virtual Machine Manager server as shown and click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

Properties	
Computer name	FT-SCVMM
VMM Server	FT-SCVMM.FELXP0D.TEST
User	FT-VMM-SVC
Domain	flexpod
Password	*****
Authentication Type (Remote only)	Default
Port (Remote only)	5985

While still in the Orchestrator Runbook Designer Console and go to the Options drop-down menu and select SC 2012 Operations Manager option.

System Center 2012 Orchestrator Runbook Designer

Actions Edit Options View Help

Refresh

Connections

FT-SCVMM

Runbook Designer

Computer Groups

Runbook Servers

Global Settings

Check Out

In the Microsoft System Center Operations Manager Connections dialog, click Add.

Microsoft System Center Operations Manager Connections

Configure the connections for the Microsoft System Center Operations Manager objects

Connections

Connection	Domain	Server

Add... Edit... Remove

Finish Cancel Help



In the **MS System Center Operations Manager Connection Settings** dialog, fill in the required information for the Operations Manager management server and click **Test Connection**²³. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

In the **Orchestrator Runbook Designer** console, go to the **Options** drop-down menu and select **SC 2012 Service Manager** option.



In the **Connections** dialog, click **Add**.

²³ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.



In the **Connection** dialog, fill in the required information for the Operations Manager management server²⁴ and click **Test Connection**. When connectivity is verified, click **OK**. After returning to the **Prerequisite Configuration** dialog, click **Finish** to save the changes.

Connection

Name: FT-SCSM

Server: FT-SCSM.FLEXPOD.TEST

Credentials

Domain: FELEXPOD

User name: Administrator

Password:

Monitoring Intervals

Polling: 10 seconds

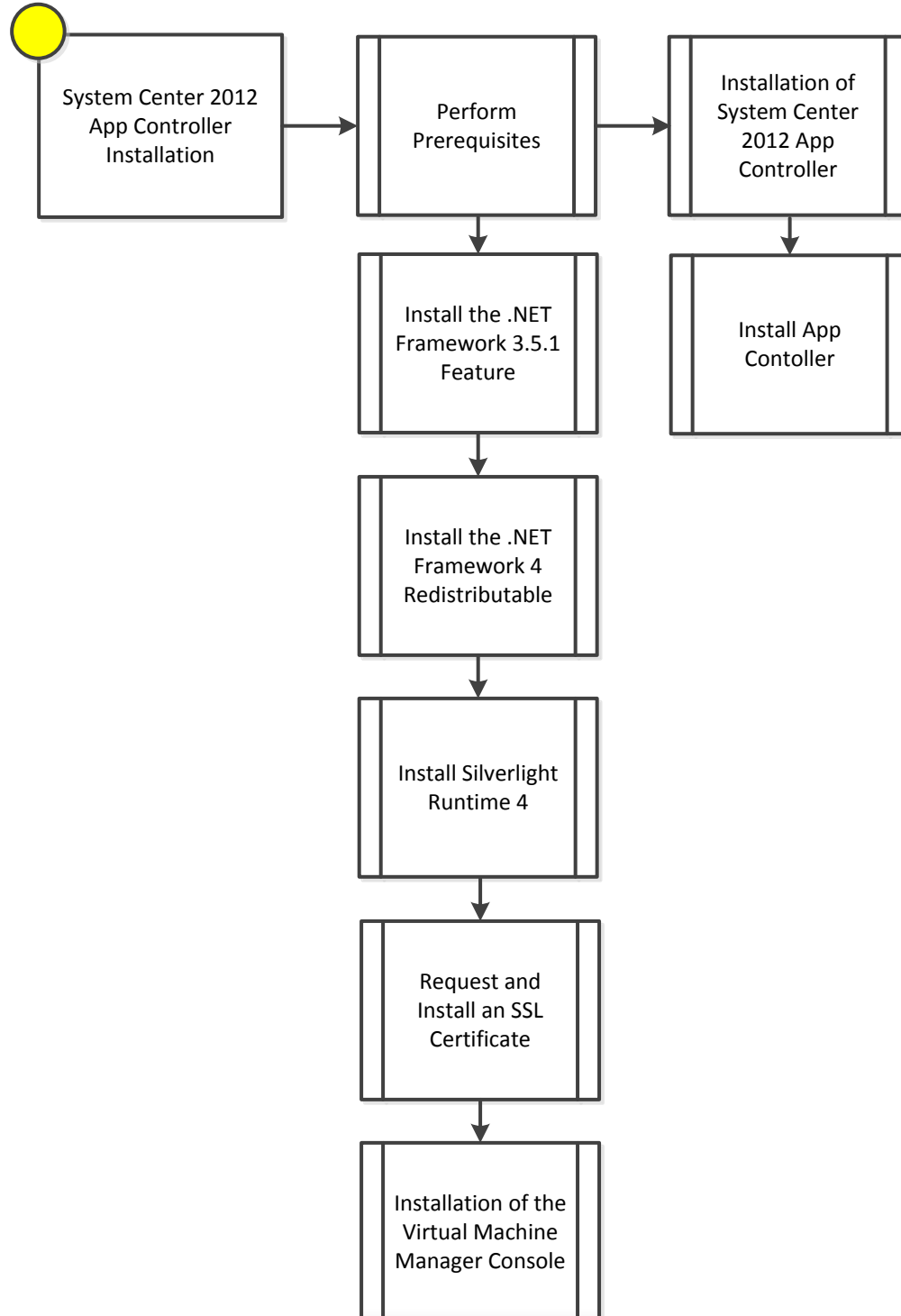
Reconnect: 10 seconds

Test Connection Ok Cancel

App Controller

The App Controller installation process is comprised of the following high-level steps:

²⁴ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.



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 2008 R2 (x64) has been provisioned for App Controller.
- A SQL Server 2008 R2 cluster with dedicated instance that has been established in previous steps for App Controller.
- All the System Center products have been hydrated and validated.
- The .NET Framework 3.5.1 Feature is installed.
- The .NET Framework 4 Redistributable is installed.
- Microsoft Silverlight® Runtime 4 is installed.
- A Trusted Server Authentication (SSL) Certificate (the CN field of the certificate must match server name) is installed.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User Name	Purpose	Permissions
<DOMAIN>\ FT-SCAC-SVC	App Controller service account	This account will need to be a member in the following groups: 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	App controller admins. <DOMAIN>\ FT-SCAC-SVC <DOMAIN>\ FT-VMM-Admins

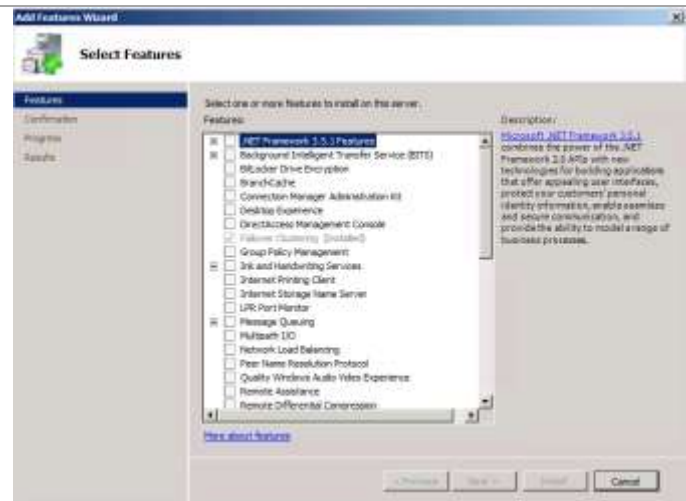
Adding the .NET Framework 3.5.1 Feature

The App Controller installation requires the .NET Framework 3.5.1 Feature be enabled to support installation. Follow the provided steps to enable the .NET Framework 3.5.1 feature.

Perform the following steps on the **App Controller** virtual machine.



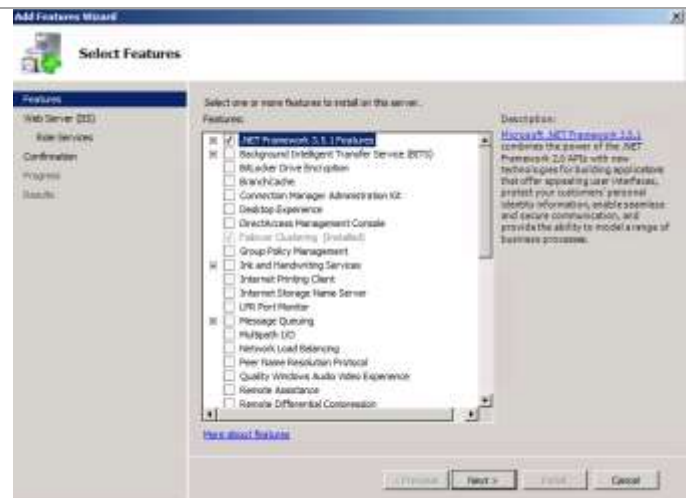
To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Features** node and click **Add Features**. The **Add Features Wizard** will appear. In the **Select Features** dialog, select **.NET Framework 3.5.1 Features** check box.



The Add role services and features required for .NET Framework 3.5.1 dialog will appear. Click the Add Required Role Services button.



After returning to the **Select Features** dialog, the **.NET Framework 3.5.1 Features** check box will show selected. Click **Next** to continue.





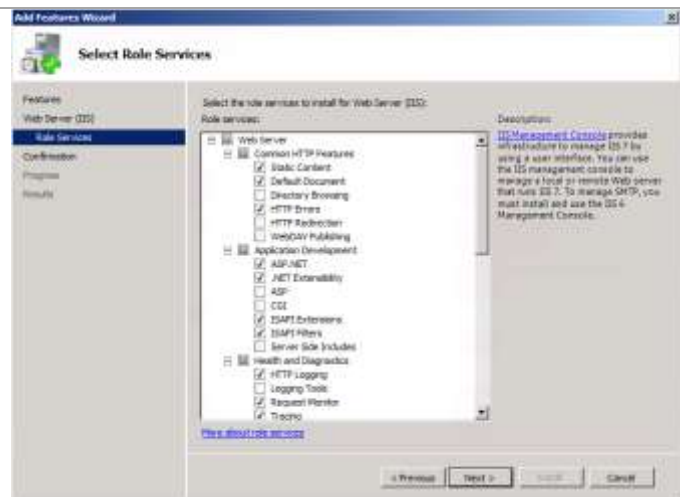
The **Web Server (IIS)** dialog will appear outlining information about the dependent role services. Click **Next** to continue.



The **Select Role Features** dialog will appear with default selections required by the .NET Framework feature. To support App Controller installation, the following additional role services are required:

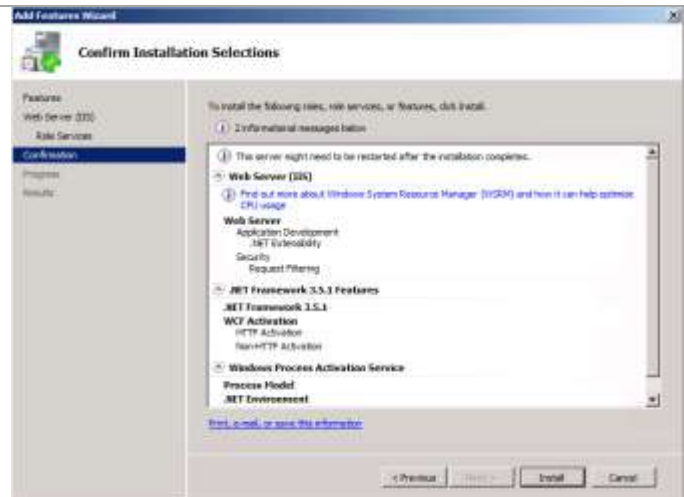
- Static Content.
- Default Document.
- Directory Browsing.
- HTTP Errors.
- ASP.NET.
- .NET Extensibility.
- ISAPI Extensions.
- ISAPI Filters.
- HTTP Logging.
- Request Monitor.
- Tracing.
- Basic Authentication.
- Windows Authentication.
- Request Filtering.
- Static Content Compression.
- IIS Management Console.

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

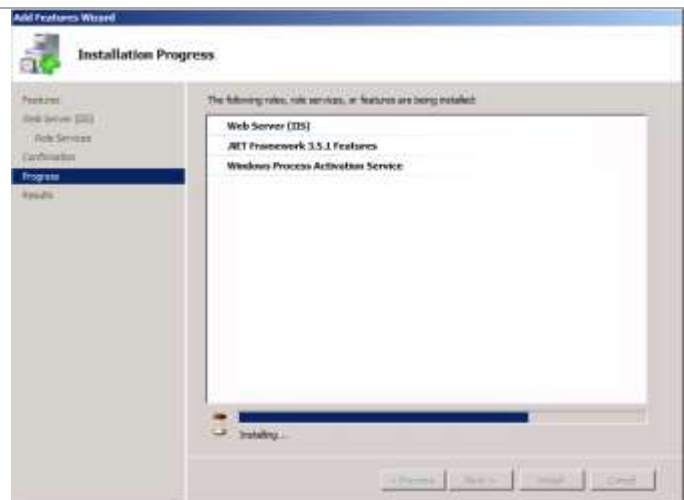




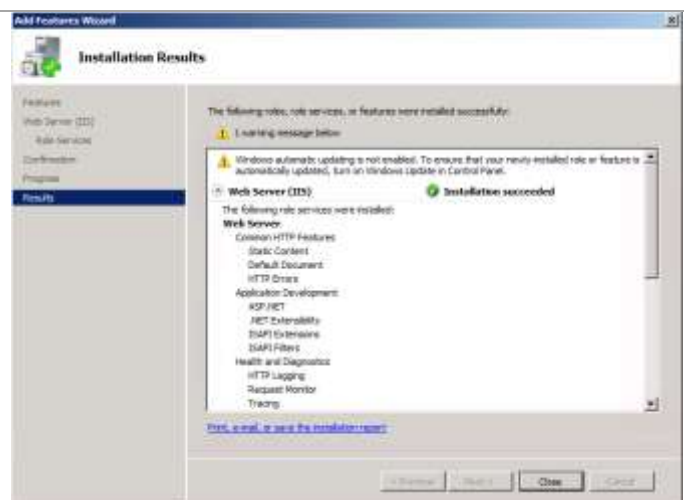
In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.



The **Installation Progress** dialog will show the progress of the feature install.



When complete, the **Installation Results** dialog will appear. Verify that all features and dependent role services installed correctly. When verified, click **Close** to complete the installation of the .NET Framework 3.5.1 Feature.



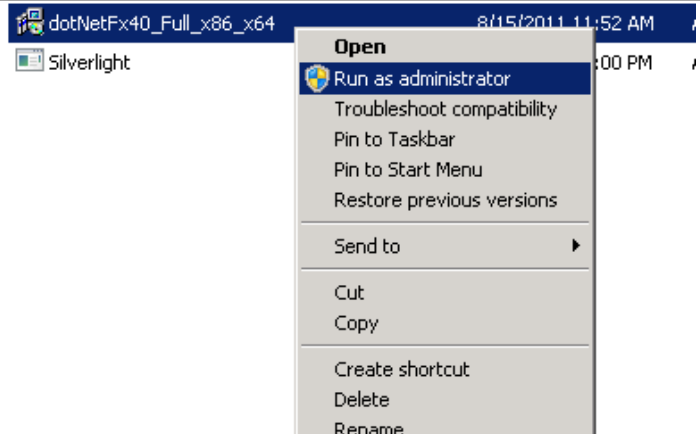


Installing .NET Framework 4

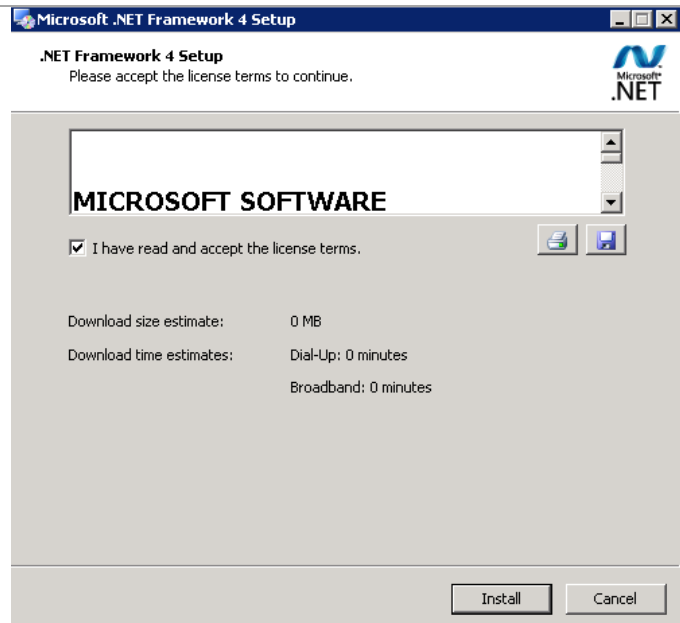
Additionally, the App Controller installation also requires prior installation of the .NET Framework 4 package. Follow the provided steps to install the .NET Framework 4 package.

Perform the following steps on the **App Controller** 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.

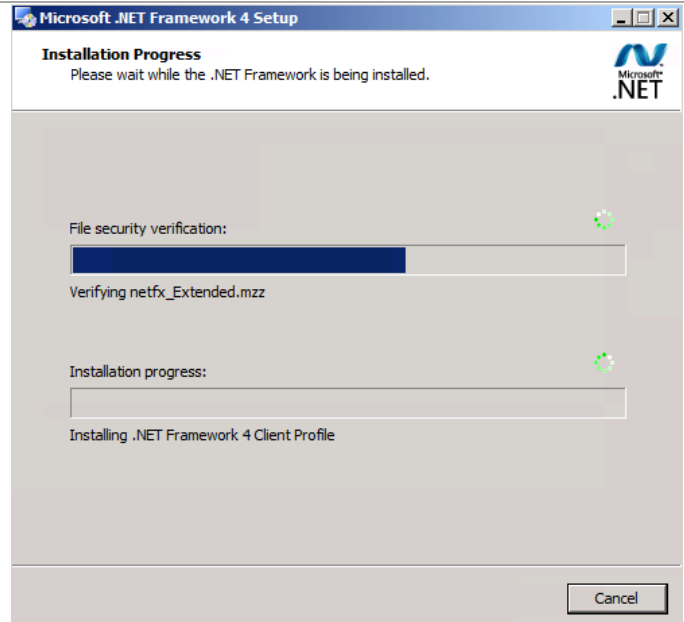


Within the Microsoft .NET Framework 4 Setup dialog, select the I have read and accept the license terms checkbox and click Install to begin the installation.

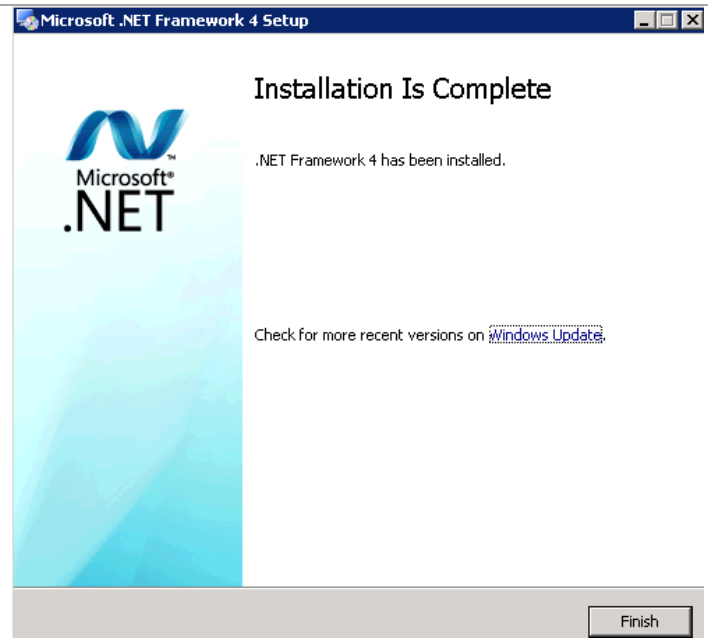




The installation progress will be displayed in the setup wizard.



When completed, click **Finish** to exit the installation.

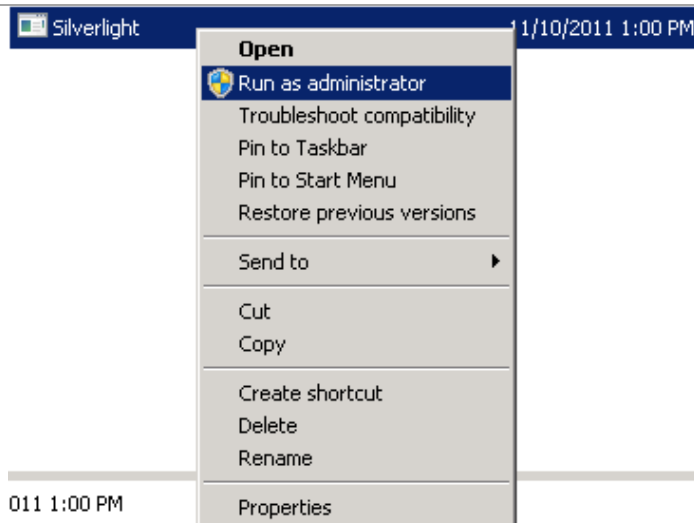




Installing Silverlight Runtime 4

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.



The Silverlight installation wizard will appear. In the **Install Silverlight** dialog, click the **Install now** button.



In the **Enable Microsoft Update** dialog, select or deselect the **Enable Microsoft Update** checkbox based on the policies of your organization. Click **Next** to begin the installation.





After installation, click **Close** to complete the setup.

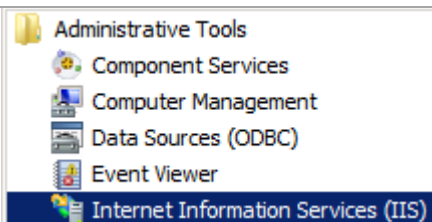


Requesting and Installing an SSL Certificate

For IIS, there are several ways to request a SSL Certificate. One method, through the IIS Manager console, is outlined below.

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. 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, select **Server Certificates**.

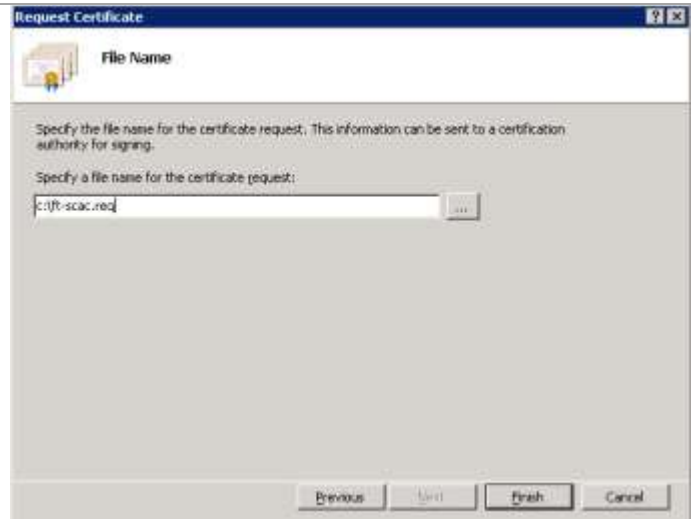




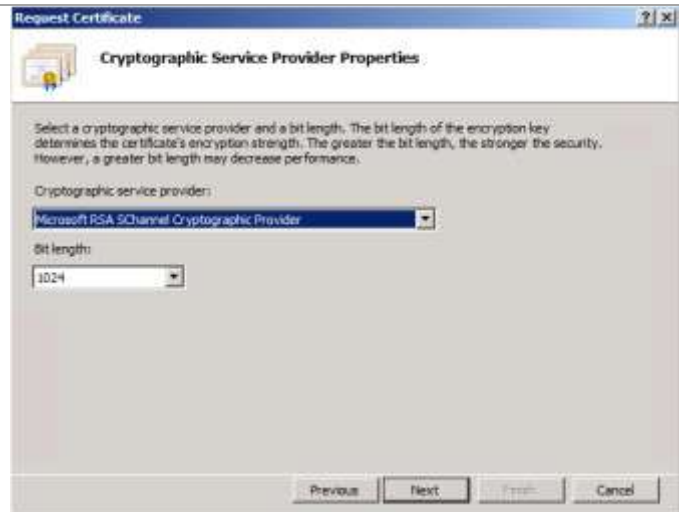
The Server Certificates pane will expand. Under actions, click Create Certificate Request...



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.



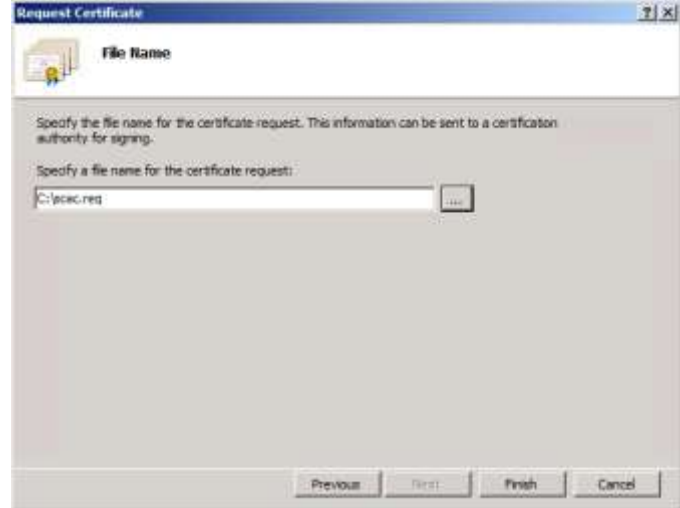
In the **Cryptographic Service Provider Properties** dialog, select a Cryptographic Service Provider (CSP) that is appropriate for your issuing CA. In most cases, selecting the default CSP and default bit length is satisfactory. Click **Next** to continue.





In the **File Name** dialog, provide a complete path to save the certificate request file. Click **Finish** to generate the certificate request.

When completed, submit the request to your issuing CA or certificate provider of choice and follow the next steps on installing the newly issued certificate.



After receiving the issued certificate, open the **Internet Information Services (IIS) Manager** console and select **Server Certificates** when again. From the **Actions** pane, select **Complete Certificate Request...**



The **Complete Certificate Request** wizard will appear. In the **Specify Certificate Authority Response** dialog, specify the file name and location of the issued certificate and supply a friendly name for the certificate in the provided text boxes. Click **OK** to complete the operation.



In the **Server Certificates** section of the IIS Manager, you will now see the newly created and installed certificate.



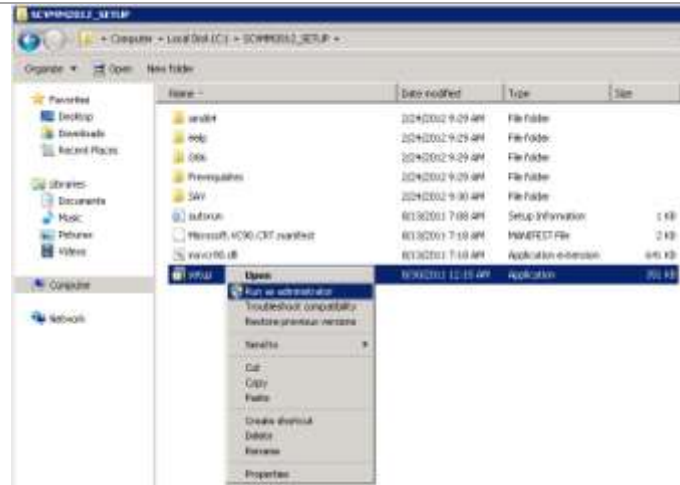


Installing the Virtual Machine Manager Console

The following steps need to be completed in order to install the VMM Console on the target App Controller virtual machine.

Perform the following steps on the **App Controller** virtual machine.

From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** from the context menu to begin setup.

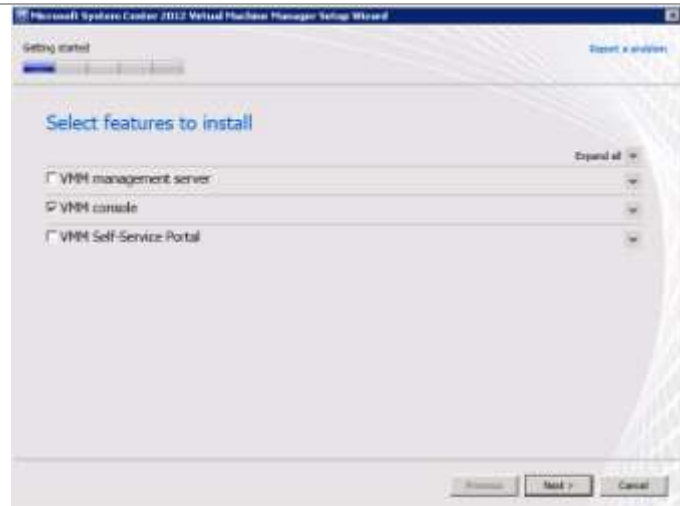


The Virtual Machine Manager installation wizard will begin. At the splash page, click **Install** to begin the Virtual Machine Manager server installation.





