

Cisco Solution for EMC VSPEX Microsoft Private Cloud Fast Track 4.0

July 2014



Building Architectures to Solve Business Problems



About Cisco Validated Design (CVD) Program

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

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)

© 2014 Cisco Systems, Inc. All rights reserved

About the Authors

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

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

Mike McGhee, Consulting Solutions Engineer, EMC

Mike is a consulting solutions engineer with EMC Corporation based outside of Boston, Massachusetts. Mike has been with EMC for 15 years focusing on enterprise storage and Microsoft platforms. Currently Mike is focusing on System Center, Hyper-V and Windows Server 2012 integration with storage technologies, and how such technologies help to enable cloud infrastructures.

David Feisthammel, Consulting Solutions Engineer, EMC

Dave is a consulting solutions engineer with EMC Corporation based in Bellevue, Washington, just blocks from the Microsoft headquarters campus. As a member of EMC's Microsoft Partner Engineering team, he focuses on Microsoft's enterprise hybrid cloud technologies, including Windows Server, Hyper-V, and System Center. Dave is an accomplished IT professional with progressive international and domestic experience in the development, implementation, and market launch of IT solutions and products. With nearly three decades of experience in Information Technology, he has presented, lectured, taught, and written on various topics related to systems management.

Acknowledgments

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

Mike Mankovsky, Technical Leader Engineering, Cisco Systems, Inc.

Cisco Solution for EMC VSPEX Microsoft Private Cloud Fast Track 4.0

Introduction

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

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

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

Private Cloud Fast Track Program Description

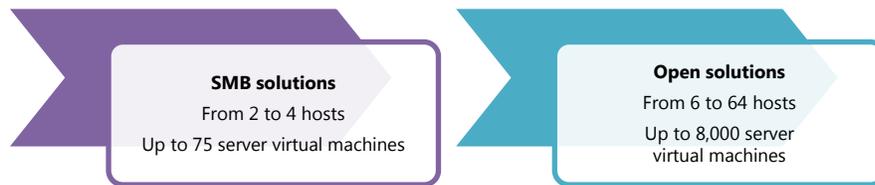
The Infrastructure as a Service Product Line Architecture (PLA) is focused on deploying virtualization fabric and fabric management technologies in Windows Server and System Center to support private cloud scenarios. This PLA includes reference architectures, best practices, and processes for streamlining deployment of these platforms to support private cloud scenarios.

This component of the IaaS PLA focuses on delivering core foundational virtualization fabric infrastructure guidance that aligns to the defined architectural patterns within this and other Windows Server 2012 R2 private cloud programs. The resulting Hyper-V infrastructure in Windows Server 2012 R2 can be leveraged to host advanced workloads, and subsequent releases will contain fabric management scenarios using System Center components. Scenarios relevant to this release include:

- Resilient infrastructure – Maximize the availability of IT infrastructure through cost-effective redundant systems that prevent downtime, whether planned or unplanned.
- Centralized IT – Create pooled resources with a highly virtualized infrastructure that supports maintaining individual tenant rights and service levels.
- Consolidation and migration – Remove legacy systems and move workloads to a scalable high-performance infrastructure.
- Preparation for the cloud – Create the foundational infrastructure to begin transition to a private cloud solution.

The Fast Track program has two main solutions, as shown in the following figure. This guide will focus exclusively on the Open Solutions branch.

Figure 1. Branches of the Microsoft Private Cloud



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

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

The Cisco and EMC VSPEX Fast Track Solution presented here is an Open solution. The Cisco and EMC VSPEX with Microsoft Private Cloud Fast Track solution utilizes the core capabilities of Windows Server 2012 R2, Hyper-V, and System Center 2012 R2 to deliver a Private Cloud - Infrastructure as a Service offering. The key software components of every Reference Implementation are Windows Server 2012 R2, Hyper-V, and System Center 2012 R2. The solution also includes software from Cisco and EMC to form a complete solution that is ready for your enterprise.

Business Value

The Cisco and EMC VSPEX with Microsoft Private Cloud Fast Track solution provides a reference architecture for building private clouds on each organization's unique terms. Each Fast-Track solution helps organizations implement private clouds with increased ease and confidence. Among the benefits of the Microsoft Private Cloud Fast Track Program are faster deployment, reduced risk, and a lower cost of ownership.

Reduced risk:

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

Lower cost of ownership:

- A cost-optimized, platform and software-independent solution for rack system integration
- High performance and scalability with Windows Server 2012 R2 operating system and Hyper-V
- Minimized backup times and fulfilled recovery time objectives for each business critical environment

Technical Benefits

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

Faster deployment:

- End-to-end architectural and deployment guidance
- Streamlined infrastructure planning due to predefined capacity

- Enhanced functionality and automation through deep knowledge of infrastructure
- Integrated management for virtual machine (VM) and infrastructure deployment
- Self-service portal for rapid and simplified provisioning of resources

Program Requirements and Validation

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

Design Patterns Overview

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

Table 1. Design Pattern Summaries

Design Pattern	Key Features
1. Software-defined infrastructure	<ul style="list-style-type: none"> • File-based Storage Networking through SMB3 • Deep guidance for using Windows as the storage platform i.e. Storage Spaces, SMB Direct, etc.
2. Non-Converged infrastructure	<ul style="list-style-type: none"> • Dedicated Ethernet NICs and Storage HBAs • iSCSI, FCoE, or Fibre Channel storage networking
3. Converged infrastructure	<ul style="list-style-type: none"> • Converged Networking • FC, FCoE, or iSCSI storage networking

The Cisco and EMC solution is a converged solution deployed with Fibre Channel.

Design Pattern #3: Converged Infrastructure

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

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

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

Core Fast Track Infrastructure

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

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

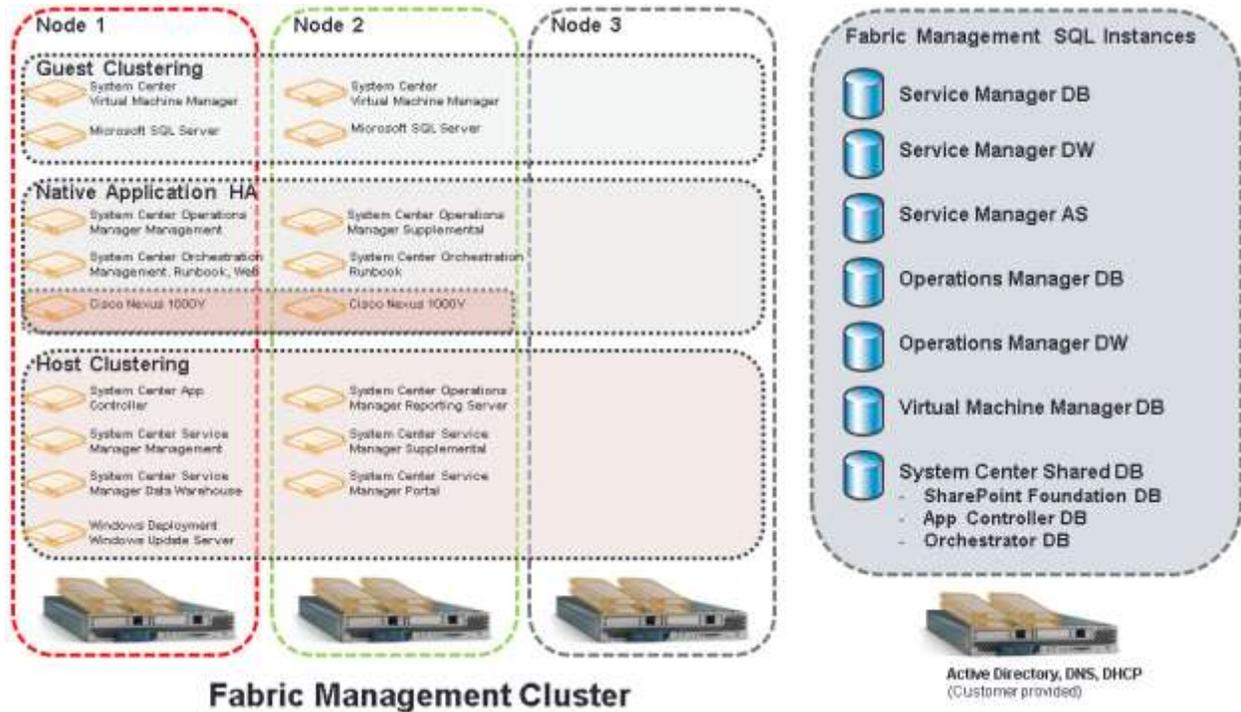
It is recommended that the systems that make up the Fabric Management layer be physically separated from the rest of the Fabric. Dedicated Fabric Management servers should be used to host those virtual machines which provide management for all of the resources within the cloud infrastructure. This model helps ensure that, regardless of the state of the majority of Fabric resources, management of the infrastructure and its workloads is maintained at all times.

To support this level of availability and separation, IaaS PLA cloud architectures contains a separate set of hosts, running Windows Server 2012 R2 configured as a failover cluster with the Hyper-V role enabled. It should contain a minimum two-node Fabric Management cluster (a three-node cluster is recommended for scale and availability). This Fabric Management cluster is dedicated to the virtual machines running the suite of products that provide IaaS management functionality, and it is not intended to run additional customer workloads over the Fabric infrastructure.

Furthermore, to support Fabric Management operations, these hosts contain high availability virtualized instances (virtual machines) of the management infrastructure (System Center components and their dependencies). However, for some components of the management stack, native high availability is maintained on the application level, for example, a Guest Cluster, built-in availability constructs, or a network load balanced array.

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

Figure 2. Private Cloud Fabric Management Infrastructure



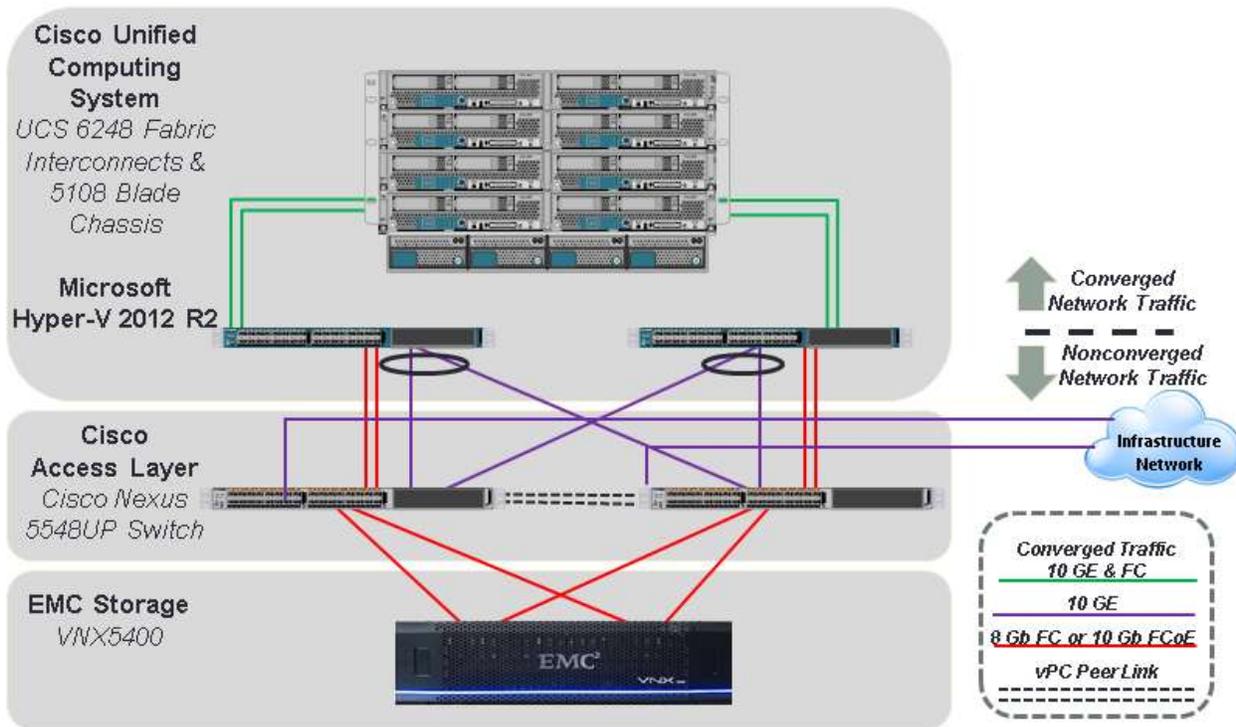
The Fabric Management cluster is configured in such a manner to make sure maximum availability of all components of the environment. Each Cisco UCS B200 M3 blade server is configured with sufficient memory to support the running of all the listed virtual machines illustrated above. By provisioning a third node, the environment retains its highly available capability even during those periods of time when the host nodes are individually taken down for maintenance. For example, in the above figure, even if Node 3 was down for maintenance, a catastrophic failure of Node 2 would not prevent all the virtual machines from continuing to run on Node 1.

Architecture

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

The Cisco UCS solution validated with Microsoft Private Cloud includes EMC VNX5400 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 3. Implementation Diagram



The above reference configuration contains the following components:

- One 5108 chassis each with two Cisco UCS 2204XP Fabric Extenders
- Eight Cisco UCS B200 M3 Blade Servers
 - Dual Intel E5-2660V2 2.20 GHz processors
 - 256 GB memory
 - Cisco UCS 1240 Virtual Interface Card
- Two Cisco UCS 6248UP Fabric Interconnects
- Two Cisco Nexus 5548UP Switches
- 10 GE and 8 Gb FC connections
- EMC VNX5400 Unified Platform
 - 75 x 300 GB SAS 10K disks
 - EMC SnapView

Storage is provided by an EMC VNX5400 storage array with accompanying disk shelves. All systems and fabric links feature redundancy, providing for end-to-end high availability (HA configuration within a single chassis). For server virtualization, the deployment includes Microsoft Hyper-V. While this is the default base design, each of the components can be scaled flexibly to support the specific business requirements in question. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves or SSDs could be deployed to improve I/O capacity and throughput, or special hardware or software features could be added to introduce new features.

The remainder of this document provides guidance through the low-level steps of deploying the base architecture, as shown in the above figure. This includes everything from physical cabling, to compute and storage configuration, to configuring virtualization with Microsoft Windows Server 2012 R2 Hyper-V.

Prerequisite Infrastructure

Active Directory Domain Services (AD DS)

Active Directory Domain Services (AD DS) is a required foundational component. The IaaS PLA supports customer deployments for AD DS in Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008. Previous versions of the Windows operating system are not directly supported for all workflow provisioning and deprovisioning automation. It is assumed that AD DS deployments exist at the customer site and deployment of these services is not in scope for the typical IaaS PLA deployment.

- **Forests and domains:** The preferred approach is to integrate into an existing AD DS forest and domain, but this is not a hard requirement. A dedicated resource forest or domain may also be employed as an additional part of the deployment. System Center does support multiple domains or multiple forests in a trusted environment using two-way forest trusts.
- **Trusts:** System Center allows multi-domain support within a single forest in which two-way forest (Kerberos) trusts exist between all domains. This is referred to as multi-domain or intra-forest support.

Domain Name System (DNS)

Name resolution is a required element for System Center 2012 R2 components installation and the process automation solution. Domain Name System (DNS) integrated in AD DS is required for automated provisioning and deprovisioning components. This solution provides full support for deployments running Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008 DNS.

Use of non-Microsoft or non-AD DS integrated DNS solutions might be possible, but they would not provide automated creation and removal of DNS records that are related to component installation as well as virtual machine provisioning and deprovisioning processes. Use of solutions outside of AD DS integrated DNS would require manual intervention for these scenarios. Use of non-AD DS integrated DNS is not covered as part of this CVD.

IP Address Assignment and Management

To support dynamic provisioning and runbook automation, and to manage physical and virtual compute capacity within the IaaS infrastructure, by default, Dynamic Host Configuration Protocol (DHCP) is used by default for all physical computers and virtual machines. For physical hosts like the Fabric Management cluster nodes and the scale unit cluster nodes, DHCP reservations or fixed IP addresses are recommended so that physical servers and network adapters have known Internet Protocol (IP) addresses. DHCP provides centralized management of these addresses.

Virtual Machine Manager (VMM) can provide address management both for physical computers (Hyper-V Host Servers and Scale-Out File Servers) and for virtual machines. These IP addresses are assigned statically from IP Address Pools managed by Virtual Machine Manager. This approach is recommended as an alternative to DHCP and also provides centralized management.

If a particular subnet or IP Address range is maintained by Virtual Machine Manager, it should not be served by DHCP. However, other subnets, e.g. used by physical servers, which are not managed by Virtual Machine Manager, can still leverage DHCP.

Regardless of the IP address assignment mechanism chosen (DHCP, Virtual Machine Manager, or both), Windows Server IP Address Management (IPAM) feature can be leveraged to keep track in-use IP addresses for reporting and advanced automation. Optionally, both DHCP and Virtual Machine Manager features can be integrated with IPAM. Use of IPAM within Windows Server is outside the scope of this document.

Software Revisions

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

Table 2. Software Revisions

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect	2.2(1b)	http://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821
	Cisco UCS B-200-M3	2.2(1b)	http://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821
Network	Nexus Fabric Switch	5.0(3)N2(2a)	Operating system version
Storage	EMC VNX5400 Block	05.33.000.5.038	Operating system version
	EMC VNX5400 File (Optional)	8.1.1-33	Operating system version
Software	Cisco UCS Hosts	2012 R2	Microsoft Windows Server Datacenter Edition + Hyper-V Role
	.NET Framework	3.5.1	Feature enabled within Windows Server 2012 R2 (Required for SQL installations)
	.NET Framework	4.0	http://download.microsoft.com/download/9/5/A/95A9616B-7A37-4AF6-BC36-D6EA96C8DAAE/dotNetFx40_Full_x86_x64.exe
	Windows MPIO software		Feature within Windows Server 2012 R2
	Cisco UCS Management Pack for SCOM 2012 R2	2.6.2	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=283034298&release=2.6.2&relinid=AVAILABLE&rellifecycle=&reltype=latest
	Cisco UCS Power Tools	1.1.1	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574017&release=1.1.1&relinid=AVAILABLE&rellifecycle=&reltype=latest
	Cisco UCS Integration Pack for SCO	1.0	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574013&release=1.0.0&relinid=AVAILABLE&rellifecycle=&reltype=latest
	Cisco UCS SCO Sample Runbook		https://communities.cisco.com/servlet/JiveServlet/download/36898-2-54853/CiscoUcsSampleRunbooks_v1.0.ois_export.zip
	Cisco Nexus 1000V	1.5.2b	http://software.cisco.com/download/release.html?mdfid=284786025&softwareid=282088129&release=5.2(1)SM1(5.2b)&relinid=AVAILABLE&rellifecycle=&reltype=latest&i=rm
	Cisco Nexus 1000V PowerShell	1.0	https://developer.cisco.com/fileMedia/download/8bf948fb-83a5-4c9e-af5c-4faac735c8d3
	Cisco UCS SCVMM	1.0.2	http://software.cisco.com/download/release.html?mdfid=283850978&flowid=25021&softwareid=284574016&release=1.0.2&relinid=AVAILABLE&rellifecycle=&reltype=latest

	Extension		d=AVAILABLE&rellifecycle=&reltype=latest
	EMC Navisphere	7.32.25.1.63-1	EMC CLI
	EMC PowerPath	5.7.SP2.b447	EMC integration within Windows operating system
	EMC Storage Integrator (ESI)	2.1.812.5137	EMC Storage Integrator with EMC PowerShell
	EMC Management Pack	2.1.812.5137	Systems Center Operations Manager Management Pack
	EMC SMI-S Provider	4.5.1	Provider for Systems Center Virtual Machine Manager Integration.
	EMC Unisphere Host Agent	1.2.25.1.0163	Automated host registration with VNX
VM Software	Windows Server Datacenter Edition	2012 R2	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/6/D/A/6DAB58BA-F939-451D-9101-7DE07DC09C03/9200.16384.WIN8_RTM.120725-1247_X64FRE_SERVER_EVAL_EN-US-HRM_SSS_X64FREE_EN-US_DV5.ISO
	Windows Server Datacenter Edition	2008 R2 SP1	Evaluation software – can be upgraded. http://www.microsoft.com/en-us/download/details.aspx?id=11093
	MS SQL Server (2 VMs in HA cluster)	2012 SP1	Evaluation software – can be upgraded http://download.microsoft.com/download/3/B/D/3BD9DD65-D3E3-43C3-BB50-0ED850A82AD5/SQLServer2012SP1-FullSlipstream-ENU-x64.iso
	SQL Server Cumulative Update	2012 SP1	http://support.microsoft.com/kb/2917531/en-us
	Operations Manager Management Server	2012 R2	Evaluation software – can be upgraded http://care.dlservice.microsoft.com/dl/download/0/3/F/03F1B876-E7D7-45BE-8B0B-0BDBD02DD800/SC2012_SP1_SCOM_EN.exe
	Operations Manager Supplemental Management Server	2012 R2	Same as above
	Operations Manager Reporting Server	2012 R2	Same as above.

Virtual Machine Manager (2 VMs in HA configuration)	2012 R2	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/4/8/5/485D6D85-5811-4E7E-83F5-84F9492D3234/SC2012_SP1_SCVMM.exe
Orchestrator Management and Action Server	2012 R2	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/9/9/4/99473D48-B8E2-453D-9B34-33FEA42038F7/SC2012_SP1_SCO.exe
Orchestrator Supplemental Action Server	2012 R2	Same as above.
Service Manager Management Server	2012 R2	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/B/F/5/BF5B6A61-D12C-41F3-B220-6A127E24C57F/SC2012_SP1_SCSM.exe
Service Manager Supplemental Management Server	2012 R2	Same as above.
Service Manager Data Warehouse	2012 R2	Same as above.
Service Manager Self-Service Portal	2012 R2	Same as above.
App Controller	2012 R2	Evaluation software – can be upgraded. http://care.dlservice.microsoft.com/dl/download/F/9/1/F916020F-CCFF-427C-BF88-30318B72582F/SC2012_SP1_SCAC.exe
Windows Deployment Server	2012 R2	Optional: Enabled role within Windows Server 2012 R2
Windows Assessment and Deployment Kit (ADK) for Windows 8.1		http://download.microsoft.com/download/6/A/E/6AEA92B0-A412-4622-983E-5B305D2EBE56/adk/adksetup.exe
System Center 2012 R2 Integration Packs	2012 R2	http://www.microsoft.com/en-us/download/confirmation.aspx?id=39622&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1
System Center 2012 Operations Manager management packs	2012 R2	http://download.microsoft.com/download/f/7/b/f7b960c9-7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.Library.mp http://download.microsoft.com/download/f/7/b/f7b960c9-7392-4c5a-bab4-efbb8a66ec2a/Microsoft.Windows.Server.2008.Discovery.mp http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServic

			<p>es.CommonLibrary.mp</p> <p>http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2003.mp</p> <p>http://download.microsoft.com/download/F/F/1/FF13C2CF-C955-4D3F-94EA-4094AD0DBFF3/Microsoft.Windows.InternetInformationServices.2008.mp</p> <p>http://download.microsoft.com/download/0/7/7/07714012-3B7C-4691-9F2B-7ADE4188E552/Microsoft.SQLServer.Library.mp</p>
	SQL Server 2012 Analysis Management Objects	2012	http://download.microsoft.com/download/4/B/1/4B1E9B0E-A4F3-4715-B417-31C82302A70A/ENU/x64/SQL_AS_AMO.msi
	SQL Server 2008 R2 SP1 Analysis Management Objects	2008	http://download.microsoft.com/download/9/1/3/9138773A-505D-43E2-AC08-9A77E1E0490B/1033/IA64/SQLSERVER2008_ASAMO10.msi
	Microsoft Report Viewer 2010 SP1	2010	http://download.microsoft.com/download/5/B/9/5B95F704-F7E3-440D-8C68-A88635EA4F87/ReportViewer.exe
	Microsoft Report Viewer 2008 SP1	2008 SP1	http://download.microsoft.com/download/0/4/F/04F99ADD-9E02-4C40-838E-76A95BCEFB8B/ReportViewer.exe
	SQL Server 2012 SP1 Native Client	2012	http://download.microsoft.com/download/4/B/1/4B1E9B0E-A4F3-4715-B417-31C82302A70A/ENU/x64/sqlncli.msi
	Microsoft SharePoint Foundation 2010	2010	http://download.microsoft.com/download/3/5/C/35C62B58-0C29-4A8F-BC6B-D28CD1A6EEDD/SharePointFoundation.exe
	Microsoft SharePoint Foundation 2010 SP1	2010 SP1	http://download.microsoft.com/download/7/0/0/7002DFA1-831C-414A-AE71-A5D18BEF1E32/sharepointfoundation2010sp1-kb2460058-x64-fullfile-en-us.exe
	Silverlight		http://download.microsoft.com/download/5/A/C/5AC56802-B26B-4876-8872-7303C8F27072/20125.00/runtime/Silverlight_x64.exe
Miscellaneous	Java	7.0 or later	http://java.com/en/download/ie_manual.jsp?locale=en
	PuTTY	0.62	http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
	PL-2303 USB-to-Serial driver	1.7.0	https://s3.amazonaws.com/plugable/bin/PL2303_Prolific_DriverInstaller_v1.7.0.zip

Configuration Guidelines

This document provides details for configuring a fully redundant, highly-available configuration. As such, references are made as to which component is being configured with each step whether that be A or B. For example, Storage Processor A (SP A) and Storage Processor B (SP B), are used to identify the two EMC storage controllers that are provisioned with this document while Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are configured likewise. Additionally, this document details steps for provisioning multiple UCS hosts and these are identified sequentially, FT4-Infra01 and FT4-Infra02, and so on. Finally, when indicating that the reader should include information pertinent to their environment in a given step, this is indicated with the inclusion of *<italicized text>* as part of the command structure. See the example below for the vlan create command:

```
controller A> vlan create

Usage:

vlan create [-g {on|off}] <ifname> <vlanid_list>
vlan add <ifname> <vlanid_list>
vlan delete -q <ifname> [<vlanid_list>]
vlan modify -g {on|off} <ifname>
vlan stat <ifname> [<vlanid_list>]

Example:
controller A> vlan create vif0 <management VLAN ID>
```

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

This document is intended to allow the reader to fully configure the customer environment. In order to do so, there are various steps which will require you to insert your own naming conventions, IP address and VLAN schemes as well as record appropriate WWPN, WWNN, or MAC addresses. The following table details the list of VLANs necessary for deployment as outlined in this guide. Note that in this document the VMaccess VLAN is used for virtual machine access. The Mgmt VLAN is used for management interfaces of the Hyper-V hosts. A Layer-3 route must exist between the Mgmt and VMaccess VLANs.

Table 3. VLAN Names and IDs Used in this Document

VLAN Name	VLAN Purpose	VLAN ID
Default	VLAN to which untagged frames are assigned	1
VMaccess	VM access	10
LiveMigration	Hyper-V Live Migration	11
CSV	Cluster Shared Volume	12
ClusComm	VM guest cluster communication	13
VEM	Virtual Ethernet Module for Nexus 1000V	200
Mgmt	Host management interface	177

Configuration Workstation

It is recommended to have a Windows 8.1 or Windows Server 2012 R2 workstation configured with certain prerequisite software and joined to the same domain as the Hyper-V servers will be joined. Using a properly configured workstation makes the job of installing the solution easier. The following is the recommendation for software to be installed on the workstation.

Note: The Remote Server Administration Toolkit (RSAT) is operating system version specific. In order to fully manage the Windows Server 2012 R2 systems, you must use either a Windows 8.1 or Windows Server 2012 R2 workstation. Earlier versions will not work properly.

Windows 8.1 Workstation

- Install .NET Framework 3.5 by issuing the following command from an elevated command prompt: `Enable-WindowsOptionalFeature -Online -FeatureName NetFx3 -Source D:\sources\sxs`. This assumes the drive D: is the location of your Windows distribution media.
- Install the Remote Server Administration Tools for Windows 8.1. This is found at <http://www.microsoft.com/en-us/download/details.aspx?id=39296>. This is available in both a 32-bit and 64-bit distribution. Make sure you select the copy that matches your Windows 8.1 installation.
- After installing the Remote Server Administration Tools, install specific management tools.
 - *Hyper-V Management Tools* – issue the following command from an elevated command prompt:
`dism /online /enable-feature /all /featurename:Microsoft-Hyper-V-Tools-All`
 - *Failover Clustering Tools* – issue the following command from an elevated command prompt:
`dism /online /enable-feature /featurename:RemoteServerAdministrationTools-Features-Clustering`

Windows Server 2012 R2 Workstation

- Install .NET Framework 3.5 by issuing the following command from an elevated command prompt: `Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs`. This assumes the drive D: is the location of your Windows distribution media.
- Install the Hyper-V Management Tools by issuing this PowerShell cmdlet: `Install-WindowsFeature -Name RSAT-Hyper-V-Tools`
- Install the Windows Failover Clustering Tools by issuing this PowerShell cmdlet: `Install-WindowsFeature -Name RSAT-Clustering`

Both Workstations

- Cisco UCS PowerTool for UCSM, version 1.1.1. Installation instructions are found in section on Cisco Integration Components.
- Cisco Nexus 1000V PowerShell, version 1.0. Installation instructions are found in the section on Cisco Integration Components.
- Naviseccli – Navisphere Secure Command Line Interface
- ESI (EMC Storage Integrator) – EMC PowerShell library
- Java 7 – required for running UCS Manager. Installed from the web.
- PuTTY – an SSH and Telnet client helpful in initial configuration of the Cisco UCS 6248UP Fabric Interconnects. This program just needs to be copied to the system.
- PL-2303 USB-to-Serial driver – used to connect to the Cisco UCS 6248UP Fabric Interconnects through a serial cable connected to a USB port on the workstation. The download is a .zip file. Extract the executable from the .zip file and load it on the system.

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

Deployment

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

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

The Microsoft Private Cloud Solution validated with the Cisco and EMC architecture is flexible; therefore, the exact configuration detailed in this section might vary for customer implementations depending on specific requirements. Although customer implementations might deviate from the information that follows, the best practices, features,

and configurations listed in this section should still be used as a reference for building a customized Cisco and EMC with Microsoft Private Cloud solution.

Cabling Information

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

The tables in this section contain details for the prescribed and supported configuration of the EMC VNX5400.

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

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

It is possible to order an EMC VNX5400 system in a different configuration from what is described in the tables in this section. Before starting, be sure the configuration matches what is described in the tables and diagrams in this section.

Note: Fibre Channel connections to the EMC VNX5400 are assumed to be connected to the first and second onboard IO ports. The onboard ports used for these connections are numbered 2 -5.

Table 4. Cisco Nexus 5548 A Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Cisco Nexus 5548 B	Eth 1/1
Eth 1/2	10 GE	Cisco Nexus 5548 B	Eth 1/2
Eth 1/17	10 GE	Cisco 6248 A	Eth 1/17
Eth 1/18	10 GE	Cisco 6248 B	Eth 1/17
Eth 1/29	FC	EMC SPA	A2
Eth 1/30	FC	EMC SPB	B2
FC 1/31	FC	Cisco 6248 A	FC 1/31
FC 1/32	FC	Cisco 6248 A	FC 1/32

Table 5. Cisco Nexus B Cabling Information

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

Table 6. Cisco 6248 Fabric Interconnect A Cabling Information

Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Chassis 1 FEX A	Port 1
Eth 1/2	10 GE	Chassis 1 FEX A	Port 2
Eth 1/17	10 GE	Cisco 5548 A	Eth 1/17
Eth 1/18	10 GE	Cisco 5548 B	Eth 1/17
FC 1/31	FC	Cisco 5548 A	FC 1/31
FC 1/32	FC	Cisco 5548 A	FC 1/32

Table 7. Cisco 6248 Fabric Interconnect B Cabling Information

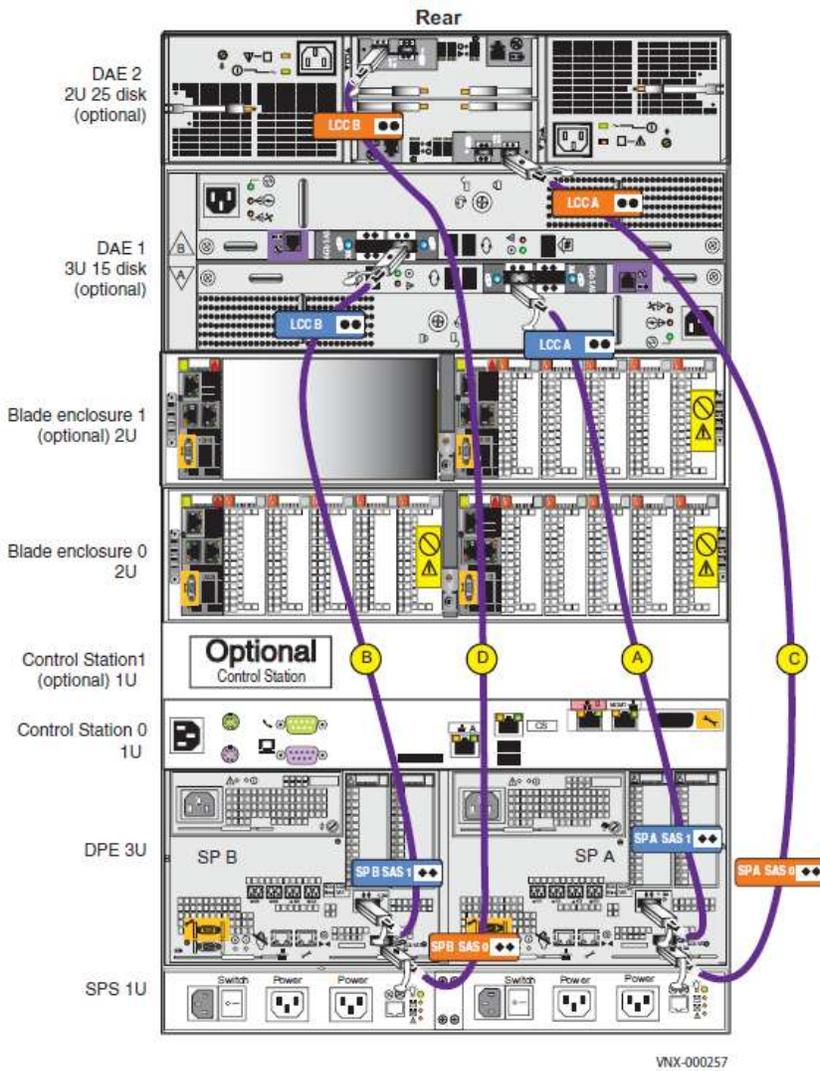
Local Port	Connection	Remote Device	Remote Port
Eth 1/1	10 GE	Chassis 1 FEX B	Port 1
Eth 1/2	10 GE	Chassis 1 FEX B	Port 2
Eth 1/17	10 GE	Cisco 5548 B	Eth 1/18
Eth 1/18	10 GE	Cisco 5548 A	Eth 1/18
FC 1/31	FC	Cisco 5548 B	FC 1/31
FC 1/32	FC	Cisco 5548 B	FC 1/32

EMC VNX5400 Deployment: Part 1

Initial configuration and implementation of an EMC VNX5400 is covered in detail from the EMC documentation library. This is accessible at <https://mydocs.emc.com/VNX/> and select Install VNX, using the VNX5400 series as the installation type. Installation documentation covers all areas from unpacking VNX storage components, installing in rack, provisioning power requirements, and physical cabling.

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

Figure 4. Cabling Diagram for VNX5400 with 2 DAE



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

VNX Worksheets

With your network administrator, determine the IP addresses and network parameters you plan to use with the storage system, and record the information on the following worksheet. You must have this information to set up and initialize the system. The VNX5400 array is managed through a dedicated LAN port on the Control Station and each storage processor. These ports must share a subnet with the host you use to initialize the system. After initialization, any host on the same network and with a supported browser can manage the system through the management ports. This information can be recorded in the following table.

Table 8. IPv4 Management Port Information

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

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

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

It is possible to more fully configure management IP addresses for the VNX5400 array. The following table lists some of the addresses you can optionally configure.

Table 9. Optional Control Station LAN Settings

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

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

Table 10. Login Information for the Storage System Administrator

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

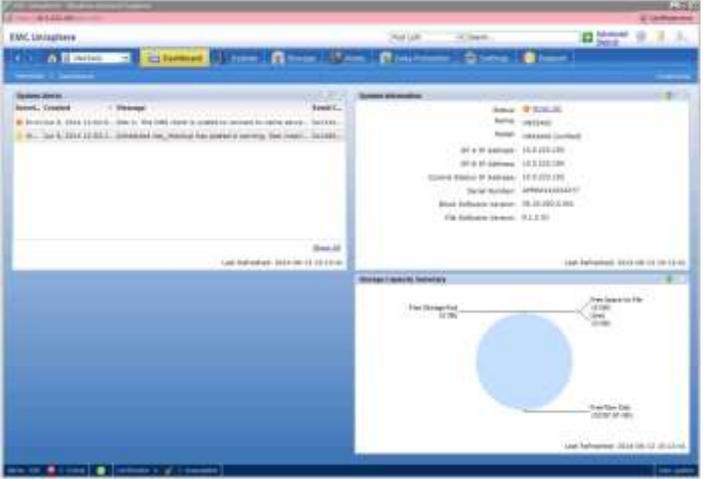
It is also necessary at this time to install the NaviSecCLI command line interface from a supported Windows client environment. The client should have network access to the VNX5400 array for both HTTP/HTTPS access and for remote NaviSecCLI command execution.

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

After array installation, it will also be possible to connect to the VNX5400 array through the Unisphere graphical user interface at the IP address assigned to either SP-A or SP-B, or the control station in the event that a Unified version of the VNX is being implemented.



After entering appropriate login credentials, the Unisphere home page will be presented, providing an overview of the VNX5400 storage array. Summary alerts and errors will be visible as well as full management capabilities for all array features.



The following configuration details assume the VNX5400 array as defined, will be configured with 75 x SAS drives across the DPE and two DAEs. It is also assumed that the array has been configured with IP address assignments to the Control Station and both SP-A and SP-B as previously indicated in Part 1. It is also necessary to have appropriately configured a Windows-based management system with network connectivity to the VNX array that has an appropriate version of the NaviSecCLI software installed.

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

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

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

Creation of Storage Pools

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

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

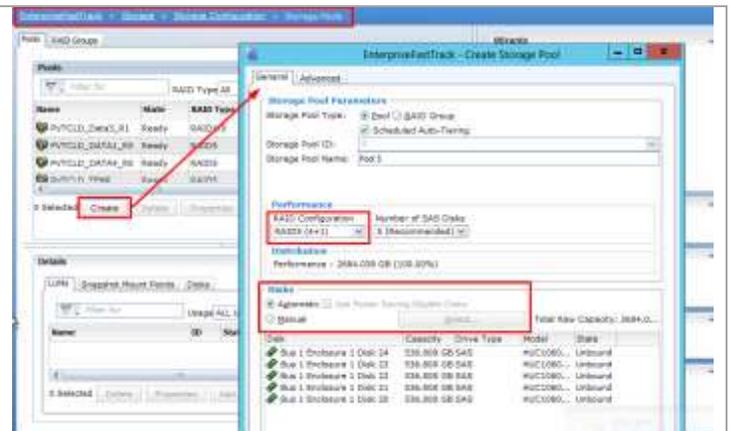
The first command defines the IP address for the array, and should be modified as necessary for the implementation.

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

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

From within the **Storage > Storage Configuration > Storage Pools** menu in Unisphere, select **Create**.

The RAID configuration, desired number of drives and specific drive locations (by choosing Manual) can be selected from the Create Storage Pool menu as outlined in the Figure below.



Create Support for Clone Private LUNs

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

The following example PowerShell can be used to create the RAID Groups and LUNs that will be used to facilitate the clone private LUNs. Make sure that it is modified to reflect the customer environment.

```

#Replace VNX management IP address in the next line
$VNX="10.5.223.128"

#create raid group for clone private LUNs
naviseccli -h $VNX createrg 0 0_0_2 0_0_3

#bind clone private LUNs to raid group 0
Function bindcheck {
    Foreach ($lun in $lunarray)
    {
        $bound = naviseccli -address $vnx getlun $lun -bind
        Foreach ($entry in $bound)
        {
            $newentry = $entry -split ":"
            Foreach ($sentry in $newentry[1])
            {
                $sentry = $sentry.trim()
                $lun
                naviseccli -address $vnx getlun $lun -state
                naviseccli -address $vnx getlun $lun -owner
                write-host $sentry "% bound for lun $lun"
                If ($sentry -ne "100")
                {
                    Start-Sleep 20
                    bindcheck4044
                }
            }
        }
    }
}

naviseccli -h $VNX bind r1 4044 -rg 0 -cap 1 -sp a -sq gb
naviseccli -h $VNX bind r1 4045 -rg 0 -cap 1 -sp b -sq gb
$lunarray = 4044,4045
bindcheck

#add clone private luns
naviseccli -h $VNX clone -allocatcpl -Spa 4044 -Spb 4045 -o
If ($LastEXITCODE -ne 0)
{
    naviseccli -h $VNX clone -allocatcpl -Spa 4044 -Spb 4045 -o
    If ($LASTEXITCODE -EQ 0)
    {
        Write-Host "Retry was successful"
    }
    else
    {
        Write-Host "Retry failed"
    }
}
}

```

Hot Spares in the VNX Array

There is no need to define hot spares on the latest generation of VNX arrays. Failed drives are spared to compatible unbound drives automatically. The VNX series now supports a new hot spare policy where any unbound disk is available for use as a hot spare. The hot spare policy defaults to the EMC recommended best practices for disk type

and capacity, but you can customize the policy to either increase or decrease the ratio of disks that you want to keep unused as hot spares.

The hot spare policy is enforced whenever disks are provisioned, such as when creating RAID Groups, pools, or FAST Cache. If a policy is violated, alerts automatically display in Unisphere or the Command Line Interface (CLI) to identify the disks.

When a drive is used in a sparing function, the particular drive becomes a permanent member of the RAID group. There is no need to rebalance and copy back (equalize) the spare drive to a new drive, thereby reducing the performance load caused by sparing operations.

Cisco Nexus 5548 Deployment: Part 1

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

Before you begin, identify the following information in Table 11.

Table 11. Nexus Management Information

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

Set up Initial Cisco Nexus 5548 Switch

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

Cisco Nexus 5548 A

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

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

- 11) Mgmt0 IPv4 netmask: <**Nexus A mgmt0 netmask**> Enter.
- 12) Configure the default gateway? (yes/no) [y]: Enter.
- 13) IPv4 address of the default gateway: <**Nexus A mgmt0 gateway**> Enter.
- 14) Enable the telnet service? (yes/no) [n]: Enter.
- 15) Enable the ssh service? (yes/no) [y]: Enter.
- 16) Type of ssh key you would like to generate (dsa/rsa):rsa.
- 17) Number of key bits <768–2048> :**1024** Enter.
- 18) Configure the ntp server? (yes/no) [y]: Enter.
- 19) NTP server IPv4 address: <**NTP Server IP**> Enter.
- 20) Enter basic FC configurations (yes/no) [n]: Enter.
- 21) Would you like to edit the configuration? (yes/no) [n]: Enter.
- 22) Be sure to review the configuration summary before enabling it.
- 23) Use this configuration and save it? (yes/no) [y]: Enter.
- 24) Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
- 25) Log in as user admin with the password previously entered.

Cisco Nexus 5548 B

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

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

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

Enable Appropriate Cisco Nexus Features

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

Cisco Nexus A and Nexus B

```
config t
feature lacp
feature fcoe
feature npiv
feature vpc
feature fport-channel-trunk
feature interface-vlan
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
copy run start
```

Configure Fibre Channel Ports

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

Cisco Nexus A and Nexus B

```
slot 1
port 29-32 type fc
copy run start
reload
```

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

Create Necessary VLANs

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

Nexus A and Nexus B

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

```
config t
vlan <MGMT VLAN ID>
  name Mgmt
  exit
vlan <CSV VLAN ID>
  name CSV
  exit
vlan <Live Migration VLAN ID>
  name LiveMigration
  exit
vlan <ClusComm VLAN ID>
  name ClusComm
  exit
vlan <VMaccess VLAN ID>
  name VMaccess
  exit
vlan <VEM VLAN ID>
  name VEM
  exit
copy run start
```

Add Individual Port Descriptions for Troubleshooting

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

Cisco Nexus 5548 A

```
interface Eth1/1
  description <Nexus B:Eth1/1>
  exit
interface Eth1/2
  description <Nexus B:Eth1/2>
  exit
interface Eth1/17
  description <UCSM A:Eth1/17>
  exit
interface Eth1/18
  description <UCSM B:Eth1/17>
  exit
copy run start
```

Cisco Nexus 5548 B

```
interface Eth1/1
  description <Nexus A:Eth1/1>
  exit
interface Eth1/2
  description <Nexus A:Eth1/2>
  exit
interface Eth1/17
  description <UCSM B:Eth1/18>
  exit
interface Eth1/18
  description <UCSM A:Eth1/18>
  exit
copy run start
```

Create Necessary Port Channels

These steps provide details for creating the necessary PortChannels between devices.

Cisco Nexus 5548 A

```
interface Po10
  description vPC Peer-Link
  exit
interface Eth1/1-2
  channel-group 10 mode active
  no shutdown
  exit
interface Po201
  description <PvtCld-UCS-A>
  exit
interface Eth1/17
  channel-group 201 mode active
  no shutdown
  exit
interface Po202
  description <PvtCld-UCS-B>
  exit
  interface Eth1/18
channel-group 202 mode active
  no shutdown
  exit
copy run start
```

Cisco Nexus 5548 B

```
interface Po10
  description vPC Peer-Link
  exit
interface Eth1/1-2
  channel-group 10 mode active
  no shutdown
  exit
interface Po201
  description <PvtCld-UCS-B>
  exit
interface Eth1/17
  channel-group 201 mode active
  no shutdown
  exit
interface Po202
  description <PvtCld-UCS-A>
  exit
interface Eth1/18
  channel-group 202 mode active
  no shutdown
  exit
copy run start
```

Add PortChannel Configurations

These steps provide details for adding PortChannel configurations.

Cisco Nexus 5548 A

```
interface Po10
  switchport mode trunk
  switchport trunk native vlan <Native VLAN ID>
  switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type network
  no shutdown
  exit
interface Po201
  switchport mode trunk
  switchport trunk native vlan <MGMT VLAN ID>
  switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type edge trunk
  no shut
  exit
interface Po202
  switchport mode trunk
  switchport trunk native vlan <MGMT VLAN ID>
  switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type edge trunk
  no shut
  exit
copy run star
```

Cisco Nexus 5548 B

```
interface Po10
  switchport mode trunk
  switchport trunk native vlan <Native VLAN ID>
  switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type network
  no shutdown
  exit
interface Po201
  switchport mode trunk
  switchport trunk native vlan <MGMT VLAN ID>
  switchport trunk allowed vlan MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type edge trunk
  no shut
  exit
interface Po202
  switchport mode trunk
  switchport trunk native vlan <MGMT VLAN ID>
  switchport trunk allowed vlan MGMT VLAN ID, CSV VLAN ID, LiveMigration VLAN ID, ClusComm VLAN
ID, VMaccess VLAN ID, VEM VLAN ID >
  spanning-tree port type edge trunk
  no shut
  exit
copy run start
```

Configure Virtual PortChannels

These steps provide details for configuring virtual PortChannels (vPCs)

Cisco Nexus 5548 A

```
vpc domain <Nexus vPC domain ID>
  role priority 10
  peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0 IP>
  exit
interface Po10
  vpc peer-link
  exit
interface Po201
  vpc 201
  exit
interface Po202
  vpc 202
  exit
copy run start
```

Cisco Nexus 5548 B

```
vpc domain <Nexus vPC domain ID>
  role priority 20
  peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0 IP>
  exit
interface Po10
  vpc peer-link
  exit
interface Po201
  vpc 201
  exit
interface Po202
  vpc 202
  exit
copy run start
```

Configure Fibre Channel Ports

Nexus A and Nexus B

```
interface fcl/29
  switchport trunk mode off
  no shutdown
  exit
interface fcl/30
  switchport trunk mode off
  no shutdown
  exit
interface fcl/31
  switchport trunk mode off
  no shutdown
  exit
interface fcl/32
  switchport trunk mode off
  no shutdown
  exit
copy run start
```

Link into Existing Network Infrastructure

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

Configure Cisco Unified Computing System Fabric Interconnects

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

Before you begin, identify the following information in Table 12.

Table 12. Cisco UCS Manager Configuration Information

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

Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects

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

Cisco UCS 6248 A

- 1) Connect to the console port on the first Cisco UCS 6248 fabric interconnect.
- 2) At the prompt to enter the configuration method, enter **console** to continue.

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

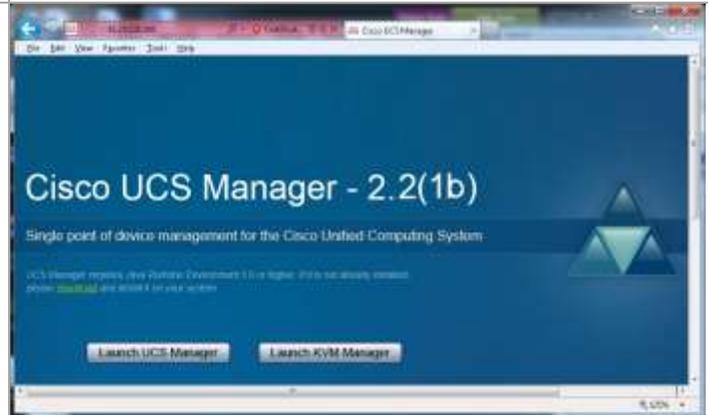
Open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.

You will see a web page complaining about the website's security certificate. Click **Continue to this website (not recommended)**.

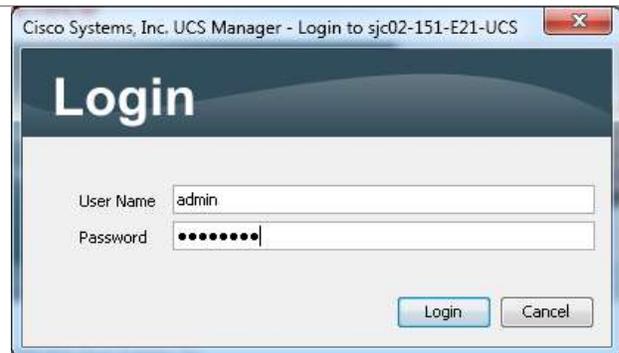


Select the **Launch UCS Manager** link to download the Cisco UCS Manager software.

If prompted to accept security certificates, accept as necessary.



When prompted, enter admin for the username and enter the administrative password and click Login to log in to the Cisco UCS Manager software.

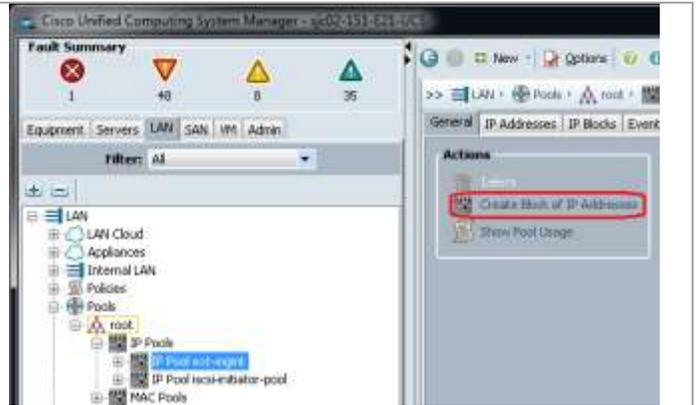


Add a Block of IP Addresses for KVM Access

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

Cisco UCS Manager

Select the **LAN** tab at the top of the left window.
Select **Pools > root > IP Pools > IP Pool ext-mgmt**.
Select **Create Block of IP Addresses**.



Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.

Click **OK** to create the IP block.

Click **OK** in the message box

Note: This block of addresses must be on the same subnet as the management addresses assigned to the UCS Manager.



Cisco UCS PowerTool

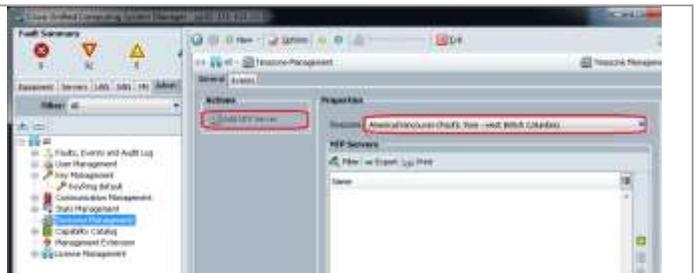
```
Get-UcsOrg -Level root | Get-UcsIpPool -Name "ext-mgmt" -LimitScope | Add-UcsIpPoolBlock -DefGw "10.5.177.1" -From "10.5.177.200" -To "10.5.177.209"
```

Synchronize Cisco UCS to NTP

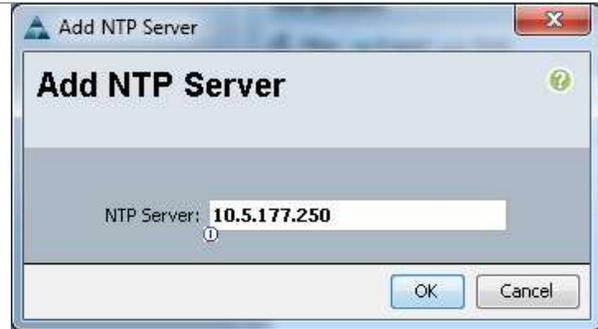
These steps provide details for synchronizing the Cisco UCS environment to the NTP server.

Cisco UCS Manager

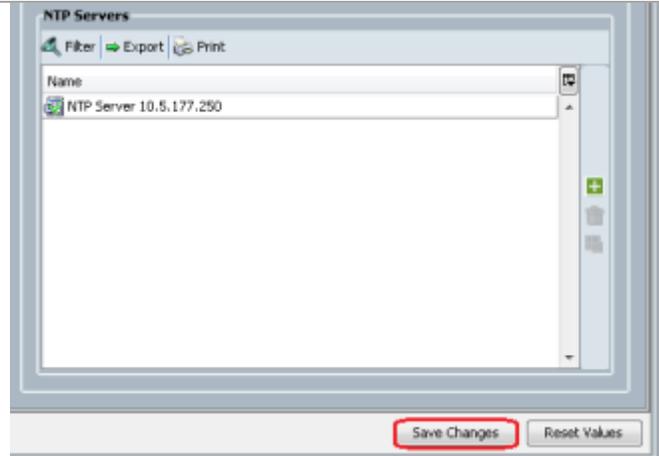
Select the **Admin** tab at the top of the left window.
Select **All > Timezone Management**.
In the right pane, select the appropriate timezone in the **Timezone** drop-down menu.
Click **Add NTP Server**.



Input the NTP server IP and click **OK**.



Click **Save Changes** and then **OK**.



Edit the Chassis Discovery Policy

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

Cisco UCS Manager

Navigate to the **Equipment** tab in the left pane.

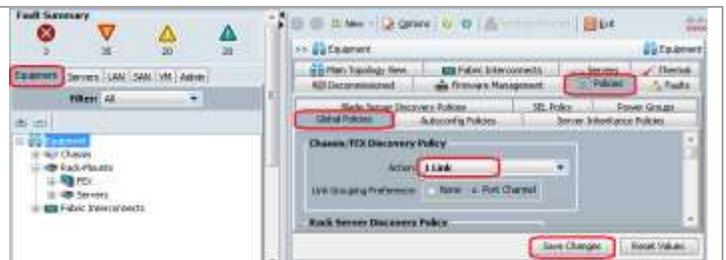
In the right pane, click the **Policies** tab.

Under Global Policies, set the Chassis Discovery Policy to **1 Link**.

Select the **Port Channel** radio button for the Link Grouping Preference.

Click **Save Changes** in the bottom right corner.

Note: Setting this policy to 1 Link helps Make sure valid discovery of any configuration. In a later step when the chassis is re-acked, all valid links will be discovered and activated.