In the **Select features to install** dialog, ensure the **VMM console** installation option check box is selected. Click **Next** to continue.



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

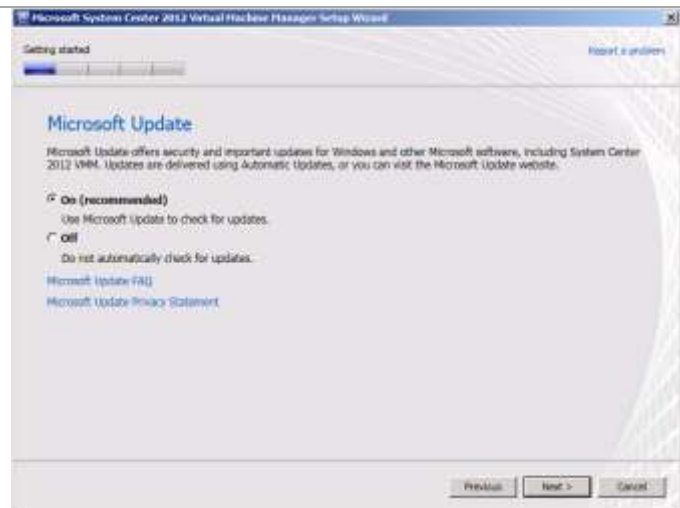




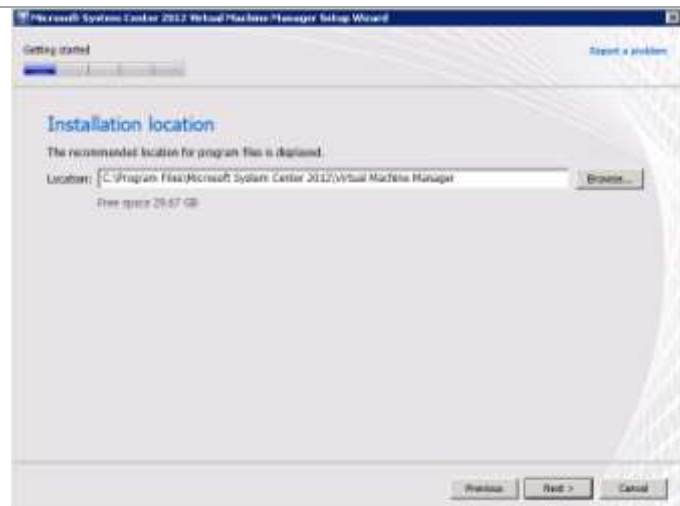
In the **Join the Customer Experience Improvement Program (CEIP)** dialog, select the option to either participate or not participate in the Customer Experience Improvement Program (CEIP) by providing selected system information to Microsoft. Click **Next** to continue.



In the **Microsoft Update** dialog, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click **Next** to continue.



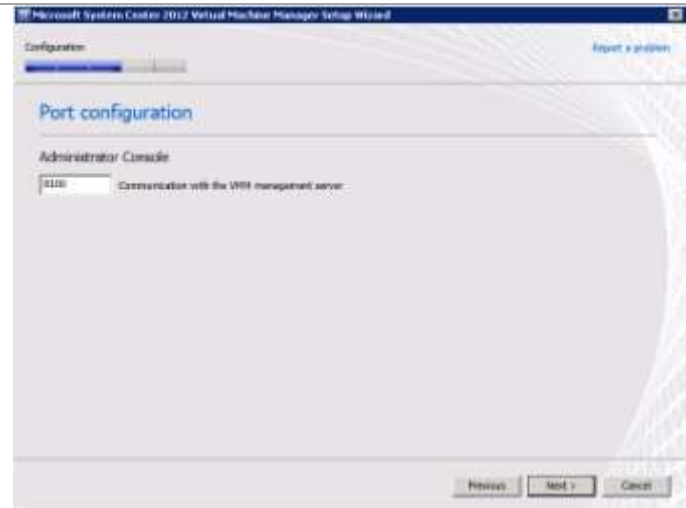
In the **Select installation location** dialog, specify a specific location or accept the default location of %ProgramFiles%\Microsoft System Center 2012\Virtual Machine Manager for the installation. Click **Next** to continue.



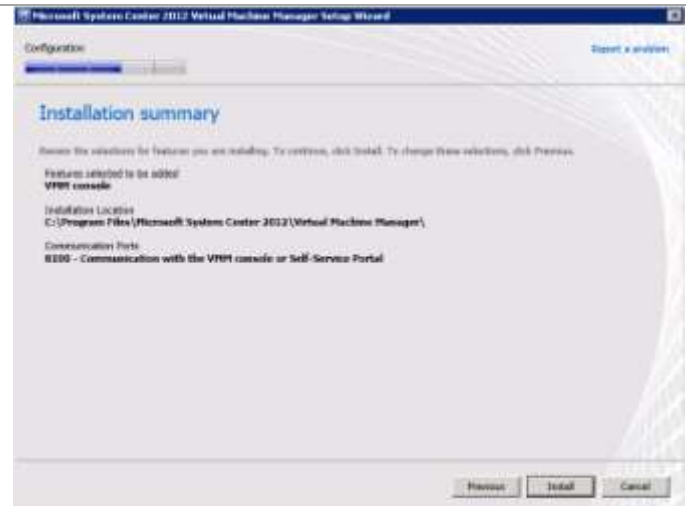


In the **Port Configuration** dialog, specify the port used for communication with the Virtual Machine Manager management server in the provided text box. If no modifications were made during Virtual Machine Manager install, the default port would be 8100. Click **Next** to continue.

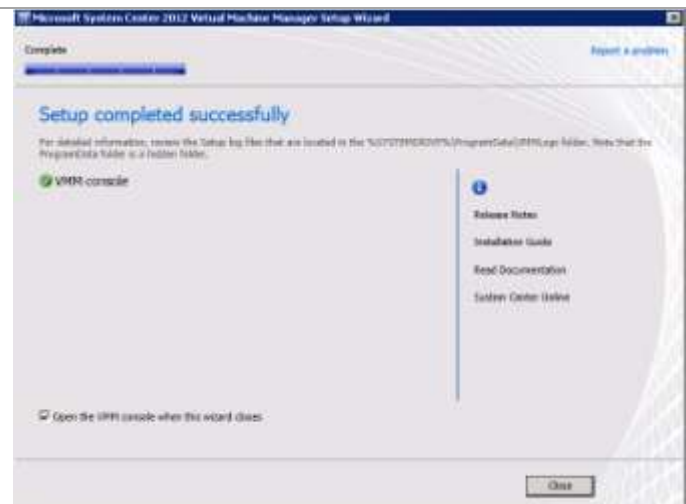
The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



The **Installation summary** dialog will appear displaying the selections made during the installation wizard. Review the options selected and click **Install** to continue.

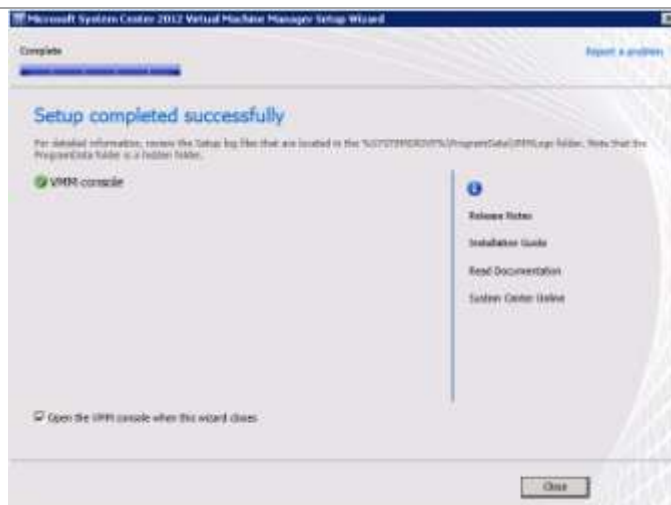


When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.

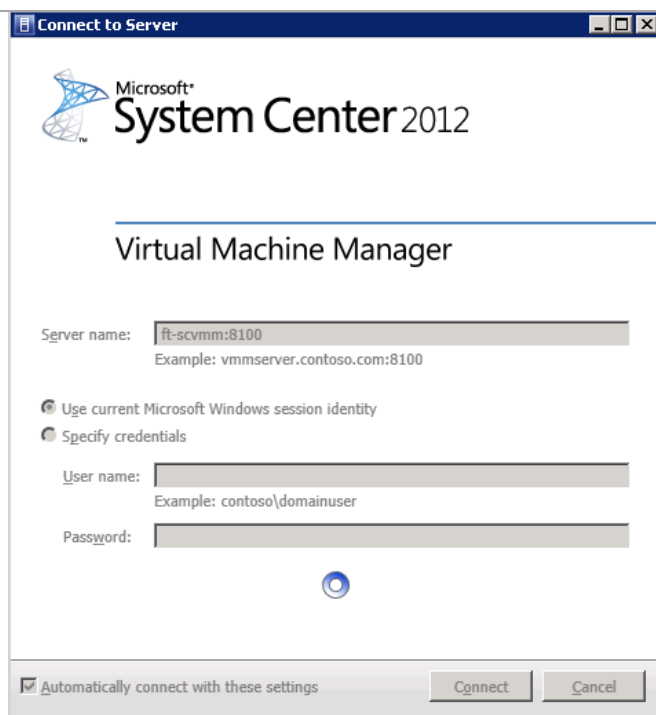




When the installation completes, the wizard will display the **Setup completed successfully** dialog. Click **Close** to complete the installation.



When complete, launch the **Virtual Machine Manager** console to verify the installation occurred properly. Verify that the console launches and connects to the Virtual Machine Manager instance installed.





Installation

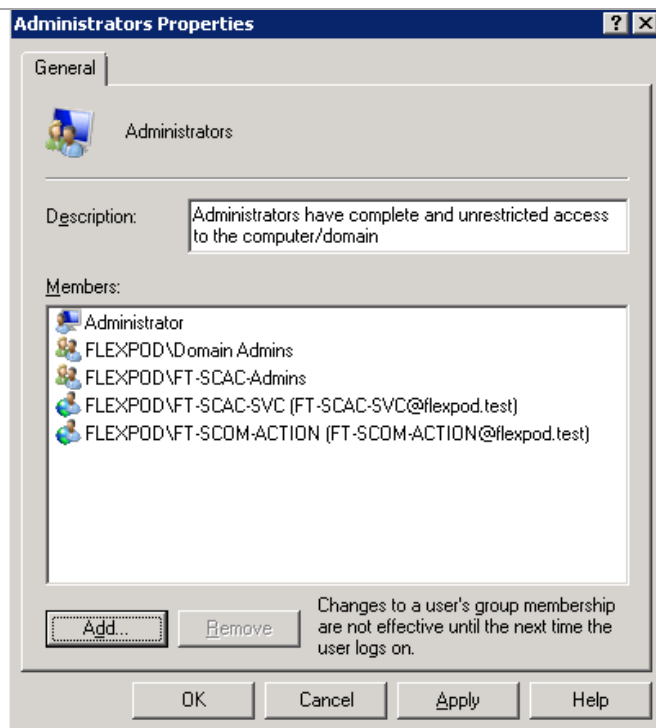
The following steps need to be completed in order to install App Controller.

Perform the following steps on the **App Controller** virtual machine.

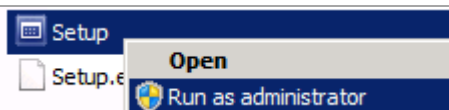
Log on to the App Controller virtual machine with a user with local admin rights.

Verify the following accounts and/or groups are members of the Local Administrators group on the App Controller portal virtual machine:

- Fast Track Operations Manager Action account
- Fast Track App Controller service account
- Fast Track App Controller Admins group



Logon on to System Center App Controller server. From the **System Center App Controller** installation media source right-click **AppController.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 Please read this License Terms dialog, ensure the I have read, understood and agree with the terms of this license agreement installation option checkbox is selected and click Next to continue.

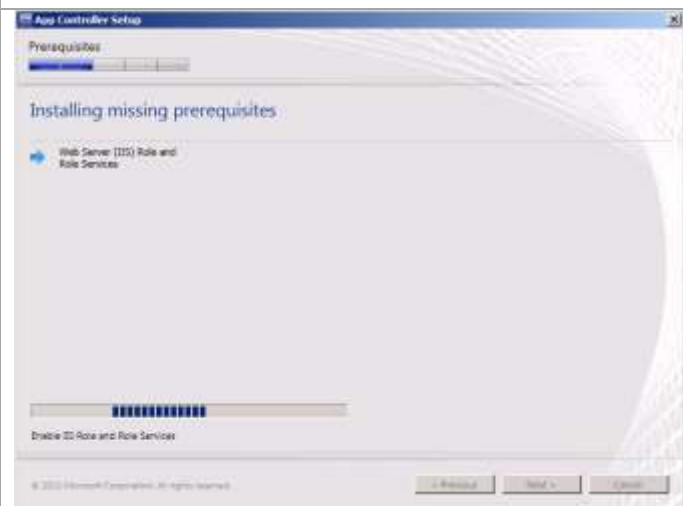




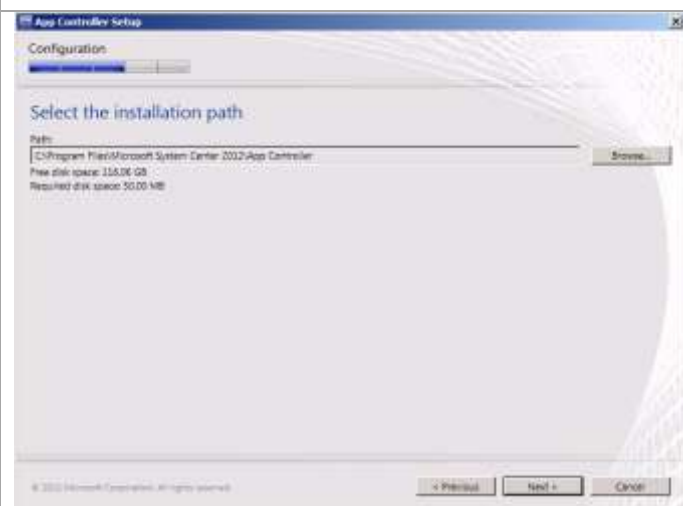
In the **Install missing software** dialog, the wizard will detect missing roles and software and attempt installation of missing prerequisites. Click **Install** to enable missing roles and features.



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 location** 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.

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

In the **Configure the website** dialog, provide the following information:

- Under Website, in **Type: HTTPS**, set the **IP address** drop-down menu to **All unassigned**. Set the **Port** value to **443**.
- Verify that the **Use existing certificate** option is selected and select the proper Server Authentication certificate that installed within the virtual machine from the drop-down menu.

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

Note: while not recommended, if a Server Authentication certificate cannot be obtained and installed on the App Controller server, you may choose the **Generate self-signed certificate** option to satisfy installation requirements.



In the **Configure the SQL Server database** dialog, make the following selections install the App Controller database in the SCO instance (refer to the worksheet created earlier):

- **Server Name** – specify the cluster network name of the SQL Server failover cluster hosting the instance.
- **Port** – specify the TCP port used for SQL Server connectivity (1433 by default).
- **Instance name** - specify the instance name where the AppController database will be installed to (the SCO 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 'Configuration' tab is selected. The dialog contains four input fields: 'Server name' with the value 'SQLSCACOE', 'Port' with the value '1433', 'Instance name' with a dropdown menu showing 'SCACOE', and 'Database name' with the value 'AppController'. At the bottom, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'Next' button is highlighted.

The **Help Improve App Controller for System Center 2012** dialog provides options for participating in various product feedback mechanisms. These include:

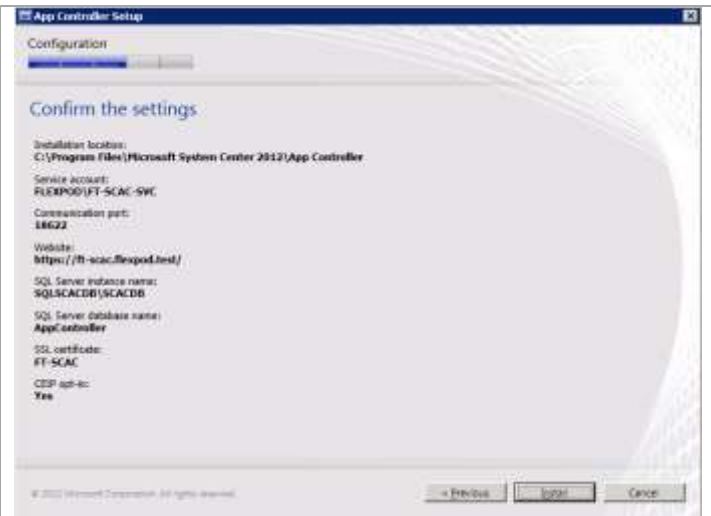
- CEIP
- Microsoft Update

Select the appropriate option based on your organization's policies and click **Install** to continue

The screenshot shows the 'Help improve App Controller for System Center 2012' dialog box within the 'App Controller Setup' window. The dialog contains two sections: 'Customer Experience Improvement Program' and 'Microsoft Update'. Under 'Customer Experience Improvement Program', there are two radio buttons: 'Yes, I am willing to participate in CEIP' (which is selected) and 'No, I am not willing to participate'. Below this is a link to 'Read the Customer Experience Improvement Program (CEIP) privacy statement'. Under 'Microsoft Update', there is a checked checkbox for 'Use Microsoft Update to receive updates for App Controller for System Center 2012 and other Microsoft products.' and a link to 'Read the Update Services privacy statement'. At the bottom, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'Next' button is highlighted.



In the **Confirm the settings** dialog, verify the settings provided during the installation wizard and click **Install** to begin the installation.



The required components will install and progress of the installation will be provided in the wizard.



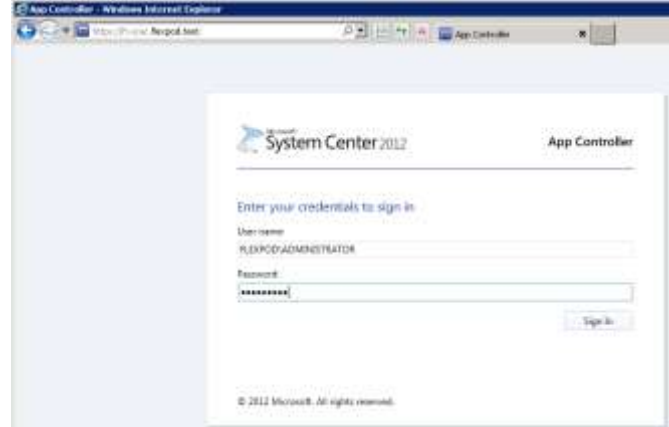
When complete, the **Setup completed successfully** dialog will appear with progress of each component. Verify that each component successfully. Note the App Controller website in the provided textbox.

Ensure the Start the App Controller website checkbox is selected and click Finish.

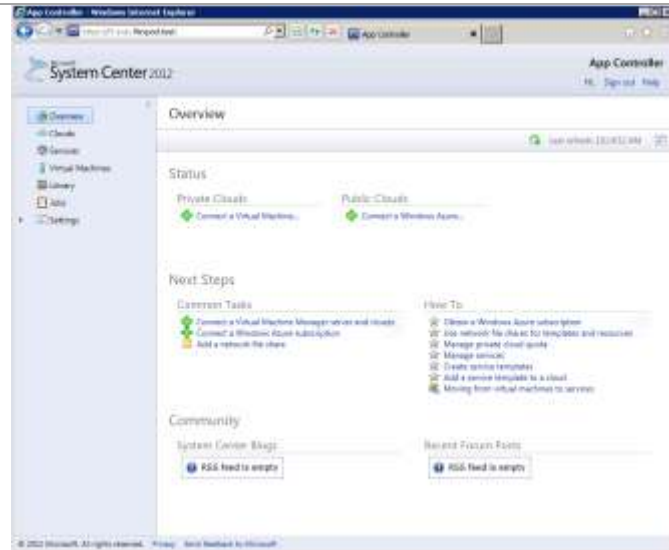




The **System Center 2012 App Controller website** will launch. Because no users have been created in SCVMM, enter in the App Controller service account (which has been assigned an admin role in SCVMM). When complete, click **Sign in**.

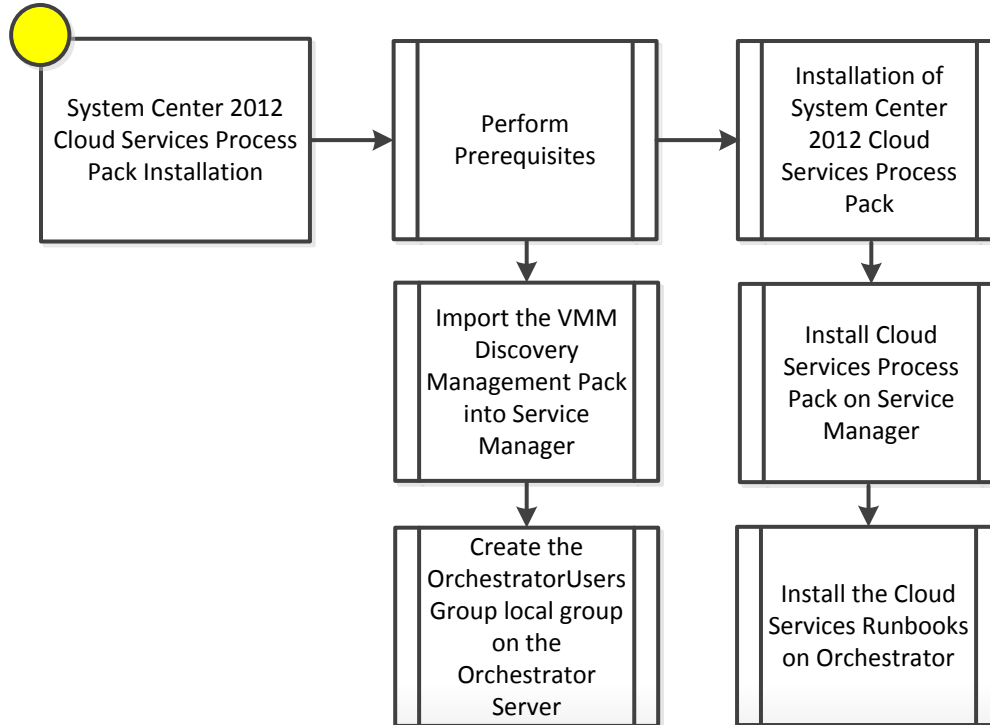


The App Controller portal will appear. After validating functionality the App Controller installation is considered complete.



System Center Cloud Services Process Pack

The Cloud Services Process Pack installation process includes the following high-level steps:



Overview

This section provides the setup procedure for Orchestrator 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 VMM should already be complete per previous steps.

System Center Cloud Services Process Pack is available at <http://technet.microsoft.com/en-us/library/hh562067.aspx>. 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.

Prerequisites

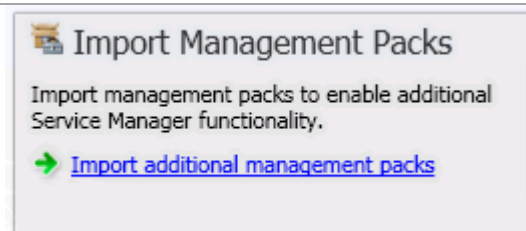
The following environment prerequisites must be met before proceeding.

Importing the VMM Discovery Management Pack into Service Manager

The VMM Discovery Management Pack must be installed prior to the installation of CSPP. The following steps are provided.

Perform the following steps on the **Service Manager management server** virtual machine.

From the Service Manager Console, select the Administration node. In the Import Management Packs section, click the Import additional management packs link.

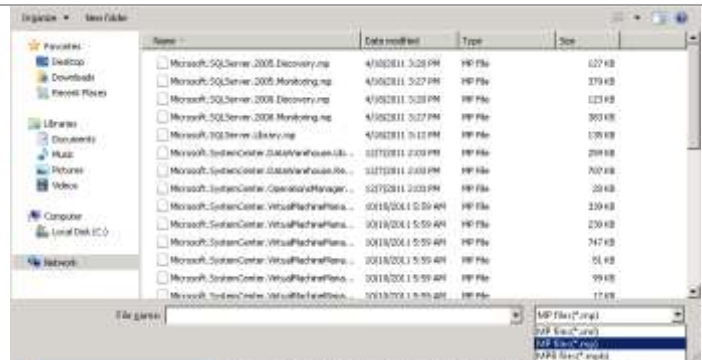


In the Select Management Packs to Import dialog opens.

Navigate to the `\Setup\ManagementPacks` directory of the CSPP installation files.

Select the file type **MP files (*.mp)** from the file type dropdown menu.

The management packs must be imported individually and in order. Begin with the management pack file named **Microsoft.SystemCenter.DataWarehouse.Libary** and click **Open**.





The following steps must be repeated for each set of management packs which must be installed to remove management pack dependencies. The required management packs can be found in the \Setup\ManagementPacks of the CSPP installation media.

After each set of management packs are added, click Import to begin the process.

Note: After selection each management pack file from the list and clicking Open, the management pack name may take a few seconds to show in the Management Pack List.

Install the following management packs in this order:

- Data Warehouse Library
(Microsoft.SystemCenter.DataWarehouse.Library.mp)
- Microsoft Generic Report Library
(Microsoft.SystemCenter.DataWarehouse.Report.Library.mp)
- Windows Server Operating System Library
(Microsoft.Windows.Server.Library.mp)
- Windows Server 2008 Operating System (Discovery)
(Microsoft.Windows.Server.2008.Discovery.mp)
- Windows Server Internet Information Services Library
(Microsoft.Windows.InternetInformationServices.CommonLibrary.mp)
- Windows Server Internet Information Services 2000
(Microsoft.Windows.InternetInformationServices.2000.mp)
- Windows Server Internet Information Services 2003
(Microsoft.Windows.InternetInformationServices.2003.mp)
- Windows Server 2008 Internet Information Services 7
(Microsoft.Windows.InternetInformationServices.2008.mp)

Management Pack List:

Name	Version	Sealed
✓ Data Warehouse Library	7.0.8427.0	Yes
✓ Microsoft Generic Report Library	7.0.8560.0	Yes

Management Pack List:

Name	Version	Sealed
✓ Windows Server Operating System Library	6.0.6957.0	Yes
✓ Windows Server 2008 Operating System (Discovery)	6.0.6957.0	Yes

Management Pack List:

Name	Version	Sealed
✓ Windows Server Internet Information Services Library	6.0.6658.0	Yes
✓ Windows Server Internet Information Services 2000	6.0.6658.0	Yes
✓ Windows Server Internet Information Services 2003	6.0.6658.0	Yes
✓ Windows Server 2008 Internet Information Services 7	6.0.7600.0	Yes



- SQL Server Core Library (Microsoft.SqlServer.Library.mp)
- Microsoft System Center Operations Manager Library (Microsoft.SystemCenter.OperationsManager.Library.mp)
- Image Library (System) (System.Image.Library.mp)
- System Virtualization Library (System.Virtualization.Library.mp)
- SQL Server 2008 (Discovery) (Microsoft.SqlServer.2008.Discovery.mp)
- SQL Server 2008 (Monitoring) (Microsoft.SqlServer.2008.Monitoring.mp)
- SQL Server 2008 Mirroring (Discovery) (Microsoft.SqlServer.2005.Discovery.mp)
- SQL Server 2008 Mirroring (Monitoring) (Microsoft.SqlServer.2005.Monitoring.mp)
- Virtual Machine Manager Library (Microsoft.SystemCenter.VirtualMachineManager.Library.mp)
- System Center Virtual Machine Manager 2008 R2 PRO Library (Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library.mp)
- Virtual Machine Manager PRO Library (Microsoft.SystemCenter.VirtualMachineManager.PRO.Library.mp)
- Virtual Machine Manager PRO V2 Library (Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Library.mp)

When complete, follow the same steps to import the required System Center 2012 Virtual Machine Manager Discovery management pack.

Management Pack List:

Name	Version	Sealed
✓ SQL Server Core Library	6.1.400.0	Yes
✓ Microsoft System Center Operations Manager Library	7.0.8560.0	Yes
✓ Image Library (System)	7.5.8501.0	Yes
✓ System Virtualization Library	7.0.8427.0	Yes
✓ SQL Server 2005 (Discovery)	6.1.400.0	Yes
✓ SQL Server 2008 (Discovery)	6.1.400.0	Yes
✓ SQL Server 2005 (Monitoring)	6.1.400.0	Yes
✓ SQL Server 2008 (Monitoring)	6.1.400.0	Yes

Management Pack List:

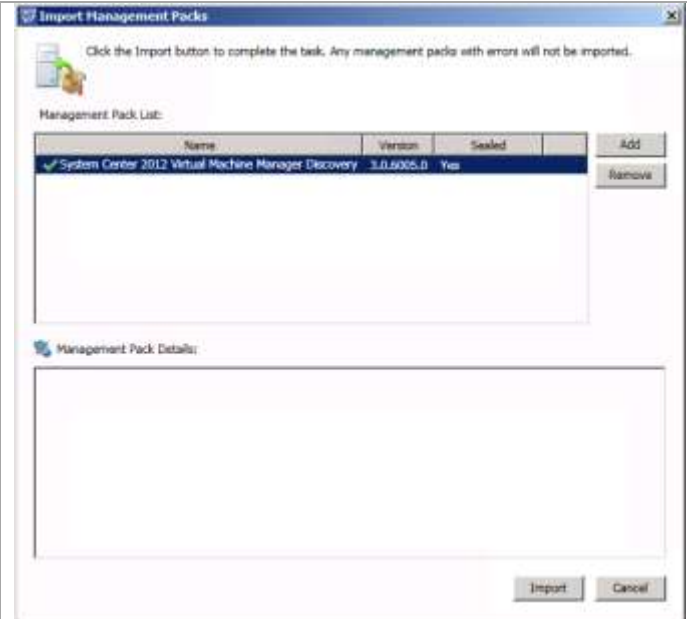
Name	Version	Sealed
✓ Virtual Machine Manager Library	3.0.6005.0	Yes
✓ System Center Virtual Machine Manager 2008 R2 P	3.0.6005.0	Yes
✓ Virtual Machine Manager PRO Library	3.0.6005.0	Yes
✓ Virtual Machine Manager PRO V2 Library	3.0.6005.0	Yes

Management Pack List:

Name	Version	Sealed
✓ System Center 2012 Virtual Machine Manager Discovery	3.0.6005.0	Yes



When completed, exit the wizard.





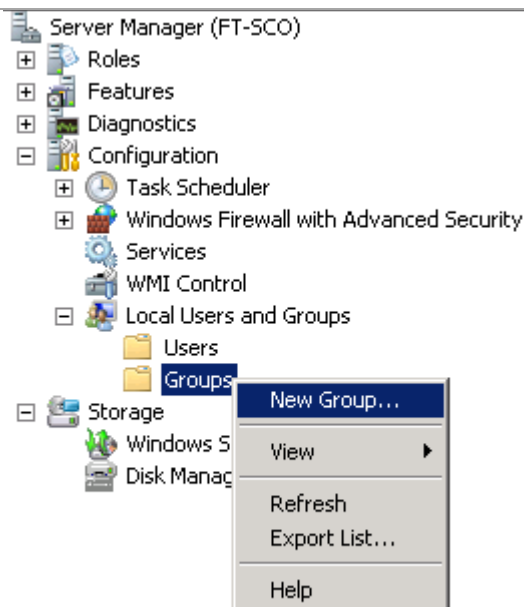
Creating the **OrchestratorUsersGroup** local group on the Orchestrator Server

Perform the following steps to avoid issues related to CSPP setup on Orchestrator.

Perform the following steps on the **Orchestrator** virtual machine.

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 setup²⁵.

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.



²⁵ <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>



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.

New Group

Group name: OrchestratorUsersGroup

Description:

Members:

- FLEXP0D\Administrator
- FLEXP0D\FT-SCO-SVC (FT-SCO-SVC@flexpod.test)

Add... Remove

Help Create Close

Installing the Cloud Services Process Pack

The following steps need to be completed in order to install the Cloud Services Process Pack.

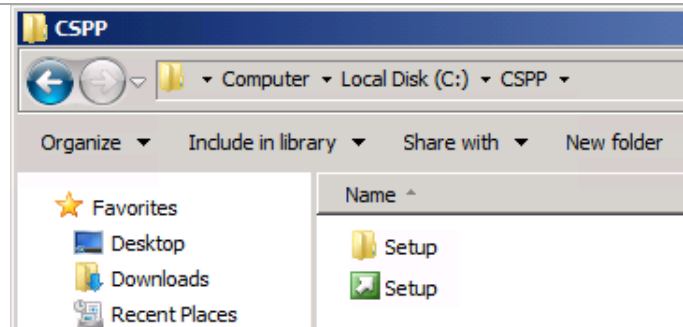
Perform the following steps on the **Service Manager management server** virtual machine.

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 click **Setup.exe**.





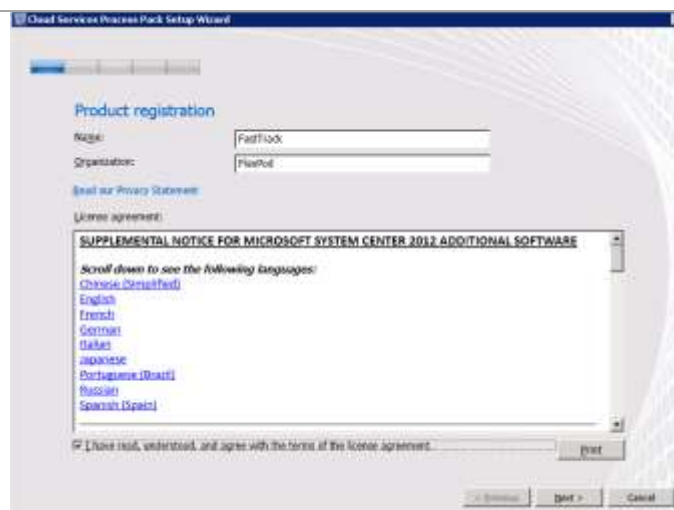
The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud Services Process Pack.



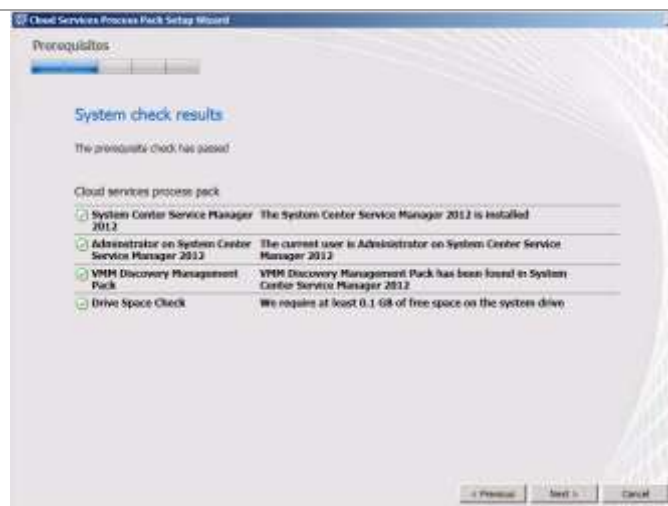
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – specify the name of primary user or responsible party within your organization.
- **Organization** - specify the name of the licensed organization.

Click **Next** to continue.

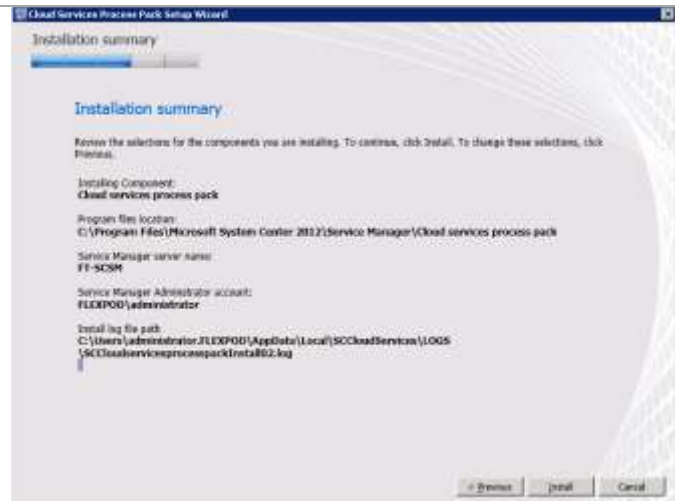


The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.



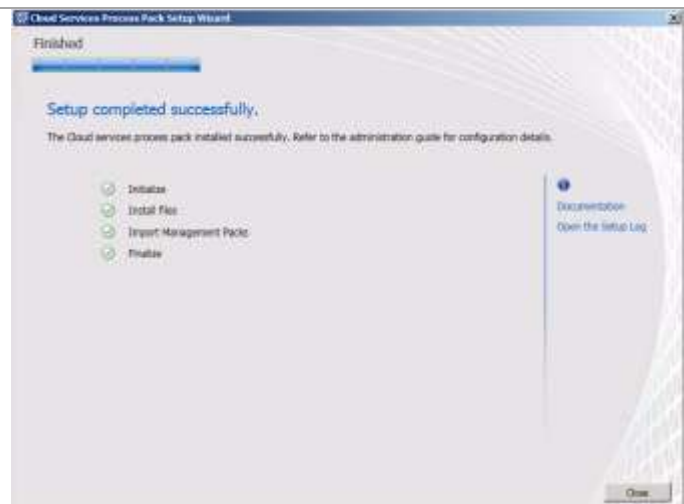


The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.



When the installation completes, the wizard will display the **Setup completed successfully** dialog.

Click **Close** to complete the installation.





Installing the Cloud Services Runbooks

The following steps need to be completed in order to install the Cloud Services Process Pack Orchestrator runbooks.

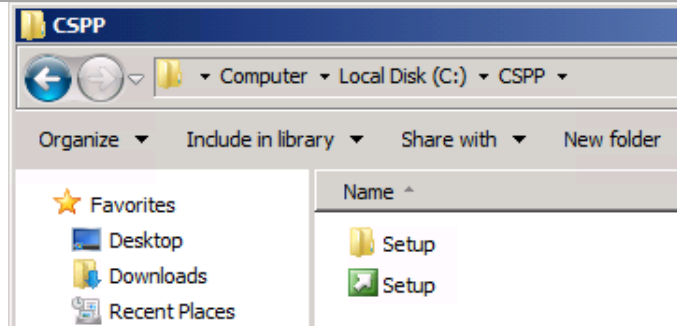
Perform the following steps on the **Orchestrator** virtual machine.

Log on to the Orchestrator management server virtual machine with a user with local admin rights.

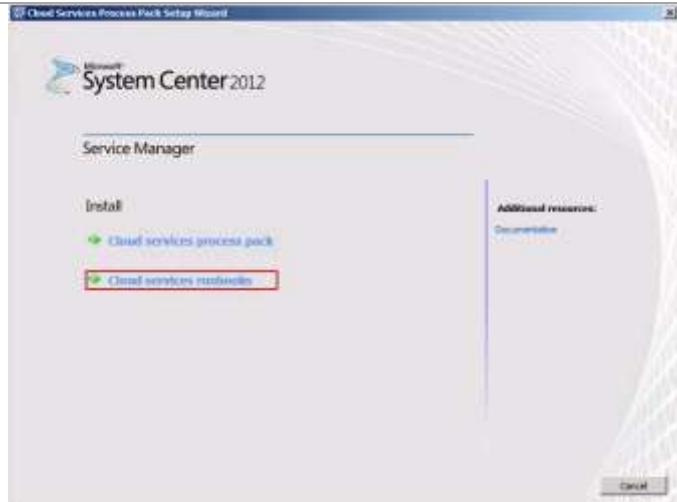
Verify the account has the following rights:

- 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 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**.



The Cloud Services Process Pack Setup Wizard will appear. In the Install section, select Cloud services process pack.

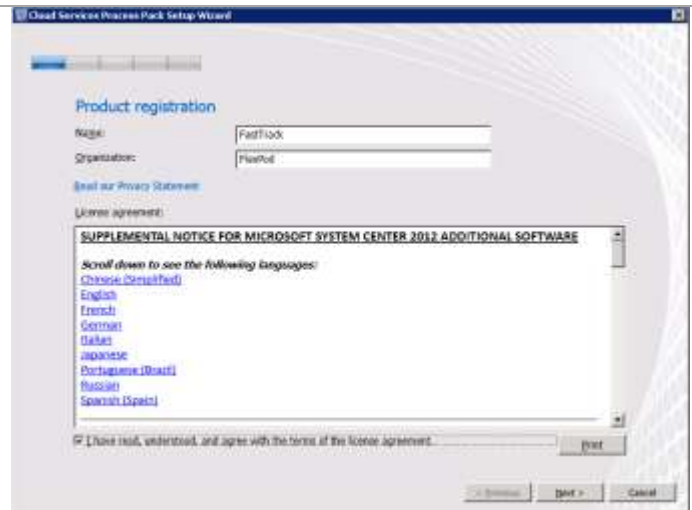




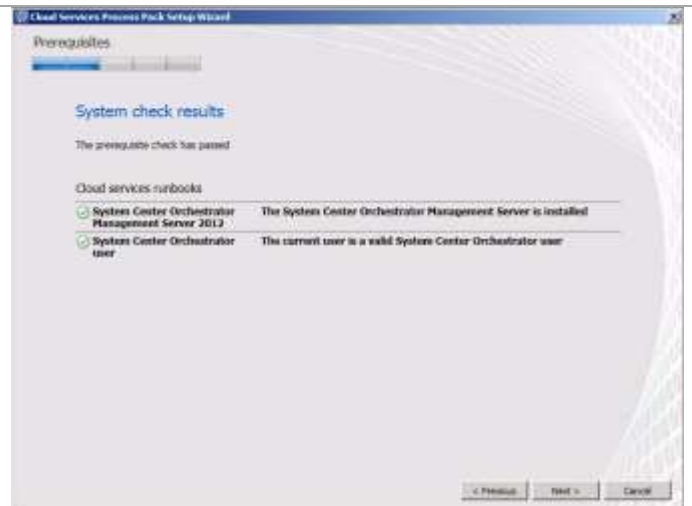
In the **Product registration information** dialog, enter the following information in the provided text boxes:

- **Name** – specify the name of primary user or responsible party within your organization.
- **Organization** - specify the name of the licensed organization.

Click **Next** to continue.



The setup will verify that all system prerequisites are met in the **System check results** dialog. If any prerequisites are not met, they will be displayed in this dialog. When verified, click **Next** to continue.





In the **Configure System Center Orchestrator account and Database** dialog, enter the following information in the provided text boxes and dropdown menus:

- **Username** – Enter the System Center Orchestrator service account.
- **Password** - Enter the System Center Orchestrator service account password
- **Domain** – Select the domain where the System Center Orchestrator service account resides.

Click the **Test Credentials** button to verify the correct credentials were entered.

- **Orchestrator Database Server** – Enter the Orchestrator database server network name.
- **SQL Server Instance** - Select the Orchestrator database server SQL Server instance.
- **Orchestrator Database** - Select the Orchestrator database server SQL Server database name.

Click **Next** to continue.

Cloud Service Process Pack Setup Wizard

Configuration

Configure System Center Orchestrator account and Database

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.

System Center Orchestrator user account:

User name: FT-SO-SVC

Password: [masked]

Domain: FLEXPOD

Test Credentials

System Center Orchestrator Database Server:

SQLCODE

SQL Server instance: SCODE

Orchestrator Database: Orchestrator

The credentials were accepted.

< Previous Next > Cancel



In the **Configure System Center Orchestrator connections** dialog, enter the following information in the provided text boxes and dropdown menus:

- **System Center Service Manager connections name** – Enter the System Center Service Manager server name.

Click **Next** to continue.

Cloud Services Process Pack Setup Wizard

Configuration

Configure the System Center Orchestrator connections

Specify the System Center Service Manager connection name that is configured in the System Center Orchestrator server.

Runbook folder name:
SM-CloudServices

System Center Service Manager connection name:
FT-SCSM

< Previous Next > Cancel

SC 2012 Service Manager

Connections

Configure the connections for Microsoft System Center Service Manager.

Name	Server	User	Domain
FT-SCSM	FT-SCSM.FLEXPOD.TEST	Administrator	FLEXPOD

Add... Edit... Remove

Finish Cancel Help

The **Installation summary** dialog will appear and display the selections made during the installation wizard. Review the options selected and click **Install** to continue.

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.

Program files location:
C:\Program Files (x86)\Microsoft System Center 2012\Orchestrator\Cloud services runbooks

System Center Orchestrator Database Server:
SQLSC0008\SC0008

Orchestrator Administrator account:
FLEXPOD\Administrator

Orchestrator Database:
Orchestrator

Runbook folder name:
SM-CloudServices

System Center Service Manager connection name:
FT-SCSM

Install log file path:
C:\Users\administrator.FLEXPOD\AppData\Local\SCCloudServices\LOGS\SCCloudServicesrunbookinstall05.log

< Previous Install Cancel

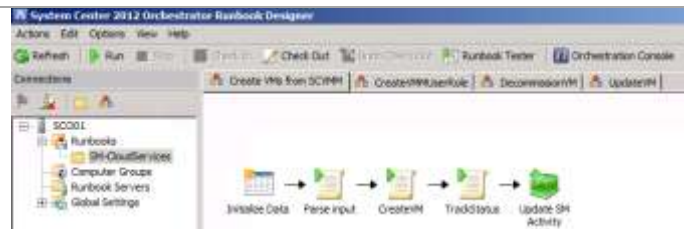


When the installation completes, the wizard will display the **Setup completed successfully** dialog.

Click **Close** to complete the installation.



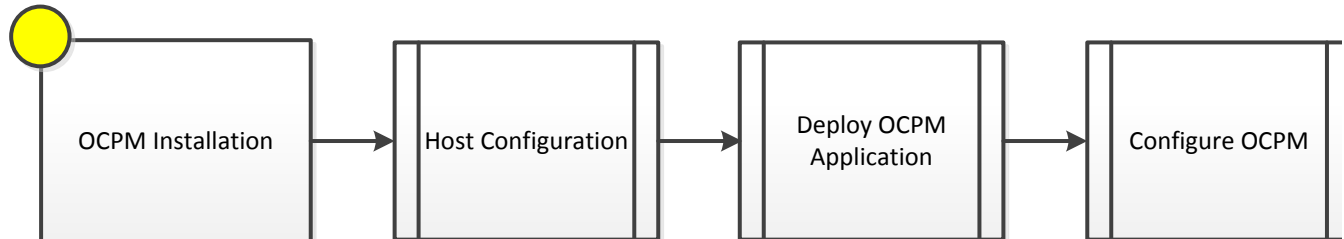
To verify the installation, open **Runbook Designer** and validate that the SM-CloudServices runbooks were added to the Orchestrator instance.





OnCommand Plug-in for Microsoft (OCPM)

The OCPM installation process is comprised of the following high-level steps:



Overview

This section provides high-level walkthrough on how to install and configure OCPM. The following assumptions are made:

- All previous steps in this guide are complete.
- All virtual machines are fully patched and joined to the domain.

OCPM is used for management and provisioning tasks. The OCPM software will need to be installed on the following servers:

- The SCOM VM
- The SCO VM
- All Hyper-V Host Blades (any windows machine that will be running the Hyper-V role)

In addition, each host will need to have a local cache for every NetApp storage controller in the environment. By default, this is the two nodes included in the FlexPod deployment. You will need to expand these steps for any additional storage infrastructure you choose to deploy.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User Name	Purpose	Permissions
<DOMAIN>\FT-OCPM-SVC	OCPM Service Account	This account will need to be a local admin of any server where provisioning will be performed.

Configuring Hosts

For each host to be managed, use the following steps. .NET 3.51 may already be installed, but the steps are listed here for reference.



Perform the following steps on all machines to be managed by OCPM.

Windows Features

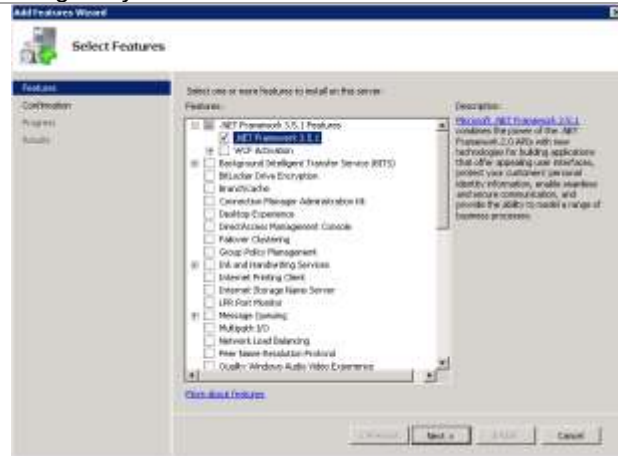
Open Server Manager and select Features.

Click the Add Features link launching the Add Features wizard.

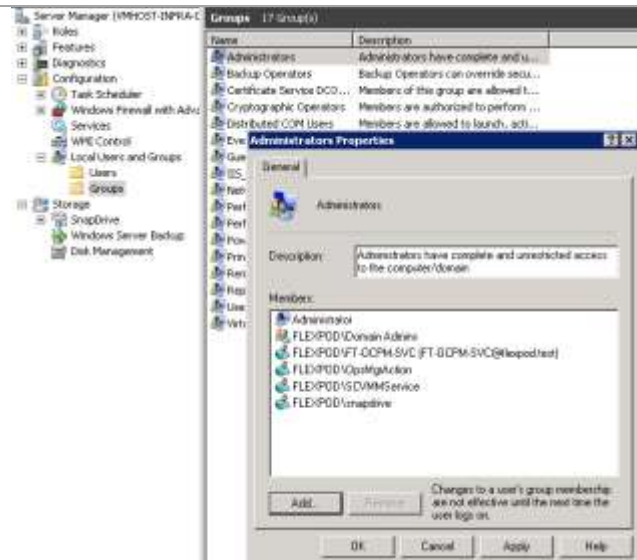
Expand .NET Framework 3.5.1 Features.

Select the .NET Framework 3.5.1 Feature.

Click Next > Install.



The OCPM service account will need to have local administrator rights to each server being managed. Use server manager to add the FT-OCPM-SVC account to the local administrators group.

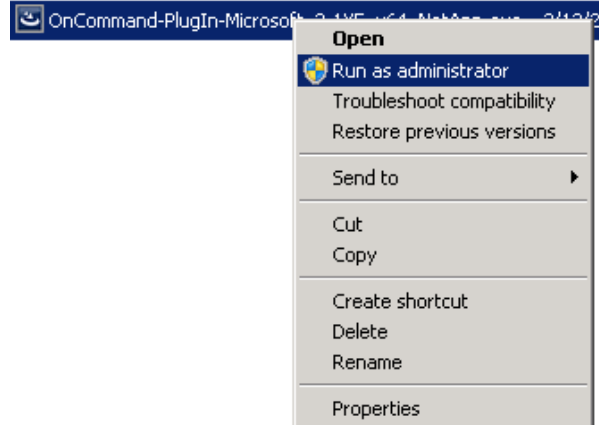


Installing OCPM

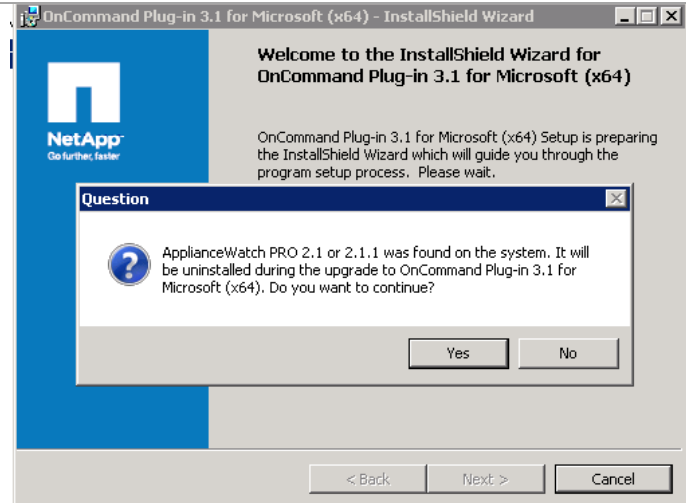
Perform the following steps on all machines to be managed by OCPM.



Right click on the OCPM install source and select "Run as Administrator"



If you are upgrading your install from a previous version, you will be prompted to un-install. Click yes to proceed.

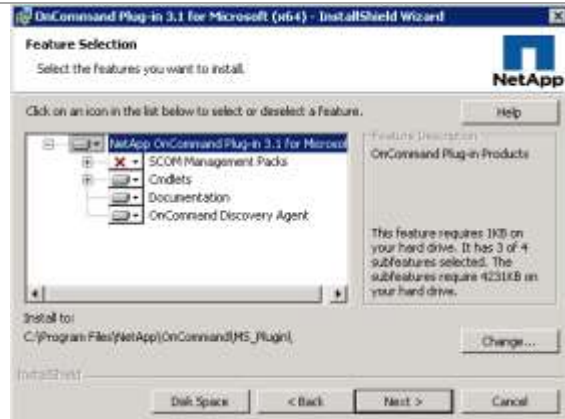


Click next, accept the license agreement, click next then click next again to accept the default installation location.

For all machines except the SCOM VM, install all components EXCEPT the SCOM management packs. On THAT VM ONLY, install the SCOM Management Packs also.

On the SCO VM, you will also be allowed to install the System Center Orchestrator Integration Packs, ensure that they are selected for installation.

Click next.





Enter the OCPM service account created above.
Enter the password and click Next.

Click Install on the next screen to begin the installation.

The screenshot shows the 'Web Service Credentials' screen of the 'OnCommand Plug-in 3.1 for Microsoft (x64) - InstallShield Wizard'. The title bar includes the NetApp logo. The subtitle is 'Specify User Credentials and Port for Web Service'. The form contains the following fields and controls:

- Account (example: Domain\Administrator):** A text box containing 'FLEXPOD\FT-OCPM-SVC' and an 'Add...' button.
- Password:** A text box with masked characters (dots).
- Confirm Password:** A text box with masked characters (dots).
- Web Service Tcp/Ip Endpoint (Port):** A text box containing '808'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.
- Footer:** 'InstallShield'.

Click Finish to complete the installation.

The screenshot shows the 'InstallShield Wizard Completed' screen of the 'OnCommand Plug-in 3.1 for Microsoft (x64) - InstallShield Wizard'. The title bar includes the NetApp logo. The subtitle is 'InstallShield Wizard Completed'. The content area contains the following text and controls:

- Text:** 'The InstallShield Wizard has successfully installed OnCommand Plug-in 3.1 for Microsoft (x64). Click Finish to exit the wizard.'
- Checkbox:** 'Show the Windows Installer log' (unchecked).
- Buttons:** '< Back', 'Finish', and 'Cancel'.
- Footer:** The NetApp logo and the tagline 'Go further, faster'.



Test the installation by opening the OCPM prompt on your desktop and using the Get-OCStorage cmdlet.

You should see output similar to the picture to the right.

Note that the command will only return results if the Windows server has NetApp LUNs mounted.

```
Administrator: OnCommand Cmdlets
CLIENTNAME: FLEXP0D-JUMP
COMPUTERNAME: UPM001-1MFR0-01
LOGONSERVER: \\1MFR0-DC-01
SESSIONNAME: RDP-Tcp08
USERNAME: administrator
USERDOMAIN: FLEXP0D
USERDNSDOMAIN: FLEXP0D.TEST
OS: Windows_NT
PS C:\Users\administrator.FLEXP0D> Get-OCStorage

DeviceID : \\?\PhysicalDrive0
LunSize : 139591226880
VolumeGUID : \\?\Volume{a6bdda99-1c65-11e1-a656-886e6f6e6963}\
LunPath : Hyper-V\FlexPod-P0S-0:\vol\acc_boot\vn-host-info-01
MountPoint : \\?\Volume{a6bdda99-1c65-11e1-a656-886e6f6e6963}\
SCSIAddress : Port number = 1 Bus no = 0 Target Id = 0 LUN Id = 0
DiskSerialNumber : 60L472M390
DiskGUID : 03bf47c6-0000-0000-0000-000000000000
DiskClustered : False
DiskResourceNodeOwner :
DiskResourceClusterName :
DiskResourceClusterGroup :
DiskResourceName :
CSWDisk : False
CSUNodeOwnerName :
CSUParsePoint :

DeviceID : \\?\PhysicalDrive1
LunSize : 193285854720
VolumeGUID : \\?\Volume{ac3e19b7-3506-11e1-9fb9-0825b6e126fd}\
LunPath : Hyper-V\FlexPod-P0S-0:\vol\acc_boot\vn-host-info-01
MountPoint : C:\NBD\
SCSIAddress : Port number = 1 Bus no = 0 Target Id = 0 LUN Id = 1
DiskSerialNumber : 78C218A1377e
DiskGUID : 65f97497-0000-0000-0000-000000000000
DiskClustered : False
DiskResourceNodeOwner :
DiskResourceClusterName :
DiskResourceClusterGroup :
DiskResourceName :
CSWDisk : False
CSUNodeOwnerName :
CSUParsePoint :

DeviceID : \\?\PhysicalDrive2
LunSize : 10995258193280
VolumeGUID : \\?\Volume{fb12156d-ced3-4d25-b93e-d24515f93356}\
LunPath : Hyper-V\FlexPod-P0S-0:\vol\FI_Gold\CSU_Gold
MountPoint : \\?\Volume{fb12156d-ced3-4d25-b93e-d24515f93356}\
SCSIAddress : Port number = 2 Bus no = 0 Target Id = 1 LUN Id = 2
DiskSerialNumber : 78C218A1786c
DiskGUID : 6b27408d-47dc-4352-95cc-c989916c6d57
DiskClustered : True
```

Depending on your PowerShell security settings, you may receive an error message like the one on the right.