Cisco UCS PowerTool

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

Enable Server and Uplink Ports

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

Cisco UCS Manager

Select the **Equipment** tab on the top left of the window.

Select **Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module**.

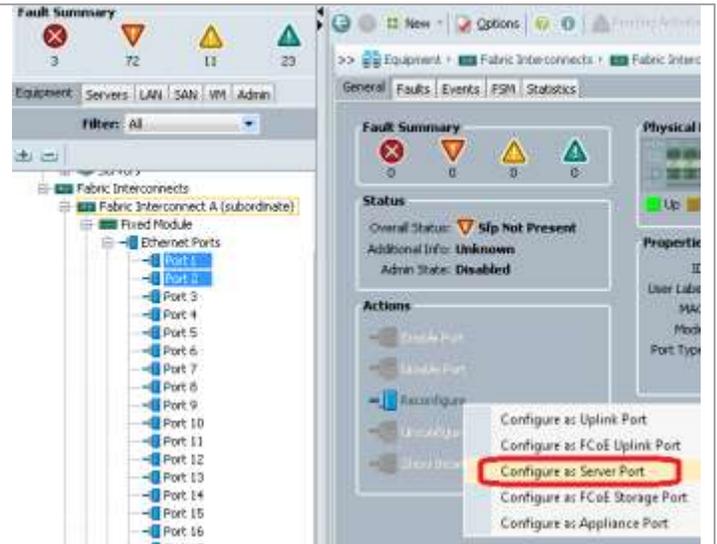
Expand the **Unconfigured Ethernet Ports** section.

Select the ports that are connected to the Cisco UCS chassis (2 per chassis).

Click **Reconfigure**, then select **Configure as Server Port** from the drop-down menu.

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

Repeat for Fabric Interconnect B.



Continue working on Fabric Interconnect B.

Select ports 17 and 18 that are connected to the Cisco Nexus 5548 switches.

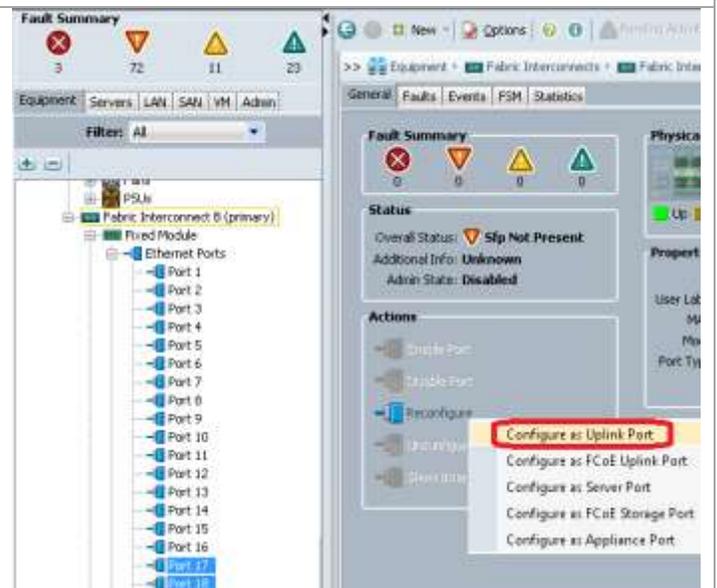
Click **Reconfigure**, then select **Configure as Uplink Port** from the drop-down menu.

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

Switch back to working on Fabric Interconnect A.

Repeat for Fabric Interconnect A.

Note: After a port is configured, you can select the port and select the option to Show Interface. This allows you to add a description, if you so desire.



Cisco UCS PowerTool

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

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

Configure Unified Ports for Fibre Channel

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

Note: Modification of the unified ports on the built-in ports leads to a reboot of the Fabric Interconnect being modified. This reboot can take up to 10 minutes. Modification of the unified ports on an expansion module only takes a few seconds and does not cause the loss of connectivity to UCS Manager. This CVD assumes no expansion module.

Cisco UCS Manager

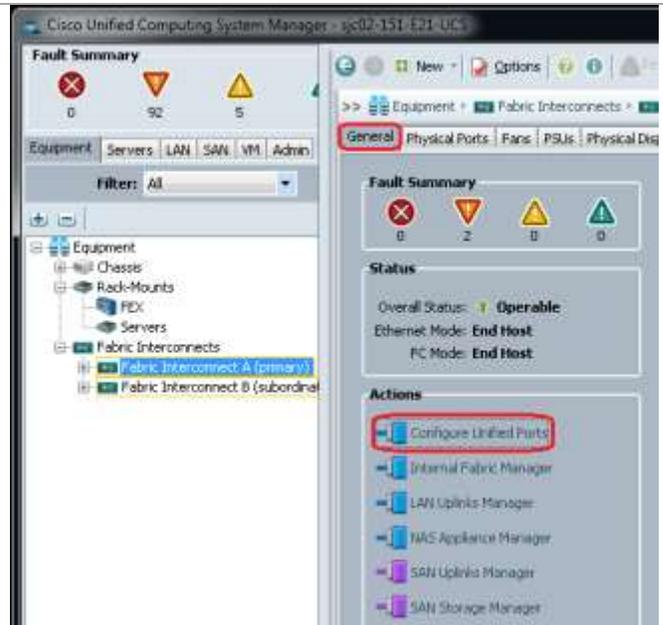
Navigate to the **Equipment** tab in the left pane.

Select **Fabric Interconnect A**.

In the right pane, click the **General** tab.

Select **Configure Unified Ports**.

Select **Yes** to launch the wizard.



Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports. Ports 31 and 32 now have the “B” indicator indicating their reconfiguration as FC uplink ports.

Click **Finish**, then click **OK**.

The Cisco UCSM GUI will close as the primary fabric interconnect reboots. Upon successful reboot, open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.

When prompted, enter `admin` for the username and enter the administrative password and click **Login** to log in to the Cisco UCS Manager software.

Repeat the above steps for Fabric B.

Navigate to the **Equipment** tab in the left pane.

Select **Fabric Interconnect B**.

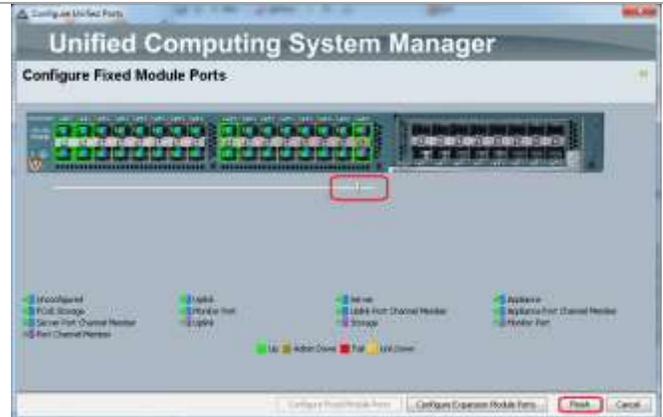
In the right pane, click the **General** tab.

Select **Configure Unified Ports**.

Select **Yes** to launch the wizard.

Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports. Ports 31 and 32 now have the “B” indicator indicating their reconfiguration as FC uplink ports.

Click **Finish**, then click **OK**.



Cisco UCS PowerTool

```
Connect to Fabric Interconnect A, Connect-UCS <FQDN or IP>
Start-UcsTransaction
Get-UcsFabricSanCloud -Id "A" | Add-UcsFcUplinkPort -SlotId 1 -PortId 32 -AdminState "enabled"
-ModifyPresent
Get-UcsFabricSanCloud -Id "A" | Add-UcsFcUplinkPort -SlotId 1 -PortId 31 -AdminState "enabled"
-ModifyPresent
Complete-UcsTransaction
#This causes the Fabric Interconnect A to reboot. Upon successful reboot
Connect-Ucs <FQDN or IP>.
#Repeat the above transaction on Fabric B
#Upon successful reboot
Connect-Ucs <FQDN or IP>
```

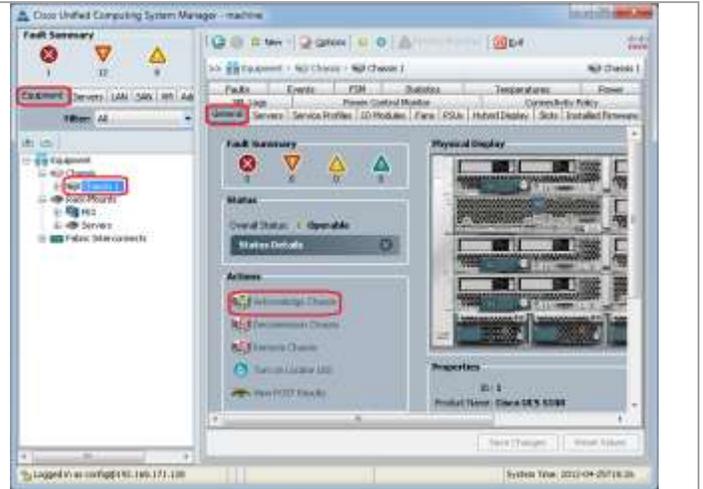
Acknowledge the Cisco UCS Chassis

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

Cisco UCS Manager

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

Click **Acknowledge Chassis**.



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

Cisco UCS PowerTool

```
Get-UcsChassis -Id 1 | Set-UcsChassis -AdminState "re-acknowledge"
```

Create Uplink PortChannels to the Cisco Nexus 5548 Switches

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

Cisco UCS Manager

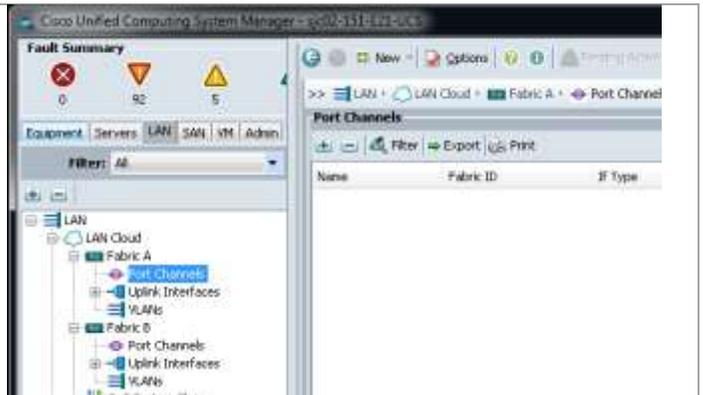
Select the **LAN** tab on the left of the window.

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

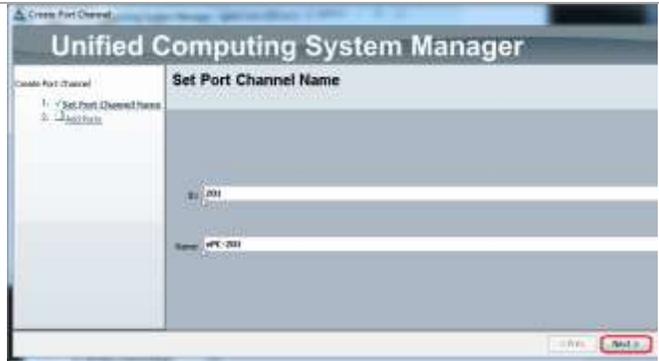
Under **LAN Cloud**, expand the **Fabric A** tree.

Right-click **Port Channels**.

Select **Create Port Channel**.



Enter 201 as the unique **ID** of the PortChannel.
 Enter vPC-201 as the **Name** of the PortChannel.
 Click **Next**.



Select the port with slot ID 1 and port 17 and also the port with slot ID 1 and port 18 to be added to the PortChannel.

Click >> to add the ports to the PortChannel.

Click **Finish** to create the PortChannel.

Right-click the newly created port channel and select **Show navigator**



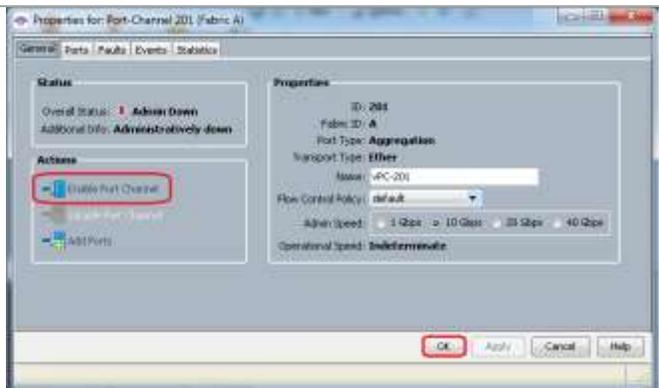
Under Actions, select **Enable Port Channel**.

In the pop-up box, click **Yes**, then **OK** to enable.

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

Click **OK** to close the Navigator.

Repeat for Fabric B using 202 as the unique ID of the Port Channel and vPC-202 as the name.



Cisco UCS PowerTool

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

Configure Service Profiles

Create an Organization (Optional)

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

This document assumes no use of an organization. If the organization is implemented, you must remember the search order Cisco UCS employs when searching for components. For example, when creating a template in a sub-organization, Cisco UCS will search first in the sub-organization to resolve a reference. If it does not find the reference there, it will search up through its parent tree, ending at root. A sub-organization cannot resolve a reference to an item that exists in a different peer sub-organization or child sub-organization.

Cisco UCS Manager

From the **New...** menu at the top of the window, select **Create Organization**



Enter a name for the organization.
Enter a description for the organization (optional).
Click **OK**.
In the message box that displays, click **OK**.



Cisco UCS PowerTool

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

Create a MAC Address Pool

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

Cisco UCS Manager

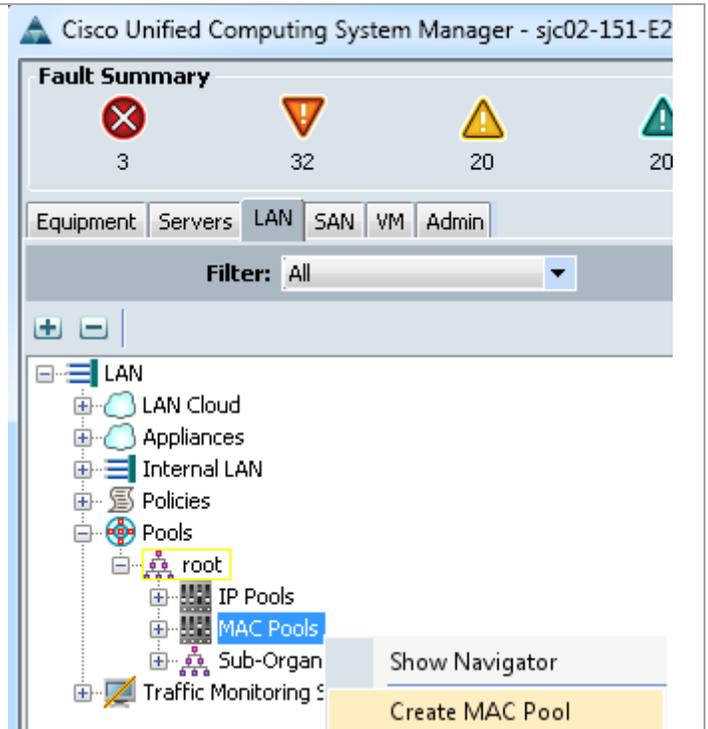
Select the **LAN** tab on the left of the window.

Select **Pools > root**.

Right-click **MAC Pools** under the FastTrack4 organization.

Select **Create MAC Pool** to create the MAC address pool.

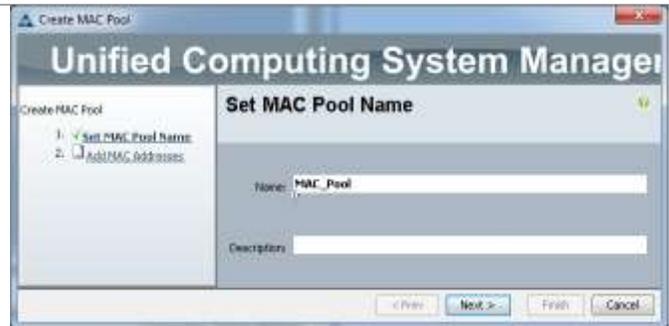
Note: Depending on the desired configuration of MAC addresses, you can create multiple pools.



Enter `<MAC_Pool>` for the name of the MAC pool.

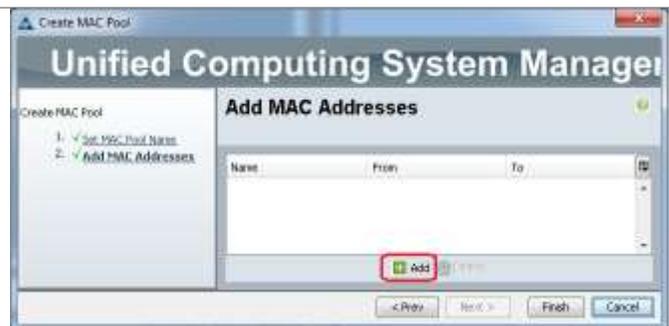
(Optional) Enter a description of the MAC pool.

Note: You may want to consider creating different MAC pools for each vNIC template. This can facilitate management of NICs based upon MAC ranges.



Click **Next**.

Click **Add**.

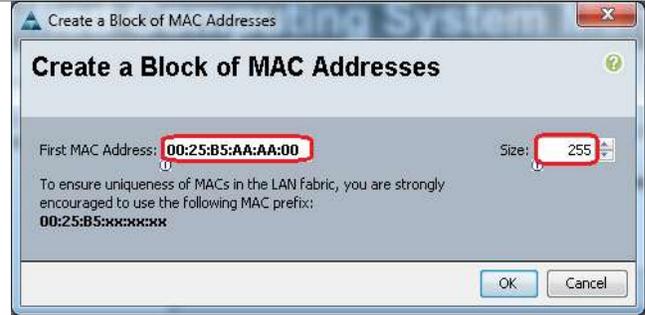


Specify a starting MAC address.

Specify a size of the MAC address pool sufficient to support the available blade resources.

Click **OK**, then click **Finish**.

In the message box that displays, click **OK**.



Cisco UCS PowerTool

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

Create WWNN Pools

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

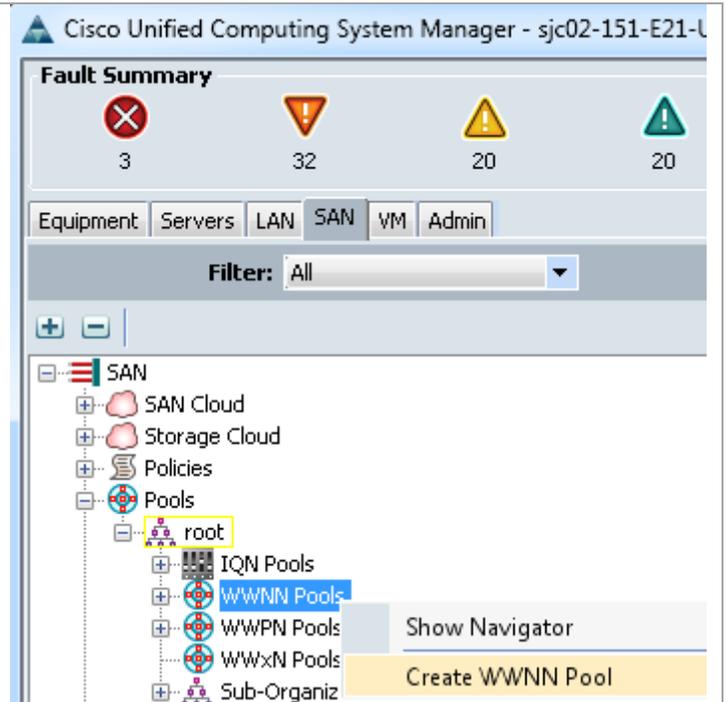
Cisco UCS Manager

Select the **SAN** tab at the top left of the window.

Select **Pools > root**.

Right-click **WWNN Pools**

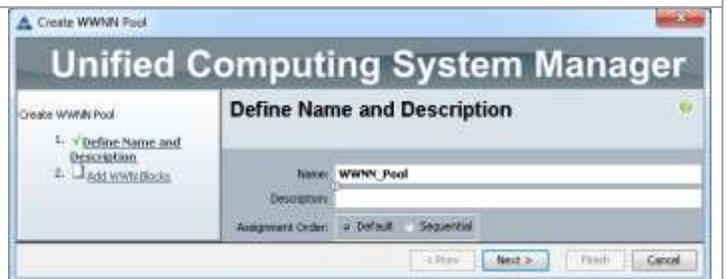
Select **Create WWNN Pool**.



Enter *<WWNN_Pool>* as the Name of the WWNN pool.

(Optional) Add a description for the WWNN pool.

Click **Next** to continue.



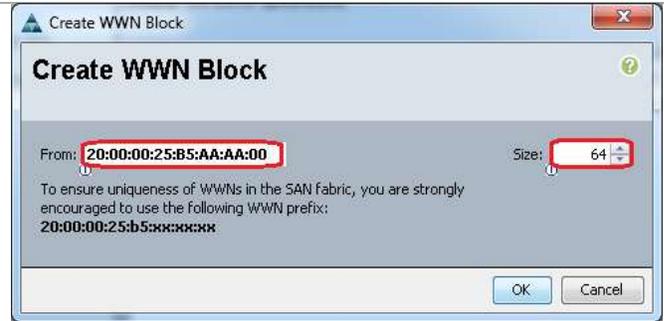
Click **Add** to add a block of WWNN's.

The default is fine, modify if necessary.

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

Click **OK**, then click **Finish** to proceed.

Click **OK** to finish.



Cisco UCS PowerTool

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

Create WWPN Pools

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

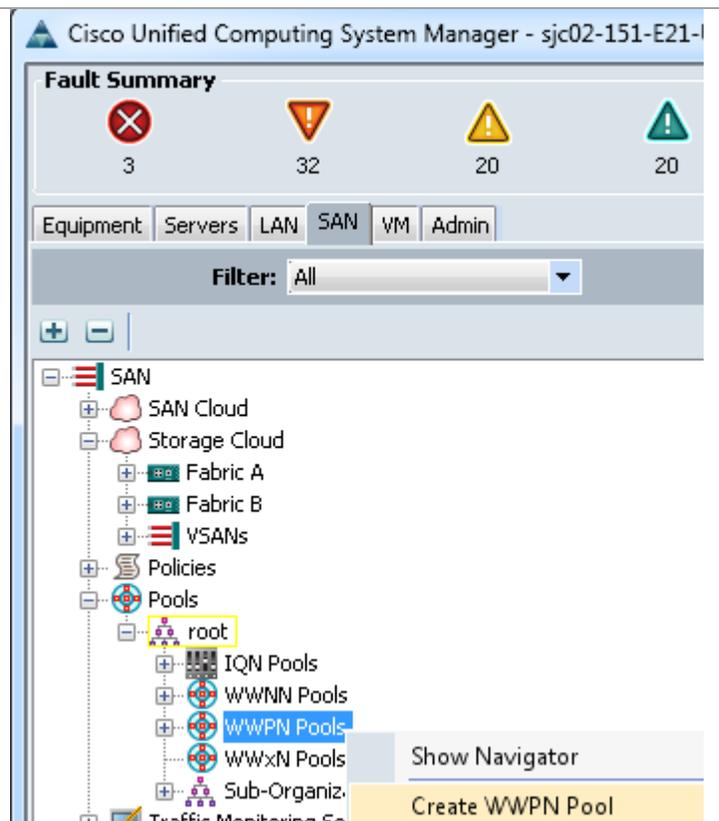
Cisco UCS Manager

Select the **SAN** tab at the top left of the window.

Select **Pools > root**.

Right-click **WWPN Pools**

Select **Create WWPN Pool**.



Enter <WWPN_Pool_A> as the Name for the WWPN pool for fabric A.

(Optional). Give the WWPN pool a description.

Click **Next**.



Click **Add** to add a block of WWPNs.

Enter the starting WWPN in the From block for fabric A.

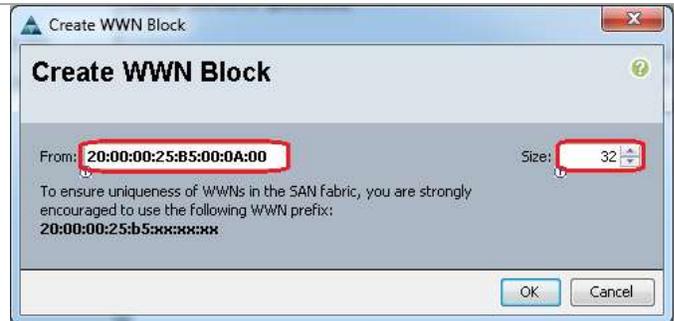
Specify a Size of the WWPN block sufficient to support the available blade resources.

Click **OK**.

Click **Finish** to create the WWPN pool.

Click **OK**.

(Optional, but recommended) Repeat the above steps to create a pool for the B fabric.



Cisco UCS PowerTool

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

Create UUID Suffix Pools

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

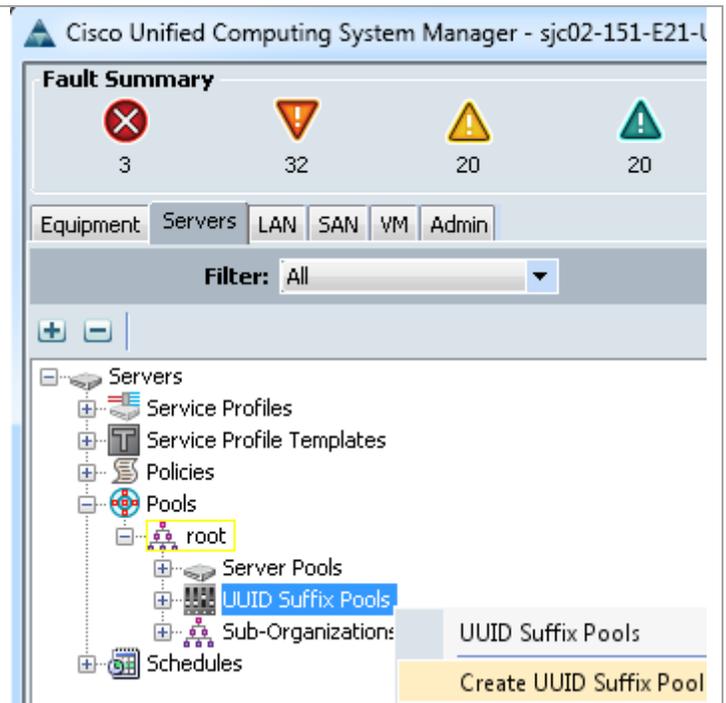
Cisco UCS Manager

Select the **Servers** tab on the top left of the window.

Select **Pools > root**.

Right-click **UUID Suffix Pools**

Select **Create UUID Suffix Pool**.

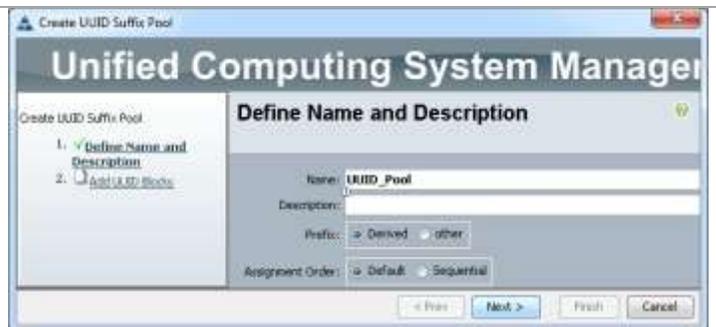


Name the UUID suffix pool <UUID_Pool>.

(Optional) Give the UUID suffix pool a description.

Leave the prefix at the derived option.

Click **Next** to continue.



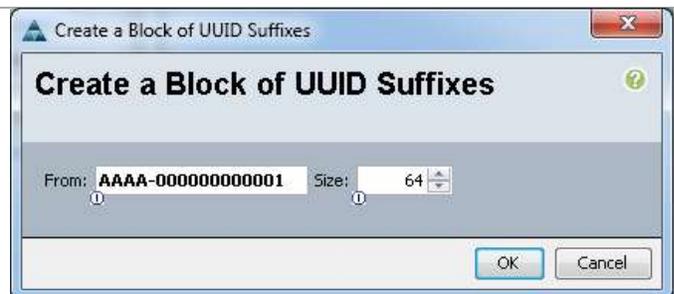
Click **Add** to add a block of UUID's

The **From** field is fine at the default setting, or you can create a hexadecimal string that is unique for your environment.

Specify a **Size** of the UUID block sufficient to support the available blade resources.

Click **OK**, then click **Finish** to proceed.

Click **OK** to finish.



Cisco UCS PowerTool

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

Create Server Pools

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

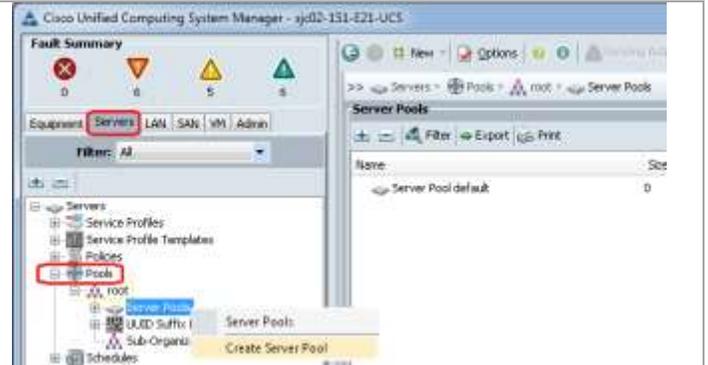
Cisco UCS Manager

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

Select **Pools > root**.

Right-click **Server Pools**.

Select **Create Server Pool**.



Name the server pool <PvtCld-Pool>.

(Optional) Give the server pool a description.

Click **Next** to continue to add servers.

Select the **B200 servers** to be added to the PvtCld-Pool server pool. Click >> to add them to the pool.

Click **Finish**, then select **OK** to finish.



Cisco UCS PowerTool

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

Create VLANs

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

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

Cisco UCS Manager

<p>Select the LAN tab on the left of the window.</p> <p>Select LAN Cloud.</p> <p>Right-click VLANs.</p> <p>Select Create VLANs.</p>	
<p>Enter <Mgmt> as the name of the VLAN to be used for management traffic.</p> <p>Keep the Common/Global option selected for the scope of the VLAN.</p> <p>Enter the <Mgmt VLAN ID> for the management VLAN. Keep the sharing type as none.</p> <p>Click OK.</p>	
<p>Repeat above steps to create the CSV, ClusComm, Live Migration, VEM, and VMaccess VLANs.</p>	

Cisco UCS PowerTool

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

Create Host Firmware Package Policy

These steps provide details for creating a firmware management policy for a given server configuration in the Cisco UCS environment. Firmware management policies allow the administrator to select the corresponding packages for

a given server configuration. These often include adapter, BIOS, board controller, FC adapters, HBA option ROM, and storage controller properties.

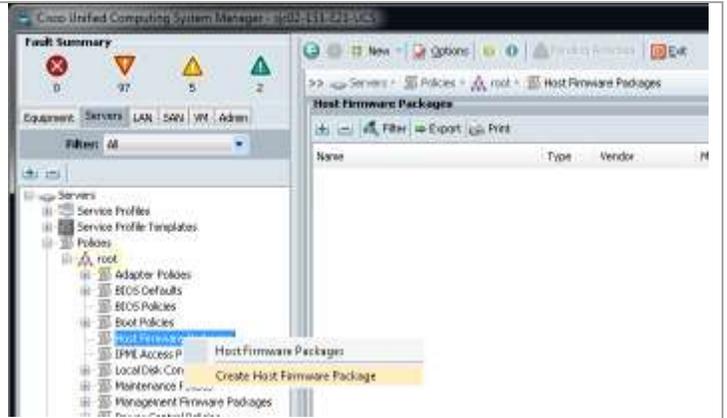
Cisco UCS Manager

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

Select **Policies > root**.

Right-click **Host Firmware Packages**.

Select **Create Host Firmware Package**.



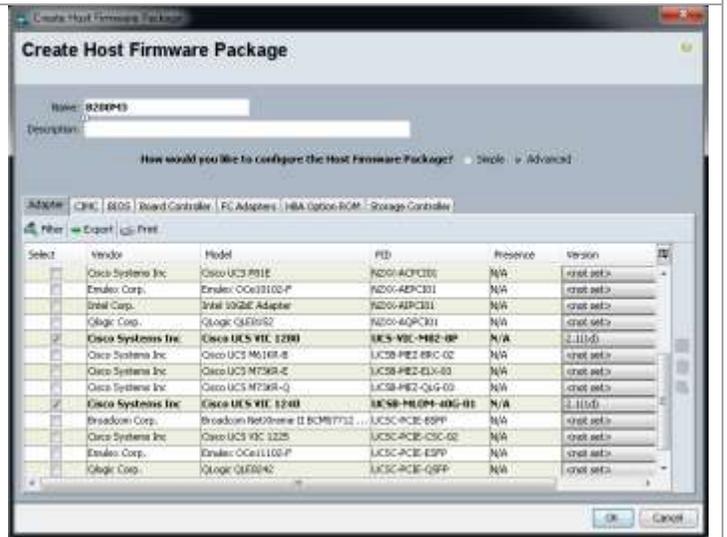
Enter the name of the host firmware package for the corresponding server configuration.

Select the radio button for **Advanced** configuration.

Navigate the tabs of the Create Host Firmware Package Navigator and select the appropriate packages and versions for the server configuration.

Click **OK** to complete creating the host firmware package.

Click **OK**.



Enable Quality of Service in Cisco UCS Fabric

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

Cisco UCS Manager

Select the **LAN** tab at the top left of the window.

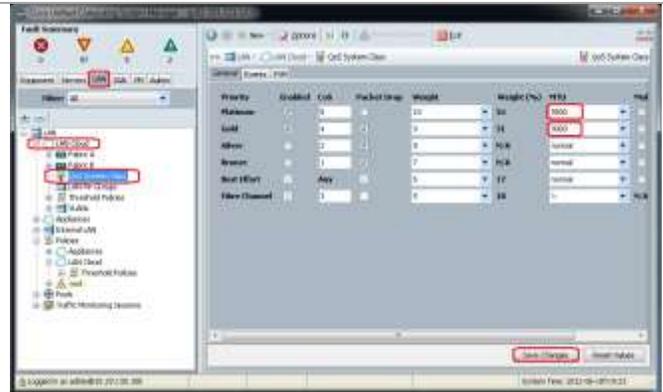
Go to **LAN Cloud > QoS System Class**.

In the right pane, click the **General** tab

On the Platinum, Gold, and Best Effort rows, type **9000** in the MTU boxes.

Click **Save Changes** in the bottom right corner.

Click **OK** to continue.

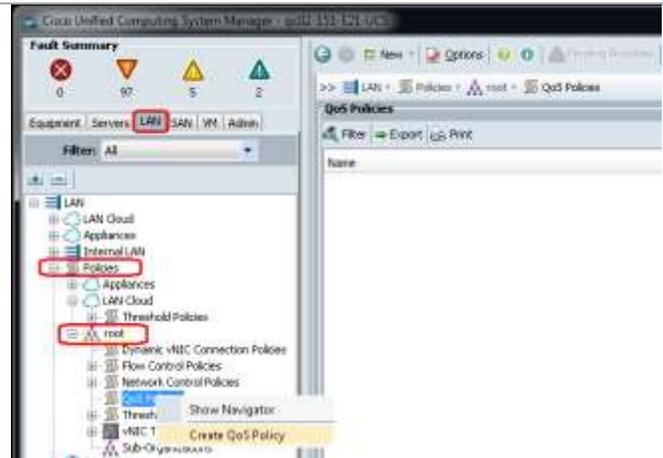


Select the **LAN** tab on the left of the window.

Go to **LAN > Policies > Root >**

Right-click **QoS Policies**.

Select **Create QoS Policy**.



Enter <LiveMigration> as the QoS Policy name.

Change the Priority to Platinum. Leave Burst (Bytes) set to **10240**. Leave Rate (Kbps) set to **line-rate**.

Leave Host Control set to **None**.

Click **OK** twice to complete.



Repeat to create a QoS policy for CSV.

Right-click **QoS Policies**.

Select **Create QoS Policy**.

Enter <CSV> as the QoS Policy **name**.

Change the Priority to Gold. Leave Burst (Bytes) set to **10240**. Leave Rate (Kbps) set to **line-rate**. Leave Host Control set to **None**.

Click **OK** twice to complete.

```
Set-UcsQosClass -QosClass (Get-UcsQosClass -Priority gold) -AdminState enabled -Mtu 9000 -Force
Set-UcsQosClass -QosClass (Get-UcsQosClass -Priority platinum) -AdminState enabled -Mtu 9000 -
Force
$var = Add-UcsQosPolicy -Name "LiveMigration"
$var | Get-UcsVnicEgressPolicy | Set-UcsVnicEgressPolicy -Prio platinum -Force
$var = Add-UcsQosPolicy -Name "CSV"
$var | Get-UcsVnicEgressPolicy | Set-UcsVnicEgressPolicy -Prio gold -Force
```

Create a Power Control Policy

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

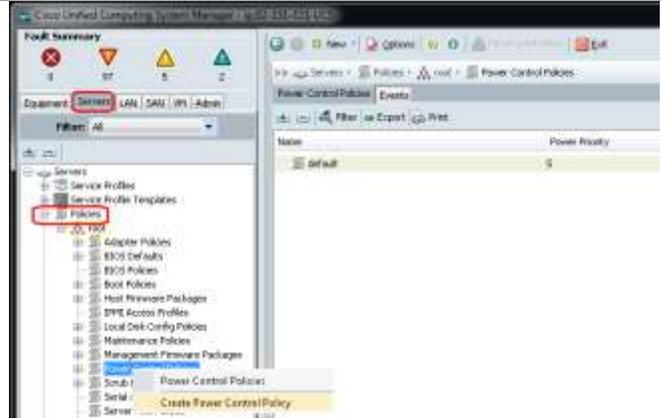
Cisco UCS Manager

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

Go to **Policies > root**.

Right-click **Power Controller Policies**.

Select **Create Power Control Policy**

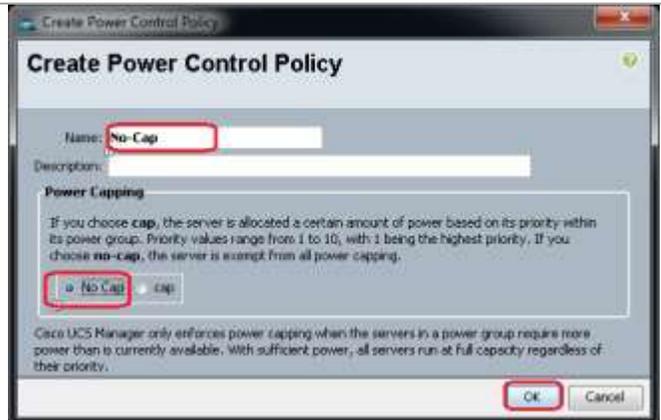


Enter <No-Cap> as the power control policy **Name**.

Change the **Power Capping** to **No Cap**.

Click **OK** to complete creating the power control policy.

Click **OK** twice to complete.



Cisco UCS PowerTool

```
Add-UcsPowerPolicy -Name <No-Cap> -Prio "no-cap"
```

Create a Scrub Policy

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

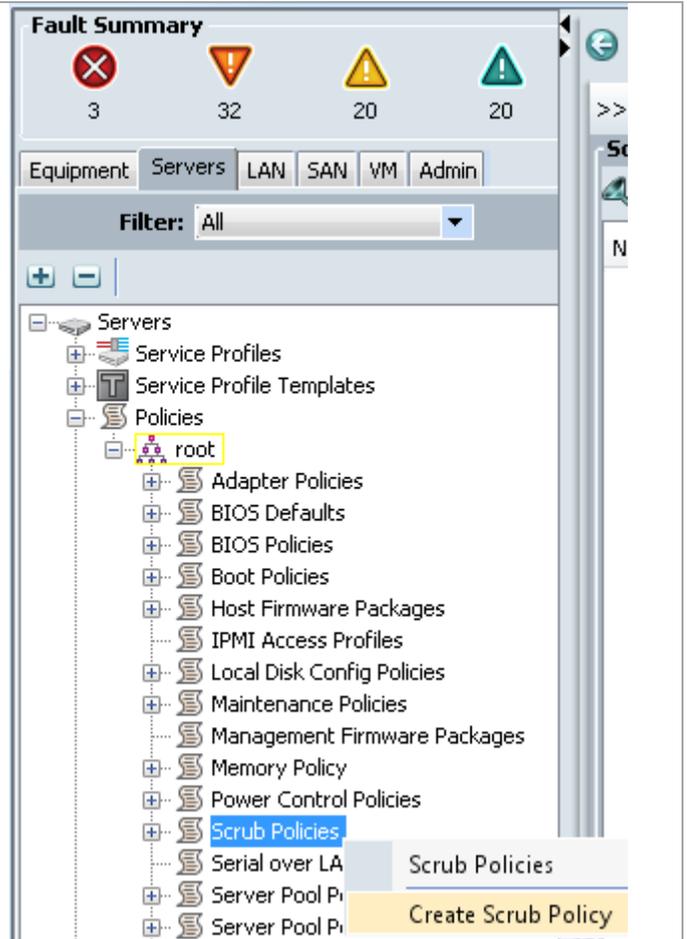
Cisco UCS Manager

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

Go to **Policies > root**.

Right-click **Scrub Policies**.

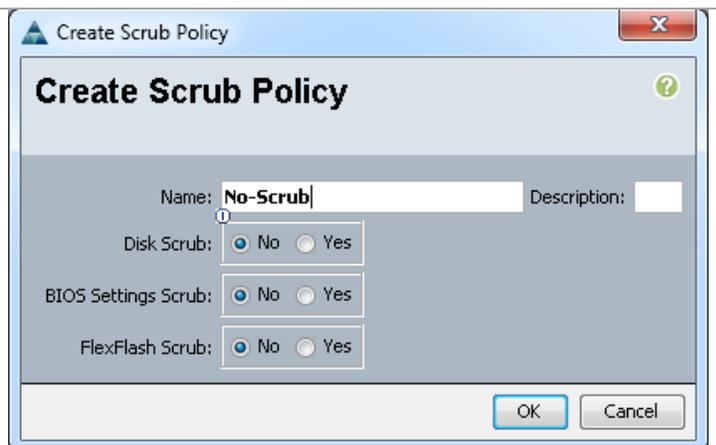
Select **Create Scrub Policy**



Enter <No-Scrub> as the scrub policy **Name**.

Make sure the radio buttons are selecting **No**.

Click **OK** twice to complete.



```
Add-UcsScrubPolicy -BiosSettingsScrub "no" -DiskScrub "no" -FlexFlashScrub "no" -Name "No-Scrub"  
-PolicyOwner "local"
```

Create a Local Disk Configuration Policy

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

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

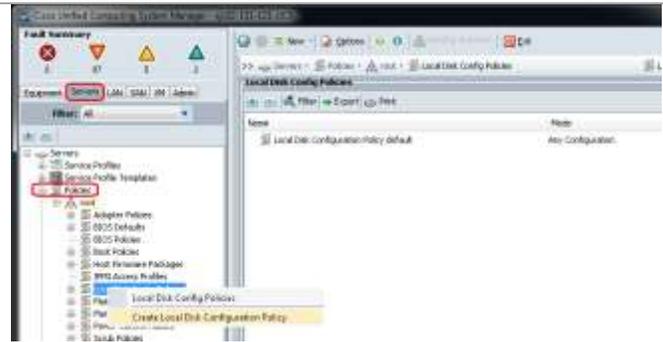
Cisco UCS Manager

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

Go to **Policies > root**.

Right-click **Local Disk Config Policies**.

Select **Create Local Disk Configuration Policy**.

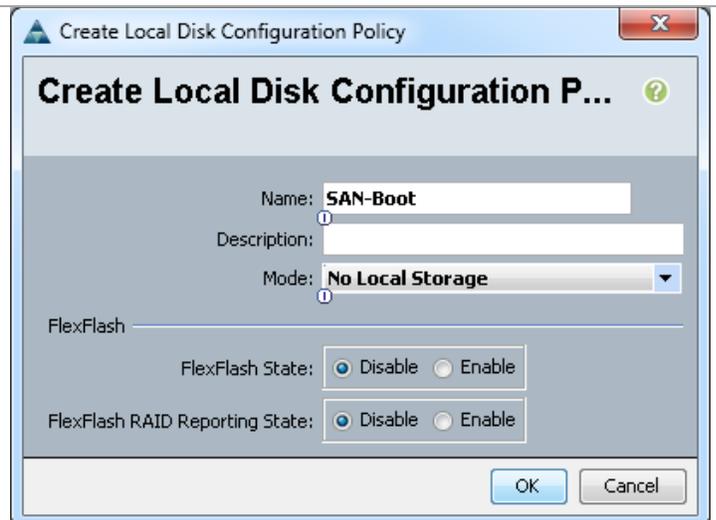


Enter <SAN-Boot> as the local disk configuration policy **Name**.

Change the **Mode** to **No Local Storage**.

Click **OK** to complete creating the local disk configuration policy.

Click **OK**.



Cisco UCS PowerTool

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

Create a Server Pool Qualification Policy

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

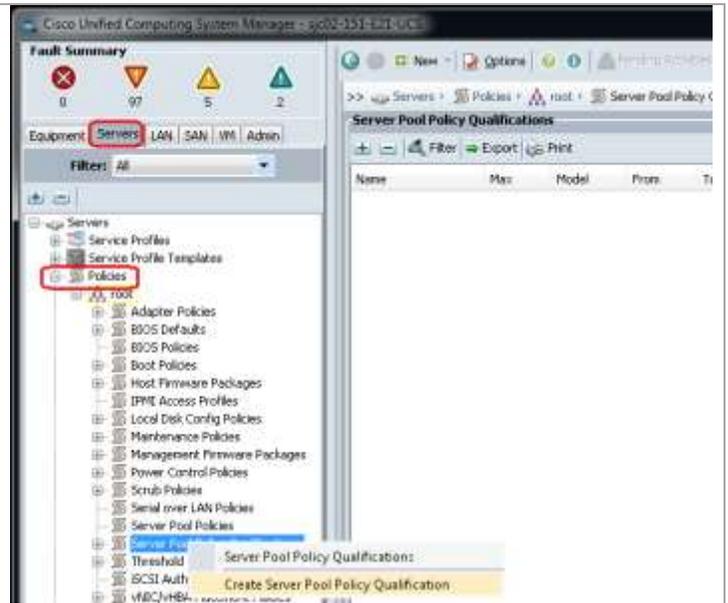
Cisco UCS Manager

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

Go to **Policies > root**.

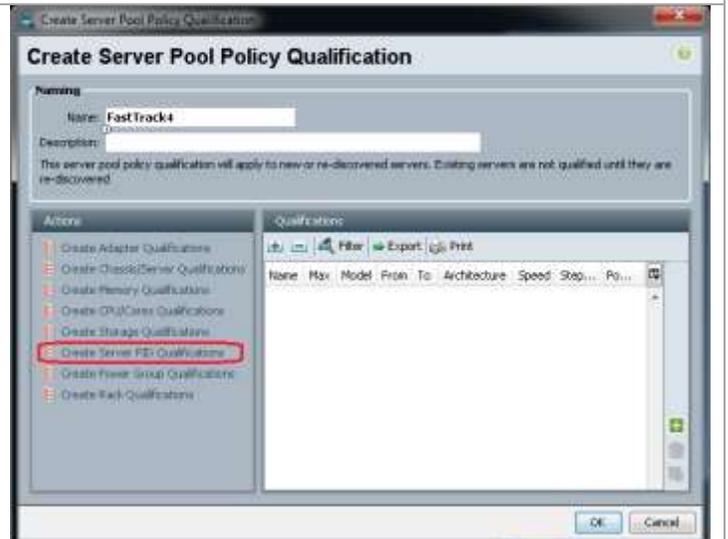
Right-click **Server Pool Policy Qualification**.

Select **Create Server Pool Policy Qualification**.



Enter <FastTrack4> as the **name**.

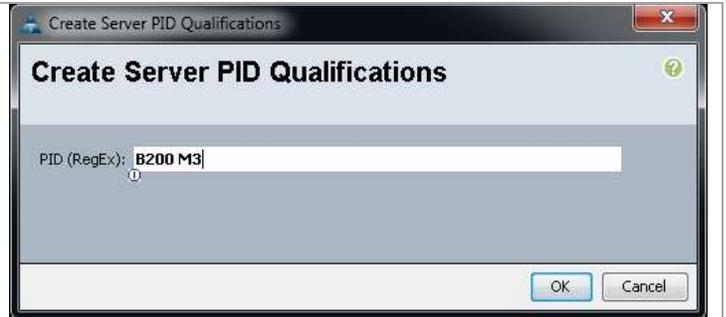
Select **Create Server PID Qualifications**.



Enter **B200 M3** as the **Model (RegEx)**.

Click **OK** to complete creating the server pool qualification policy.

Click **OK**.



Create a Server BIOS Policy

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

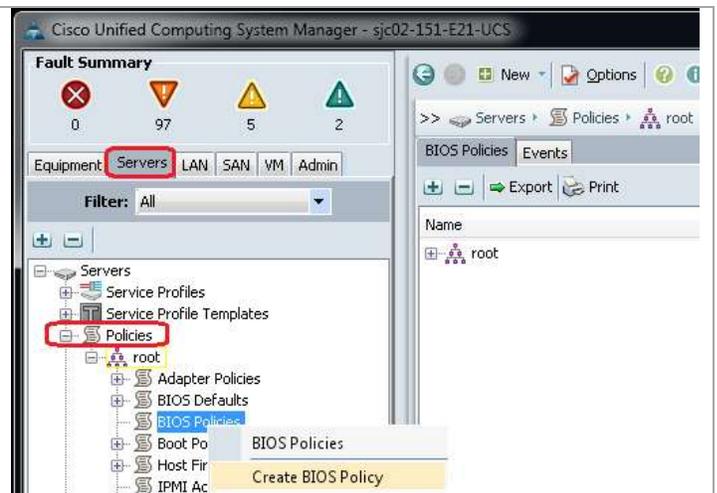
Cisco UCS Manager

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

Go to **Policies > root**.

Right-click **BIOS Policies**.

Select **Create BIOS Policy**.



Enter **<FastTrack4-Host>** as the BIOS policy **Name**.

Change the **Quiet Boot** property to **Disabled**.

Click **Finish** to complete creating the BIOS policy.

Click **OK**.



Cisco UCS PowerTool

```
Add-UcsBiosPolicy -Name <FastTrack4-Host> | Set-UcsBiosVfQuietBoot -VpQuietBoot disabled -Force
```

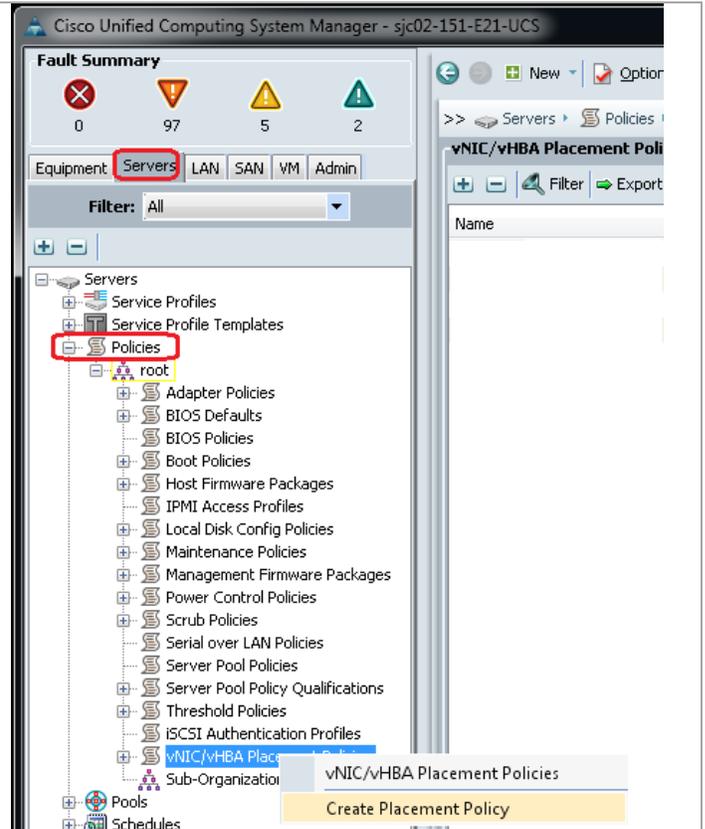
Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts

Cisco UCS Manager

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

Go to **Policies > root**.

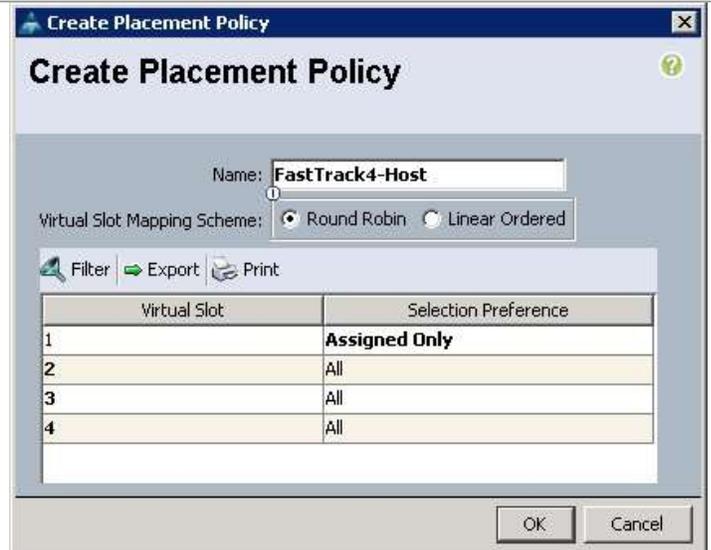
Right-click **vNIC/HBA Placement Policies** and select **Create Placement Policy**.



Enter the **Name** <FastTrack4-Host>.

Click **1** and select **Assigned Only**.

Click **OK**.



Create vNIC Templates

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

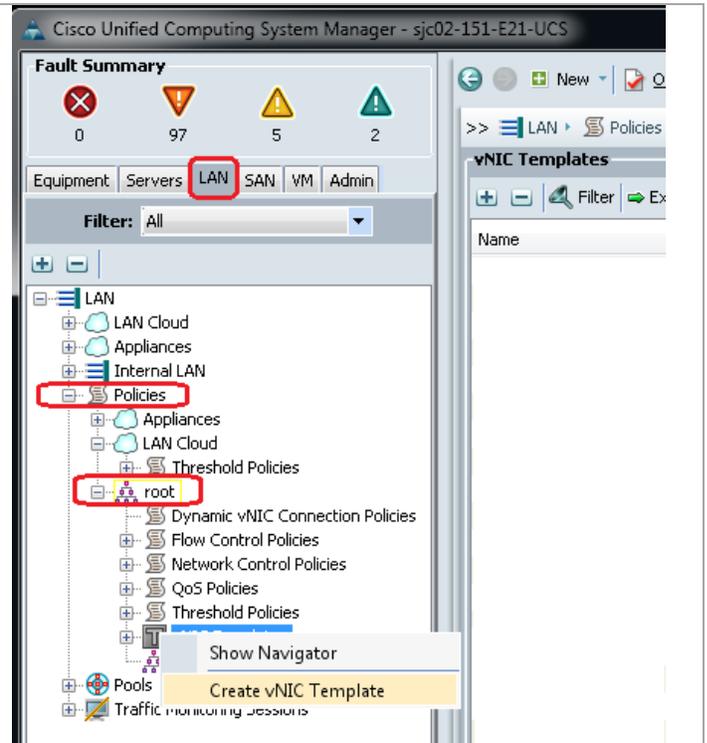
Cisco UCS Manager

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

Go to **Policies > root**.

Right-click **vNIC Templates**.

Select **Create vNIC Template**.



Enter **<CSV>** as the vNIC template **Name**.

Check **Fabric A**.

Check the **Enable Failover** box.

Under target, unselect the **VM** box.

Select **Updating Template** as the Template Type.