You may need to change your execution level by using the Set-ExecutionPolicy cmdlet.

For example:

Set-ExecutionPolicy RemoteSigned

```
Administrator: OnCommand Cmdlets
PS C:\Program Files\NetApp\OnCommand\PS_Plugin> Get-OCStorage
Get-OCStorage: The execution of scripts is disabled on this system. Please see 'get-help about_executionpolicy' for more details.
PS C:\Program Files\NetApp\OnCommand\PS_Plugin> Set-ExecutionPolicy RemoteSigned
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic. Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y") y
PS C:\Program Files\NetApp\OnCommand\PS_Plugin>
```



Add your storage system credentials by using the Add-OCStorageSystem cmdlet.

For example:

Add-OCStorageSystem <Controller> -User
<username> -Password <Password>

Please NOTE: Although the Data ONTAP PS Toolkit can use either user level or system level credential cache, OCPM supports only SYSTEM level credential cache. If you would like to use both the PS toolkit and OCPM, you must use only SYSTEM level cache which is the only type of credential you can create with the Add-OCStorageSystem cmdlet but is optional if you use the New-NaCredential cmdlet from the Data ONTAP PS Toolkit.

```
Administrator OnCommand Gridlets
PS C:\Users\Administrator.FLEXPOD> Add-OCStorageSystem Hyper-9-FlexPod-FRS-A -Us
er administrator -Password [REDACTED]

OperationStatus : Success
Type            :
ScriptLink      :
Source          :
Resolution      :
RecoverableError : True
Description     :
StackTrace      :
Detail          :
Message         : Add-OCStorageSystem: Successfully added the Hyper-9-FlexPo
d-FRS-A StorageSystem.
ErrorCode       : 0
Error           : Add-OCStorageSystem: Successfully added the Hyper-9-FlexPo
d-FRS-A StorageSystem.
ErrorCode       : 0
IsRecoverableError : True
ShowError       : False

PS C:\Users\Administrator.FLEXPOD> Add-OCStorageSystem Hyper-9-FlexPod-FRS-B -Us
er administrator -Password [REDACTED]

OperationStatus : Success
Type            :
ScriptLink      :
Source          :
Resolution      :
RecoverableError : True
Description     :
StackTrace      :
Detail          :
Message         : Add-OCStorageSystem: Successfully added the Hyper-9-FlexPo
d-FRS-B StorageSystem.
ErrorCode       : 0
Error           : Add-OCStorageSystem: Successfully added the Hyper-9-FlexPo
d-FRS-B StorageSystem.
ErrorCode       : 0
IsRecoverableError : True
ShowError       : False

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

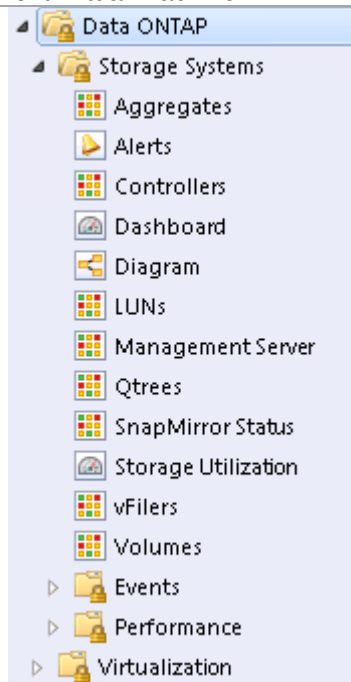
Configuring OCPM

Before using OCPM's System Center integration capabilities, you must first configure it. There are specific steps for both SCOM and SCO. We will handle them separately.

OCPM SCOM MP

Perform the following steps on the SCOM management virtual machine.

Open the SCOM management console, you should now see a DataONTAP element in the left hand tree view in the monitoring pane.





Click on the "Management Server" element.
Wait for the right hand pane to populate. Then select "Data ONTAP: Add Controller"

Health Service Tasks

- Check Health Service Startup Configuration Diag
- Computer Management
- Data ONTAP PRO: Run PRO discovery task
- Data ONTAP Virtualization: Run virtualization dis
- Data ONTAP: Add Controller
- Data ONTAP: Manage Controller Credentials
- Data ONTAP: Manage DFM Servers
- Data ONTAP: Run discovery task
- Disable Audit Collection
- Enable Audit Collection
- Flush Health Service State and Cache
- Get the agent processor utilization
- Get The Pool Member Monitoring a Top Level In
- Get Top Level Instances Monitored By a Pool Me

Enter the name or IP address of your NetApp storage controller then click Add.

Do this for all controllers that you wish to manage.

Add Controller

Management Server Name: FT-SCOM.flexpod.test

SNMP Community String: public

Controller to add

Enter the name, or network address, of the controller you want to add.

Name or address: 10.10.0.11

Add

Cancel



Note that the SNMP Community String above will need to match your controller's string. You can check this setting in System Manager under Configuration, System Tools, SNMP.

SNMP

 Edit  Refresh

SNMP:  Enabled
Traps:  Enabled
Location: UCS TME LAB
Contact:

Trap Host IP Addresses

10.10.0.60

Community Names

1FlexPod1



From the same right hand pane, select “Data ONTAP: Run Discovery Task”

The dialog box titled "Run Task - Data ONTAP: Run discovery task" contains the following sections:

- Run the task on these targets:** A table with two columns: "Target" and "Run Location". It contains one entry: "FT-SCOM.flexpod.test" in both columns.
- Task Parameters:** A table with two columns: "Name" and "Value". It contains one entry: "TimeoutSeconds" with a value of "3600".
- Override:** A button.
- Task credentials:** Radio buttons for "Use the predefined Run As Account" (selected) and "Other". Below are fields for "User name:", "Password:", and a dropdown for "Domain:" set to "FLEXPOD".
- Task description:** A text block stating: "This task runs the Data ONTAP discovery rule on the selected management server. Rather than waiting for the normal discovery rule to run, the operator may wish to run this task manually after importing this management pack or after making changes to the Data ONTAP storage systems being monitored."
- Task confirmation:** A checkbox labeled "Don't prompt when running this task in the future".
- Buttons:** "Run" and "Cancel" at the bottom right.

Confirm that the task completes successfully.

The dialog box titled "Task Status - Data ONTAP: Run discovery task" displays the following information:

- Task completed successfully:** A message at the top.
- Task Table:** A table with columns "Task", "Status", and "Task Target". It shows one task: "Data ONTAP: Run discovery t..." with a status of "Success" and target "ft-scom.flexpod.test".
- Task Output:** A section with a "Copy Text" and "Copy HTML" button. It contains a table with two columns: "Data ONTAP: Run discovery task" and "Task Description".

Status:	Success	This task runs the Data ONTAP discovery rule on the selected management server. Rather than waiting for the normal discovery rule to run, the operator may wish to run this task manually after importing this management pack or after making changes to the Data ONTAP storage systems being monitored.
Scheduled Time:	3/14/2012 3:54:57 PM	
Start Time:	3/14/2012 3:54:58 PM	
Submitted By:	FLEXPODAdministrator	
Run As:		
Run Location:		
Target:		
Target Type:	Management Server	
Category:	Discovery	
- Footer:** A note stating "You can close this dialog at any time. Doing so will not interrupt executing tasks. You can check the status of tasks in a task status view." and a "Close" button.



On the left pane, navigate to Authoring. Open “Management Pack Objects” and click on “rules.”

Reduce the number of rules in the view by typing “Data ONTAP” into the search box and clicking “Find Now.” You should see only Data ONTAP related rules. Scroll down to “Type: Management Server” and double click “Data ONTAP: Discovery Rule”

Click on the “Overrides” tab and click “Override.”

Select “For all objects of class: Management Server”

Rules (16)

Management pack objects are now scoped to: Computer, Mobile device, Windows Comp

Look for: Data ONTAP Find Now Clear

Name	Inherited from
Type: Collection Server (2)	
Data ONTAP Virtualization: Discovery Rule	Management Server
Data ONTAP: Discovery Rule	Management Server
Type: Data Warehouse Connection Server (2)	
Data ONTAP Virtualization: Discovery Rule	Management Server
Data ONTAP: Discovery Rule	Management Server
Type: Gateway (2)	
Data ONTAP Virtualization: Discovery Rule	Management Server
Data ONTAP: Discovery Rule	Management Server
Type: Management Server (2)	
Data ONTAP Virtualization: Discovery Rule	Management Server
Data ONTAP: Discovery Rule	Management Server

Data ONTAP: Discovery Rule Properties

General Configuration Product Knowledge Company Knowledge Overrides

Overrides are used to modify the rule configuration. You can override the configuration by choosing one of the options below:

Disable this rule through overrides:

Choose the context in which you want to disable the rule and click "Disable" button.

Example: Disable the rule for all Windows computers.

Disable...

Override one or more parameters of this rule through overrides:

Example: Change threshold value from 20% to 40% for all Windows computers.

Override...

For all objects of class: Management Server

For a group...

For a specific object of class: Management Server

For all objects of another class...

Summary

You can view all overrides

Example: View the objects this rule has been enabled for.

View summary...

Close



In the Override properties dialog box, check the box next to “enabled” and set the override value to “true”.

VERY IMPORTANT: Do not save these changes to the default management pack. If you do, you will not be able to uninstall OCPM or upgrade to a new version! This is because you will have created a dependency between OCPM and the default MP.

Click “New” to create a new MP to store your changes.

Override Properties

Rule name: Data (ONTAP) Discovery Rule
Category: Discovery
Override target: Class: Management Server

Override-controlled parameters:

Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
☒	Enabled	Boolean	False	True	False	Added
☐	Interval Seconds	Integer	65400	65400	65400	(No change)
☐	Sync Time	String	21:00	21:00	21:00	(No change)
☐	Forward Seconds	Integer	3000	3000	3000	(No change)

Default: Enabled Description: The new custom override will be created in the [Not available] Click apply to view the new effective value for the parameter.

Management pack: Select destination management pack: [Select Management Pack] New

Help OK Cancel

Give your new MP a name, then click Next then create.

Create a Management Pack

General Properties

Management Pack General Properties

ID: Fast Track, Default Settings

Name: Fast Track, Default Settings

Version: 1.0.0.0 For example, 1.0.0.0

Description:

Previous Next Cancel



Your new MP should be listed as “Destination management pack.” Click OK to finish the wizard.

Override Properties

Rule name: Data ONTAP: Discovery Rule
Category: Discovery
Overrides target: Class: Management Server

Override-controlled parameters:

Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
☒	Enabled	Boolean	False	True	False	[Added]
☐	IntervalSeconds	Integer	65400	65400	65400	[No change]
☐	Sync Time	String	21:00	21:00	21:00	[No change]
☐	TimeoutSeconds	Integer	3600	3600	3600	[No change]

Details:

Enabled Description
The new custom override will be created in the Fast Track Default Settings. Click apply to view the new effective value for this parameter.

Management pack
Select destination management pack:
Fast Track Default Settings [New...]

Help OK Apply Cancel

Repeat this process for the Data ONTAP Virtualization: Discovery Rule. Except this time, simply select the same MP you created above. You do not need to create another new MP.

Click OK to finish the wizard.

Override Properties

Rule name: Data ONTAP Virtualization: Discovery Rule
Category: Discovery
Overrides target: Class: Management Server

Override-controlled parameters:

Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
☒	Enabled	Boolean	False	True	False	[Added]
☐	IntervalSeconds	Integer	14400	14400	14400	[No change]
☐	Sync Time	String	2:30	2:30	2:30	[No change]
☐	TimeoutSeconds	Integer	3600	3600	3600	[No change]

Details:

Enabled Description [Link](#)
The new custom override will be created in the Fast Track Default Settings. Click apply to view the new effective value for this parameter.

Management pack
Select destination management pack:
Fast Track Default Settings [New...]

Help OK Apply Cancel



Navigate back to the monitoring pane and open the ONTAP section of the tree view. Select controllers.

On the left, select “Data ONTAP: Manage Controller Credentials”

Data ONTAP Controller Tasks

- ☐ Data ONTAP: Launch FilrView
- ☐ Data ONTAP: Manage Controller Credentials
- ☐ Data ONTAP: Manage DFM Servers
- ☐ Data ONTAP: Remove Controller

Enter valid administrator credentials for each of the controllers you wish to manage. Confirm that the credentials were accepted as indicated by a green check mark next to each controller.

Click OK to close the wizard.

Valid Connection	Name	IP Address	Type	Requires HTTPS
☒	HyperV FlexPod FAS-A-01	10.10.0.11	Controller	Yes
☒	HyperV FlexPod FAS-B-01	10.10.0.12	Controller	Yes

Controller/Vfiler: HyperV FlexPod FAS-B-172.25.205.7 Total controllers and vfiler: 2

User name: administrator

Password: *****

Domain:

Requires HTTPS: IP

OK Cancel Help

Discovery and inventory will now proceed on a scheduled basis. You can speed up this process by manually running the Data ONTAP discovery task again manually.

It may take several hours for inventory information to begin populating.

OCPM OIP

Perform the following steps on the SCO virtual machine.

Open the SCO deployment manager.

SCO Deployment Manager

Tasks

Task Name	Status
SCO Deployment Manager	Success
SCO Deployment Manager	Success
SCO Deployment Manager	Success

Log

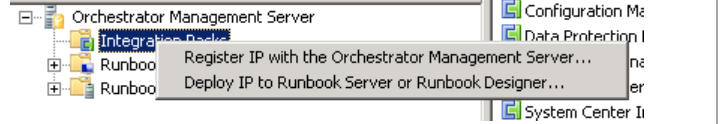
SCO Deployment Manager

SCO Deployment Manager

SCO Deployment Manager



Right click on “Integration Packs” and select “Register IP with the Orchestrator Management Server”



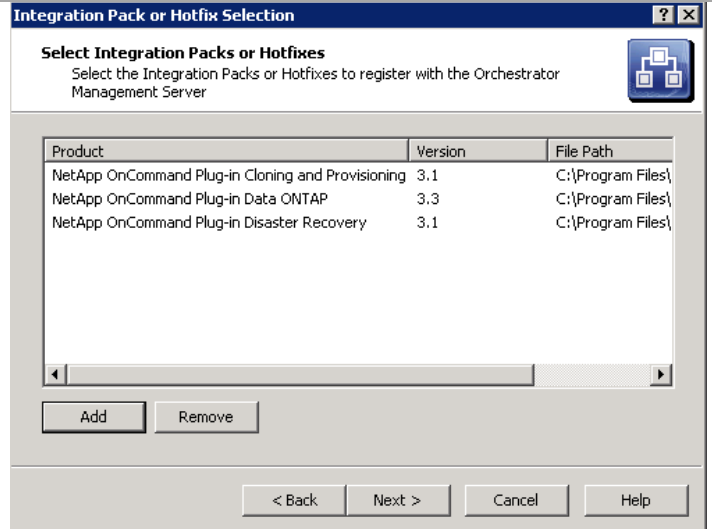
Click next to start the wizard and then add the three OCPM OIP's using the “Add” Button.

By default, these files are installed into:

C:\Program
Files\NetApp\OnCommand\MS_Plugin

Or whatever directory was specified at install time.

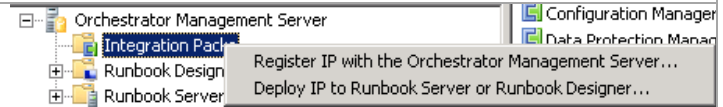
Click Next, then finish.



Confirm that the registration was successful by checking the list of registered OIPs on the main screen.



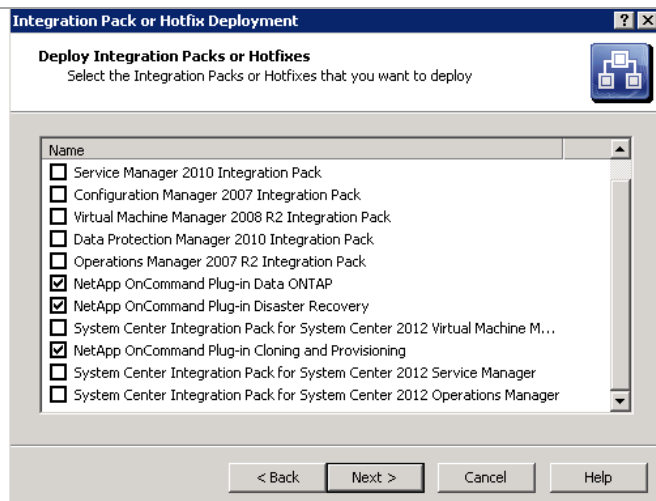
Right click on “Integration Packs” and select “Deploy IP to Runbook Server or Runbook designer”



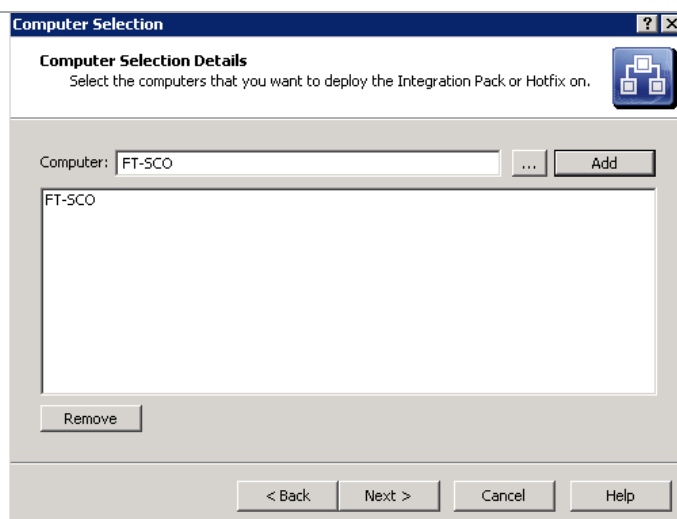


Click next to start the wizard.

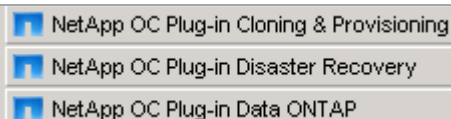
Select the three NetApp OIP's to deploy them.
Click Next.



Enter your SCO server name and click ADD to add it to the list of targeted servers. Click Next, Next, Finish to begin the deployment.



Confirm the installation was successful by opening the Runbook designer and confirming that the OIPs are listed on the right.



Appendix A: SQL Cluster Named Instance Worksheet

SQL Instance Name
SQL Instance Failover Cluster Network Name



SQL Instance DATA Cluster Disk Resource
SQL Instance LOG Cluster Disk Resource
SQL Instance Install Drive
SQL Instance DATA Drive
SQL Instance LOG Drive
SQL Instance TEMPDB Drive
Cluster Service Name
Clustered SQL Instance IP Address
Host Cluster Public Network Interface Subnet Mask
Host Cluster Public Network Interface Name



Appendix B: Installing a WDS Server

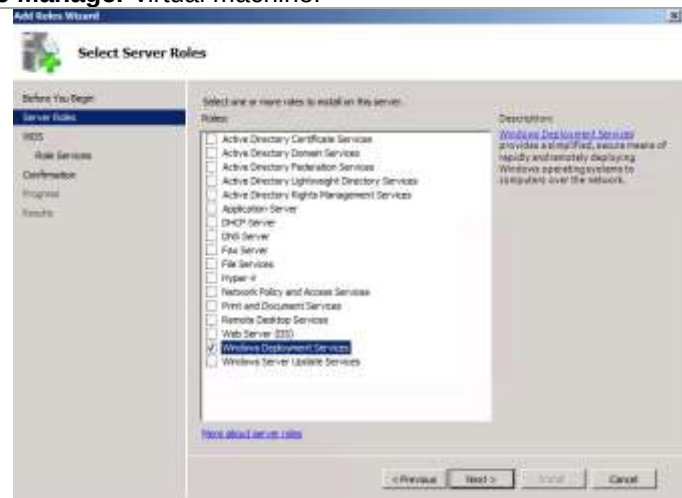
For customers who choose to use traditional PXE based VM or windows server deployment, WDS Server is required. This is not recommended by NetApp or Cisco, but customers may use this method if they prefer. The following steps are provided for deployment of WDS:

Adding the Windows Deployment Services Role

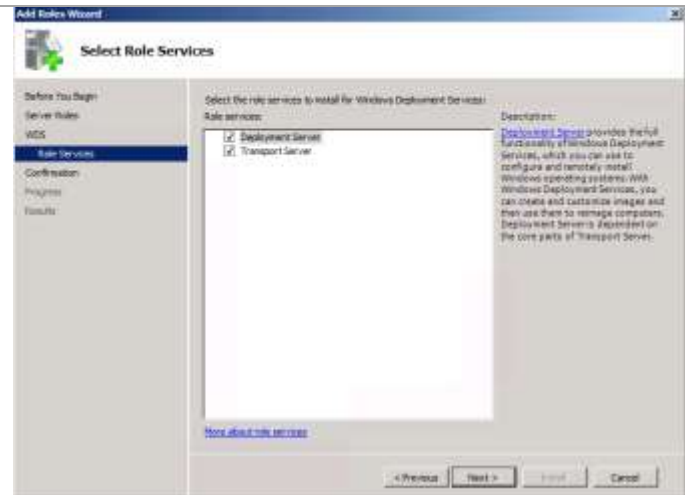
The following steps are provided in the event a WDS server must be installed:

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

To add the .NET Framework 3.5.1 Feature, from **Server Manager**, select the **Roles** node and click **Add Roles**. The **Add Roles Wizard** will appear. In the **Select Server Roles** dialog, select the **Windows Deployment Services** checkbox.

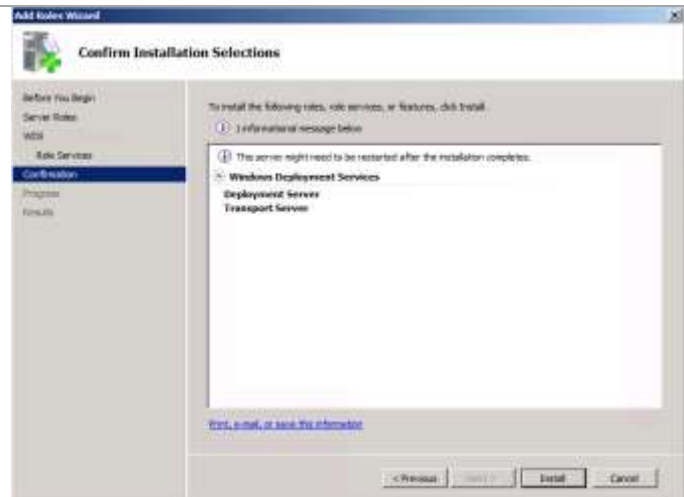


The **Add role services** dialog will appear. Select the **Deployment Server** and **Transport Server** checkboxes. Click **Next** to continue.

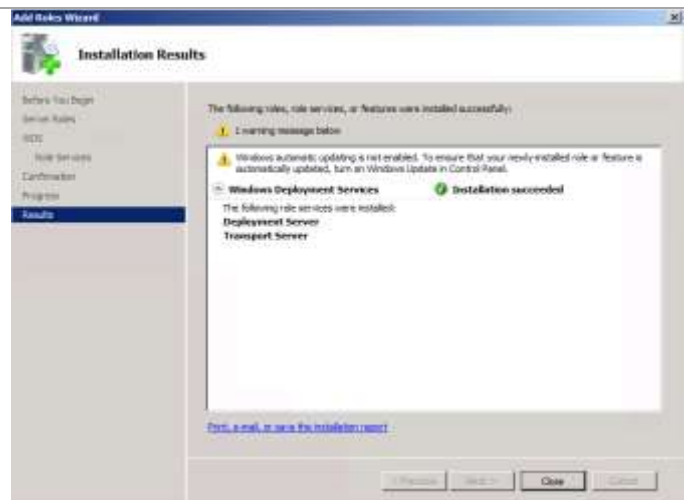




In the **Confirm Installation Selections** dialog, review the choices made during the wizard and click **Install** to add the feature.



When complete, the **Installation Results** dialog will appear. Verify that all dependent role services installed correctly. When verified, click **Close** to complete the installation of Windows Deployment Services role.



Cisco UCS PowerTool

The Cisco UCS PowerTool should be installed within the Virtual Machine Manager and Orchestrator runbook servers.

Download the Cisco UCS PowerTool version 0.9.9.0 or newer from the Cisco Developer Network. It can be found in the Microsoft Management section - <http://developer.cisco.com/web/unifiedcomputing/microsoft>.

Extract the zip file and execute the extracted exe file.

Cisco PowerTool need to be installed in the Virtual Machine Manager virtual machine and the Orchestrator virtual machine.

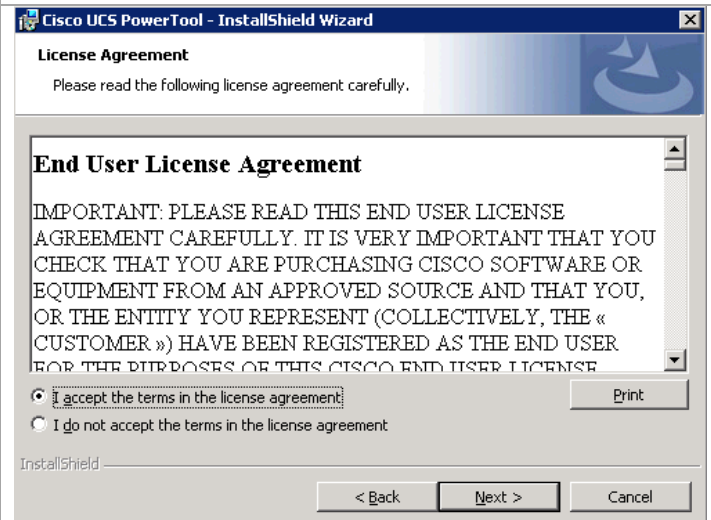
Perform the following steps on the Virtual Machine Manager and Orchestrator virtual machines



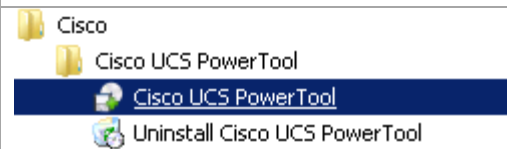
Launch the Cisco UCS PowerTool Installer. The **Setup Wizard** screen appears.



Read and accept the end user license agreement. Click **Next** to continue.

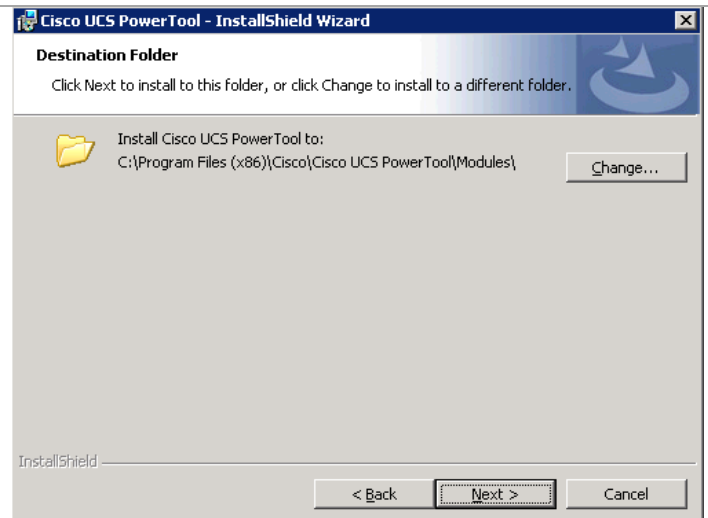


Verify proper PowerTool installation by launching the PowerTool console. Click **Start** and **All Programs**. Expand **Cisco** and select **Cisco UCS PowerTool**.

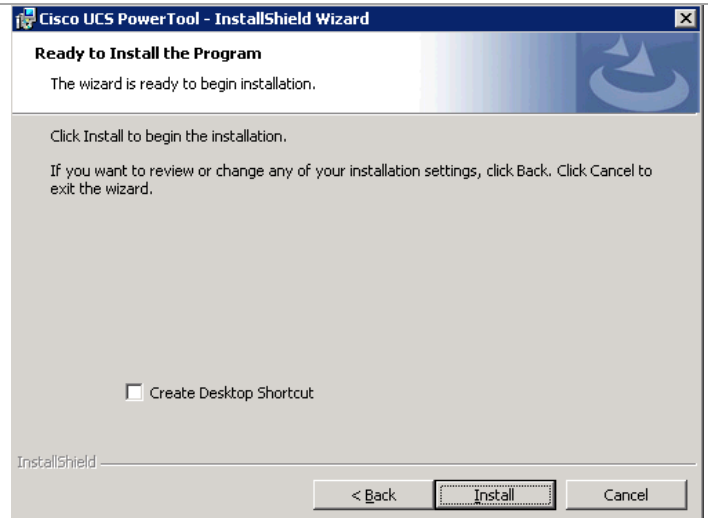




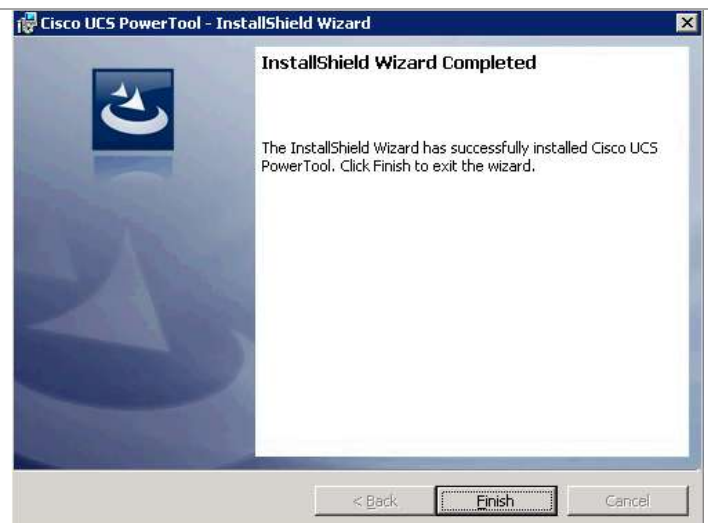
Select the **Destination Folder** and click **Next** to continue.



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.





Enter the command:

Connect-ucs <FI cluster FQDN or IP>

Note:

To manually load into a different PowerShell environment, such as Microsoft's ISE or PowerGUI, modify your PowerShell startup file, or manually import the module with the PowerShell command

Import-Module CiscoUcsPs

or use the command

Import-Module "C:\Program Files (x86)\Cisco\Cisco UCS PowerTool\Modules\CiscoUcsPs\CiscoUcsPs.ps1"