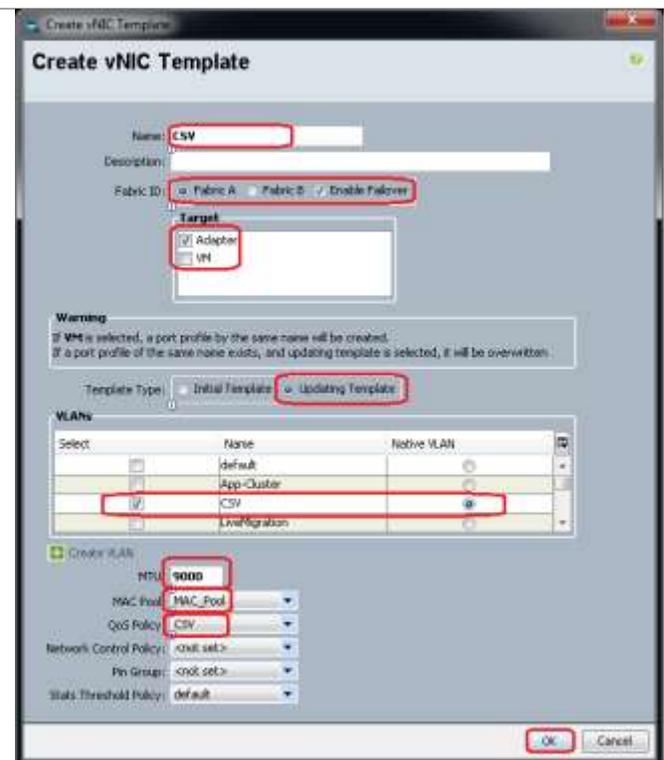
Under VLANs, select **<CSV>**. Set **Native VLAN**.

Under MTU, set to **9000**.

Under MAC Pool, select **<MAC-Pool>**.

For QoS Policy, select **<CSV>**

Click **OK** to complete creating the vNIC template



Right-click **vNIC Templates**.

Select **Create vNIC Template**.

Enter *<LiveMigration>* as the vNIC template **Name**.

Check **Fabric A**.

Make sure the **Enable Failover** box is cleared.

Under target, unselect the **VM** box.

Select **Updating Template** as the Template Type.

Under VLANs, select *<LiveMigration>*. Set **Native VLAN**.

Under MTU, set to **9000**.

Under MAC Pool, select *<MAC-Pool>*.

For QoS Policy, select *<LiveMigration>*.

Click **OK** to complete creating the vNIC template

The screenshot shows the 'Create vNIC Template' dialog box with the following configuration:

- Name: LiveMigration
- Description: (empty)
- Fabric ID: Fabric A
- Enable Failover:
- Target: Adaptm, VM
- Template Type: Initial Template, Updating Template
- VLANs Table:

Select	Name	Native VLAN
<input type="checkbox"/>	CSV	
<input type="checkbox"/>	ClusComm	
<input type="checkbox"/>	External	
<input checked="" type="checkbox"/>	LiveMigration	
- MTU: 9000
- MAC Pool: MAC_Pool
- QoS Policy: LiveMigration
- Network Control Policy: <not set>
- Pin Group: <not set>
- Stats Threshold Policy: default
- Dynamic vNIC Connection Policy: <not set>

Buttons: OK, Cancel

Right-click **vNIC Templates**.

Select **Create vNIC Template**.

Enter *<Mgmt>* as the vNIC template **Name**.

Check **Fabric A**.

Check the **Enable Failover** box.

Under target, unselect the **VM** box.

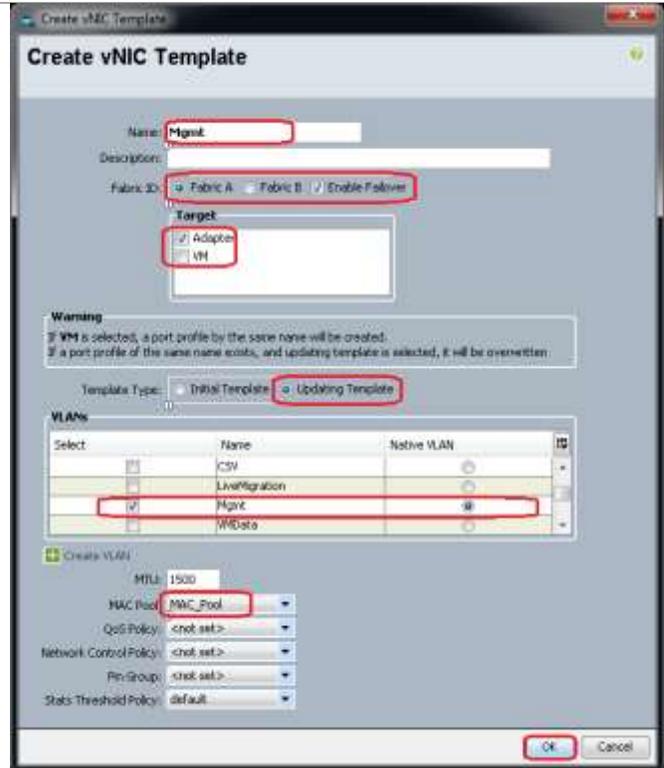
Select **Updating Template** as the Template Type.

Under VLANs, select *<Mgmt>*. Set Native **VLAN**.

Under MTU, leave **1500**.

Under MAC Pool, select *<MAC-Pool>*.

Click **OK** to complete creating the vNIC template



Right-click **vNIC Templates**.

Select **Create vNIC Template**.

Enter *<ClusComm>* as the vNIC template **Name**.

Check **Fabric B**.

Check the **Enable Failover** box.

Under target, unselect the **VM** box.

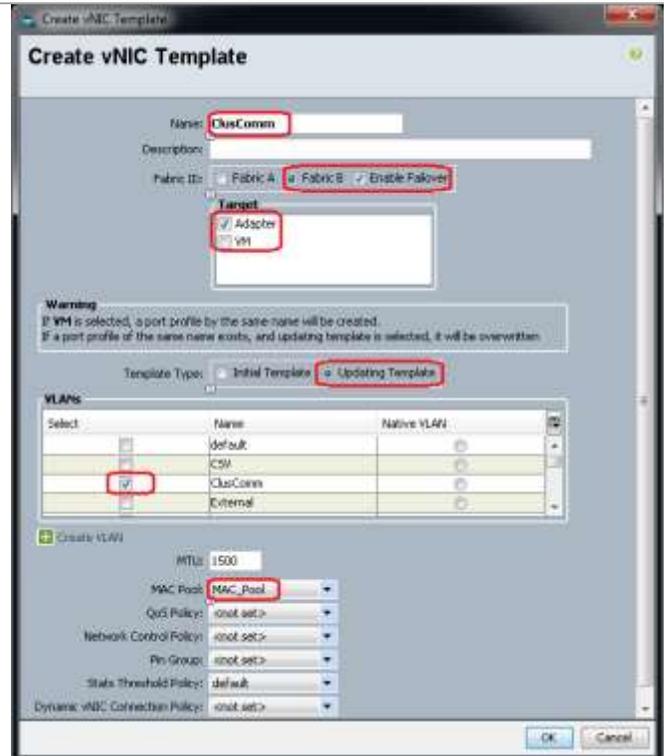
Select **Updating Template** as the Template Type.

Under VLANs, select *<ClusComm>*. Do not set a Native VLAN.

Under MTU, leave **1500**.

Under MAC Pool, select *<MAC-Pool>*.

Click **OK** to complete creating the vNIC template



Right-click **vNIC Templates**.

Select **Create vNIC Template**.

Enter <VMaccess> as the vNIC template **Name**.

Check **Fabric B**.

Check the **Enable Failover** box.

Under target, unselect the **VM** box.

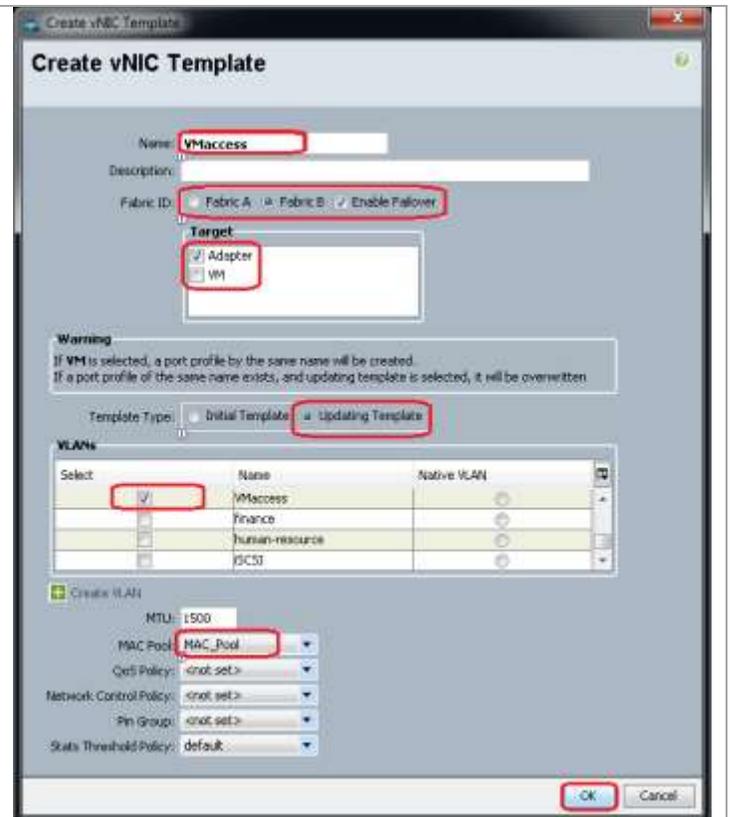
Select **Updating Template** as the Template Type.

Under **VLANs**, select <VMaccess>. Do not set a Native VLAN.

Under MTU, leave **1500**.

Under MAC Pool, select <MAC-Pool>.

Click **OK** to complete creating the vNIC template.



Right-click **vNIC Templates**.

Select **Create vNIC Template**.

Enter <VEM> as the vNIC template **Name**.

Check **Fabric B**.

Check the **Enable Failover** box.

Under target, unselect the **VM** box.

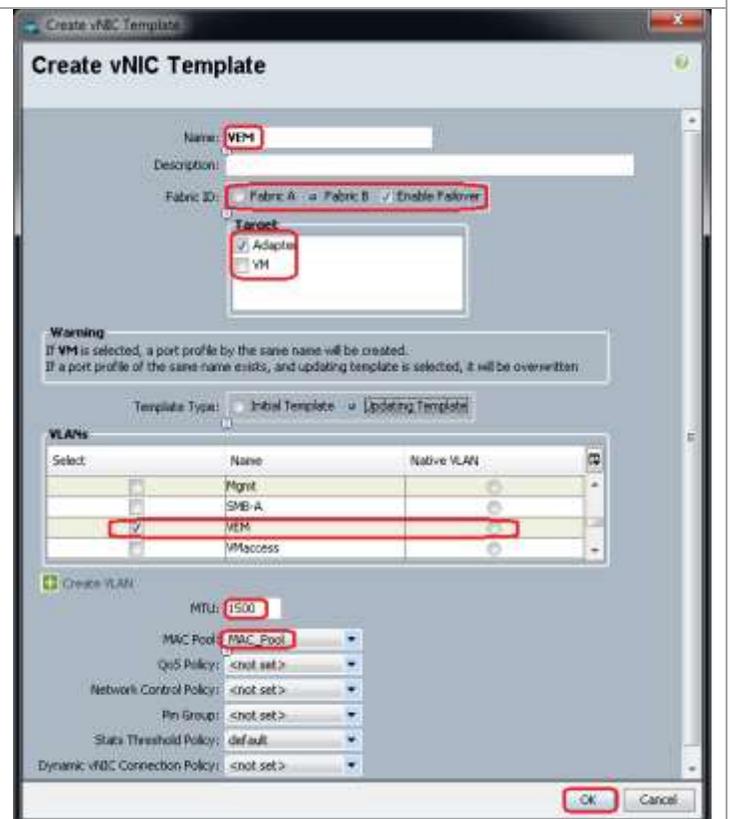
Select **Updating Template** as the Template Type.

Under **VLANs**, select <VEM>. Do not set a Native VLAN.

Under MTU, enter **1500**.

Under MAC Pool, select <MAC-Pool>.

Click **OK** to complete creating the vNIC template.



Cisco UCS PowerTool

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

Create vHBA Templates for Fabric A and B

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

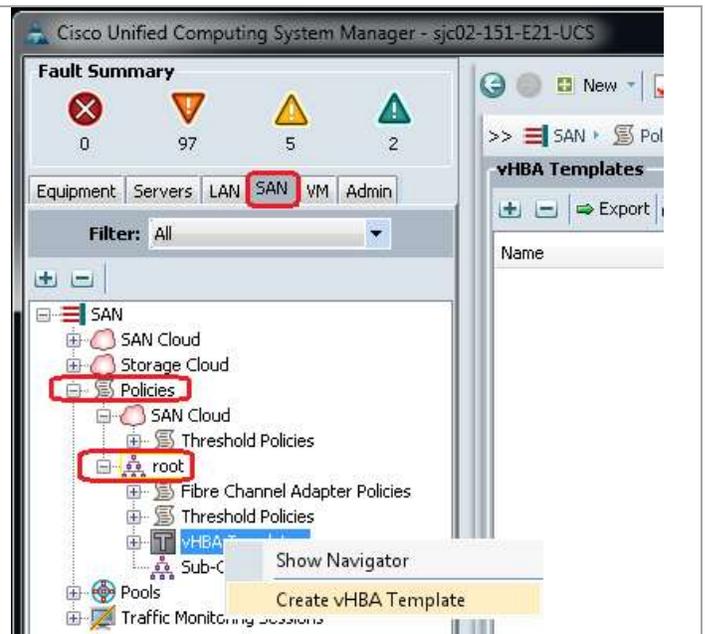
Cisco UCS Manager

Select the **SAN** tab on the left of the window.

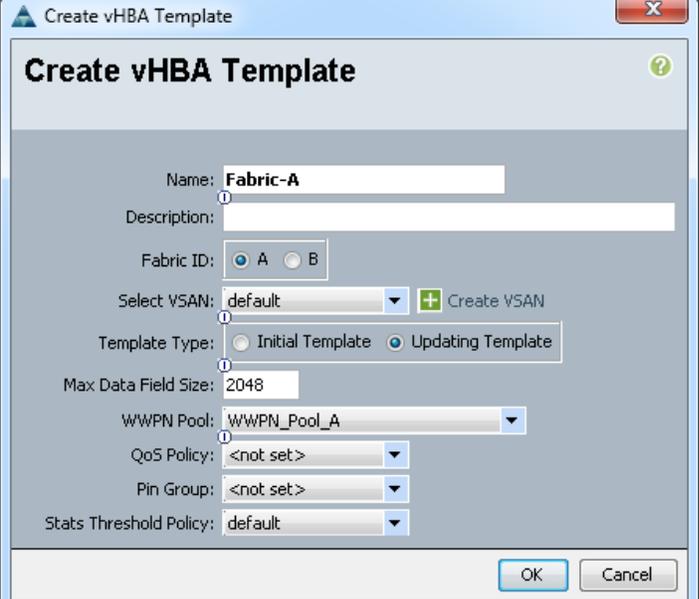
Go to **Policies > root**.

Right-click **vHBA Templates**.

Select **Create vHBA Template**.

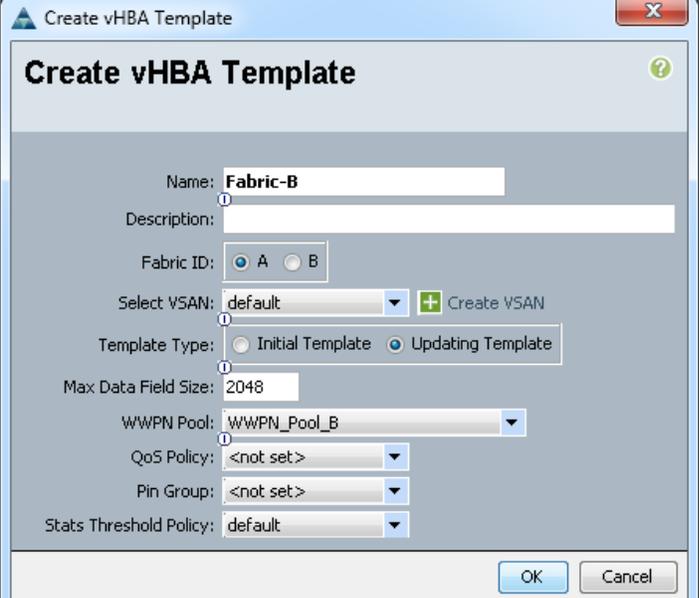


Enter <Fabric-A> as the vHBA template **Name**.
Select **Fabric A**.
Under Template Type select **Updating Template**.
Under WWN Pool, select <WWPN_Pool>.
Click **OK** to complete creating the vHBA template.
Click **OK**.



The screenshot shows the 'Create vHBA Template' dialog box. The 'Name' field is filled with 'Fabric-A'. The 'Fabric ID' section has radio buttons for 'A' (selected) and 'B'. The 'Select VSAN' dropdown is set to 'default'. The 'Template Type' section has radio buttons for 'Initial Template' and 'Updating Template' (selected). The 'Max Data Field Size' is set to '2048'. The 'WWPN Pool' dropdown is set to 'WWPN_Pool_A'. Other fields like 'QoS Policy', 'Pin Group', and 'Stats Threshold Policy' are set to '<not set>', 'default', and 'default' respectively. 'OK' and 'Cancel' buttons are at the bottom right.

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



The screenshot shows the 'Create vHBA Template' dialog box. The 'Name' field is filled with 'Fabric-B'. The 'Fabric ID' section has radio buttons for 'A' and 'B' (selected). The 'Select VSAN' dropdown is set to 'default'. The 'Template Type' section has radio buttons for 'Initial Template' and 'Updating Template' (selected). The 'Max Data Field Size' is set to '2048'. The 'WWPN Pool' dropdown is set to 'WWPN_Pool_B'. Other fields like 'QoS Policy', 'Pin Group', and 'Stats Threshold Policy' are set to '<not set>', '<not set>', and 'default' respectively. 'OK' and 'Cancel' buttons are at the bottom right.

Cisco UCS PowerTool

```
$mo = Get-UcsOrg -Level root | Get-UcsOrg -Name "<FastTrack4>" -LimitScope | Add-UcsVhbaTemplate -Descr "" -IdentPoolName "<wwpnFastTrack4>" -MaxDataFieldSize 2048 -Name "<F3-Fabric-B>" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -SwitchId "B" -TemplType "updating-template"$mo_1 = $mo | Add-UcsVhbaInterface -ModifyPresent -Name "default"
```

Create Boot Policies

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

Table 13. WWPN Values from Customer Environment

Port	WWPN
SPA-<port>	
SPA-<port>	
SPB-<port>	
SPB-<port>	

Obtain the WWPN information from the EMC VNX5400 by using the NaviSecCLI that is installed on your Windows management system and record it in the above table. Below is an example for obtaining the WWPNs from the connections to the VNX5400. It may be necessary to provide additional parameters, for login, password and scope options. The example below returns configuration information for all ports configured within the array. This includes both Fiber Channel ports, and iSCSI targets. The WWPN for any given Fiber Channel port is derived from the last half of the SP UID entry. The first half of the SP UID is the WWNN entry. As an example, the WWPN of Port 0 on SP-A Port ID 4 is 50:06:01:64:3D:E0:25:10.

```
C:\> naviseccli -address <<IP Address of SP-A or SP-B>> -User <<Admin user>> -Password <<Admin user password>> -Scope 0 port -list -sp
SP Name:          SP A
SP Port ID:       4
SP UID:           50:06:01:60:BD:E0:25:10:50:06:01:64:3D:E0:25:10
Link Status:      Up
Port Status:      Online
Switch Present:   YES
Switch UID:       20:02:00:05:73:A1:DA:C1:20:02:00:05:73:A1:DA:C1
SP Source ID:     0
...
(report truncated)
```

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

```

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

PortLocation      : SP A I/O Module 0 Port 0
WWNN              : 50:06:01:60:BD:E0:25:10
WWPN              : 50:06:01:60:3D:E0:0A:63
PortLocation      : SP A I/O Module 0 Port 1
WWNN              : 50:06:01:60:BD:E0:25:10
WWPN              : 50:06:01:61:3D:E0:0A:63
PortLocation      : SP B I/O Module 0 Port 0
WWNN              : 50:06:01:60:BD:E0:25:10
WWPN              : 50:06:01:68:3D:E0:0A:63
PortLocation      : SP B I/O Module 0 Port 1
WWNN              : 50:06:01:60:BD:E0:25:10
WWPN              : 50:06:01:69:3D:E0:0A:63
$targetports = Get-EmcTargetPort
$targetports | Where {$_.PortLocation -like "*Module 1*"} | fl PortLocation, Iqn, Ipaddress

PortLocation      : SP A I/O Module 1 Port 0
Iqn               : iqn.1992-04.com.emc:cx.apm00122900053.a6
IpAddress         : 192.168.18.200
PortLocation      : SP A I/O Module 1 Port 1
Iqn               : iqn.1992-04.com.emc:cx.apm00122900053.a7
IpAddress         : 192.168.19.200
PortLocation      : SP B I/O Module 1 Port 0
Iqn               : iqn.1992-04.com.emc:cx.apm00122900053.b6
IpAddress         : 192.168.18.201
PortLocation      : SP B I/O Module 1 Port 1
Iqn               : iqn.1992-04.com.emc:cx.apm00122900053.b7
IpAddress         : 192.168.19.201

```

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

Figure 5: Finding WWN from Unisphere

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

When you have recorded the WWPNs from the VNX5400 for the correct ports, proceed to configuring Cisco UCS Manager.

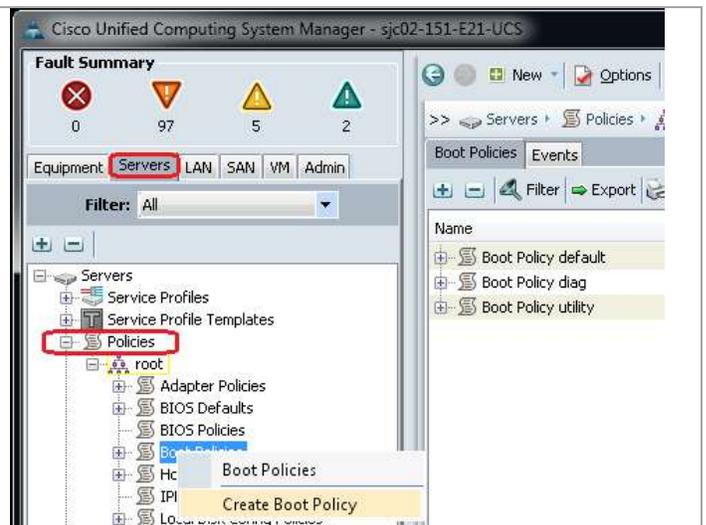
Cisco UCS Manager for Fabric A

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

Go to **Policies > root**.

Right-click **Boot Policies**.

Select **Create Boot Policy**.



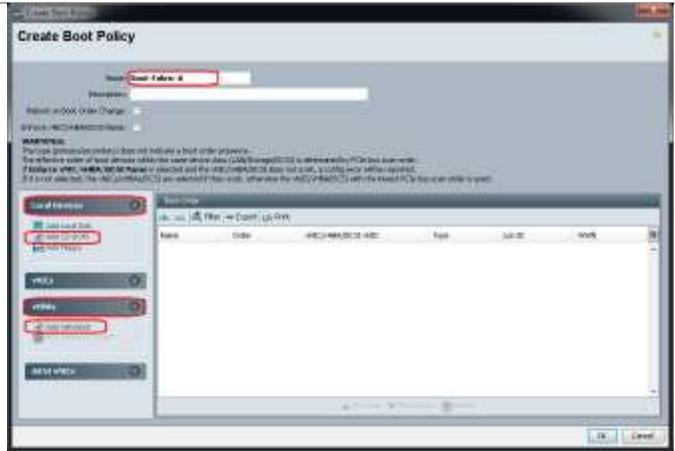
Name the boot policy <Boot-Fabric-A>.

(Optional) Give the boot policy a description.

Leave **Reboot on Boot Order Change** and **Enforce vNIC/vHBA Name** unchecked.

Expand the **Local Devices** drop-down menu and select **Add CD-ROM**.

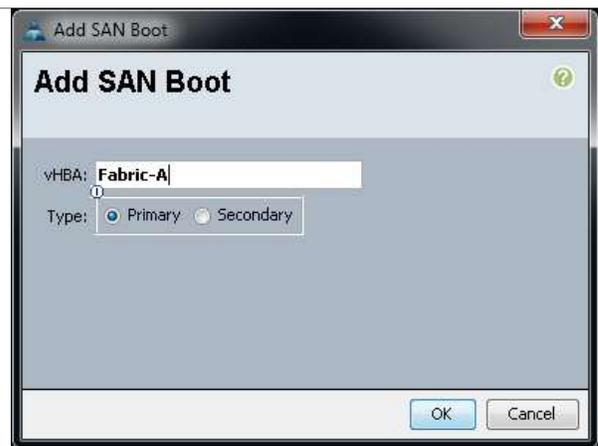
Expand the **vHBAs** drop-down menu and select **Add SAN Boot**.



Enter <Fabric-A> in the **vHBA** field in the **Add SAN Boot** window that displays.

Make sure that **Primary** is selected as the **Type**.

Click **OK** to add the SAN boot initiator

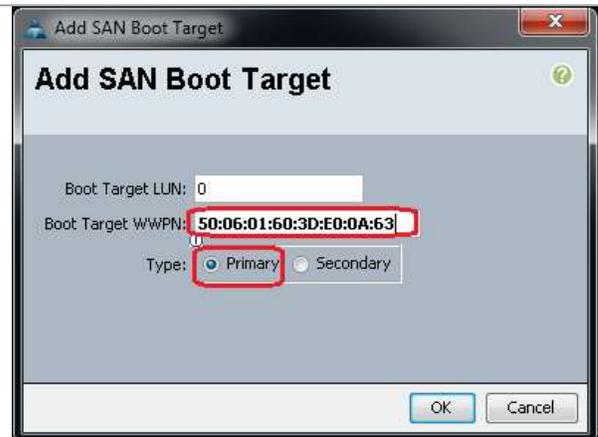


Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0.



Enter the WWPN for the primary FC adapter interface SPA-A2 as the Boot Target WWPN. Keep the **Type** as **Primary**.

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

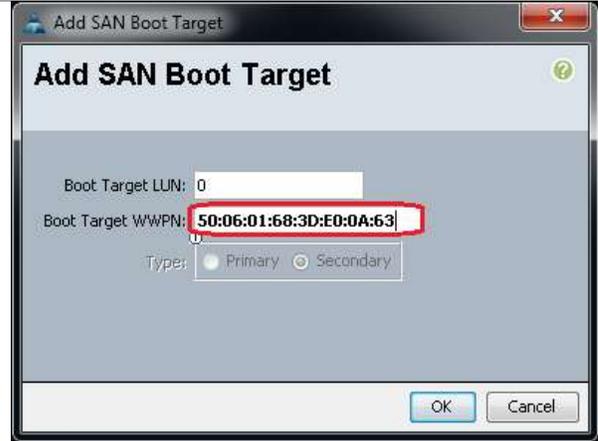


Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0.

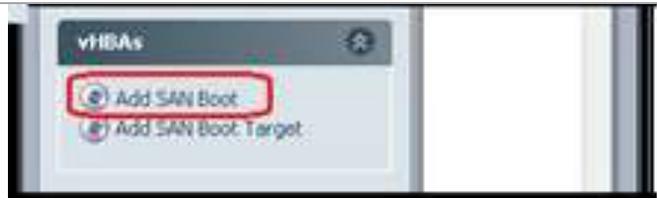


Enter the WWPN for the primary FC adapter interface SPB-B2 as the Boot Target WWPN. Select the **Type** as **Secondary**; it is the default and cannot be changed on the second entry.