```
Administrator: Cisco UCS PowerTool
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool\Modules\CiscoUcsPs>C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPs.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> Connect-ucs ucsm.flexpod.test_
```

Enter the UCS Manager login credentials.

Windows PowerShell Credential Request

Enter your credentials.

User name:

Password:

OK Cancel

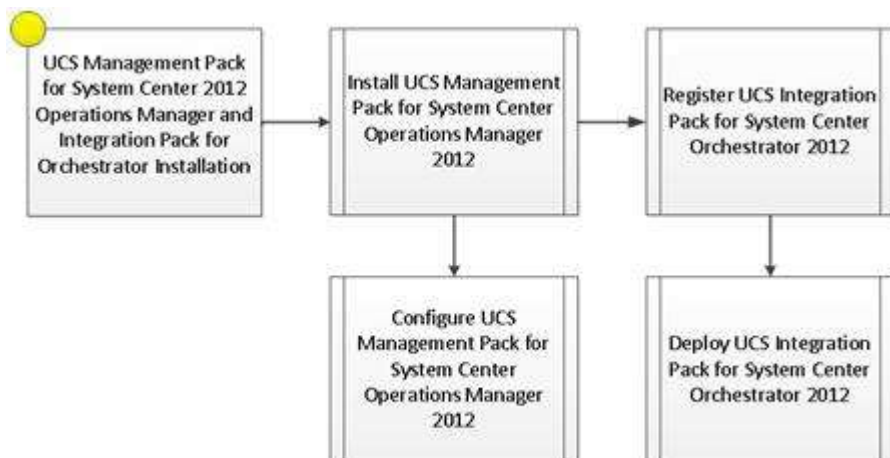
UCS PowerTool returns the UCS Manager session connection information. This indicates that PowerTool is properly installed and is operational.