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



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



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

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

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



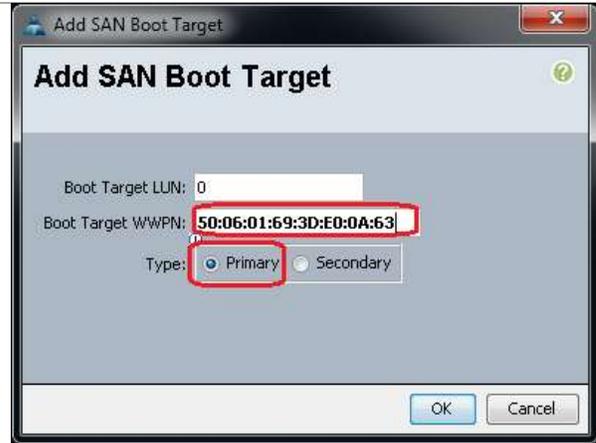
Select **Add SAN Boot Target** under the **vHBA** drop-down menu.



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

Enter the WWPN for the secondary FC adapter interface SPA-B3 as the Boot Target WWPN. Keep the **Type** as **Primary**.

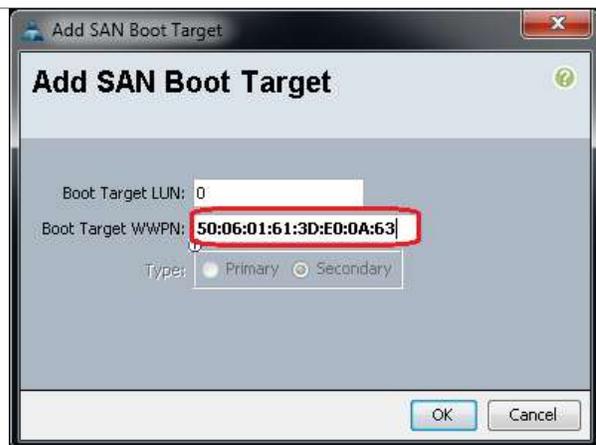
Click **OK** to add the SAN boot target.



Under the **vHBA** drop-down menu, select **Add SAN Boot Target**. Keep the value for Boot Target LUN as 0.

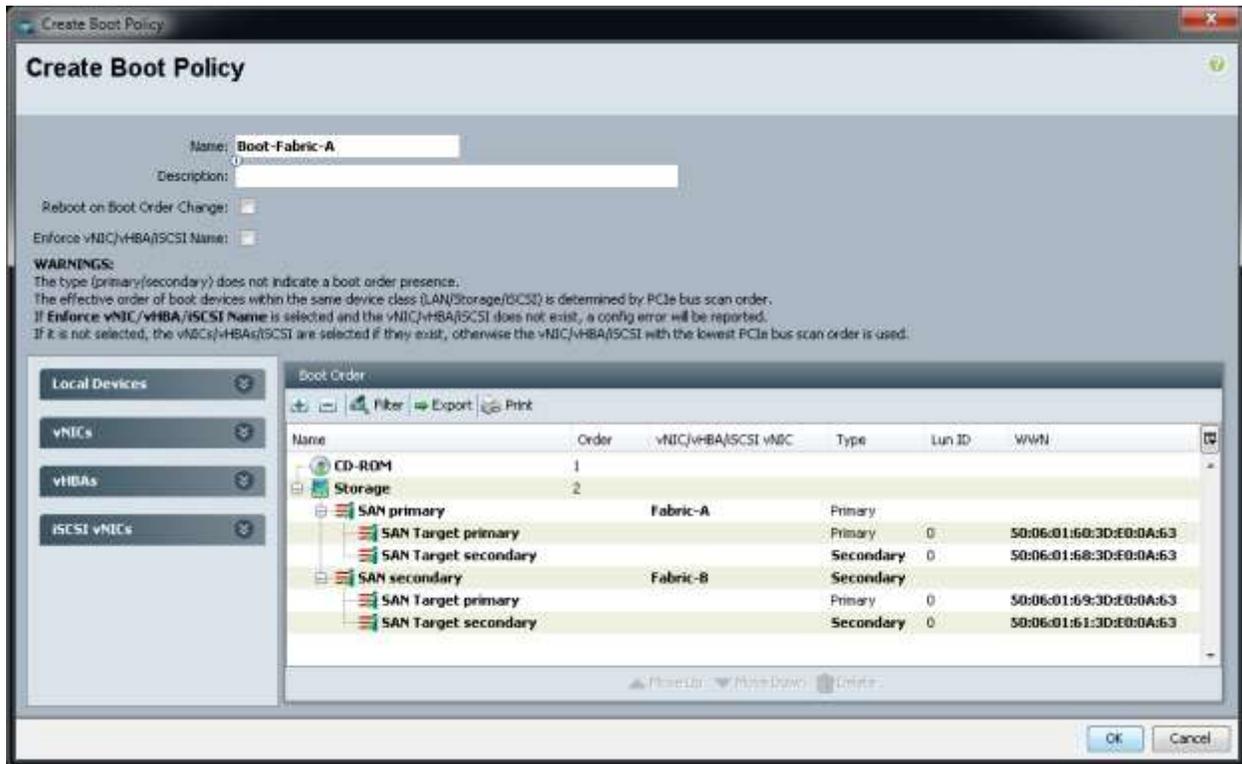
Enter the WWPN for the secondary FC adapter interface SPB-A3 as the Boot Target WWPN. Select the **Type** as **Secondary**.

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



Verify your configuration looks something like the following.

Figure 6. Boot Policy Example



Cisco UCS Manager for Fabric B

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

- 1) Select the **Servers** tab at the top left of the window.
- 2) Go to Policies > root.
- 3) Right-click **Boot Policies**.
- 4) Select **Create Boot Policy**.
- 5) **Name** the boot policy <**Boot-Fabric-B**>.
- 6) (Optional) Give the boot policy a description.
- 7) Leave **Reboot on Boot Order Change** and **Enforce vNIC/vHBA Name** unchecked.
- 8) Expand the **Local Devices** drop-down menu and select **Add CD-ROM**.
- 9) Expand the **vHBAs** drop-down menu and select **Add SAN Boot**.
- 10) Enter <**Fabric-B**> in the **vHBA** field in the Add SAN Boot window that displays.
- 11) 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 SPB-B3 as the **Boot Target WWPN**. Keep the Type as **Primary**.

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

Cisco UCS PowerTool

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

Create Service Profile Templates

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

Cisco UCS Manager

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

Go to **Service Profile Templates > root**.

Right-click **root**.

Select **Create Service Profile Template**.

The screenshot displays the Cisco UCS Manager web interface. The top navigation bar shows the 'Servers' tab selected. The main content area is divided into a left-hand navigation pane and a right-hand main pane. The left pane shows a tree view with 'Servers' expanded to 'Service Profile Templates', and 'root' selected. The right pane shows a 'Fault Summary' section with four status icons (red X, orange triangle, yellow triangle, green triangle) and counts (3, 32, 20, 20). Below this is an 'Actions' menu with several options. The 'Create Service Profile Template' option is highlighted with a red rectangle. Other visible options include 'Create Organization', 'Create Service Profile (expert)', 'Create Service Profiles From Template', 'Create Service Profile', and 'Start Fault Suppression'.

The **Create Service Profile Template** window displays.

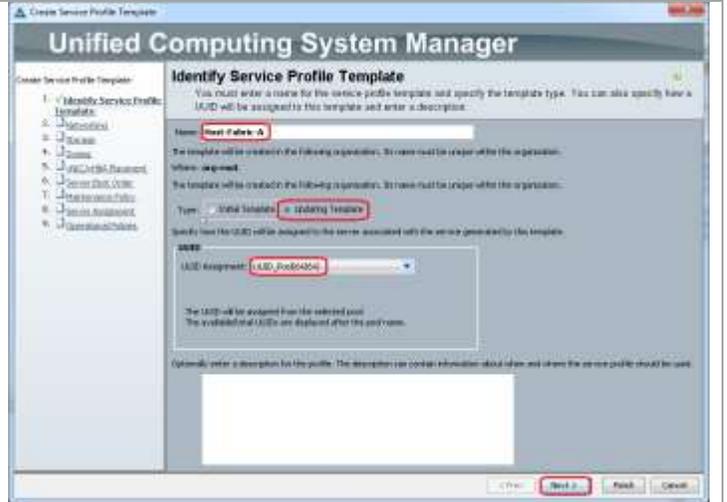
Identify the Service Profile Template Section.

Name the service profile template <Host-Fabric-A>. This service profile template is configured to boot from SPA-A2.

Select Updating Template.

In the UUID section, select <UUID_Pool> as the UUID pool.

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

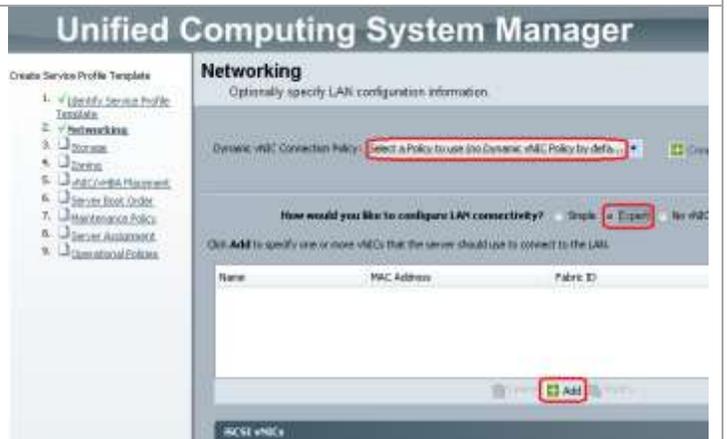


Networking Section

Leave the **Dynamic vNIC Connection Policy** field at the default.

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

Click **Add** to add a vNIC to the template.



The **Create vNIC** window displays. Name the vNIC <CSV>.

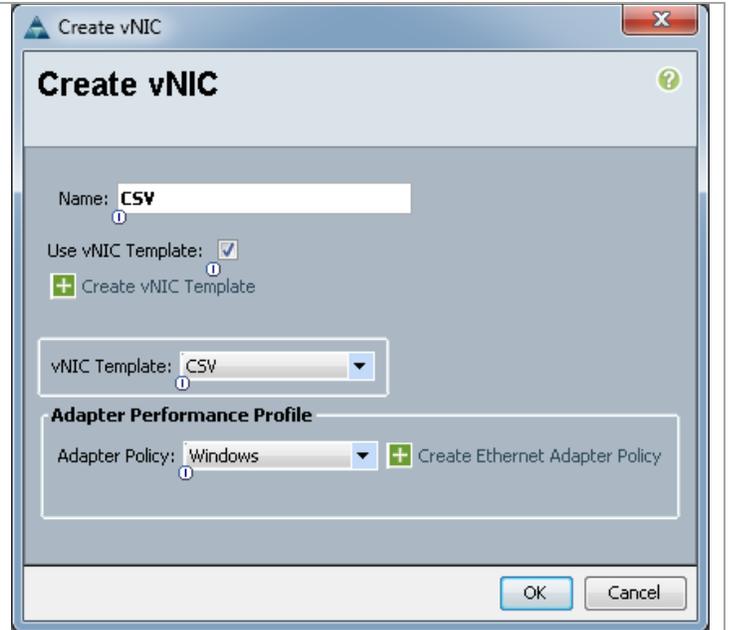
Check the **Use LAN Connectivity Template** checkbox.

Select <CSV> for the **vNIC Template** field.

Select **Windows** in the **Adapter Policy** field.

Click **OK** to add the vNIC to the template. This returns you to the **Networking** window.

Repeat for all the desired vNICs.



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

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

Storage Section

Select the **Local Storage** policy defined earlier.

Select **Expert** for the **How would you like to configure SAN connectivity?** question.

Select the appropriate pool for **WWNN Assignment**.

In the **WWPN** section, click **Add** to add the WWPNs to be used.



Enter a value in the **Name** field.

Select **Use vHBA Template**.

Select the vHBA template created to boot from Fabric A from the **vHBA Template** drop down list.

Select **Windows** from the **Adapter Policy** drop down list.

Click **OK** to accept the values entered.

Repeat to create the vHBA for Fabric B.

When both vHBAs are created, click **Next** on the Storage Section to continue to the Zoning section.



Zoning Section

This section is not used in this deployment. Click **Next** to continue to the **vNIC/vHBA Placement** Section.

vNIC/vHBA Placement Section

Select the <PvtCld-Host> placement policy in the **Select Placement** field.

Select vCon1 and assign the vNICs in the following order:

- Mgmt
- LiveMigration
- CSV
- VMaccess
- VEM
- ClusComm

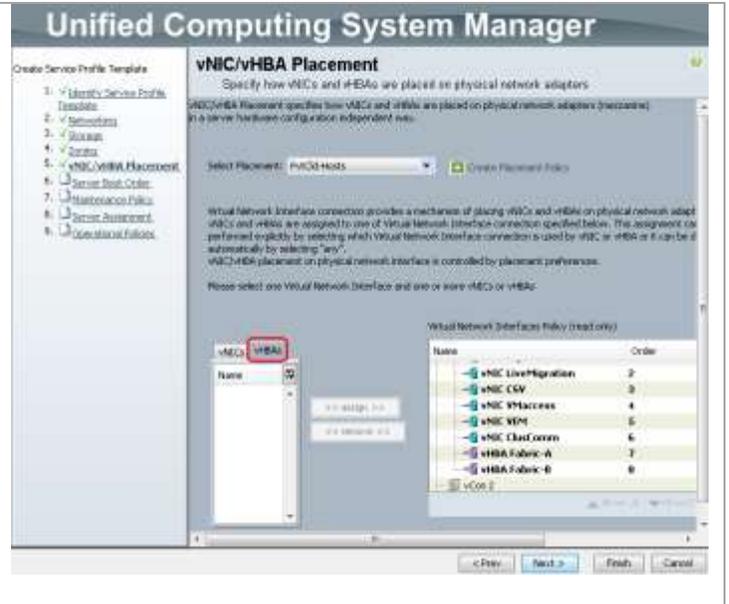


Click the **vHBA** tab and add the vHBAs in the following order:

- Fabric-A
- Fabric-B

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.

Click **Next** to move to the Server Boot Order section.



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.

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



Maintenance Policy Section

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

Server Assignment Section

- Select *<Server-Pool>* in the **Pool Assignment** field.
- Select *<PvtCld-Host>* for the **Server Pool Qualification** field.
- Select **Up** for the power state.
- Expand the **Firmware Management (BIOS, Disk Controller, Adapter)** window and select *<PvtCld-Host>* in the **Host Firmware** field.
- Expand the **Firmware Management** window and Select *<PvtCld-Host>* in the **Host Firmware** field.
- Click **Next** to continue to the next section.

Operational Policies Section

- Select *<PvtCld-Host>* in the **BIOS Policy** field.
- Expand **Power Control Policy Configuration**.
- Select *<No-Cap>* in the **Power Control Policy** field.
- Expand **Scrub Policy**.
- Select *<No-Scrub>* in the **Scrub Policy** field.

Click **Finish** to create the Service Profile template.

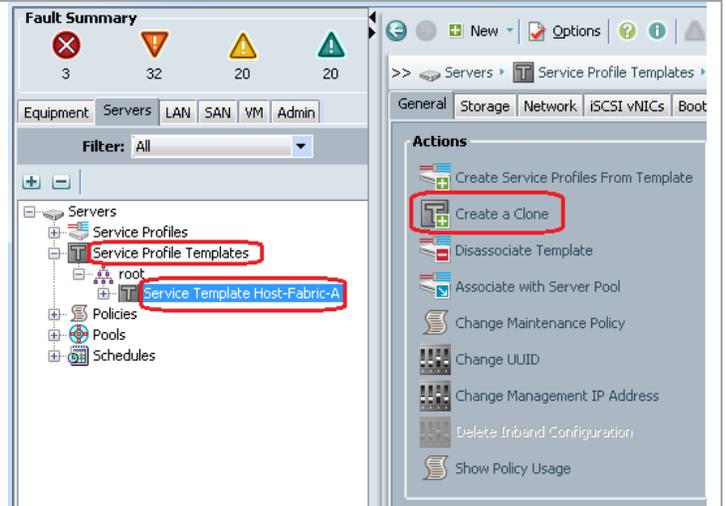
Click **OK** in the pop-up window to proceed.

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

Go to **Service Profile Templates > root**.

Select the previously created <Host-Fabric-A> template

Click **Create a Clone**.

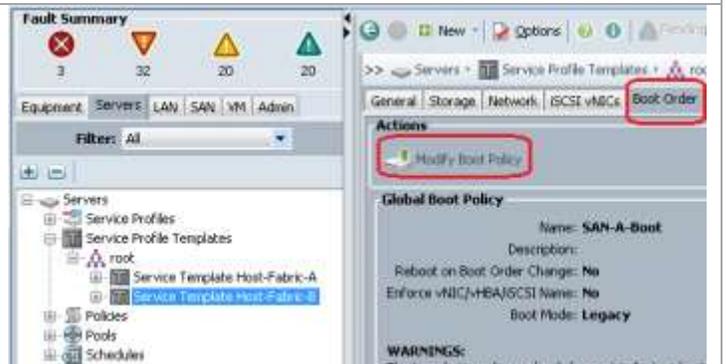


Enter <Host-Fabric-B> in the **Clone Name** field and click **OK**.

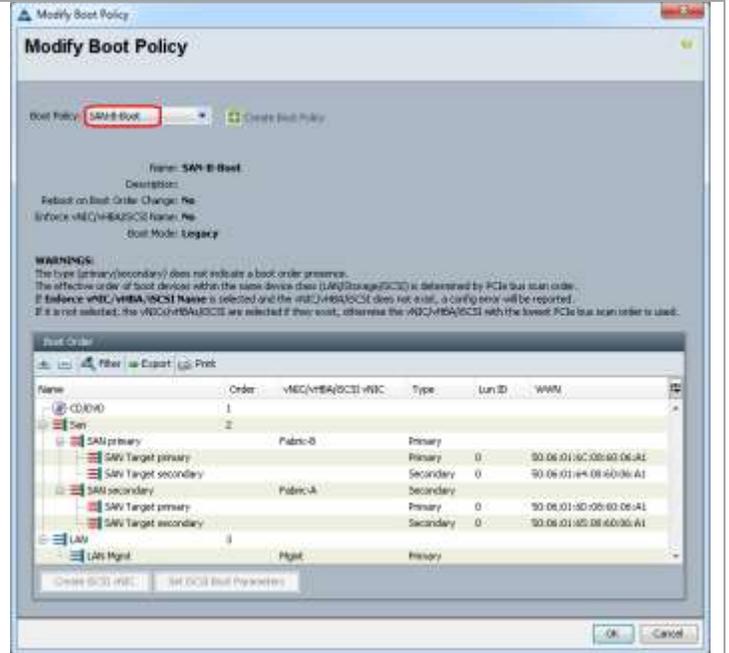


Select the newly created service profile template and select the **Boot Order** tab.

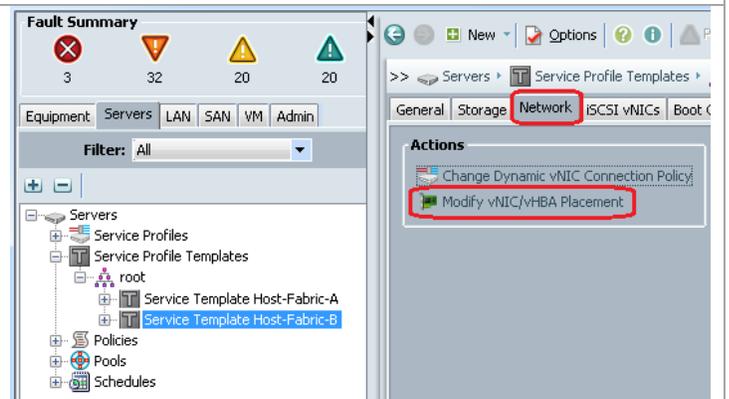
Click **Modify Boot Policy**.



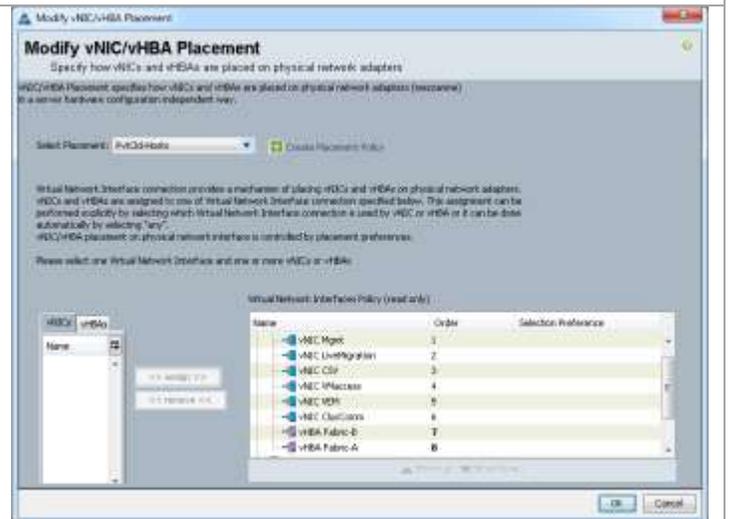
Select <Boot-Fabric-B> as the **Boot Policy** and click **OK**.



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



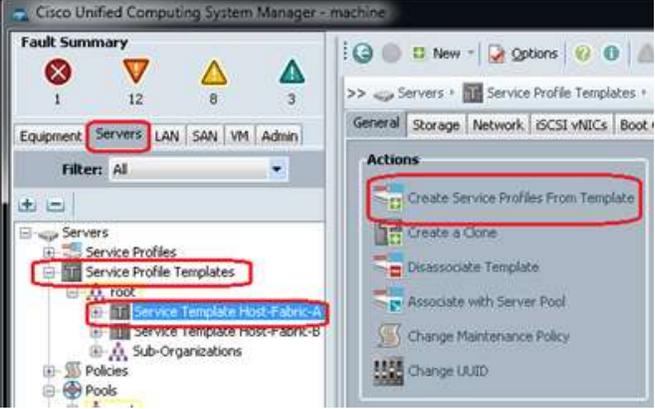
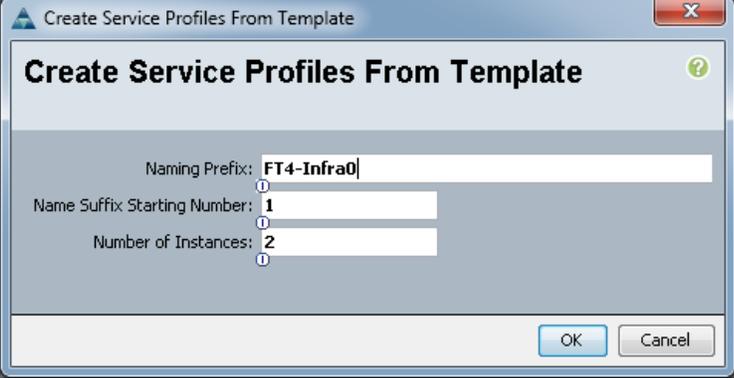
Select <PvtCld-Host> in the **Select Placement** field.
Move <vHBA Fabric-B> ahead of <vHBA Fabric-A> in the placement order and click **OK**.



Create Service Profiles

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

Cisco UCS Manager

<p>Select the Servers tab at the top left of the window.</p> <p>Select Service Profile Templates <Host-Fabric-A></p> <p>Right-click and select Create Service Profile From Template.</p>	
<p>Enter <F3-Infra0> for the Naming Prefix.</p> <p>Enter 1 for the Name Suffix Starting Number.</p> <p>Enter 2 for the Number of service profiles to create.</p> <p>Click OK to create the service profile.</p> <p>Click OK in the message box.</p>	
<p>Right-click the second Service Profile just created and select Rename Service Profile. Rename the Service Profile to be <FT4-Infra03>.</p> <p>Note: The implementation alternates fabrics from which hosts boot. Odd numbered hosts boot from Fabric A and even numbered hosts boot from Fabric B.</p>	
<p>Repeat the above process to create a single Service Profile to boot from Fabric B.</p>	

EMC VNX5400 Deployment: Part 2

Create VNX LUNs for Private Cloud Environment

The Private cloud environment implements a boot from SAN environment, using the concept of a Master Boot LUN. The Master Boot LUN is a storage area that will be used to maintain an image of a Windows Server 2012 R2 image to be used as a Clone source. This image should be configured as a base image to be used for subsequent installations, so all patching and custom configuration steps should be taken. For example, maybe a desired configuration setting is to make sure that all physical servers are able to be remotely managed. When the image is configured according to customer policy, the Microsoft sysprep utility can be run against this image to prepare it for use as a Clone. Make sure any Microsoft hotfixes listed in the software revision table have been applied before running sysprep.

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

Management of the boot LUN requires special consideration, and needs to Make sure that the LUN ID provided to the LUN, as seen from the host is set to 0 (zero). The ESI (EMC Storage Integrator) PowerShell commands do not allow the manipulation of the LUN ID for devices presented to servers, and simply default to the sequential allocation of LUN IDs as implemented by the VNX array. As a result of this behavior, the boot LUN must be the first device that is mapped to the server (Cisco UCS service profile). If this is incorrectly implemented, then the wrong target will be selected for Windows boot operations on server power-up.

As described, the ESI PowerShell commands are utilized for provisioning of the LUNs required within the environment, and assume that the storage pool creation outlined in the previous section have been completed. For this procedure, a single LUN is created, and is used to install a Windows Server 2012 R2 instance. This server instance subsequently will be processed with Windows sysprep, and be removed from the server. All compute nodes will then use a Clone of the sysprep image, and will be customized as individual server instances.

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

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

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

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

```
<StorageParams>
<Servers>
  <Server>
    <ServerName>F3-Infra01</ServerName>
    <IPAddress>10.29.130.21</IPAddress>
    <luns>
      <label>MASTER-BOOT-2012R2</label>
      <pool>PVTCLD_DATA1_R5</pool>
      <size>60GB</size>
    </luns>
  </Server>
</Servers>
<Array>EnterpriseFastTrack</Array>
<UCSAddress>10.5.177.10</UCSAddress>
</StorageParams>
```

This configuration file is read by the following sample PowerShell script to result in a LUN named Master-Boot-2012R2 of size 60 GB being created in the storage pool called PVTCLD_DATA.

```

#-----
# Filename:      ProcessStorageRequests.ps1
# Description:   Create LUNs based on xml file
#
#-----
#
# Uses an XML file with the following schema.  This same schema is used by
# - PrepMastBoot-AddViaWWPN.ps1
# - Process Storage Requests.ps1
# - PostClone_AddViaWWPN.ps1
#
# <StorageParams>
# <Servers>
#   <Server>
#     <ServerName>F3-Infra01</ServerName>
#     <IPAddress>192.168.11.150</IPAddress>
#     <luns>
#       <label>MASTER-BOOT-2012</label>
#       <pool>PVTCLD_DATA1_R5</pool>
#       <size>60GB</size>
#     </luns>
#   </Server>
# </Servers>
# <Array>EnterpriseFastTrack</Array>
# <UCSAddress>10.5.177.10</UCSAddress>
# </StorageParams>
#
#-----

$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\CFG_STORAGE_LUNS.xml"

function ReadStorageConfig ([String]$filename) {
    $xmlConfigFile = [xml](Get-Content $filename )
    $global:StorageConfig = $xmlConfigFile.SelectSingleNode( '/StorageParams' )
}

ReadStorageConfig $myxmlfile

Import-Module ESIPSToolkit

function LUNExists {
    param ($TGTLUN)
    $Val = Get-EmcLUN $TGTLUN -Silent
    if ($Val -eq $null) {return $false} else {return $true}
}

$StorageArray = get-EMCStorageSystem -ID $global:StorageConfig.Array -silent

if ($StorageArray -eq $null)
{
    Write-Host "ERROR: Array" $Array "is not known or registered under that name."
    exit 1
}

Update-EmcSystem $StorageArray

```

```

function createluns {
    foreach ($entry in $global:StorageConfig.Servers.Server) {
        foreach ($lun in $entry.luns) {
            IF (LUNExists $lun.label)
            { Write-Host "LUN" $lun.label "already exists."}
            else
            {
# We need to create the LUN
                write-host "Creating LUN" $lun.label
                $pool = get-emcstoragepool $lun.pool
                $Size = invoke-expression $lun.size
                $NewLUN = New-EmcLun -Pool $pool -Name $lun.label -Capacity $Size -Description
                $lun.label
            }
        }
    }
}

createluns

```

The execution of such a process is shown in the following figure.