```
Administrator: Cisco UCS PowerTool
PS C:\> Connect-ucs ucsm.flexpod.test_
Proxy :
Cookie : 1343256241/8be66ee8-ce3e-4591-94e8-227f2285b209
Domain :
LastUpdatedTime : 7/25/2012 4:13:44 PM
Name : ucsm.flexpod.test
NoSsl : False
RunPendingConfig : 0
RunMatchers : 0
Port : 443
Priv : (admin, read-only)
RefreshPeriod : 600
SessionId : web_12934_0
TransactionInProgress : False
Ucs : hyper-v-flexpod-ucsm
Url : https://ucsm.flexpod.test
UserName : admin
VirtualIp4Address : 10.10.0.6
Version : 2.0(2q)
MatchThreadStatus : None
```



Cisco UCS Management Pack for SCOM 2012 and Integration Pack for SCO 2012

The Cisco UCS Management Pack for SCOM 2012 and Integration Pack for SCO 2012 installation and configuration processes are comprised of the following high-level steps:



Overview

This section provides high-level walkthrough on how to install and configure Cisco UCS Management pack for SCOM 12201 and Cisco UCS OIP for SCO 2012. The following assumptions are made:

- All previous steps in this guide are complete.
- All virtual machines are fully patched and joined to the domain.

The Cisco UCS Management Pack for SCOM and UCS OIP for SCO are used for management and provisioning tasks. The software components need to be installed on the following servers:

- The SCOM virtual machine
- The SCO virtual machine

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following security groups have been created:

User Name	Purpose	Permissions
<DOMAIN>\ FT-OCPM-SVC	OCPM Service Account	This account will need to be a local admin of any server where provisioning will be performed.



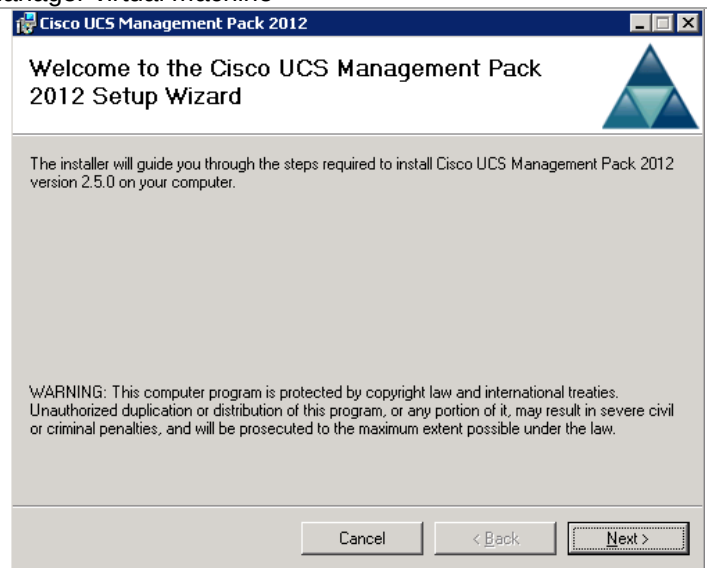
Installing the Cisco UCS Management Pack for SCOM 2012

Verify the following Components are installed in the virtual machine where management pack will be installed

- Windows PowerShell 2.0
- .NET Framework 4
- Microsoft XM Core Services 6.0 (with latest Service Pack)
- System Center 2012 Operations Manager

Perform the following steps on all the Operations Manager virtual machine

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.

The screenshot shows a window titled "Cisco UCS Management Pack 2012" with a "License Agreement" header. Below the header is a text area with the following content: "Please take a moment to read the license agreement now. If you accept the terms below, click 'I Agree', then 'Next'. Otherwise click 'Cancel'." Below this is a scrollable text box titled "End User License Agreement" containing the text: "IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE « CUSTOMER ») HAVE BEEN". At the bottom of the window are three buttons: "Cancel", "< Back", and "Next >". There are also two radio buttons: "I Do Not Agree" and "I Agree", with the "I Agree" button selected.

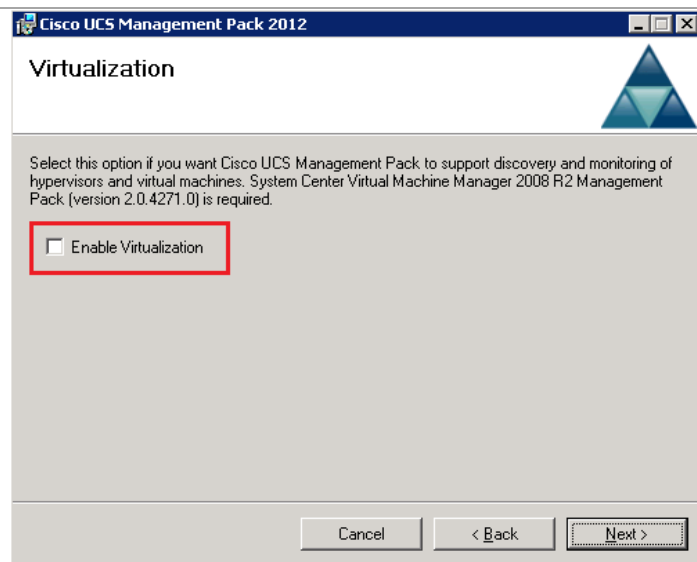
The **Connection to Management Server** screen appears. Specify the Management Server name. Click the **Next** button. **Note:** In most cases, the default value is presented from a registry value.

The screenshot shows a window titled "Cisco UCS Management Pack 2012" with a "Connection to the Management Server" header. Below the header is a text area with the following content: "Provide credentials for Management Server, where the Management Pack and script will be imported." Below this is a text box labeled "Management Server name:" containing the text "FT-SCOM.flexpod.test". At the bottom of the window are three buttons: "Cancel", "< Back", and "Next >".



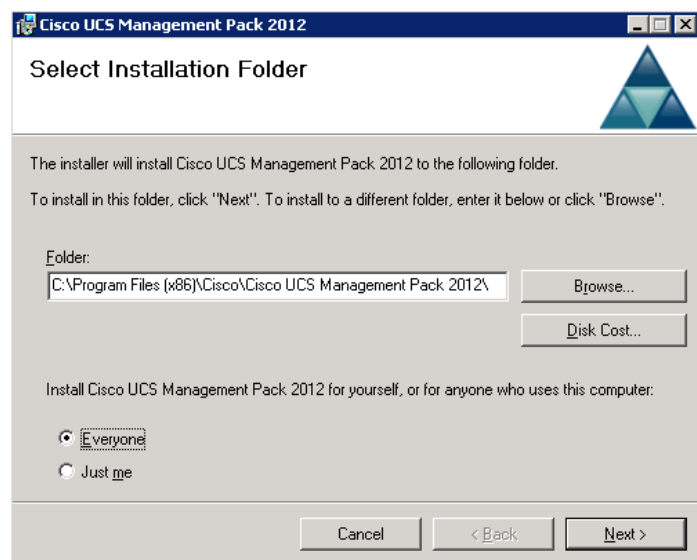
The **Virtualization** screen appears. **Do not** enable virtualization, by clicking the **Enable Virtualization** checkbox. Click the **Next** button.

Note: Cisco UCS Management Pack version 2.5.0 for SCOM 2012 does not perform discovery and monitoring of hypervisors and virtual machines managed by SCVMM 2012. This capability will be added in a future version of the UCS Management Pack for SCOM 2012.

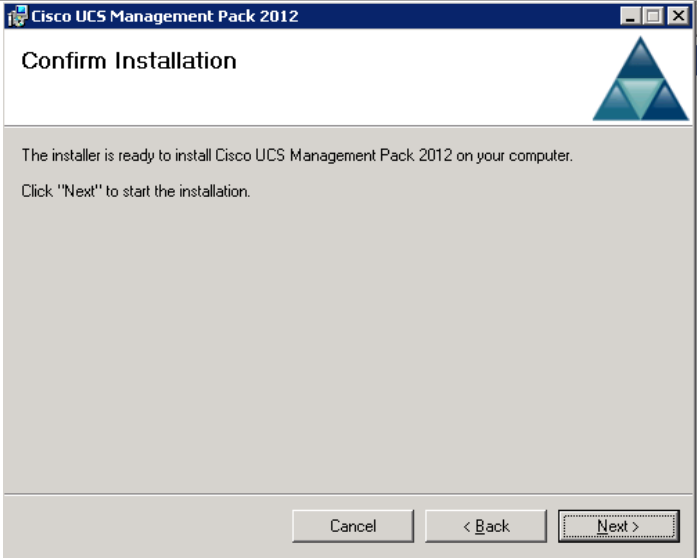


The **Select Installation Folder** Screen appears. Specify the folder location to install the Management Pack, in the **Folder** field.

Select **Everyone** and click the **Next** button.





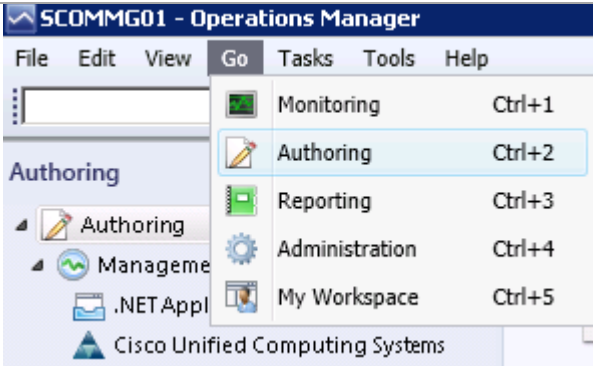
Click the Next button to start the installation.	
After successful installation of Cisco UCS Management Pack the Installation Complete screen appears. Click the Close button to exit.	

Configuring the Cisco UCS Management Pack for SCOM 2012

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.

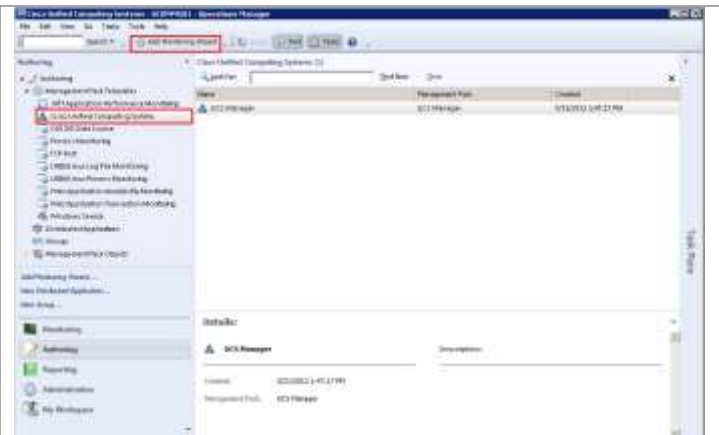
Configuring SCOM to Monitor UCS

Perform the following steps on all the Operations Manager virtual Machine

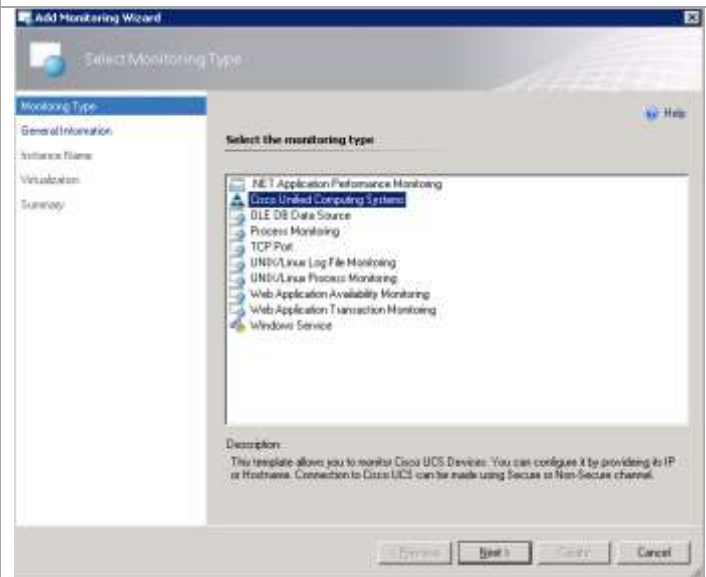
In the Operations Manager console, click the Go tab in the menu bar. Select Authoring from the drop-down menu. The Authoring column options appear.	



In the **Authoring** column, 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.





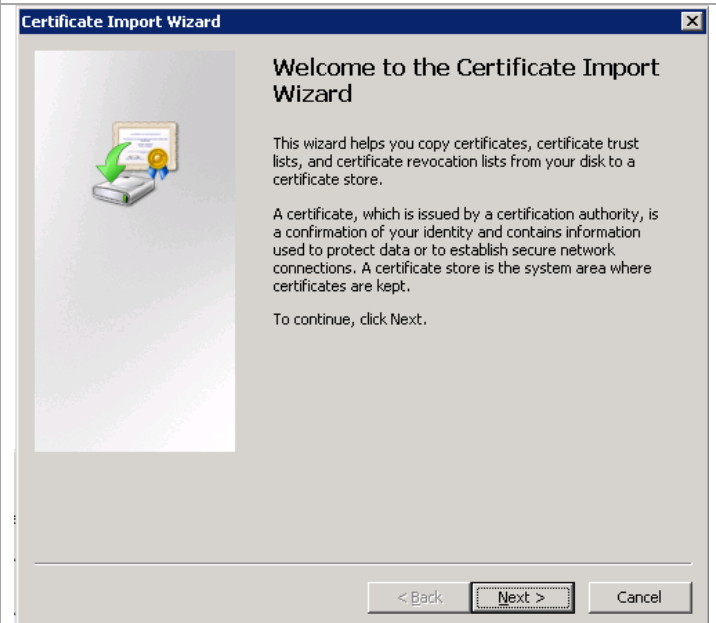
The **General Information** screen appears. Specify **IP Address/Hostname**, **Port Number** and **Connection Mode**. Click the **Test connection** button.

Click **View Certificate**.

Click **Install Certificate**.



The Certificate Import Wizard starts. Click **Next** to proceed.





Select the option **Automatically select the certificate store based on the type of certificate** and click **Next**.

The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Certificate Store' step. The window title is 'Certificate Import Wizard'. Below the title bar, the text reads 'Certificate Store' and 'Certificate stores are system areas where certificates are kept.' A paragraph follows: 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store'. Below the second option is a text box labeled 'Certificate store:' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A link 'Learn more about [certificate stores](#)' is also present.

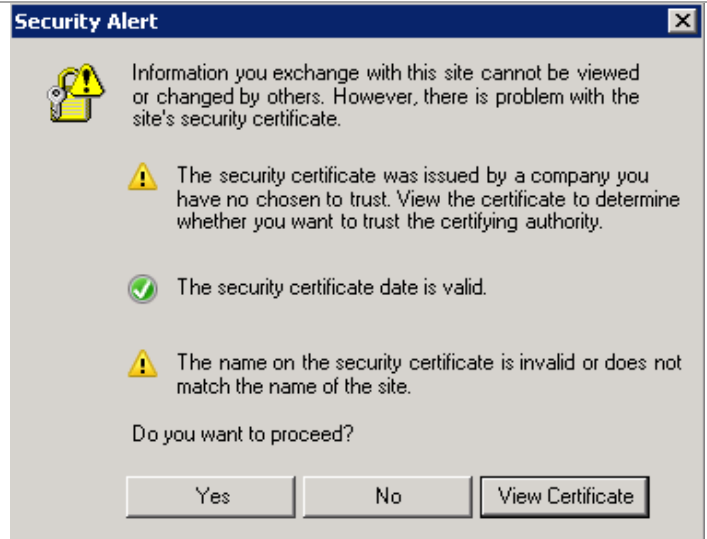
Select the default location and click **Finish**.

The screenshot shows the 'Certificate Import Wizard' window at the 'Completing the Certificate Import Wizard' step. The window title is 'Certificate Import Wizard'. On the left is an illustration of a certificate being imported. The main text says 'Completing the Certificate Import Wizard' and 'The certificate will be imported after you click Finish.' Below this, it says 'You have specified the following settings:' followed by a table. The table has two columns: 'Certificate Store Selected' and 'Automatically determined by the Content'. The first row shows 'Content' under the first column and 'Certificate' under the second. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Certificate Store Selected	Automatically determined by the Content
Content	Certificate

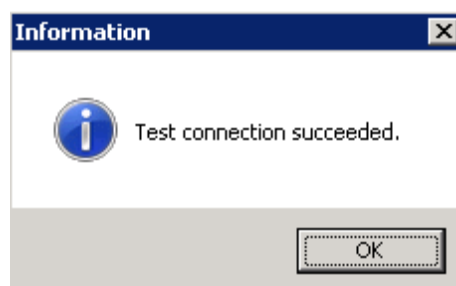
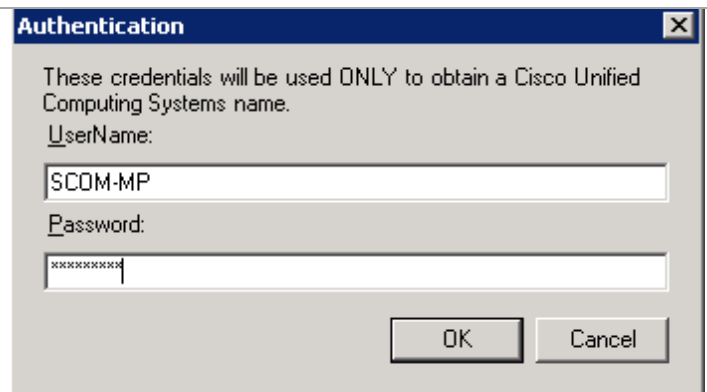


Click **Yes** to proceed.



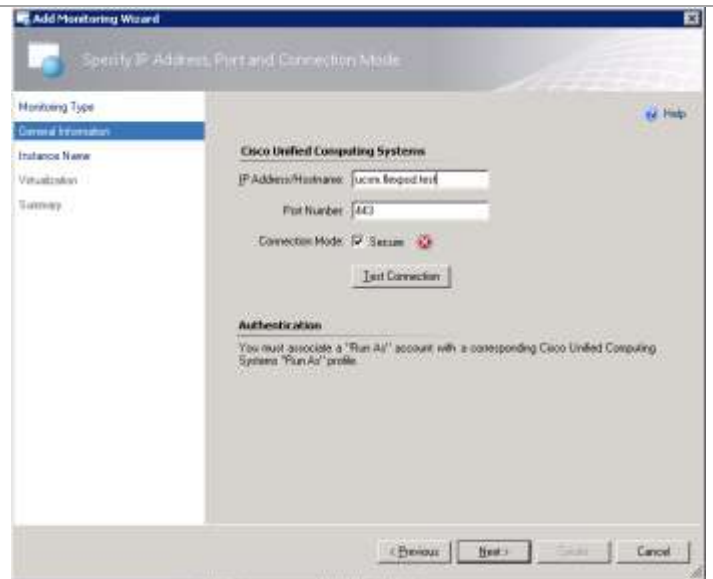
Enter the **Cisco UCS Manager SCOM Management Pack** account created earlier. Enter the account **password** and click **Next**.

Click **OK** to close the information window



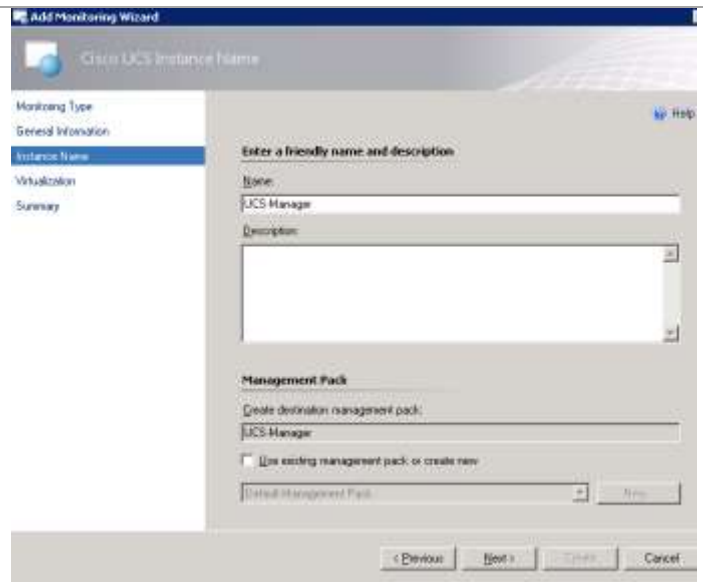


Click **Next** to proceed.



The screenshot shows the 'Add Monitoring Wizard' window with the 'Specify IP Address, Port and Connection Mode' step. The left sidebar has 'Monitoring Type' selected. The main area is titled 'Cisco Unified Computing Systems'. It contains input fields for 'IP Address/Hostname' (ucsm.bridged.net) and 'Port Number' (443). The 'Connection Mode' is set to 'Secure' with a red 'X' icon. A 'Test Connection' button is present. Below this is an 'Authentication' section with a note: 'You must associate a "Run As" account with a corresponding Cisco Unified Computing Systems "Run As" profile.' At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'OK'.

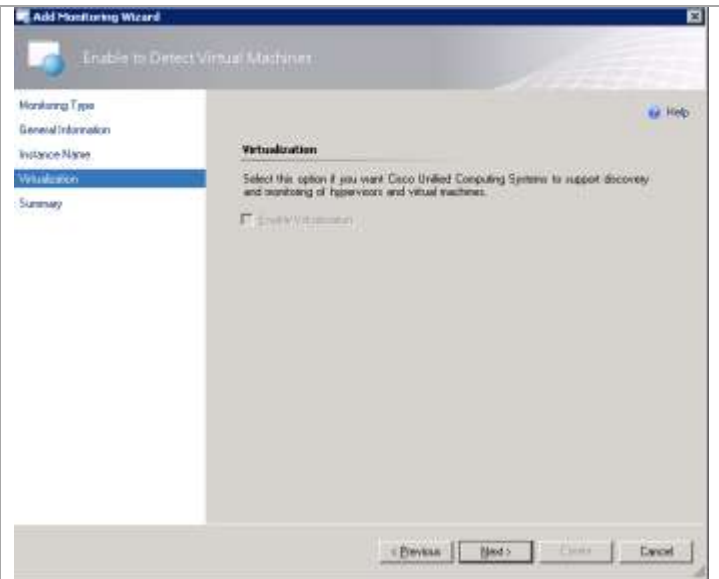
Enter the **Cisco UCS Manager** instance name and click **Next**.



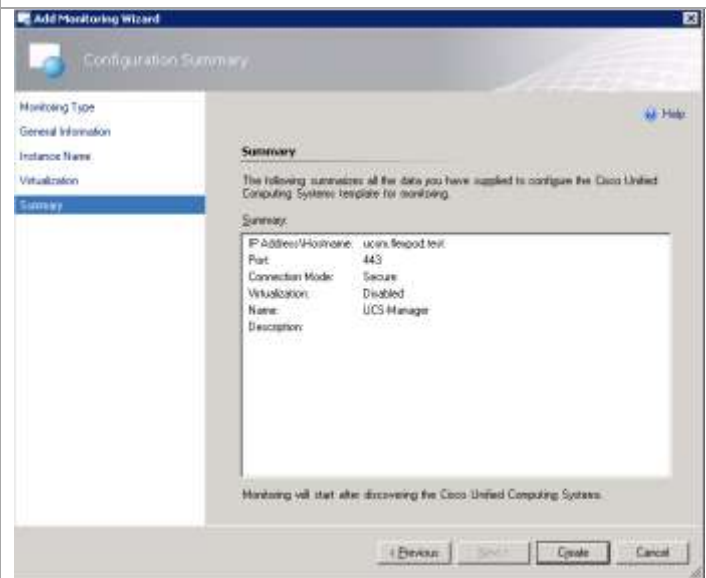
The screenshot shows the 'Add Monitoring Wizard' window with the 'Cisco UCS Instance Name' step. The left sidebar has 'Instance Name' selected. The main area is titled 'Cisco UCS Instance Name'. It contains a section 'Enter a friendly name and description' with a 'Name' field (UCS Manager) and a 'Description' text area. Below this is a 'Management Pack' section with a 'Create destination management pack:' field (UCS Manager) and a checkbox 'Use existing management pack, or create new'. At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'OK'.



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

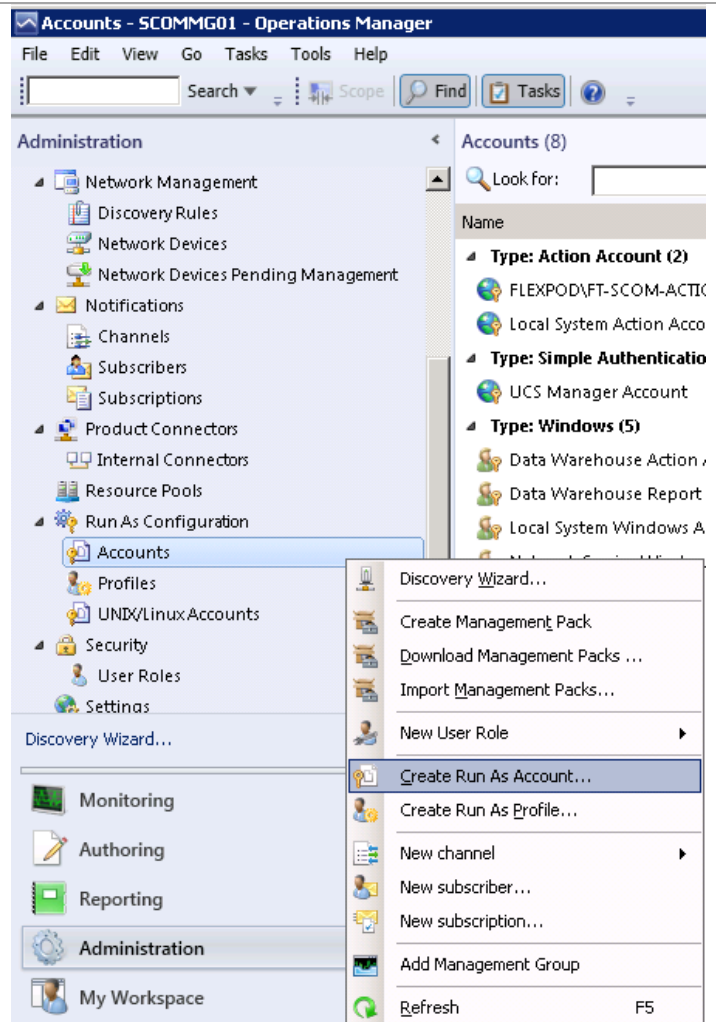


In the Operations Manager console, click the **Go** tab in the menu bar.

Select **Administration** from the drop-down menu.



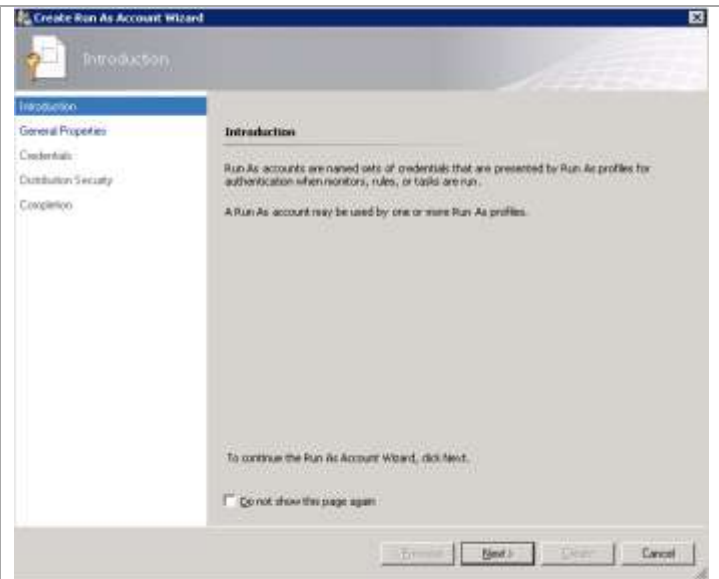
In the Administration column, right click on **Accounts**. Select **Create Run as Accounts** from the drop-down menu.



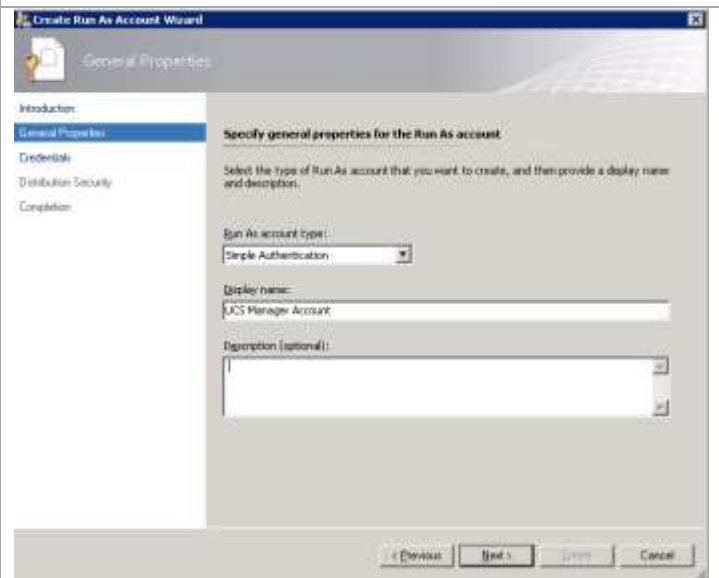


The **Create Run as Accounts Wizard** screen appears. Click the **Next** button.

Note: Operations Manager uses Run as Accounts to establish connection to Cisco UCS.



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 **Credentials** screen appears. Specify **Account name**, **Password** and **Confirm Password**. Click the **Next** button.

Note: These credentials are used for all communication with Cisco UCS.

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.



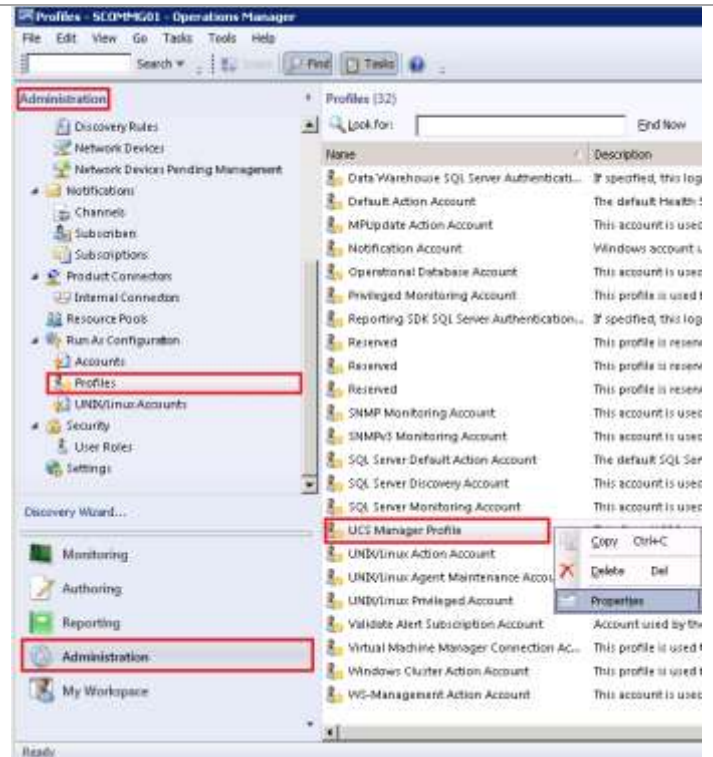
In the Operations Manager console, click the **Go** tab in the menu bar.

Select **Administration** from the drop-down menu.



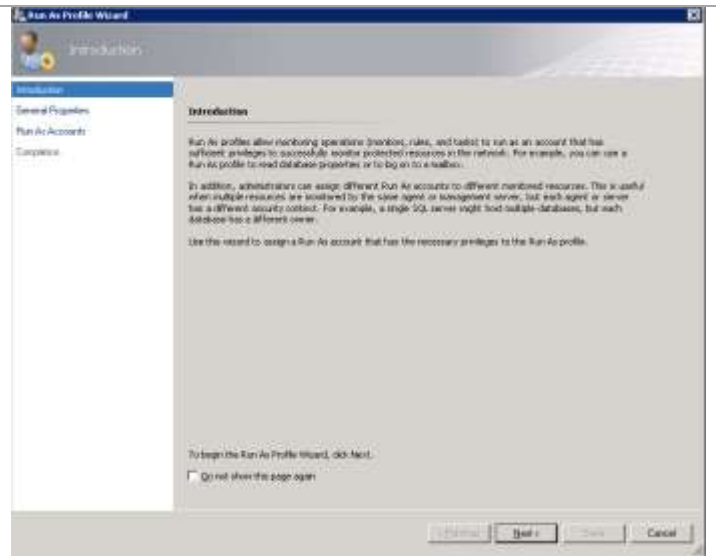
In the Administration column, click on **Profiles**. A list of profiles is displayed on the window. Choose a profile and select **Properties** from its right click menu.

Note: The Cisco UCS Manager Profile is used in this example.

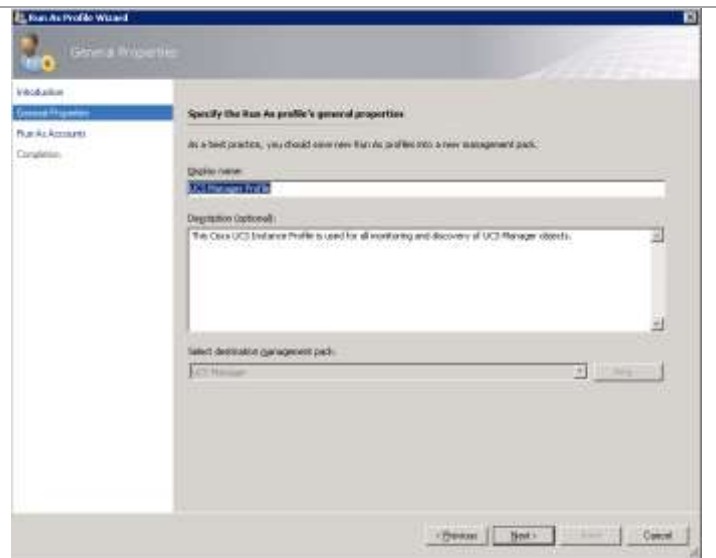




The **Run as Profile Wizard** opens. Click **Next** to continue on to the next screen.

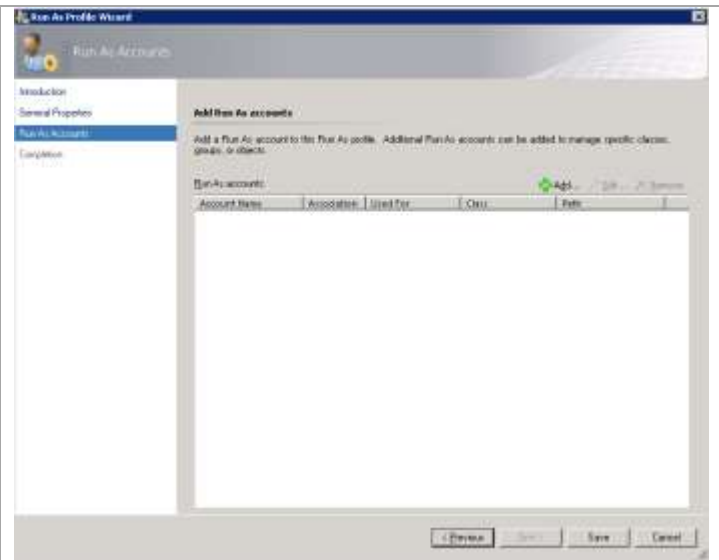


Click **Next** again to continue on to the next screen.





Click **Add** to add the Run As account.

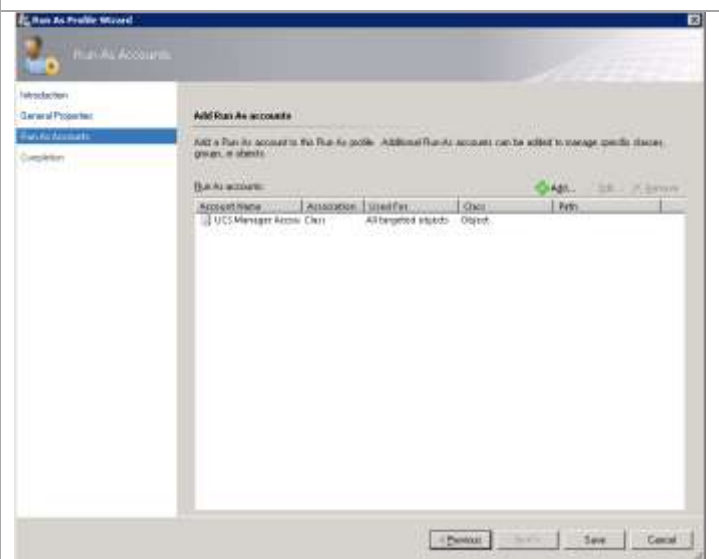


Select the **Cisco UCS Manager Account** from the **Run As Account** drop-down menu. This is the account created in the previous section.

Select the **All targeted objects** options and click **OK**.

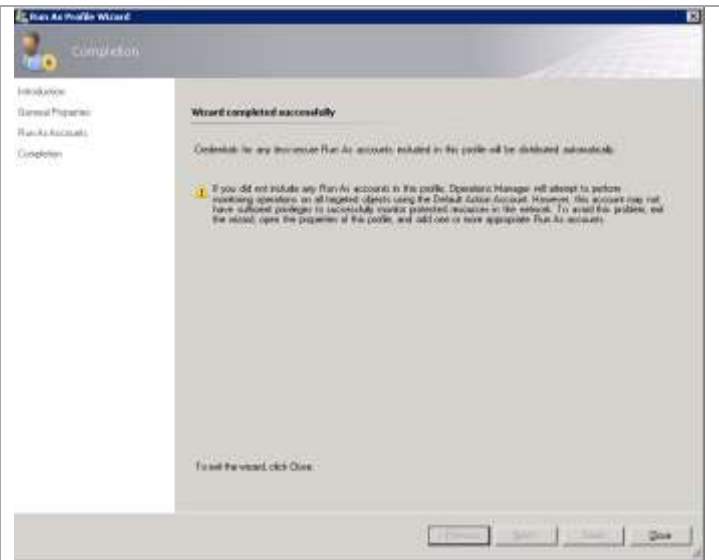


Click the **Save** button to save the account configuration.





The **Completion** screen appears. Click the **Close** button to close the wizard.

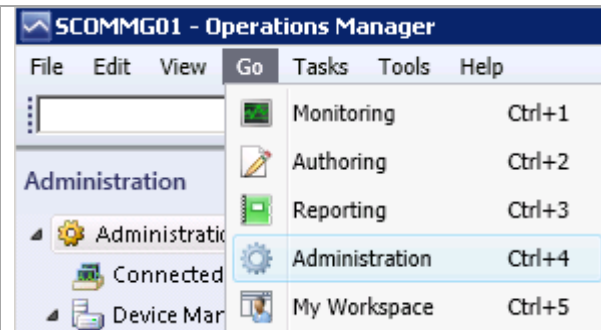


Configuring Bidirectional Communication

The following procedure describes the required configuration to communicate with Cisco UCS for acknowledging alerts from the Operations Manager Console.

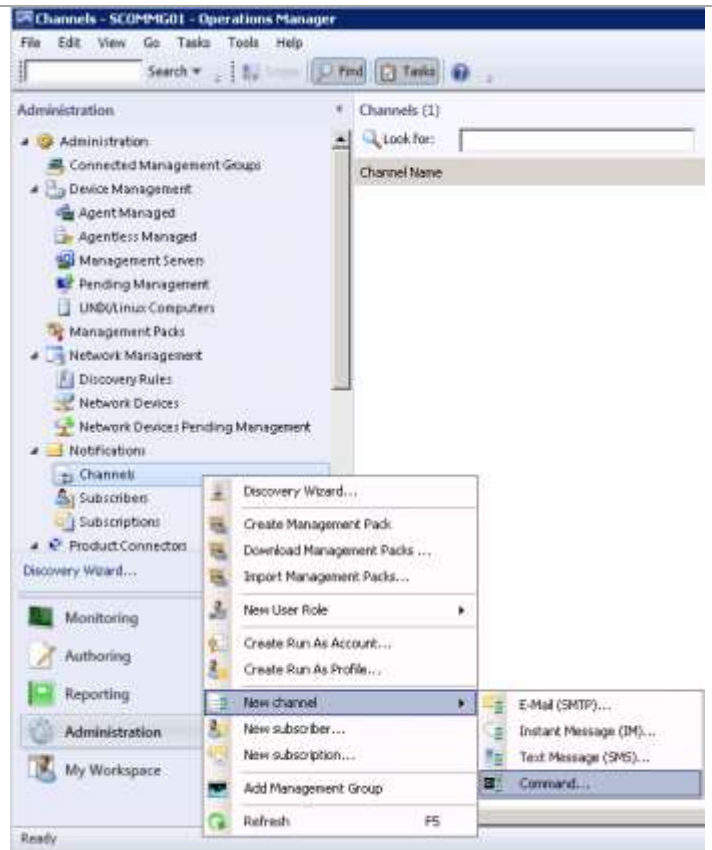
Note: The Bidirectional feature is currently limited to Management Servers on which SCOM 2012 Console and Cisco UCS MP are both installed.

In the Operations Manager console, click the **Go** tab in the menu bar. Select **Administration** from the drop-down menu.

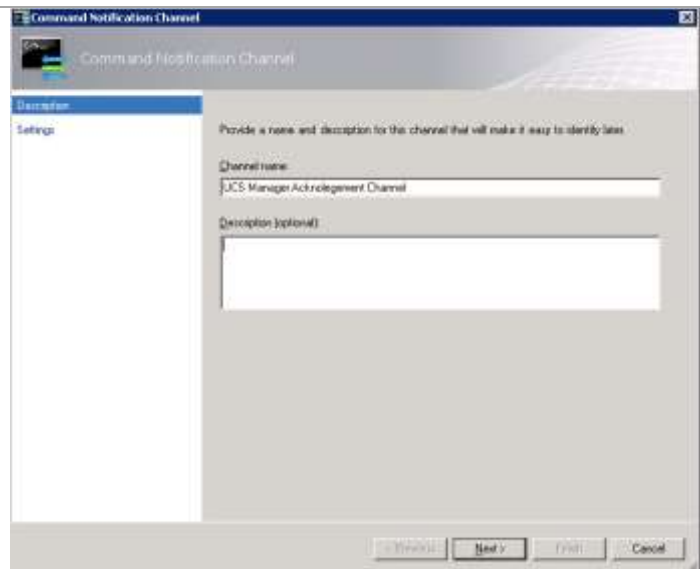




In the Administration column, right-click on **Channels**. Select **New Channel** from the menu and select the **Command** option.



The **Command Notification Channel** opens. Specify **Channel Name** and **Description**. Click the **Next** button.





The **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 (x86)\Cisco\Cisco UCS Management Pack 2012\Script\Bidirectional.ps1"" -getFaultID '\$Data/Context/DataItem/Custom7\$' -getUCSMachineName '\$Data/Context/DataItem/ManagedEntityFullName\$'

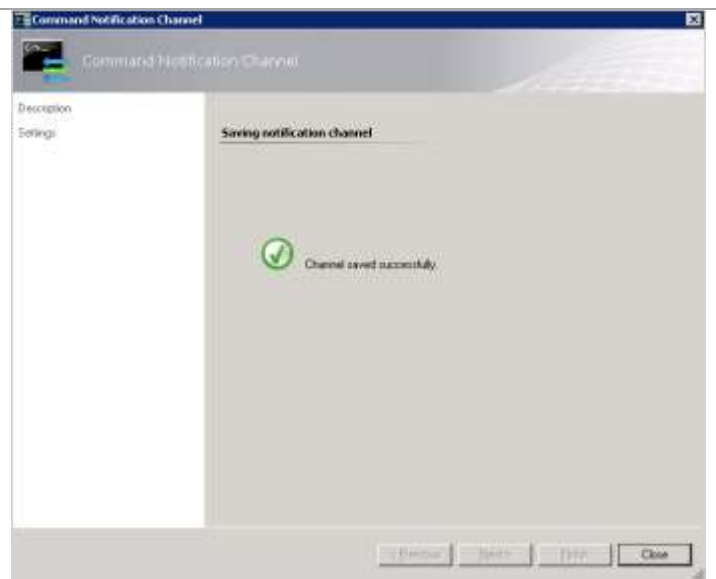
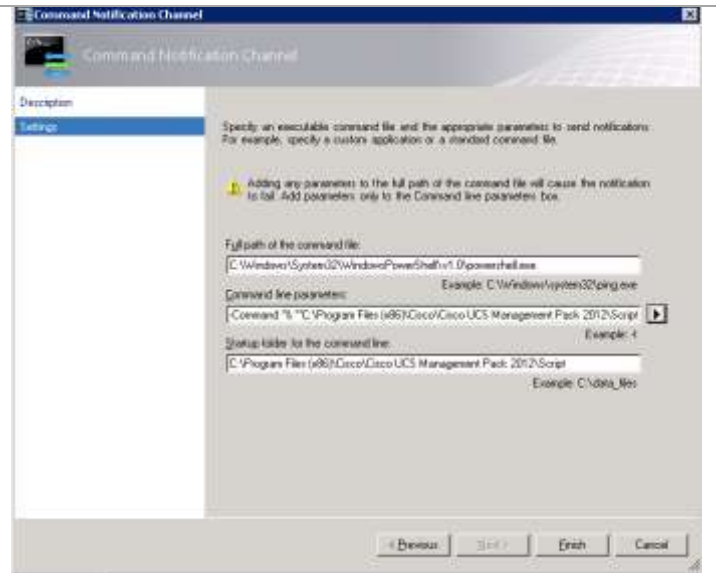
Specify **Start up folder for the command line** as

C:\Program Files (x86)\Cisco\Cisco UCS Management Pack 2012\Script

Note: Verify the path for script is valid.

Click the **Finish** button.

The new Channel is saved successfully. Click **Close** to close the wizard.





The new channel appears in the **Channel** view.



Adjusting the Discovery Interval

Discovery Interval is the time for polling the details of Cisco UCS at the specified time interval. This step is for changing the polling timings of faults and objects. The default value is 300 seconds. This is an optional procedure.

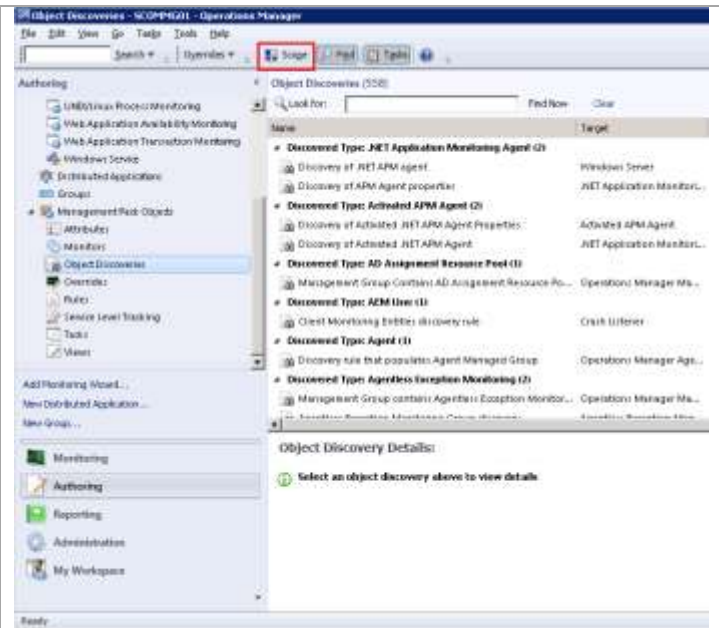
In the **Operations Manager** console, click the **Go** tab in the menu bar. Select **Authoring** from the drop-down menu. The **Authoring** column options appear.





In the Authoring column, select **Object Discoveries** in the **Management Pack Objects**. The Object Discovery details appear.

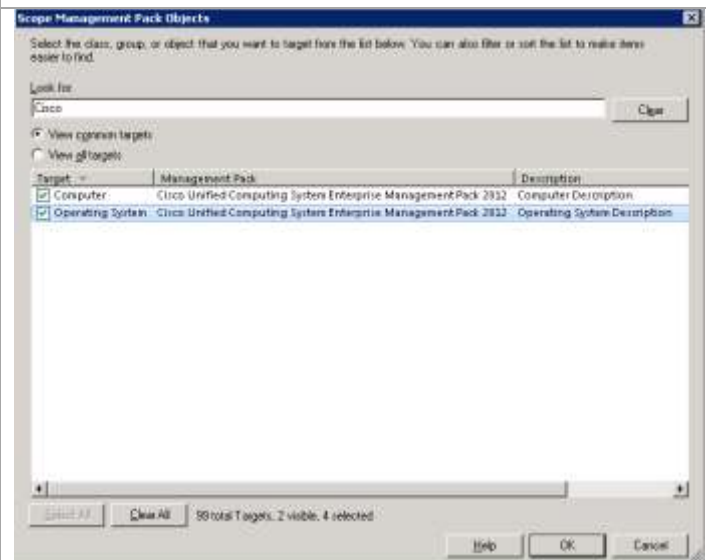
Click the **Scope** button in the toolbar.



The **Scope Management Pack Objects** window opens.

Specify the name of the management pack in the **Look for** field. Use the name **Cisco**. Click the **Select All** button.

Click the **Ok** button.



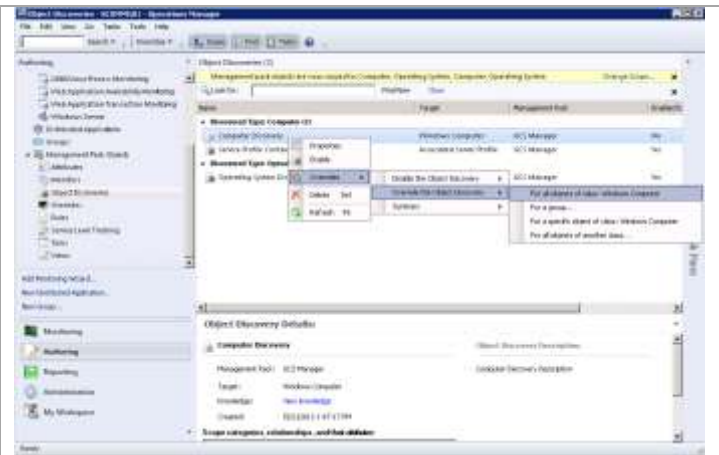


The management pack objects opens.

Select an Object and select **Overrides** from the right click menu. Select **Override the Object Discovery** from Overrides menu. Select **For All Objects of Class** from Override the Object Discovery menu.

Perform this procedure for the following objects:

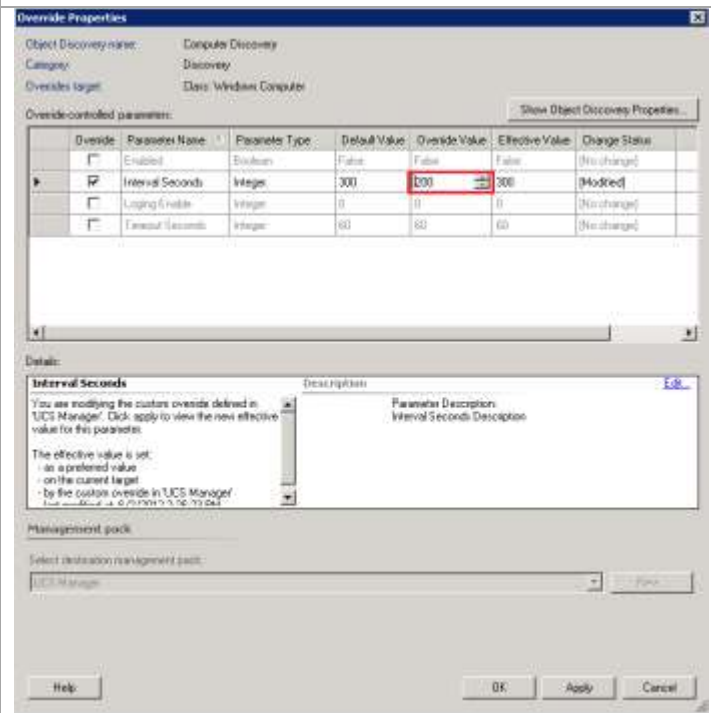
- Computer Discovery
- Operating System Discovery



The **Override Properties** window opens.

Select the **Override** checkbox against the **Interval seconds** parameter and set the **Override Value** property to 200. Click the **OK** button.

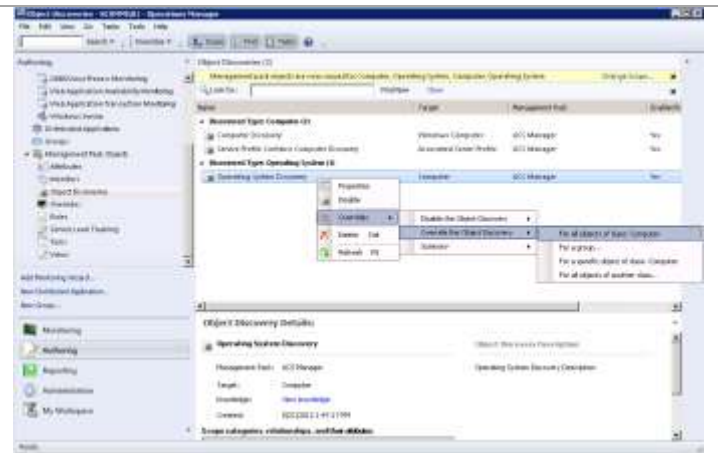
The updated property value is saved and reflected.





Repeat the Override procedure for the Operating System Discovery object.

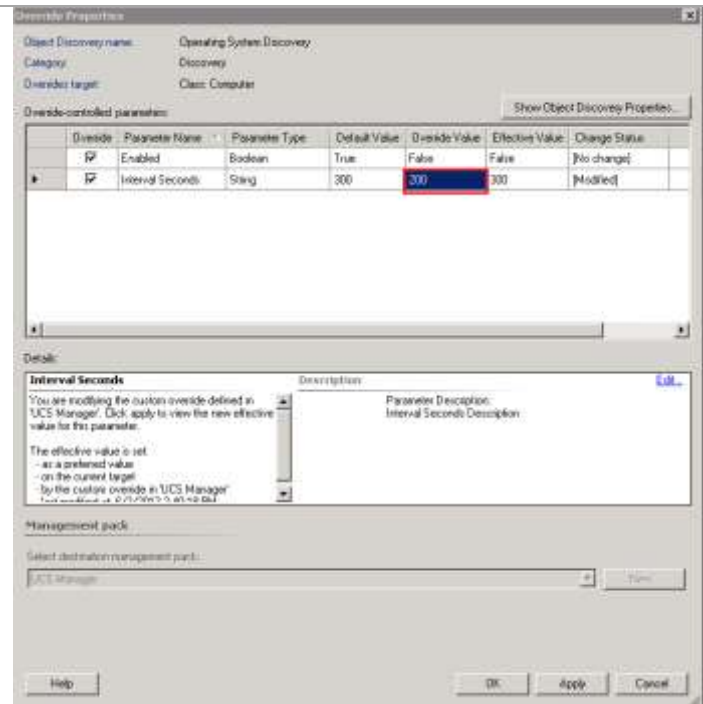
Select an Object and select **Overrides** from the right click menu. Select **Override the Object Discovery** from Overrides menu. Select **For All Objects of Class** from Override the Object Discovery menu.



The **Override Properties** window opens.

Select the **Override** checkbox against the **Interval seconds** parameter and set the **Override Value** property to 200. Click the **OK** button.

The updated property value is saved.



Registering and Deploying the UCS Integration Pack for System Center 2012 Orchestrator

Cisco UCS PowerTools version 0.9.8.1 or newer must be installed on the Orchestrator virtual machine prior to registering the UCS Integration pack.

Perform the following steps on the the Orchestrator virtual machine.

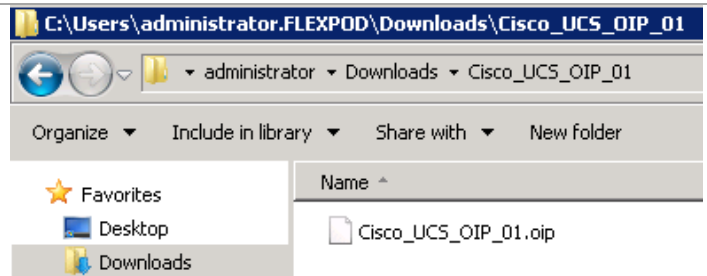


Registering the Cisco UCS Integration Pack for Orchestrator

Download and extract the **UCS Integration Pack for System Center Orchestrator** to the Orchestrator virtual machine. This file has an **.oip** extension.

Note: The Integration Pack for System Center Orchestrator can be downloaded from the following location:

<http://developer.cisco.com/web/unifiedcomputing/systemcenter>



Open the Orchestrator **Deployment Manager**

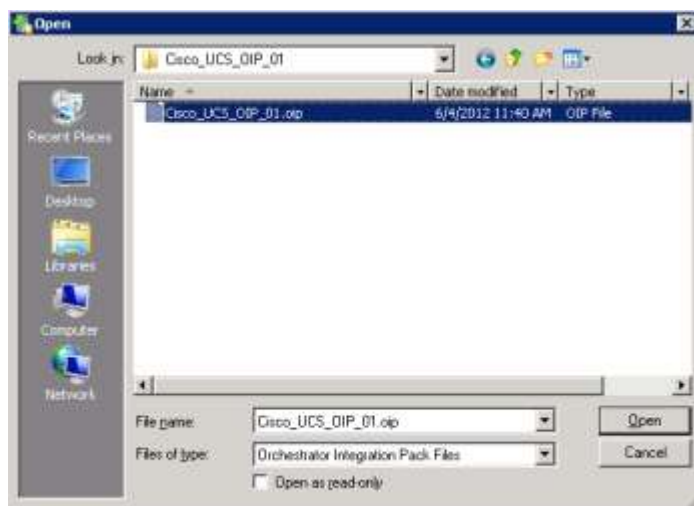
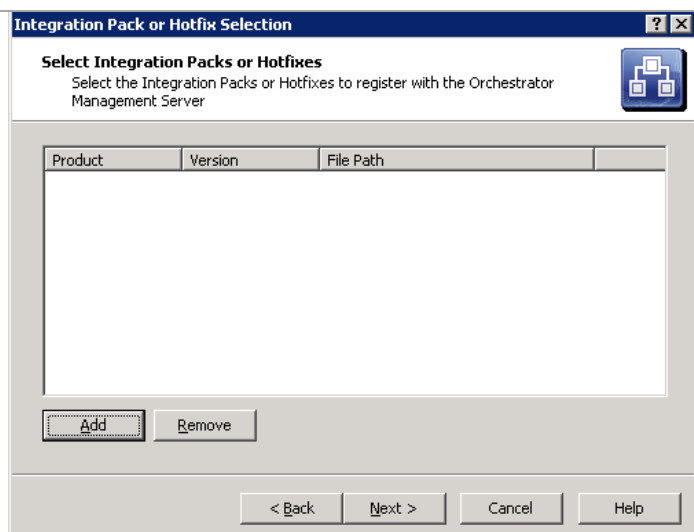
In the left pane, **right click** on the “**Integration Packs**” and select option “**Register IP with the Orchestrator Management Server**”.





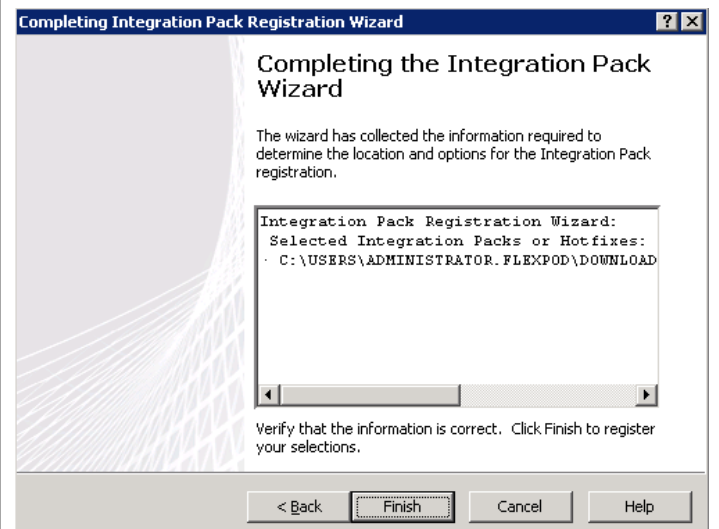
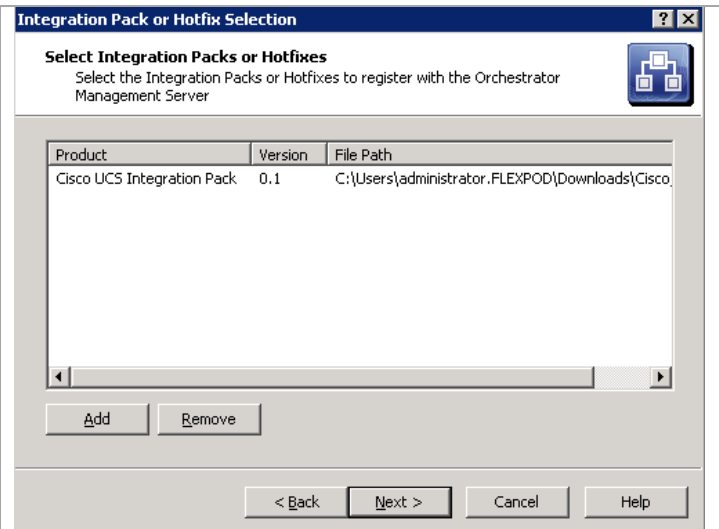
The **Integration Pack Registration Wizard** opens. Click **Next** and click the **Add** button in the Select Integration Pack or Hotfix window.

Select the downloaded **integration pack** and click **Open**.

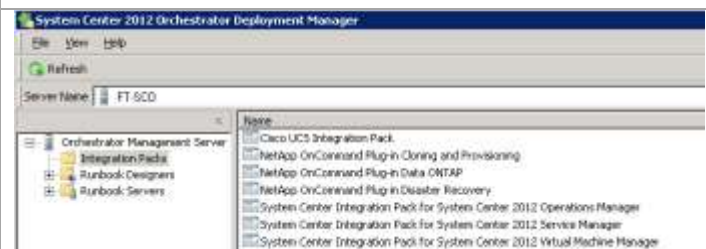




Click **Next** and click **Finish** to register the integration pack.



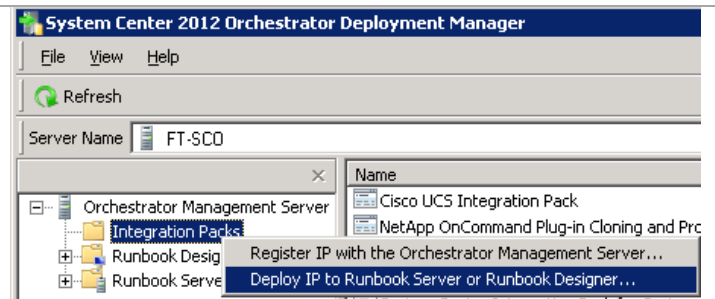
The wizard closes and the newly registered Cisco UCS Integration Pack is displayed in the integration pack list.



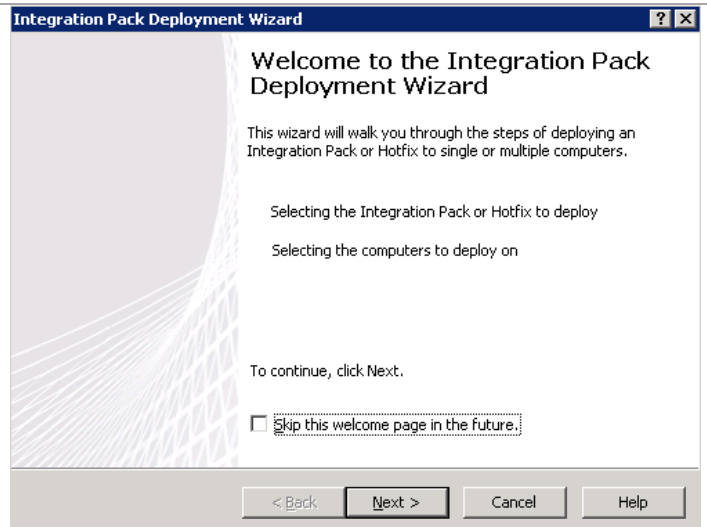


Deploying the Cisco UCS Integration Pack for Orchestrator

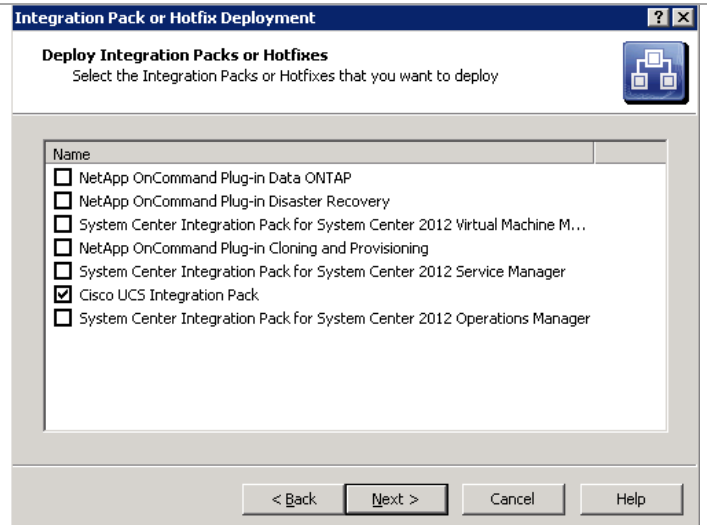
In the **Deployment Manager** left pane, right click on the “**Integration Packs**” and select option “**Deploy IP to Runbook Server or Runbook Designer**”.



Click **Next** to proceed with the Integration Pack Deployment Wizard.



In the Integration Pack or Hotfix Deployment window select **Cisco UCS Integration Pack** and click **Next**.





In the Computer Selection window type the **computer name** of the virtual machine where Orchestrator is installed. Click **Add** and **Next**.

Computer Selection

Computer Selection Details
Select the computers that you want to deploy the Integration Pack or Hotfix on.

Computer: ft-sco.flexpod.test Add

ft-sco.flexpod.test

Remove

< Back Next > Cancel Help

In the Installations Options window accept the default installations options and click **Next**.

Installation Options

Installation Configuration
Configure the installation options for the Integration Packs or Hotfixes

You can Install the Integration Packs or Hotfixes now, or at a time that you specify.

☐ Schedule installation:

Perform installation at: 9:51:48 PM 6/ 5/2012

Advanced Options

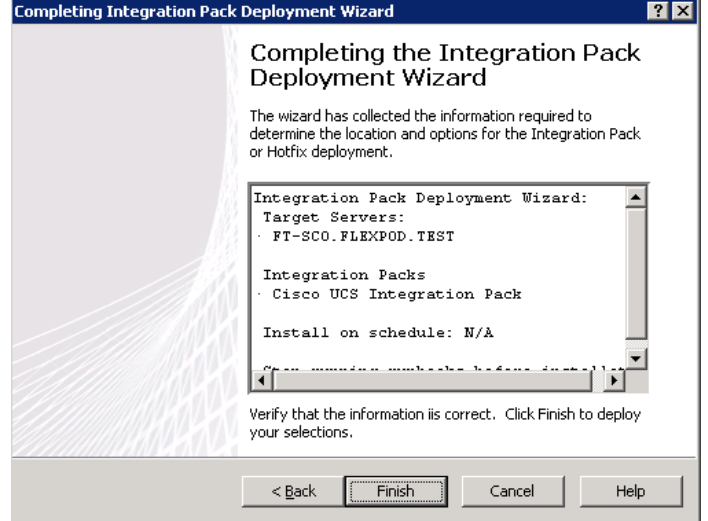
☒ Stop all running Runbooks before installing the Integration Packs or Hotfixes

☐ Install the Integration Packs or Hotfixes without stopping the running Runbooks.
You may need to restart the computer to complete the installation.

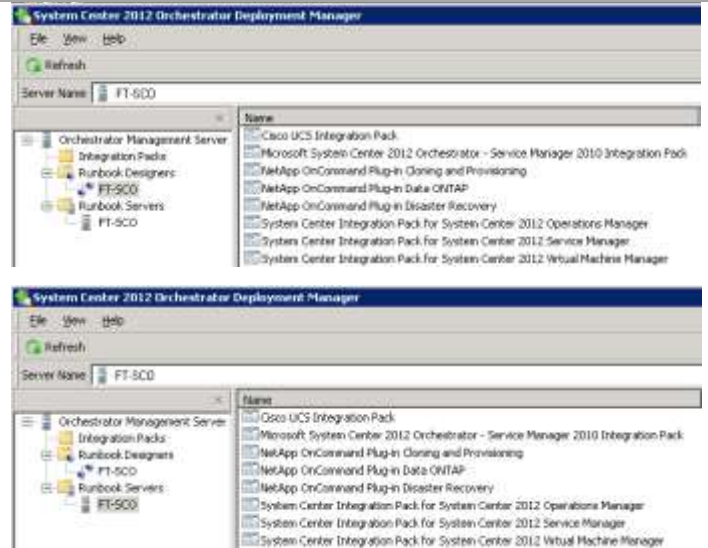
< Back Next > Cancel Help



Click **Finish** to deploy the UCS Integration Pack.

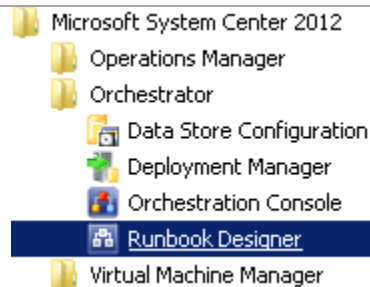


Verify the Cisco UCS Integration Pack Deployment.



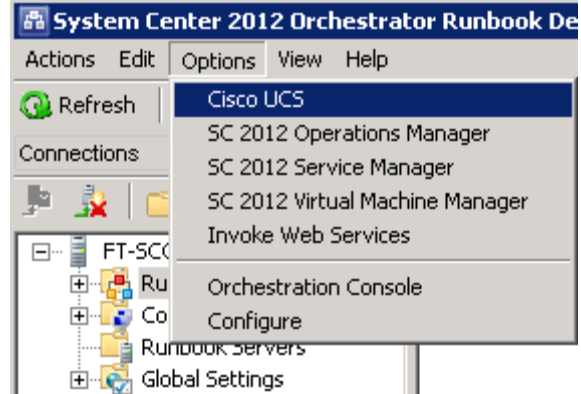
Configuring the Cisco UCS Integration Pack for Orchestrator

Click **Start** and open the Orchestrator **Runbook Designer**.

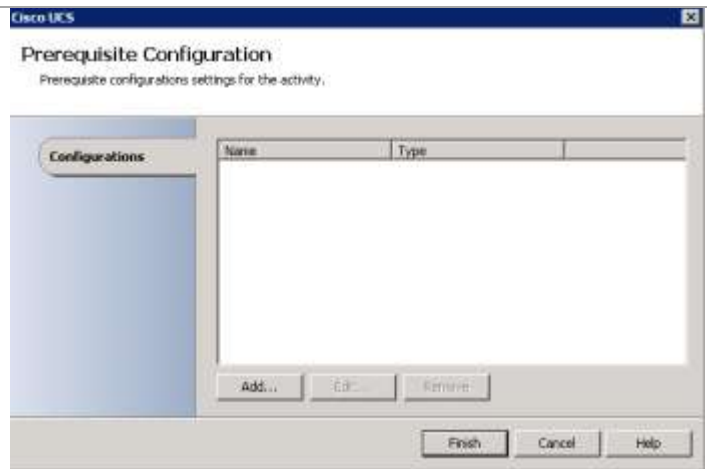




Go to **Options** and select **Cisco UCS** from the dropdown menu.

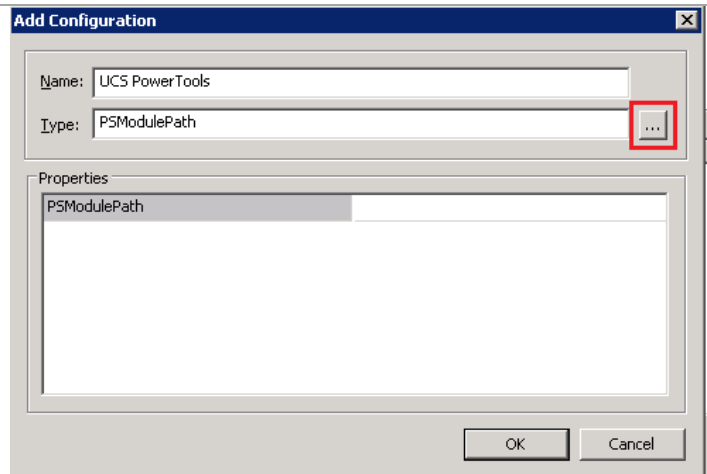


The Cisco UCS **Prerequisite Configuration** window opens. Click the **Add** button.



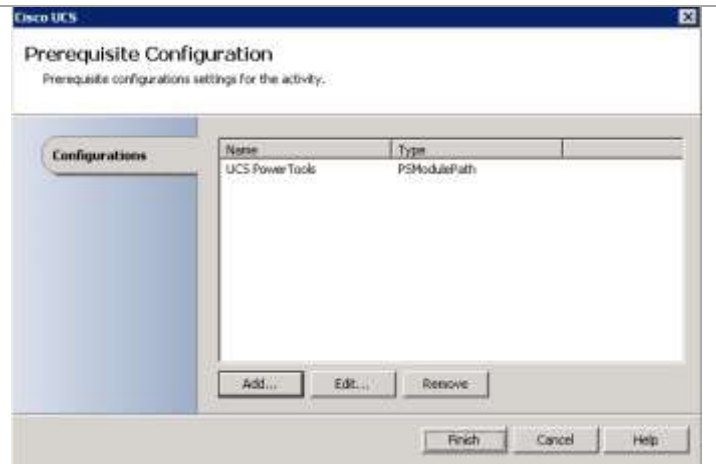
Type the configuration **name**. Click the "..."
button and select **PSModulePath**. Click **OK** to
accept the settings and close the windows.

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.



The screenshot shows the 'Cisco UCS Prerequisite Configuration' window. It has a title bar 'Cisco UCS' and a subtitle 'Prerequisite Configuration' with the text 'Prerequisite configurations settings for the activity.' below it. On the left is a 'Configurations' tab. The main area is a table with two columns: 'Name' and 'Type'. It contains one entry: 'UCS Power Tools' with type 'PSModulePath'. Below the table are buttons 'Add...', 'Edit...', and 'Remove'. At the bottom right are buttons 'Finish', 'Cancel', and 'Help'.

Name	Type
UCS Power Tools	PSModulePath



Appendix A: SlipSQL.PS1

To support slipstreamed installations of SQL, the following PowerShell script is provided to create a merged SQL source.

```
# Title: SQL 2008 R2 Build SlipStream Script
```

```
# Version: 1.1
```

```
# Last updated: 3:50 PM 2/24/2012
```

```
# Author: Joel Yoker <joely@microsoft.com>
```

```
$debug=1
```

```
Function Get-ValidPath ($path)
```

```
{  
    $IsValid = $False  
    Do  
    {  
        $path = Read-Host "Enter the location (folder)"  
        $IsValid = Test-Path $path  
        if (! $IsValid ) { Write-Error "$path is not a valid folder" }  
    }  
    Until ($IsValid)  
    return $path  
}
```

```
Function Merge-SQLFiles ($UpdatePath, $SlipStreamTargetPath, $SlipStreamTargetFolder)
```

```
{  
    # Read in the update path and loop through each file.  
    $files = Get-ChildItem $UpdatePath  
    foreach ($file in $files)  
    {  
        if ($debug -eq 1){Write-Host "Extracting file $file"}  
        $UpdateFile = $UpdatePath + "\" + $file  
        $UpdateTargetPath = $SlipStreamTargetPath + "\" + $SlipStreamTargetFolder
```




```
[diagnostics.process]::start("$UpdateFile", "/passive /x:$UpdateTargetPath").WaitForExit()
}

# Copy the updated setup.exe and setup.rll files into the build
write-host "Merging Setup files"

[diagnostics.process]::start("robocopy", "$UpdateTargetPath $SlipStreamTargetPath
setup.exe").WaitForExit()

[diagnostics.process]::start("robocopy", "$UpdateTargetPath $SlipStreamTargetPath
setup.rll").WaitForExit()

# Merge files from the ia64 update path with the exception of Microsoft.SQL.Chainer.PackageData.dll
write-host "Merging ia64 files"

$UpdateTargetPathPlatform = $UpdateTargetPath + "\ia64"
$SlipStreamTargetPathPlatform = $SlipStreamTargetPath + "\ia64"

[diagnostics.process]::start("robocopy", "$UpdateTargetPathPlatform $SlipStreamTargetPathPlatform
/XF Microsoft.SQL.Chainer.PackageData.dll").WaitForExit()

# Merge files from the x86 update path with the exception of Microsoft.SQL.Chainer.PackageData.dll
write-host "Merging x86 files"

$UpdateTargetPathPlatform = $UpdateTargetPath + "\x86"
$SlipStreamTargetPathPlatform = $SlipStreamTargetPath + "\x86"

[diagnostics.process]::start("robocopy", "$UpdateTargetPathPlatform $SlipStreamTargetPathPlatform
/XF Microsoft.SQL.Chainer.PackageData.dll").WaitForExit()

# Merge files from the x64 update path with the exception of Microsoft.SQL.Chainer.PackageData.dll
write-host "Merging x64 files"

$UpdateTargetPathPlatform = $UpdateTargetPath + "\x64"
$SlipStreamTargetPathPlatform = $SlipStreamTargetPath + "\x64"

[diagnostics.process]::start("robocopy", "$UpdateTargetPathPlatform $SlipStreamTargetPathPlatform
/XF Microsoft.SQL.Chainer.PackageData.dll").WaitForExit()

}

Write-Host "`nSQL Server Slipstream Script`n" -ForegroundColor "yellow"
```



```
Write-Host "*****" -ForegroundColor "yellow"
Write-Host "* This script will merge a SQL 2008 R2 Service Pack and *" -ForegroundColor "yellow"
Write-Host "* Cumulative Update into a single slipstreamed build  *" -ForegroundColor "yellow"
Write-Host "*****" -ForegroundColor "yellow"
Write-Host "`n"

Do {

    # Prompt the user for all source paths

    Write-Host "Enter the SQL RTM Source Path" -ForegroundColor "green"
    $SQLRTMPPath = Get-ValidPath $path

    Write-Host "Enter the SQL Service Pack Source Path" -ForegroundColor "green"
    $SQLPCUPath = Get-ValidPath $path

    Write-Host "Enter the SQL Cumulative Update Source Path" -ForegroundColor "green"
    $SQLCUPath = Get-ValidPath $path

    if ($debug -eq 1){Write-Host "`nProvided Source Paths" }
    if ($debug -eq 1){Write-Host "SQLRTMPPath: $SQLRTMPPath"}
    if ($debug -eq 1){Write-Host "SQLPCUPath: $SQLPCUPath"}
    if ($debug -eq 1){Write-Host "SQLCUPath: $SQLCUPath"}

    Write-Host "`n"
    Write-Host "Enter the desired SQL Slipstream Target Path" -ForegroundColor "green"
    Write-Host "(Note this path should not previously exist)" -ForegroundColor "green"
    $SQLSSTargetPath = Read-Host "Enter the location (folder)"

    # Present a confirmation menu to the end user
    Write-Host "`nConfirm Source and Target Folders"
    Write-Host "-----`n"
    Write-Host "SQL RTM Source Path: `t`t$SQLRTMPPath"
```



```
Write-Host "SQL Service Pack Source Path: `t`t$SQLPCUPath"
Write-Host "SQL Cumulative Update Source Path: `t$SQLCUPath"
Write-Host "SQL Cumulative Update Source Path: `t$SQLSSTargetPath"

$settings = $values

$Confirm = 0
$ConfirmTitle = ""
$ConfirmMessage = "`nAre these values correct?"
$yes = New-Object System.Management.Automation.Host.ChoiceDescription "&Yes", "Yes"
$no = New-Object System.Management.Automation.Host.ChoiceDescription "&No", "No"
$ConfirmOptions = [System.Management.Automation.Host.ChoiceDescription[]]($yes, $no)
$ConfirmResult = $host.ui.PromptForChoice($ConfirmTitle, $ConfirmMessage, $ConfirmOptions, 0)

switch ($ConfirmResult)
{
    # Set the boolean flag if the user confirms "yes" (0 = yes, 1 = no)
    0 {$Confirm = 1}
    1 {$Confirm = 0}
}
} Until ($Confirm -ne 0)
Write-Host "`n"