Figure 7. Example Execution of Master Boot LUN Creation

```

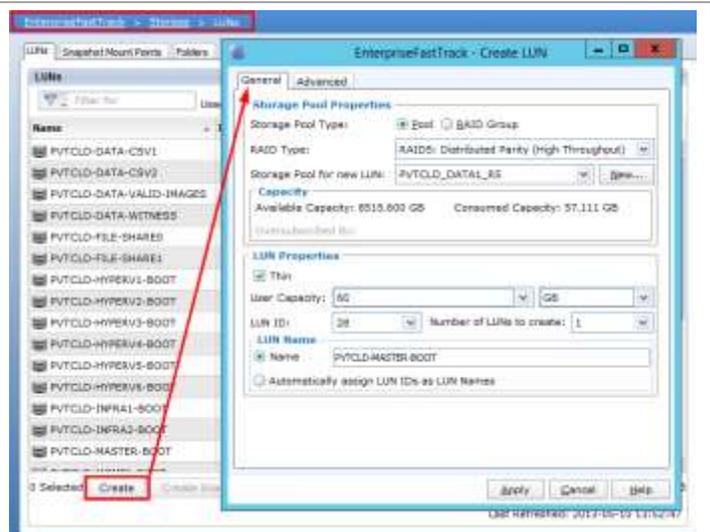
PS C:\> C:\Users\fulladmin\Desktop\ProcessStorageRequests.ps1
System '[Name = EnterpriseFastTrack, UserFriendlyName = VNXFT]' has been updated successfully.
Creating LUN MASTER-BOOT-2012
TaskStatus: Started
10% : Creating the LUN...
100% : The specified LUN has been created.
TaskStatus: Completed

PS C:\>

```

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

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



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

```

#-----
# Filename:      PrepMasterBoot_AddViaWWPN.ps1
# Description:   Set up Cisco UCS ServiceProfile to do Boot from SAN from
#               VNX5500
#-----
#
# Uses an XML file with the following schema.  This same schema is used by
# - PrepMastBoot-AddViaWWPN.ps1
# - Process Storage Requests.ps1
# - PostClone_AddViaWWPN.ps1
#
# <StorageParams>
# <Servers>
#   <Server>
#     <ServerName>F3-Infra01</ServerName>
#     <IPAddress>192.168.11.150</IPAddress>
#     <luns>
#       <label>MASTER-BOOT-2012</label>
#       <pool>PVTCLD_DATA1_R5</pool>
#       <size>60GB</size>
#     </luns>
#   </Server>
# </Servers>
# <Array>EnterpriseFastTrack</Array>
# <UCSAddress>10.5.177.10</UCSAddress>
# </StorageParams>
#
#-----

$global:rootPath = Split-Path -Parent $MyInvocation.MyCommand.Path
$myxmlfile = $global:rootPath + "\CFG_STORAGE_LUNS.xml"

Function ReadStorageConfig ([String]$filename) {
    $xmlConfigFile = [xml](Get-Content $filename )
    $global:StorageConfig = $xmlConfigFile.SelectSingleNode( '/StorageParams' )
}

ReadStorageConfig $myxmlfile

Import-Module CiscoUcsPS
Import-Module ESIPSToolkit

Function LUNExists {
    param ($TGTLUN)
    $Val = Get-EmcLUN $TGTLUN -Silent
    if ($Val -eq $null) {return $false} else {return $true}
}

Function reghostexists {
    param ($tgthost)
    $val = Get-EmcStorageRegisteredHost $tgthost
    If ($Val -eq $null) {Return $false}
    Else {Return $true}
}

$StorageArray = Get-EMCStorageSystem -ID $global:StorageConfig.Array -Silent

```

```

If ($StorageArray -eq $null)
{
    Write-Host "ERROR: Array" $Array "is not known or registered under that name."
    Exit 1
}

Update-EmcSystem $StorageArray

# Prompt user for connection to UCS environment
If ($UCS -eq $null) {$UCS = Connect-Ucs $global:StorageConfig.UCSAddress}

ForEach ($entry in $global:StorageConfig.Servers.Server)
{
    ForEach ($lun in $entry.luns)
    {
        Write-Host $entry.Servername, $lun.label
    }
}

# Check for pre-existing LUN
If (LUNExists $global:StorageConfig.Servers.Server.luns.label)
{ # We present the LUN
    $MyServiceProfile = Get-UcsServiceProfile | where {$_.Name -eq
$global:StorageConfig.Servers.Server.ServerName}
    If ($MyServiceProfile -eq $null)
    {
        Write-Host "ERROR: Cannot find ServiceProfile"
$global:StorageConfig.Servers.Server.ServerName
        exit 1
    }
    Else
    {
#
# Extract out the WWPN initiator information for the Service Profile
#
        $MyvHBAs = Get-UcsVhba -ServiceProfile $MyServiceProfile
#
# Get the Gold Master that we plan to use
#
        $MasterLUN = get-EMCLun -ID $global:StorageConfig.Servers.Server.luns.label -
BlockStorageSystem $StorageArray
#
# Add all the initiators from the Service Profile to the Storage Group on the VNX
#
        ForEach ($vHBA in $MyvHBAs)
        {
            $HostRegistration = $vHBA.NodeAddr + ":" + $vHBA.Addr
            If (reghostexists $global:StorageConfig.Servers.Server.ServerName)
            {
                $rg=get-emcstorageregisteredhost $global:StorageConfig.Servers.Server.ServerName
                Write-Host "New Init" $HostRegistration
                New-EmcStorageRegisteredInitiator -registeredhost $rg -InitiatorIds
$HostRegistration
            }
            Else

```

```

    {
        Write-Host "New Host" $HostRegistration
        New-EMCStorageRegisteredHost -StorageSystem $StorageArray -HostName
$global:StorageConfig.Servers.Server.ServerName -IPAddress
$global:StorageConfig.Servers.Server.IPAddress -HostBusAdapterIds $HostRegistration
    }
}
If (LUNExists $MasterLUN)
{
    Write-Host "unmask lun" $masterlun
    Set-EmcLunAccess -Lun $MasterLUN -InitiatorId $Hostregistration -HostName
$global:StorageConfig.Servers.Server.ServerName -HostIPAddress
$global:StorageConfig.Servers.Server.IPAddress -Available
}
Else
{ # We Fail, because the LUN cannot be found
    Write-host "ERROR: Cannot find the LUN:" $MasterLUN
    Exit 1
}
}

```

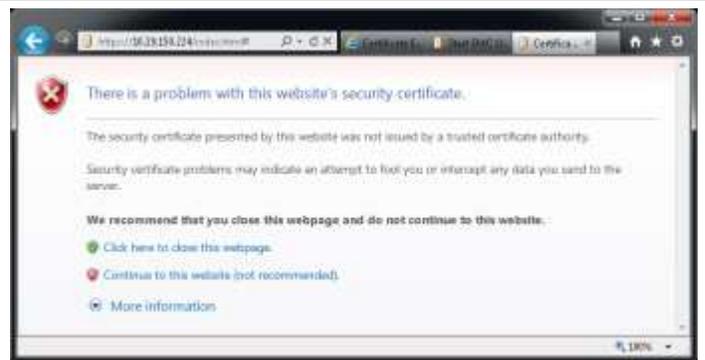
An alternative to using ESI PowerShell would be to manually present storage using Unisphere as in the following example.

Mask Boot LUN with EMC Unisphere

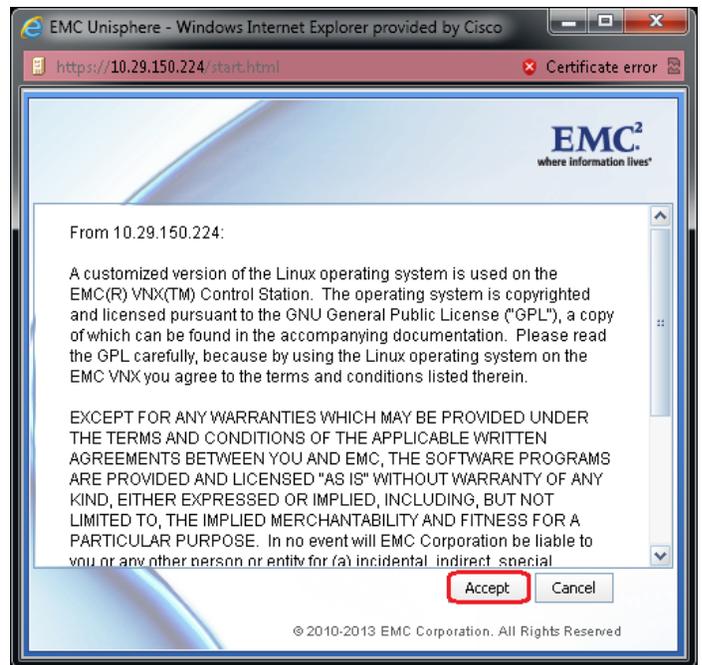
Open your browser.

Enter the IP address of your EMC VNX5400 SAN with an **https://** prefix.

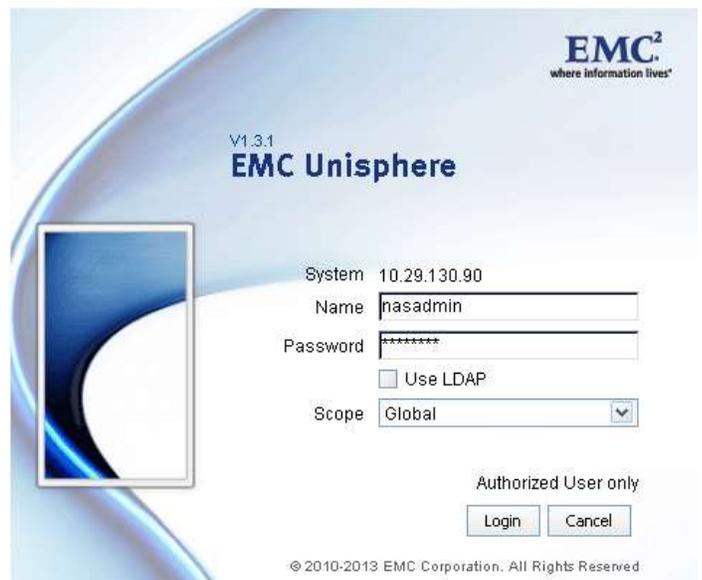
Click Continue to this website (not recommended).



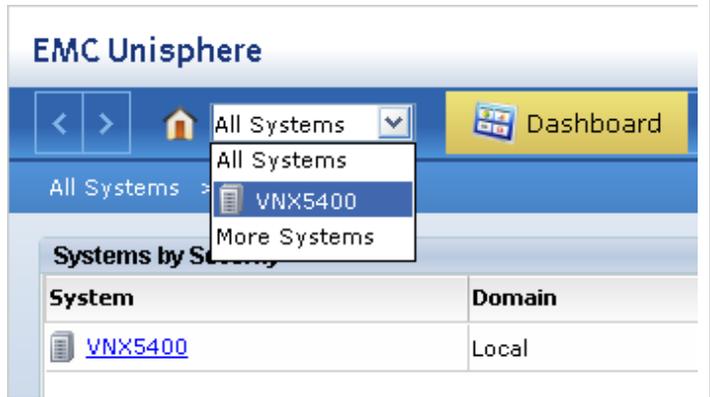
Click **Accept** to accept EMC's licensing agreement.



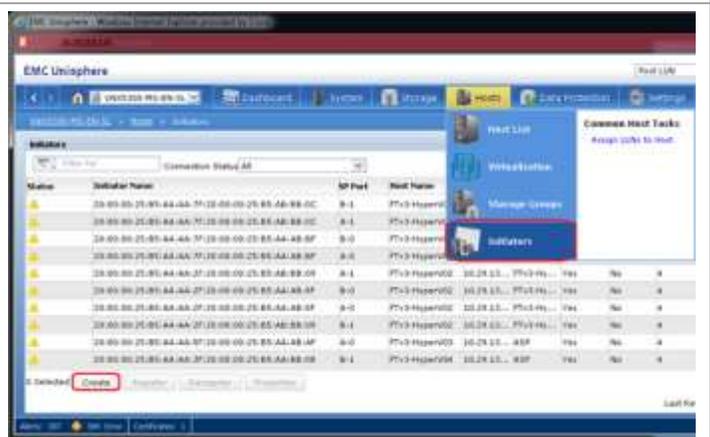
Enter the **Name** and **Password** for your installation.



From the drop-down, select your EMC VNX5400 SAN.



Select **Initiators** from the **Hosts** tab.
 Select **Create** to create a host initiator for accessing the boot LUN.

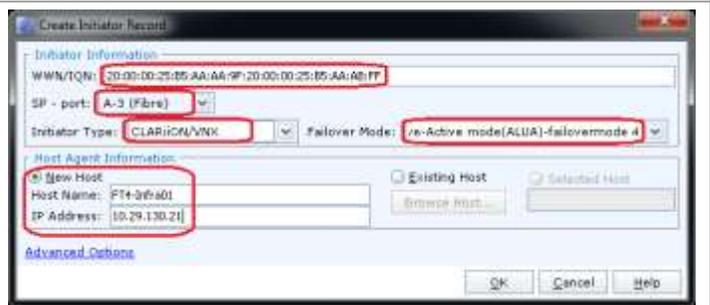


Enter the host's WWNN and WWPN in the **WWN/IQN** field.

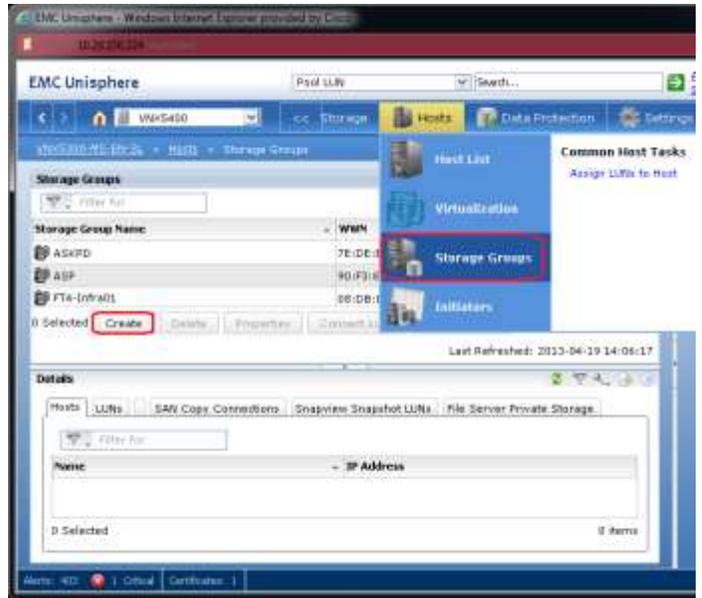
Select the A0 port in the **SP-port** drop-down list.
 Select CLARiiON/VNX from the **Initiator Type** drop-down list.

Make sure that **Failover Mode** is ALUA.
 Select the radio button for **New Host**. Enter your **Host Name** and its **IP Address**.

Click **OK**.



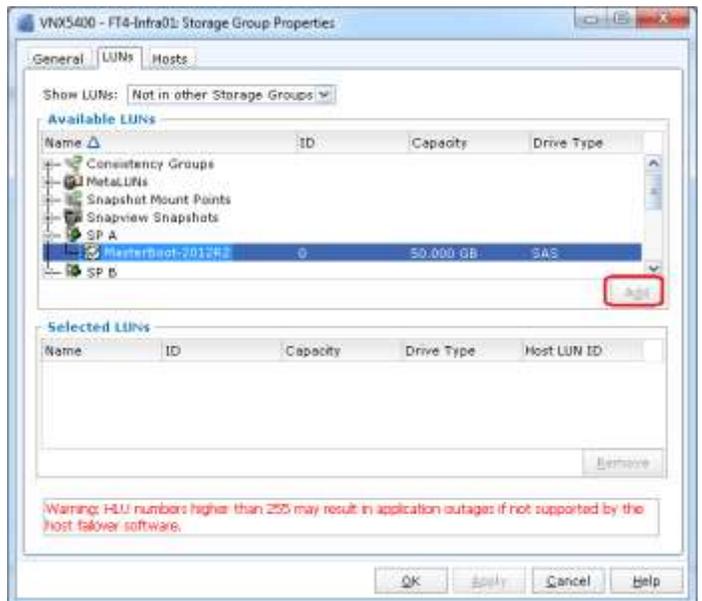
Select **Storage Groups** from the Hosts tab.
Click **Create**.



Enter a name for a storage group to be assigned to this server in the **Storage Group Name** field.



On the LUNs tab, select the boot LUN that was created for this server. Click **Add** and an entry will appear in the Selected LUNs section of the screen.



Select the **Hosts** tab.

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

Click **OK**.



Cisco Nexus 5548 Switch: Configure for SAN Boot

These steps detail the procedure for configuring the UCS environment to boot the blade servers from the EMC VNX5400 SAN.

Gather Necessary Information

After the Cisco UCS service profiles have been created (earlier section), each infrastructure management blade has a unique configuration. To proceed with the deployment, specific information must be gathered from each Cisco UCS blade server to enable SAN booting. Insert the required information in the following table. WWPNs from the EMC VNX5400 needed for this configuration were obtained in the Create Boot Policies step. Both WWNN and WWPN from the Cisco UCS service profiles are needed for masking the LUNs on the VNX5400 SAN.

Table 14. WWPN for Hyper-V Host Servers

Device	Port	WWPN	WWNN
FT4-Infra01	Fabric A		
FT4-Infra01	Fabric B		
FT4-Infra02	Fabric A		
FT4-Infra02	Fabric B		
Repeat for all profiles	...		


```
device-alias database
  device-alias name <F3-Infra01-B> pwwn <F3-Infra01 Fabric-B WWPN>
  device-alias name <VNX5400-SPA-A1> pwwn <SPA-A1 WWPN>
  device-alias name <VNX5400-SPB-B1> pwwn <SPB-B1 WWPN>
  device-alias commit
zoneset name <PvtCld> vsan 1
exit
copy run start
```

First Installation of Windows Server 2012 R2 Datacenter

The following steps provide the details necessary to prepare the host for the installation of Windows Server 2012 Datacenter Edition. It is assumed that the SAN has been zoned and the VNX5400 has masked the LUN so that only a single path to server is available.

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

- Install Windows Server 2012 R2 on a single physical server with the boot volume on the EMC VNX5400
- Perform some initial configuration tasks that are common for all servers used in the private cloud.
 - Configure the management network
 - Update the installation with the latest patches from Microsoft Update
 - Install Windows Roles and Features
 - Present the boot LUN to both vHBAs and configure MPIO
 - Sysprep the image so other servers can be deployed more quickly
- Clone the sysprepped image for future use
 - Remove the boot volume from the server on which it was installed.
 - Make clones of the sysprepped volume within the EMC VNX5400 so each physical server will have its own clone to boot from.
- Complete build of other Infrastructure hosts
 - Configure zoning and masking for other servers.
 - Start each host and complete the mini-setup to tailor each node with things like name, IP addressing (if fixed IP addresses are used), and join to the domain). It is possible to configure this sort of information with unattend command files. That is beyond the scope of this document, and many shops already have such procedures in place.

Note: In order for the Windows Installer to recognize the Fibre Channel SAN boot disk for the initial server, the Cisco UCS fnic (storage) driver must be loaded into the Windows installer during installation. Please download the latest Unified Computing System (UCS) drivers from www.cisco.com under Cisco UCS B-Series Blade Server Software and place the ISO on the same machine with the Windows Server 2012 R2 installation media.

Open your browser and browse to the address of your Cisco UCS Manager console. Click **Continue to this website (not recommended)**. Or, you can also launch the Cisco UCS Manager from a PowerShell cmdlet on your configuration workstation that has PowerTool installed. The Start-UcsGuiSession cmdlet can take either an IP address or a DNS name.



`Start-UcsGuiSession -Name 10.29.130.100`

Click **Launch UCS Manager**.

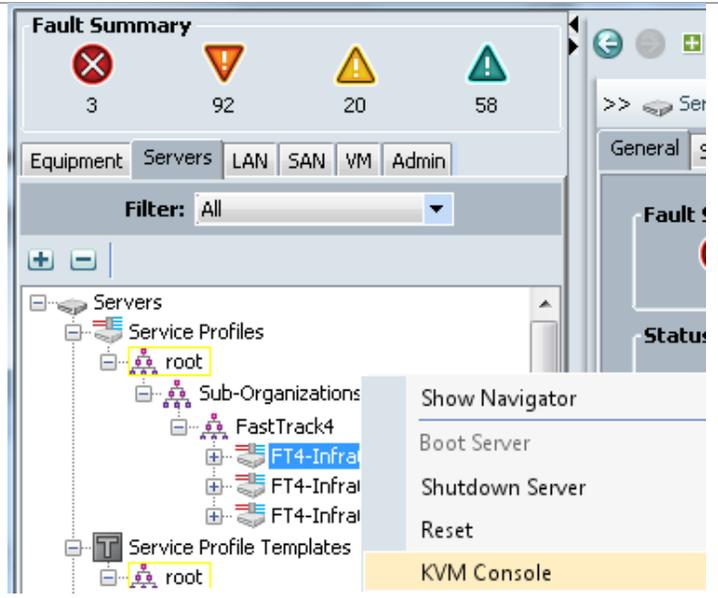


Enter admin as the user name. Enter the password specified in the initial setup.

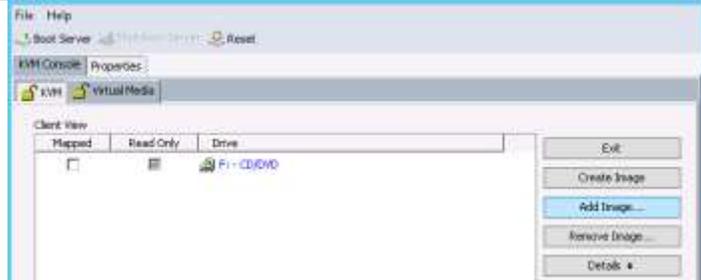


Select the **Servers** tab. Expand **Servers and Service Profiles** until you reach your first service profile. Right-click your first service profile and select **KVM Console** from the menu.

You will receive a number of Java and security warnings. Click through them until the KVM Console displays.

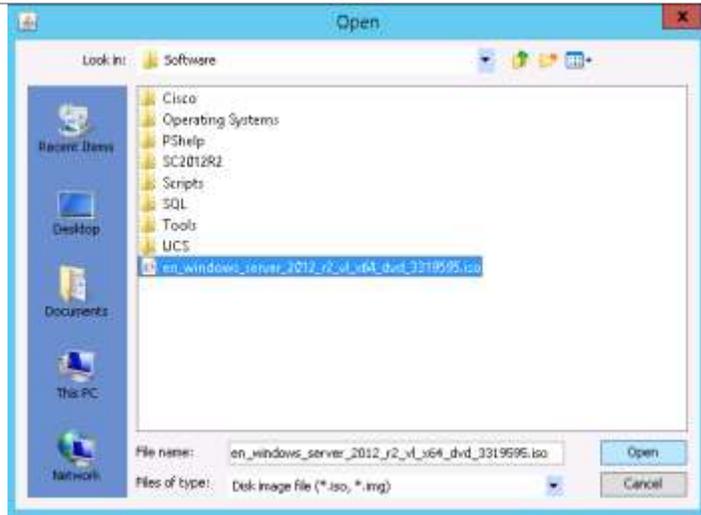


Select the **Virtual Media** tab and click **Add Image...**

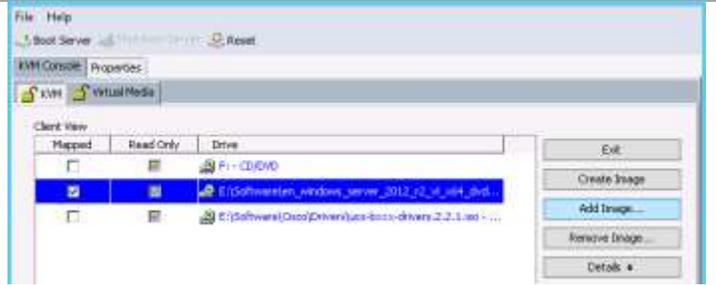


Browse to the location where you have stored the Windows Server 2012 R2 installation media on your configuration workstation. Select and open the media.

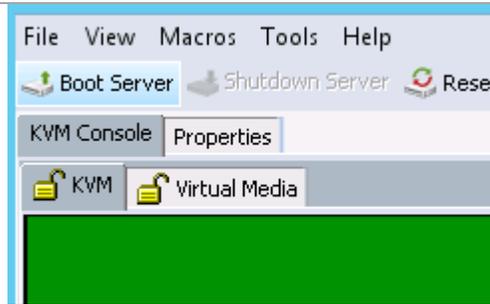
Repeat the process to add an image of the Cisco device driver installation media.



Click the check box by the Windows Server 2012 R2 installation media. Then click the **KVM** tab.



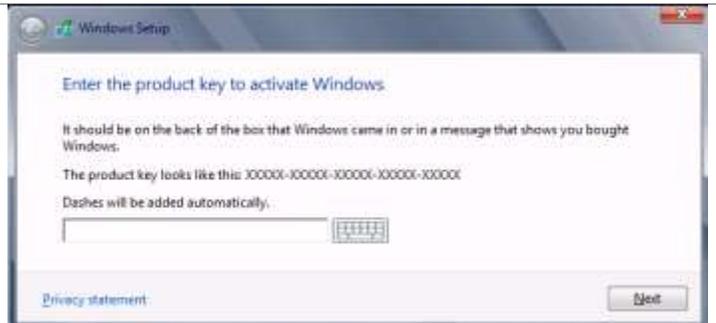
On the **KVM** tab, click **Boot Server** to boot the server. Click **OK** on the notification that you are turning on the server. The Cisco UCS blade will go through its startup and finally you will see the start of the Windows Server 2012 R2 installation.



Select the appropriate localization features and click **Next**. On the following screen click **Install Now**.

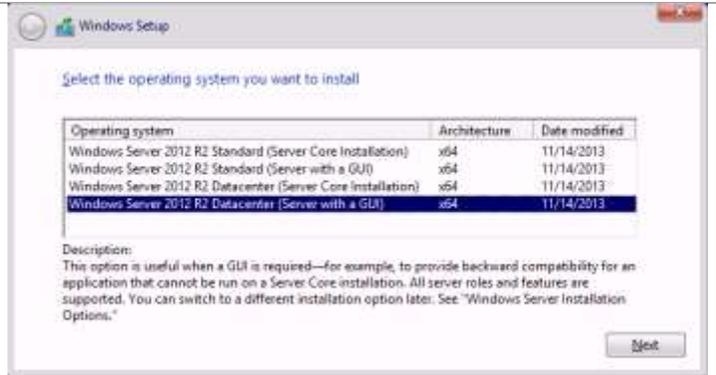


If you are using volume media, you will not see this screen for entering the activation code. If you are using Retail media, you will need to enter the activation code.

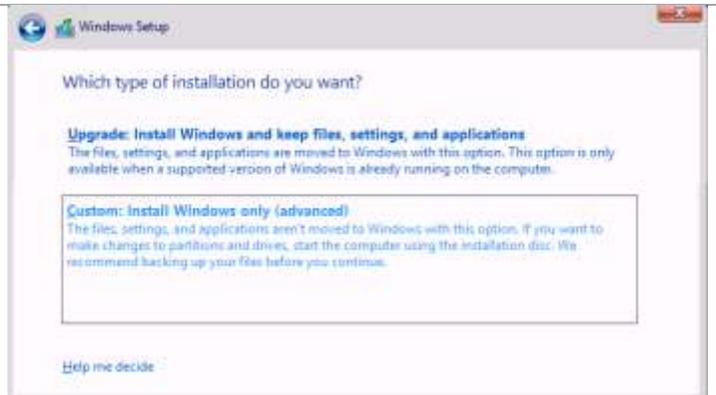


Select **Windows Server 2012 R2 Datacenter Server (with a GUI)**. As this server is going to be hosting multiple virtual machines, it is necessary to request the Datacenter Server for proper licensing. Click **Next** to continue. Accept the license terms on the following page.