# Verify if the target path provided exist if it does, exit gracefully.
# The destination path should not since we are using Copy-Item and this cmdlet
# does not handle duplicate paths and non-existent paths in the same manner

$PathExists = Test-Path $SQLSSTargetPath
if (! $PathExists )
{
    Write-Host "Path does not exist, creating $SQLSSTargetPath"
    Write-Host "`nCopying files, please be paitent..."
    Copy-Item $SQLRTMPPath $SQLSSTargetPath -recurse
```



```
Write-Host "Completed."
```

```
write-host "`nMerging Service Pack Files...Please Wait"
```

```
Merge-SQLFiles $SQLPCUPath $SQLSSTargetPath "PCU"
```

```
write-host "Completed Service Pack Merge"
```

```
write-host "`nMerging Cumulative Update Files...Please Wait"
```

```
Merge-SQLFiles $SQLCUPath $SQLSSTargetPath "CU"
```

```
write-host "Completed Cumulative Update Merge"
```

```
write-host "`nUpdating DefaultSetup INI Files...Please Wait"
```

```
"`rPCUSOURCE=.\PCU" | Out-File -append $SQLSSTargetPath\x86\DefaultSetup.ini
```

```
"`rPCUSOURCE=.\PCU" | Out-File -append $SQLSSTargetPath\x64\DefaultSetup.ini
```

```
"`rPCUSOURCE=.\PCU" | Out-File -append $SQLSSTargetPath\ia64\DefaultSetup.ini
```

```
"`rCUSOURCE=.\CU" | Out-File -append $SQLSSTargetPath\x86\DefaultSetup.ini
```

```
"`rCUSOURCE=.\CU" | Out-File -append $SQLSSTargetPath\x64\DefaultSetup.ini
```

```
"`rCUSOURCE=.\CU" | Out-File -append $SQLSSTargetPath\ia64\DefaultSetup.ini
```

```
write-host "Update DefaultSetup INI Files complete"
```

```
}
```

```
Else
```

```
{
```

```
Write-Host "$SQLSSTargetPath Path exists"
```

```
Write-Host "Please specify a new path for the target, exiting..."
```

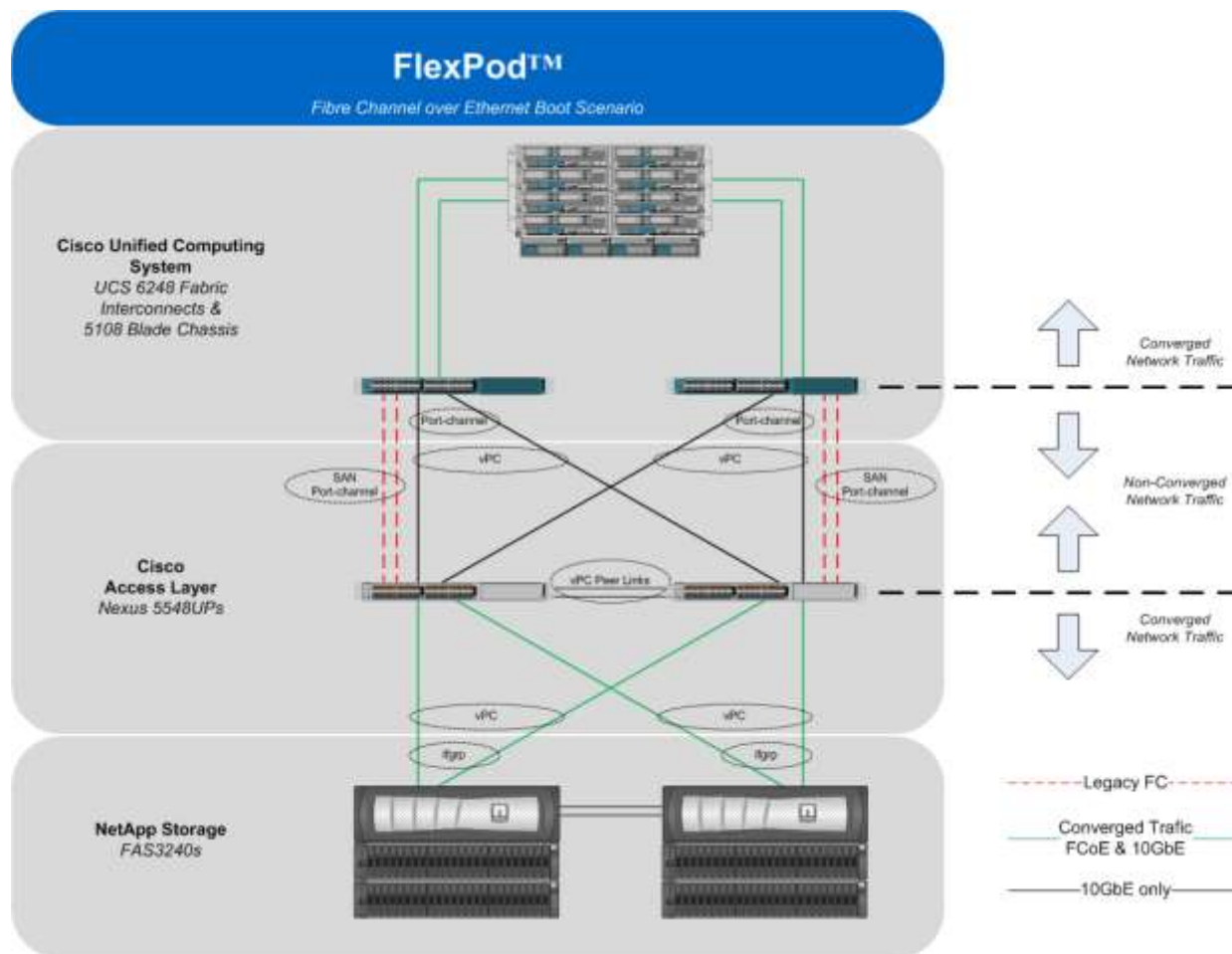
```
}
```

Appendix B: Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 for FCoE

These steps provide details for completing the configuration of the Nexus infrastructure for the FlexPod environment.



Figure 2 Nexus Infrastructure for the FlexPod Environment



Create VSANs, Assign FC Ports, Turn on FC Ports

These steps provide details for configuring VSANs, assigning FC ports and enabling FC ports.

Note: This procedure sets up FCoE connections between the Nexus 5548s and the NetApp Storage Systems. If you want to use FCoE connections between the Nexus 5548s and the NetApp Storage Systems using the NetApp Unified Target Adapter (UTA). Use the Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 in the Appendix.

Cisco Nexus 5548 A

1. From the global configuration mode, type `vlan <Fabric A FCoE VLAN ID>`.
2. Type `name FCoE_Fabric_A`.
3. Type `fcoe vsan <VSAN A ID>`.
4. Type `exit`.
5. Type `interface poll`.
6. Type `switchport trunk allowed vlan add <Fabric A FCoE VLAN ID>`.
7. Type `exit`.
8. Type `interface vfc11`.
9. Type `bind interface poll`.



10. Type `no shutdown`.
11. Type `exit`.
12. Type `interface po12`.
13. Type `switchport trunk allowed vlan add <Fabric A FCoE VLAN ID>`.
14. Type `exit`.
15. Type `interface vfc12`.
16. Type `bind interface po12`.
17. Type `no shutdown`.
18. Type `exit`.
19. Type `interface san-port-channel 1`.
20. Type `channel mode active`.
21. Type `exit`.
22. Type `vsan database`.
23. Type `vsan <VSAN A ID> name Fabric_A`.
24. Type `vsan <VSAN A ID> interface fc1/31-32`.
25. Type `vsan <VSAN A ID> interface san-port-channel 1`.
26. Type `vsan <VSAN A ID> interface vfc11`.
27. Type `vsan <VSAN A ID> interface vfc12`.
28. Type `exit`.
29. Type `interface fc1/31-32`.
30. Type `channel-group 1 force`.
31. Type `no shutdown`.
32. Type `exit`.
33. Type `show int san-port-channel 1` to confirm connectivity.
34. Type `interface fc1/31`.
35. Type `switchport description <UCSM A:fc1/31>`.
36. Type `exit`.
37. Type `interface fc1/32`.
38. Type `switchport description <UCSM A:fc1/32>`.
39. Type `exit`.

Cisco Nexus 5548 B

1. From the global configuration mode, type `vlan <Fabric B FCoE VLAN ID>`.
2. Type `name FCoE_Fabric_B`.
3. Type `fcoe vsan <VSAN B ID>`.
4. Type `exit`.
5. Type `interface po11`.
6. Type `switchport trunk allowed vlan add <Fabric B FCoE VLAN ID>`.



7. Type `exit`.
8. Type `interface vfc11`.
9. Type `bind interface pol1`.
10. Type `no shutdown`.
11. Type `exit`.
12. Type `interface pol2`.
13. Type `switchport trunk allowed vlan add <Fabric B FCoE VLAN ID>`.
14. Type `exit`.
15. Type `interface vfc12`.
16. Type `bind interface pol2`.
17. Type `no shutdown`.
18. Type `exit`.
19. Type `interface san-port-channel 2`.
20. Type `channel mode active`.
21. Type `exit`.
22. Type `vsan database`.
23. Type `vsan <VSAN B ID> name Fabric_B`.
24. Type `vsan <VSAN B ID> interface fc1/31-32`.
25. Type `vsan <VSAN B ID> interface san-port-channel 2`.
26. Type `vsan <VSAN A ID> interface vfc11`.
27. Type `vsan <VSAN A ID> interface vfc12`.
28. Type `exit`.
29. Type `interface fc1/31-32`.
30. Type `channel-group 2 force`.
31. Type `no shutdown`.
32. Type `exit`.
33. Type `show int san-port-channel 2` to confirm connectivity
34. Type `interface fc1/31`.
35. Type `switchport description <UCSM B:fc1/31>`.
36. Type `exit`.
37. Type `interface fc1/32`.
38. Type `switchport description <UCSM B:fc1/32>`.
39. Type `exit`.

Create Device Aliases and Create Zones for FCoE Devices

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.



Cisco Nexus 5548 A

24. From the global configuration mode, type `device-alias database`.
 25. Type `device-alias name VM-Host-Infra-01_A pwwn <Fabric-A WWPN>`.
 26. Type `device-alias name VM-Host-Infra-02_A pwwn <Fabric-A WWPN>`.
 27. Type `device-alias name controller_A_2a pwwn <Controller A 2a WWPN>`.
 28. Type `device-alias name controller_B_2a pwwn <Controller B 2a WWPN>`.
- Get this information from the table in section Gather Necessary Information.
29. After all of the necessary device-alias are created, type `exit`.
 30. Type `device-alias commit`.
 31. Create the zone for each service profile.
 - a. Type `zone name VM-Host-Infra-01_A vsan <Fabric A VSAN ID>`.
 - b. Type `member device-alias VM-Host-Infra-01_A`.
 - c. Type `member device-alias controller_A_2a`.
 - d. Type `exit`.
 32. After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.
 33. Create the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric A VSAN ID>`.
 - b. Type `member VM-Host-Infra-01_A`.
 - c. Type `exit`.
 34. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan < Fabric A VSAN ID>`.
 - b. Type `exit`.
 35. Type `copy run start`.

Cisco Nexus 5548 B

36. From the global configuration mode, type `device-alias database`.
 37. Type `device-alias name VM-Host-Infra-01_B pwwn <Fabric-B WWPN>`.
 38. Type `device-alias name VM-Host-Infra-02_B pwwn <Fabric-B WWPN>`.
 39. Type `device-alias name controller_A_2b pwwn <Controller A 0d WWPN>`.
 40. Type `device-alias name controller_B_2b pwwn <Controller B 0d WWPN>`.
- Get this information from the tables in the section Gather Necessary Information.
41. After all of the necessary device-alias are created, type `exit`.
 42. Type `device-alias commit`.
 43. Create the zones for each service profile.
 - a. Type `zone name VM-Host-Infra-02_B vsan <Fabric B VSAN ID>`.
 - b. Type `member device-alias VM-Host-Infra-02_B`.
 - c. Type `member device-alias controller_B_0d`.



- d. Type `exit`.
- 44. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
- 45. Create the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `member VM-Host-Infra-02_B`.
 - c. Type `exit`.
- 46. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `exit`.
- 20. Type `copy run start`.
- 47. Return to the section **Error! Reference source not found.**

Alternate Create Zones for Redundant Paths for FCoE

These steps provide details for configuring zones for the secondary boot path for each service profile.

Cisco Nexus 5548 A

1. From the global configuration mode, create the zones for the redundant path for each service profile.
 - a. Type `zone name VM-Host-Infra-01_A vsan <Fabric A VSAN ID>`.
 - b. Type `member device-alias controller_B_2a`.
 - c. Type `exit`.
 - d. Type `zone name VM-Host-Infra-02_A vsan <Fabric A VSAN ID>`.
 - e. Type `member device-alias VM-Host-Infra-02_A`.
 - f. Type `member device-alias controller_B_2a`.
 - g. Type `member device-alias controller_A_2a`.
 - h. Type `exit`.
2. Modify the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric A VSAN ID>`.
3. Type `member VM-Host-Infra-02`.
4. Type `exit`.
5. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan <Fabric A VSAN ID>`.
6. Type `exit`.
7. Type `copy run start`.

Cisco Nexus 5548 B

1. From the global configuration mode, create the zones for the redundant path for each service profile.
 - a. Type `zone name VM-Host-Infra-01_B vsan <Fabric B VSAN ID>`.
 - b. Type `member device-alias VM-Host-Infra-01_B`.
 - c. Type `member device-alias controller_A_2b`.



- d. Type `member device-alias controller_B_2b`.
- e. Type `exit`.
- f. Type `zone name VM-Host-Infra-02_B vsan <Fabric B VSAN ID>`.
- g. Type `member device-alias controller_A_2b`.
- h. Type `exit`.
- 2. Modify the zoneset and add the necessary members.
 - a. Type `zoneset name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `member VM-Host-Infra-01_B`.
 - c. Type `exit`.
- 3. Activate the zoneset.
 - a. Type `zoneset activate name flexpod vsan <Fabric B VSAN ID>`.
 - b. Type `exit`.
- 4. Type `copy run start`.

Cisco Nexus Configurations

Nexus A (sample running config)

!Command: show running-config

!Time: Thu Mar 1 13:26:52 2012

```
version 5.0(3)N2(2a)
feature fcoe
feature npiv
feature fport-channel-trunk
no feature telnet
no telnet server enable
cfs eth distribute
feature lacp
feature vpc
feature lldp
username admin password 5 $1$whyEnoq8$fEeCFXDyQDTPDBltqDhU0. role network-admin
ip domain-lookup
hostname Nexus5548-A
logging event link-status default
ip access-list classify_Silver
  10 permit ip 192.168.102.0/24 any
  20 permit ip any 192.168.102.0/24
  30 permit ip 192.168.106.0/24 any
```



```
40 permit ip any 192.168.106.0/24
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 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
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 jumbo
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    mtu 9000
    multicast-optimize
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
slot 1
  port 29-32 type fc
snmp-server user admin network-admin auth md5 0x2e8af112d36e9af1466f4e4db0ce36a3 priv
0x2e8af112d36e9af1466f4e4db0ce36a3 localizedkey
```



```
snmp-server enable traps entity fru
ntp server 10.61.185.11 use-vrf management
vrf context management
    ip route 0.0.0.0/0 10.61.185.1
vlan 1
vlan 2
    name Native-VLAN
vlan 805
    name VM-MGMT-VLAN
vlan 801
    name CSV-VLAN
vlan 802
    name iSCSI-Fabric-A
vlan 803
    name LiveMigration-VLAN
vlan 806
    name App-Cluster-Comm-VLAN
vlan 804
    name VM-Data-VLAN
vlan 807
    name iSCSI-Fabric-B
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vpc domain 23
    role priority 10
    peer-keepalive destination 10.61.185.70 source 10.61.185.69
vsan database
    vsan 101 name "Fabric_A"
device-alias database
    device-alias name FAS3270-1a_0c pwwn 50:0a:09:82:8d:73:42:07
    device-alias name FAS3270-1b_0c pwwn 50:0a:09:82:9d:73:42:07
    device-alias name vm-host-infra-01-fabric-a pwwn 20:00:00:25:b5:00:0a:0f
    device-alias name vm-host-infra-02-fabric-a pwwn 20:00:00:25:b5:00:0a:1f

device-alias commit

fcdomain fcid database
    vsan 101 wwn 24:01:54:7f:ee:23:52:40 fcid 0x550000 dynamic
    vsan 101 wwn 50:0a:09:82:8d:73:42:07 fcid 0x550001 dynamic
```



```
! [FAS3270-1a_0c]
vsan 101 wwn 50:0a:09:82:9d:73:42:07 fcid 0x550002 dynamic
! [FAS3270-1b_0c]
vsan 101 wwn 20:00:00:25:b5:00:0a:0f fcid 0x550003 dynamic
! [vm-host-infra-01-fabric-a]
vsan 101 wwn 20:00:00:25:b5:00:0a:1f fcid 0x550004 dynamic
! [vm-host-infra-02-fabric-a]
```

```
interface san-port-channel 1
channel mode active
```

```
interface port-channel10
description vPC peer-link
switchport mode trunk
vpc peer-link
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
spanning-tree port type network
```

```
interface port-channel11
description FAS3270-1a
switchport mode trunk
vpc 11
switchport trunk native vlan 805
switchport trunk allowed vlan 802,805,807
spanning-tree port type edge trunk
```

```
interface port-channel12
description FAS3270-1b
switchport mode trunk
vpc 12
switchport trunk native vlan 805
switchport trunk allowed vlan 802,805,807
spanning-tree port type edge trunk
```

```
interface port-channel13
description UCS-2a
switchport mode trunk
vpc 13
```



```
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
spanning-tree port type edge trunk
```

```
interface port-channel14
description UCS-2b
switchport mode trunk
vpc 14
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
spanning-tree port type edge trunk
```

```
interface port-channel20
description icecore
switchport mode trunk
vpc 20
switchport trunk native vlan 2
switchport trunk allowed vlan 805
spanning-tree port type network
```

```
vsan database
vsan 101 interface san-port-channel 1
vsan 101 interface fc1/29
vsan 101 interface fc1/30
```

```
interface fc1/29
switchport description FAS3270-1a:0c
no shutdown
```

```
interface fc1/30
switchport description FAS3270-1b:0c
no shutdown
```

```
interface fc1/31
switchport description UCS-2a:fc1/31
channel-group 1 force
no shutdown
```

```
interface fc1/32
switchport description UCS-2a:fc1/32
```



```
channel-group 1 force  
no shutdown
```

```
interface Ethernet1/1  
description FAS3270-1a:e2a  
switchport mode trunk  
switchport trunk native vlan 805  
switchport trunk allowed vlan 802,805,807  
channel-group 11 mode active
```

```
interface Ethernet1/2  
description FAS3270-1b:e2a  
switchport mode trunk  
switchport trunk native vlan 805  
switchport trunk allowed vlan 802,805,807  
channel-group 12 mode active
```

```
interface Ethernet1/3  
description UCS-2a:Eth1/19  
switchport mode trunk  
switchport trunk native vlan 2  
switchport trunk allowed vlan 801-807  
channel-group 13 mode active
```

```
interface Ethernet1/4  
description UCS-2b:Eth1/19  
switchport mode trunk  
switchport trunk native vlan 2  
switchport trunk allowed vlan 801-807  
channel-group 14 mode active
```

```
interface Ethernet1/5  
description Nexus5548-2:Eth1/5  
switchport mode trunk  
switchport trunk native vlan 2  
switchport trunk allowed vlan 801-807  
channel-group 10 mode active
```

```
interface Ethernet1/6  
description Nexus5548-2:Eth1/6
```




```
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
channel-group 10 mode active
```

```
interface Ethernet1/7
```

```
interface Ethernet1/8
```

```
interface Ethernet1/9
```

```
interface Ethernet1/10
```

```
interface Ethernet1/11
```

```
interface Ethernet1/12
```

```
interface Ethernet1/13
```

```
interface Ethernet1/14
```

```
interface Ethernet1/15
```

```
interface Ethernet1/16
```

```
interface Ethernet1/17
```

```
interface Ethernet1/18
```

```
interface Ethernet1/19
```

```
interface Ethernet1/20
```

```
description core:Eth1/21
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 805
channel-group 20 mode active
```

```
interface Ethernet1/21
```



interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface mgmt0

ip address 10.61.185.69/24

line console

line vty

boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N2.2a.bin

boot system bootflash:/n5000-uk9.5.0.3.N2.2a.bin

interface fc1/31

interface fc1/32

interface fc1/29

interface fc1/30

interface fc1/31

interface fc1/32

!Full Zone Database Section for vsan 101

zone name vm-host-infra-01-fabric-a vsan 101

member pwwn 20:00:00:25:b5:00:0a:0f

! [vm-host-infra-01-fabric-a]

member pwwn 50:0a:09:82:8d:73:42:07

! [FAS3270-1a_0c]

member pwwn 50:0a:09:82:9d:73:42:07

! [FAS3270-1b_0c]

zone name vm-host-infra-02-fabric-a vsan 101

member pwwn 20:00:00:25:b5:00:0a:1f

! [vm-host-infra-02-fabric-a]

member pwwn 50:0a:09:82:8d:73:42:07

! [FAS3270-1a_0c]



```
member pwwn 50:0a:09:82:9d:73:42:07
! [FAS3270-1b_0c]
```

```
zoneset name flexpod vsan 101
member vm-host-infra-01-fabric-a
member vm-host-infra-02-fabric-a
```

```
zoneset activate name flexpod vsan 101
```

Nexus B (sample running config)

```
!Command: show running-config
```

```
!Time: Thu Mar 1 13:28:07 2012
```

```
version 5.0(3)N2(2a)
feature fcoe
feature npiv
feature fport-channel-trunk
no feature telnet
no telnet server enable
cfs eth distribute
feature lacp
feature vpc
feature lldp
username admin password 5 $1$QwOvH6l4$uemTjtt9Bz9c2SSA1DPOX. role network-admin
ip domain-lookup
hostname Nexus5548-2
logging event link-status default
ip access-list classify_Silver
  10 permit ip 192.168.102.0/24 any
  20 permit ip any 192.168.102.0/24
  30 permit ip 192.168.106.0/24 any
  40 permit ip any 192.168.106.0/24
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 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
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 jumbo
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    mtu 9000
    multicast-optimize
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
slot 1
  port 28-32 type fc
snmp-server user admin network-admin auth md5 0xe481d1d2fee4aaa498237df1852270e8 priv
0xe481d1d2fee4aaa498237df1852270e8 localizedkey
snmp-server enable traps entity fru
ntp server 10.61.185.11 use-vrf management
vrf context management
  ip route 0.0.0.0/0 10.61.185.1
vlan 1
vlan 2
  name Native-VLAN
```



```
vlan 805
  name VM-MGMT-VLAN
vlan 801
  name CSV-VLAN
vlan 802
  name iSCSI-Fabric-A
vlan 803
  name LiveMigration-VLAN
vlan 806
  name App-Cluster-Comm-VLAN
vlan 804
  name VM-Data-VLAN
vlan 807
  name iSCSI-Fabric-B
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vpc domain 23
  role priority 20
  peer-keepalive destination 10.61.185.69 source 10.61.185.70
vsan database
  vsan 102 name "Fabric_B"
  vsan 202
device-alias database
  device-alias name FAS3270-1a_0d pwwn 50:0a:09:81:8d:73:42:07
  device-alias name FAS3270-1b_0d pwwn 50:0a:09:81:9d:73:42:07
  device-alias name vm-host-infra-01-fabric-b pwwn 20:00:00:25:b5:00:0b:0f
  device-alias name vm-host-infra-02-fabric-b pwwn 20:00:00:25:b5:00:0b:1f

device-alias commit

fcdomain fcid database
  vsan 102 wwn 24:02:54:7f:ee:23:8b:00 fcid 0x3f0000 dynamic
  vsan 102 wwn 50:0a:09:81:9d:73:42:07 fcid 0x3f0001 dynamic
!      [FAS3270-1b_0d]
  vsan 102 wwn 50:0a:09:81:8d:73:42:07 fcid 0x3f0002 dynamic
!      [FAS3270-1a_0d]
  vsan 102 wwn 20:00:00:25:b5:00:0b:0f fcid 0x3f0003 dynamic
!      [vm-host-infra-01-fabric-b]
  vsan 102 wwn 20:00:00:25:b5:00:0b:1f fcid 0x3f0004 dynamic
```



! [vm-host-infra-02-fabric-b]

```
interface san-port-channel 2
  channel mode active
```

```
interface port-channel10
  description vPC peer-link
  switchport mode trunk
  vpc peer-link
  switchport trunk native vlan 2
  switchport trunk allowed vlan 801-807
  spanning-tree port type network
```

```
interface port-channel11
  description FAS3270-1a
  switchport mode trunk
  vpc 11
  switchport trunk native vlan 805
  switchport trunk allowed vlan 802,805,807
  spanning-tree port type edge trunk
```

```
interface port-channel12
  description FAS3270-1b
  switchport mode trunk
  vpc 12
  switchport trunk native vlan 805
  switchport trunk allowed vlan 802,805,807
  spanning-tree port type edge trunk
```

```
interface port-channel13
  description UCS-2a
  switchport mode trunk
  vpc 13
  switchport trunk native vlan 2
  switchport trunk allowed vlan 801-807
  spanning-tree port type edge trunk
```

```
interface port-channel14
  description UCS-2b
```



```
switchport mode trunk
vpc 14
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
spanning-tree port type edge trunk
```

```
interface port-channel20
description core
switchport mode trunk
vpc 20
switchport trunk native vlan 2
switchport trunk allowed vlan 805
spanning-tree port type network
```

```
vsan database
vsan 102 interface san-port-channel 2
vsan 102 interface fc1/29
vsan 102 interface fc1/30
```

```
interface fc1/29
switchport description FAS3270-1a:0d
no shutdown
```

```
interface fc1/30
switchport description FAS3270-1b:0d
no shutdown
```

```
interface fc1/31
switchport description UCS-2b:fc1/31
channel-group 2 force
no shutdown
```

```
interface fc1/32
switchport description UCS-2b:fc1/32
channel-group 2 force
no shutdown
```

```
interface Ethernet1/1
description FAS3270-1a:e2b
switchport mode trunk
```




```
switchport trunk native vlan 805
switchport trunk allowed vlan 802,805,807
channel-group 11 mode active
```

```
interface Ethernet1/2
description FAS3270-1b:e2b
switchport mode trunk
switchport trunk native vlan 805
switchport trunk allowed vlan 802,805,807
channel-group 12 mode active
```

```
interface Ethernet1/3
description UCS-2a:Eth1/20
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
channel-group 13 mode active
```

```
interface Ethernet1/4
description UCS-2b:Eth1/20
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
channel-group 14 mode active
```

```
interface Ethernet1/5
description Nesus5548-1:Eth1/5
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
channel-group 10 mode active
```

```
interface Ethernet1/6
description Nexus5548-1:Eth1/6
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 801-807
channel-group 10 mode active
```

```
interface Ethernet1/7
```



interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

description core:Eth1/22

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 805

channel-group 20 mode active

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24



interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface mgmt0

ip address 10.61.185.70/24

line console

line vty

boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N2.2a.bin

boot system bootflash:/n5000-uk9.5.0.3.N2.2a.bin

interface fc1/31

interface fc1/32

interface fc1/29

interface fc1/30

interface fc1/31

interface fc1/32

!Full Zone Database Section for vsan 102

zone name vm-host-infra-01-fabric-b vsan 102

member pwwn 20:00:00:25:b5:00:0b:0f

! [vm-host-infra-01-fabric-b]

member pwwn 50:0a:09:81:8d:73:42:07

! [FAS3270-1a_0d]

member pwwn 50:0a:09:81:9d:73:42:07

! [FAS3270-1b_0d]

zone name vm-host-infra-02-fabric-b vsan 102

member pwwn 20:00:00:25:b5:00:0b:1f

! [vm-host-infra-02-fabric-b]

member pwwn 50:0a:09:81:8d:73:42:07

! [FAS3270-1a_0d]

member pwwn 50:0a:09:81:9d:73:42:07

! [FAS3270-1b_0d]

zoneset name flexpod vsan 102

member vm-host-infra-01-fabric-b

member vm-host-infra-02-fabric-b



zoneset activate name flexpod vsan 102



About Cisco Validated Design (CVD) Program

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2012 Cisco Systems, Inc. All rights reserved