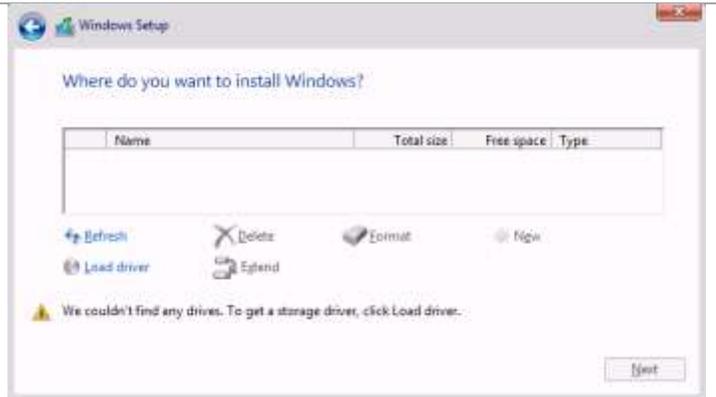
Note: This procedure assumes running installation and configuration steps from the console of the installed machine. If you are experienced with managing Windows Server remotely, you can select the Server Core Installation and perform configuration and management from the configuration workstation.



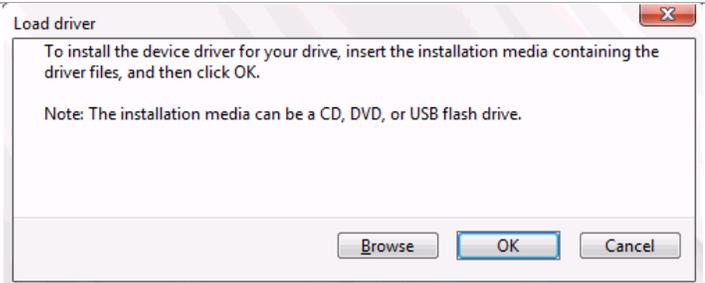
On the **Which type of installation do you want?** page select the **Custom: Install Windows only (advanced)** option.



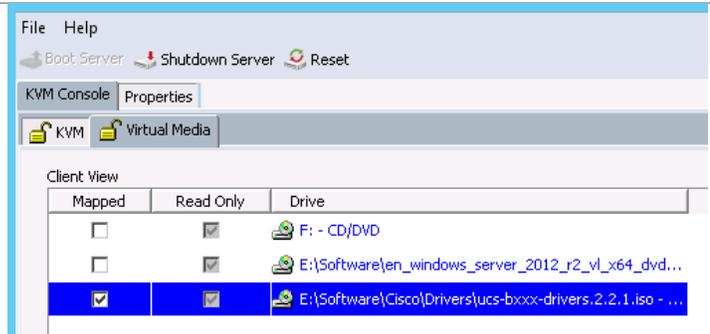
On the **Where do you want to install Windows?** page, the system will not find any disks on which to install the OS. This is because the Cisco drivers are not included in the Windows installation media. Click **Load driver**.



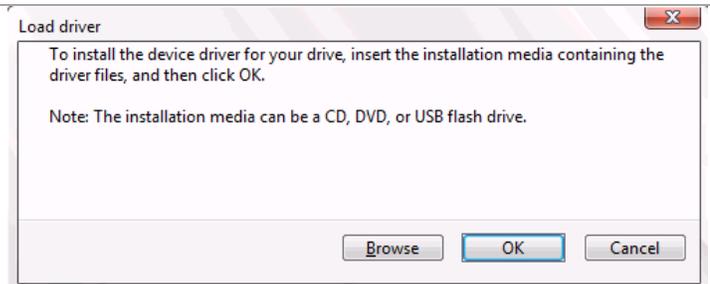
You will be presented with a **Load driver** page. Before working with this page, you must first mount the Cisco driver image.



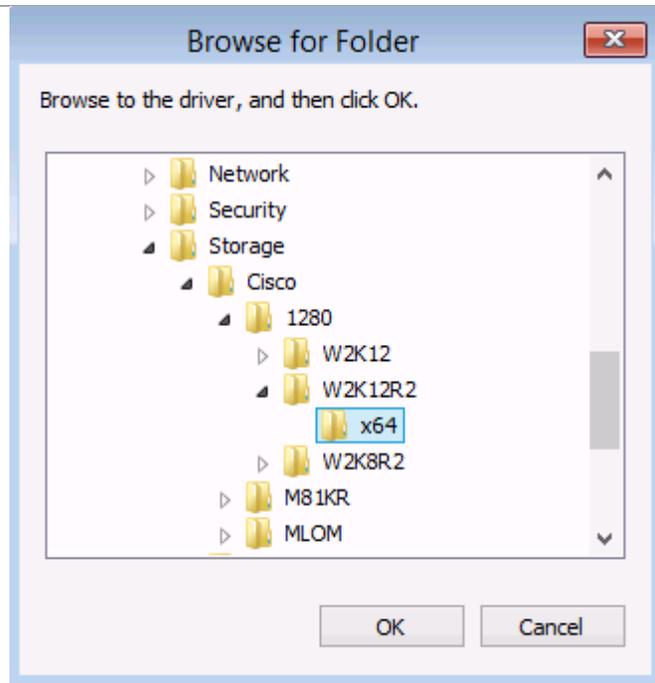
On the KVM console, select the **Virtual Media** tab. Uncheck the box by the Windows installation media. You will be presented with a warning message recommending to use the OS to dismount. Click **OK** to continue. Then check the box by the Cisco driver media. Click the **KVM** tab.



Back on the **Load driver** page, click **Browse**.

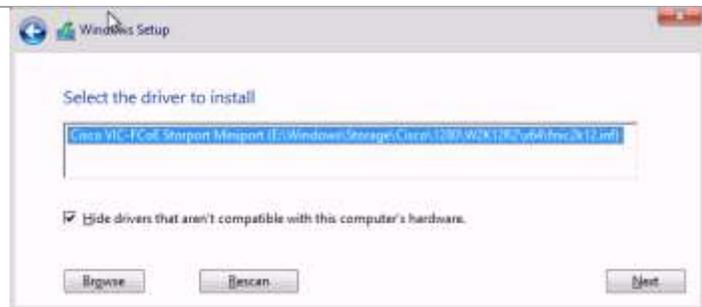


Expand the CDROM containing the Cisco driver media. Browse to **Windows > Storage > Cisco > 1280 > W2K12R2 > x64**. Click **OK** to continue.



On the **Select the driver to install** page, validate you have selected the proper driver and click **Next** to continue.

Note: It is recommended to repeat this process for the NIC driver. This Make sures those drivers are installed at this time and saves effort of loading them later.

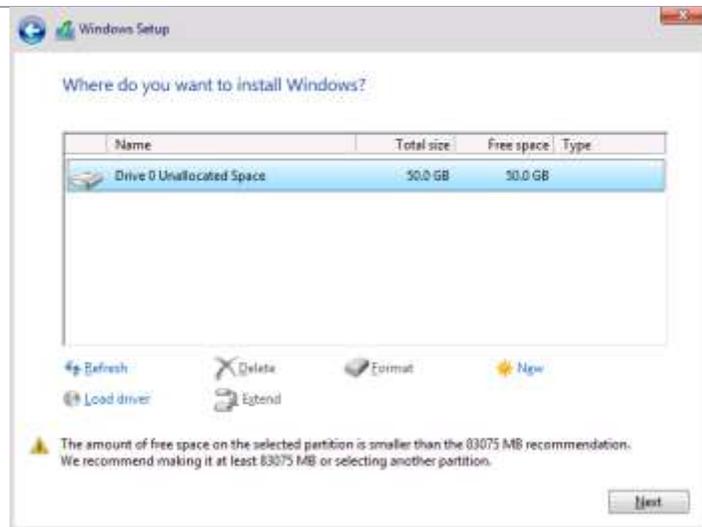


When the driver installation is complete, you will be returned to the **Where do you want to install Windows?** page. Return to the **Virtual Media** tab and re-select the Windows installation media. Back on the **KVM** tab, you might have to click **Refresh** on this screen to see the disk. Click **Next** to continue.

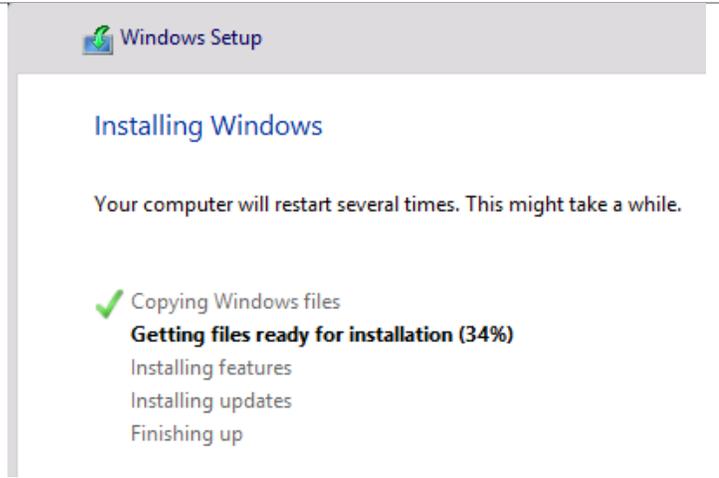
If you see more than one disk, you need to correct your zoning and masking to present only a single path to the boot LUN. Windows does not install properly if presented with a multi-pathed boot volume.

If you do not see any disks, you will need to check your zoning/masking.

Note: You can safely ignore the warning about not enough space to install. This is a bug in the Windows installation.



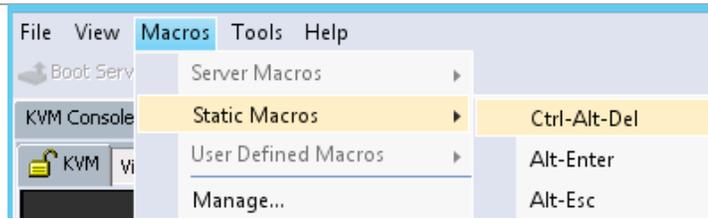
Windows will proceed with its initial setup. At the completion of this process, Windows will reboot. If you are watching, you will see a message on the screen to **Press any key to boot from CD or DVD...** Do not enter any key when you see this message or it will restart the installation process.



Enter a password for the local administrator account. Re-enter to validate. Click **Finish** to complete the installation.



Select **Macros** on the **KVM** console. From the drop down menu, select **Static Macros** and **Ctrl-Alt-Del** to bring up the Windows sign in screen.



Log into the new machine using the password entered in the previous step. Enter a carriage return after entering the password.



If you did not load the NIC drivers earlier, open a PowerShell window and issue the command to the right. The sample assumes the Cisco driver media is mounted on drive G:

```
pnputil -i -a G:\Windows\Network\Cisco\1280\W2K12R2\x64\enic6x64.inf
```

When finished with installing the device drivers, you can remove the installation media from the **Virtual Media** tab of the KVM, or dismount it from within Windows.

Local Configuration Tasks

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

Configure Management Network

From a PowerShell prompt, enter the `Get-NetAdapter` cmdlet. This will list the MAC addresses of the networks assigned within the operating system.

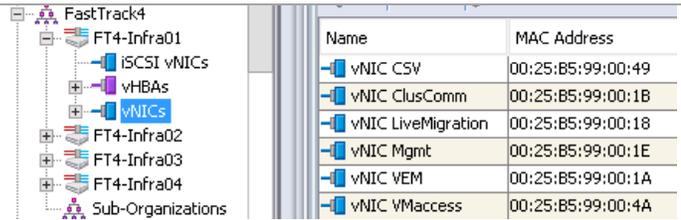
Get-Netadapter

```
PS C:\Users\administrator.VSPEX> Get-NetAdapter

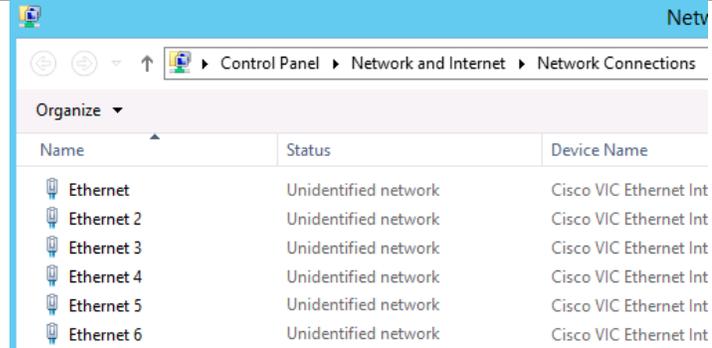
Name           InterfaceDescription      IfIndex Status      MacAddress
-----
Ethernet       Cisco VIC Ethernet Interf... 12 Up         00-25-B5-99-00-1E
Ethernet 2     Cisco VIC Ethernet Interf... #2 13 Up         00-25-B5-99-00-1A
Ethernet 3     Cisco VIC Ethernet Interf... #3 14 Up         00-25-B5-99-00-4A
Ethernet 4     Cisco VIC Ethernet Interf... #4 15 Up         00-25-B5-99-00-49
Ethernet 5     Cisco VIC Ethernet Interf... #5 16 Up         00-25-B5-99-00-1B
Ethernet 6     Cisco VIC Ethernet Interf... #6 17 Up         00-25-B5-99-00-1B

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

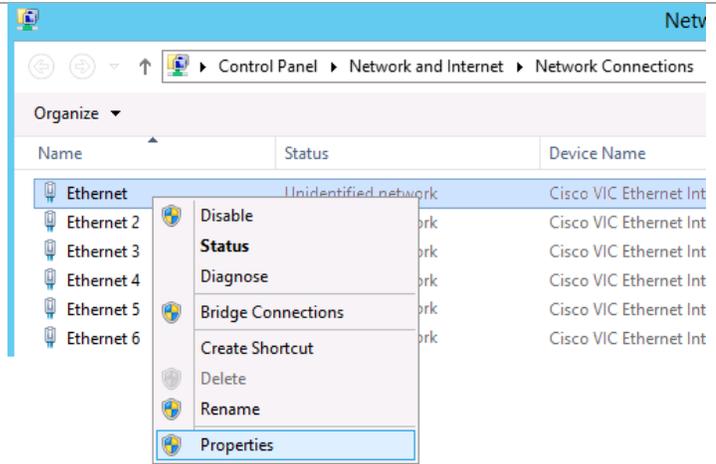
Within Cisco UCS Manager, expand the Service Profile for the machine, and select the vNICs to display the MAC addresses assigned by UCS.



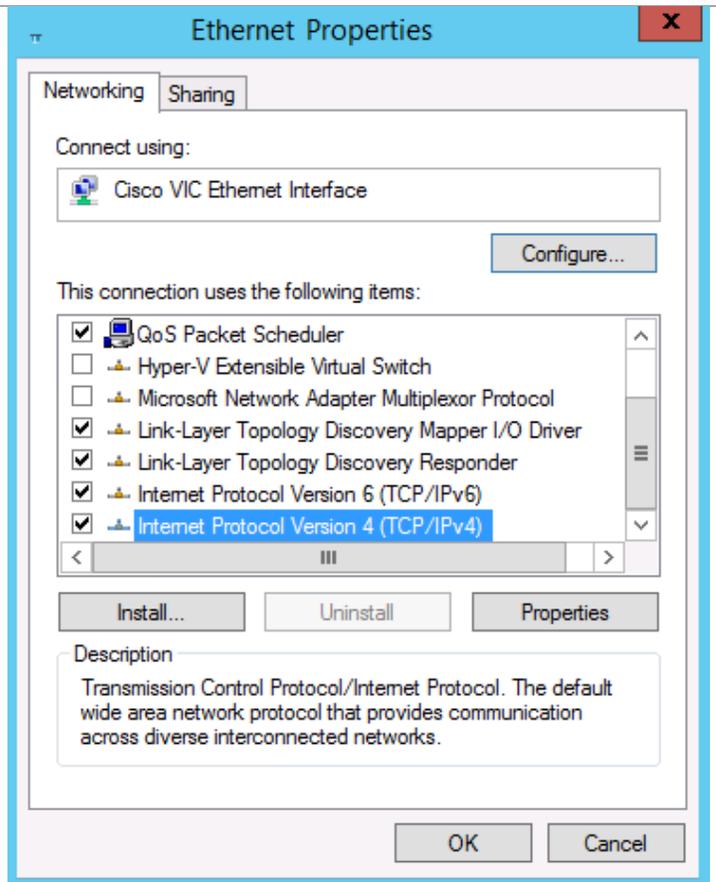
Find the MAC address for the host management NIC (Mgmt in this example). Open the Network Connections window by typing `ncpa.cpl` within the PowerShell window.



Right-click the NIC name with the matching MAC address and select **Properties**.



Scroll to the bottom of the list and select **Internet Protocol Version 4 (TCP/IPv4)**. Click **Properties** to open the window to configure the IP address for the host management network. This management network should allow access to either Windows Update on the Internet or to a local Windows Update Server in order to pull the necessary patches to bring it up to date.



Run Windows Update

It is highly recommended to fully patch the server at this time from Windows Update. Depending on the patches, it might be necessary to reboot and check for updates multiple times before the server is completely patched. This will save time by ensuring images built from this master image will not need to have as many patches applied. It is a good practice to periodically refresh your master image when more patches are released.

Install Windows Roles and Features

All hosts in the Private Cloud require the same set of base roles and features;

- Multi-port IO (MPIO)
- Failover Clustering
- Hyper-V

You can manually add the roles and features through **Server Manager > Manage > Add Roles and Features**, but the following PowerShell commands will perform the same function more quickly. This script adds MPIO feature and all the Product IDs used by EMC, adds the Failover Clustering feature, and then adds the Hyper-V role. Adding the Hyper-V role requires the system to reboot.

```
Write-Host "`nInstall the MPIO and Failover Clustering features and the Hyper-V role"
Write-Host -ForegroundColor Yellow "`nInstalling Hyper-V will cause the system to reboot`n"
Write-Host "`nInstalling the MPIO feature"
Install-WindowsFeature -Name Multipath-IO -IncludeManagementTools
Write-Host "Add new vendor and product IDs for MPIO"
# Values for EMC VNX
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "LUNZ"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "VDISK"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 0"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 1"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 10"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "RAID 5"
$trash = New-MSDSMSupportedHw -VendorId "DGC" -ProductId "VRAID"
Remove-MSDSMSupportedHw -Vendorid "Vendor 8" -Productid "Product 16"
Write-Host "List of configured vendor and product IDs"
Get-MSDSMSupportedHW | Select VendorId, ProductId | ft
Write-Host "`nInstalling the Failover Clustering feature"
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
Write-Host "`nInstalling the Hyper-V role"
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
```

Configure Paging File

Microsoft has a default formula for setting and managing the paging file. The size of the paging file is determined based upon the amount of physical memory configured on the server. The base amount of recommended memory for this solution is 256 GB. This results in a large amount of the system disk being allocated for use by the paging file.

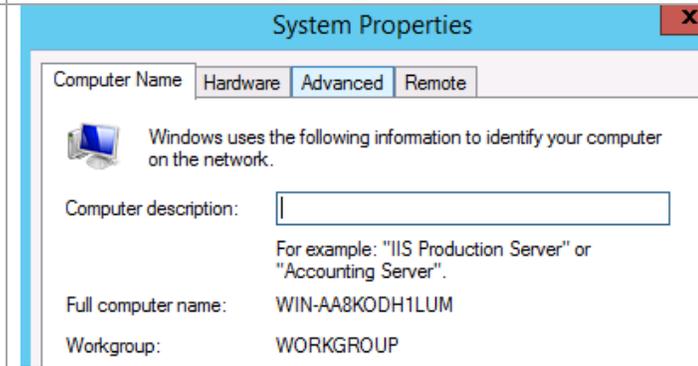
As most of the memory is allocated to VM usage, little of the overall memory is used by the Hyper-V host. That minimizes the actual amount of space needed for a paging file. Secondly, as the Hyper-V host is configured to make sure the proper amount of memory, the need to swap and/or page memory to the paging file is minimized. These factors combine to allow for a smaller paging file to be configured for the environment with no impact on the performance of the virtualized environment.

The following steps show how to set a paging file to a significantly smaller size.

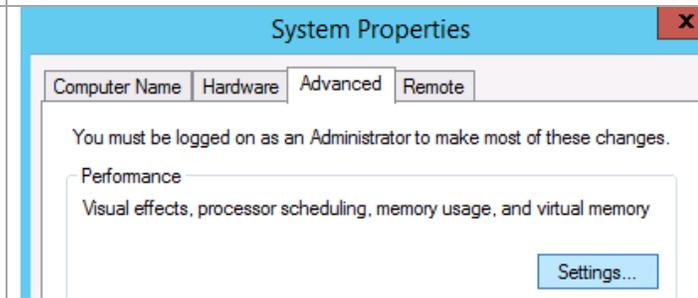
From **Server Manager** > **Local Server** click the **Computer Name**.



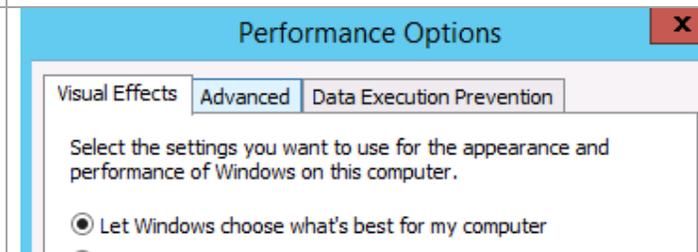
On the **System Properties** page, select the **Advanced** tab.



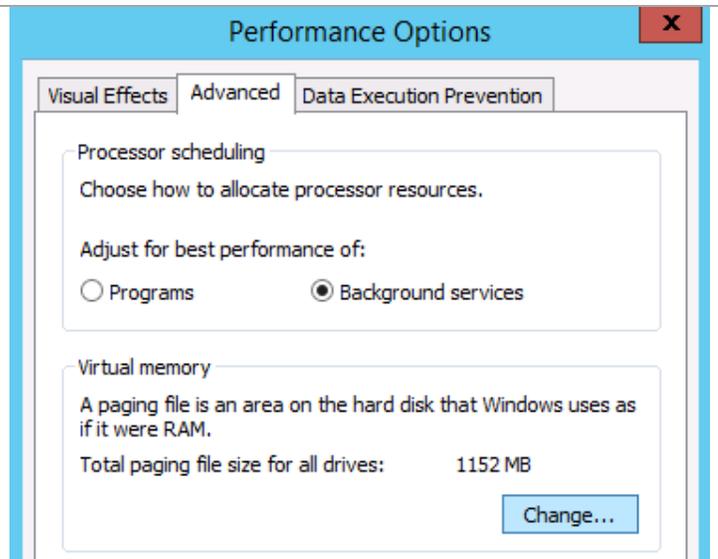
On the **Advanced** tab click **Settings...**



On the **Performance Options** page select the **Advanced** tab.



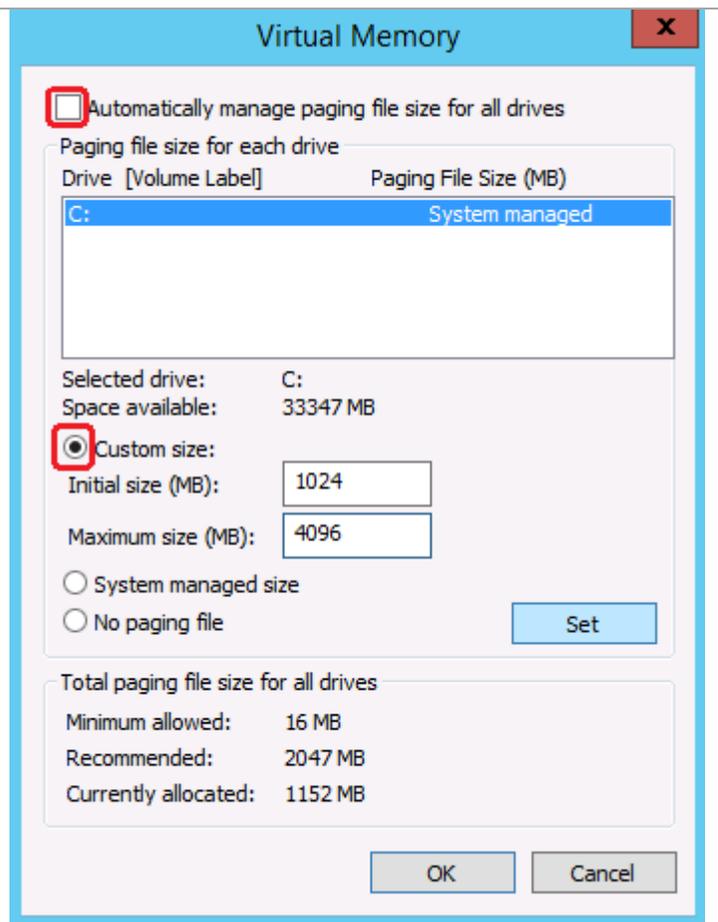
On the **Advanced** tab of the **Performance Options** page, click the **Change...** button.

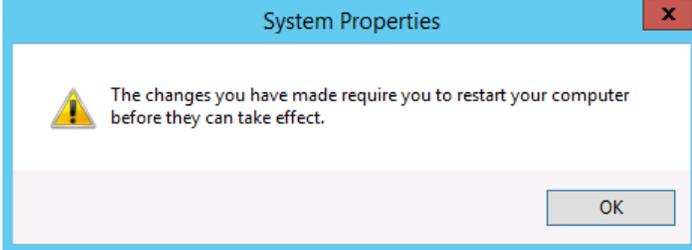
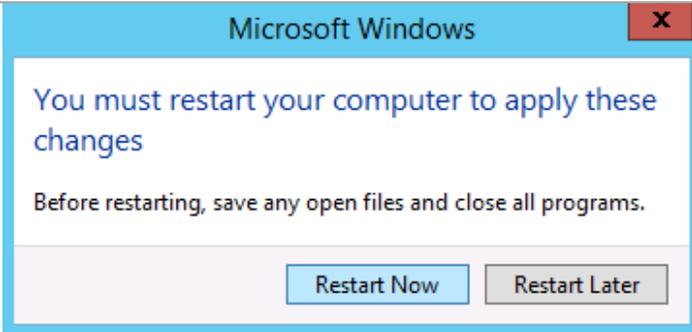


On the **Virtual Memory** page, uncheck the box by **Automatically manage paging file size for all drives**. This allows you to then select the radio button by **Custom size**: Since the systems are sized appropriately to minimize the need for paging during normal operations, a minimum page file can be created to capture a minimum memory dump should the system crash. Enter **1024** in the **Initial size (MB)**: box and **4096** in the **Maximum size (MB)**: box.

You must click the **Set** button for the change to take place.

Click **OK** to continue.



<p>Click OK on the System Properties window that displays. Click OK twice to exist the System Properties windows.</p>	
<p>Click Restart Now to accept the changes to the paging file.</p>	

Configure MPIO

After the server reboots from the previous step, it is necessary to present the additional paths to the boot LUN and configure MPIO. The goal here is to sysprep this operating system image then clone the LUN for use by all other physical servers. This means MPIO has to be configured only once. When the operating system image that will be used for booting the additional blades has MPIO configured, it is possible to configure paths through both Nexus switches for initial boot of the sysprepped image.

Note: It is not supported to configure EMC's PowerPath software before sysprepping an image. That is why Microsoft's MPIO software is configured. By configuring Microsoft's MPIO software before sysprepping and cloning the image, we enable a new server to be booted with all fabric paths defined.

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

Cisco Nexus 5548 A

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

```
configure terminal
zone name <FT4-Infra01> vsan 1
  device-alias <VNX5400-SPB-B0>
exit
zoneset activate name <VSPEX> vsan 1
--- The Nexus should respond with "Zoneset activation initiated. Check zone status."
copy running-config startup-config
```

Cisco Nexus 5548 B

```

configure terminal
zone name <FT4-Infra01> vsan 1
  member device-alias <FT4-Infra01-B>
  member device-alias <VNX5400-SPB-B1>
  member device-alias <VNX5400-SPA-A1>
  exit
zoneset name <VSPEX> vsan 1
  member <FT4-Infra01>
  exit.
zoneset activate name <VSPEX> vsan 1
--- The Nexus should respond with "Zoneset activation initiated. Check zone status."
copy running-config startup-config

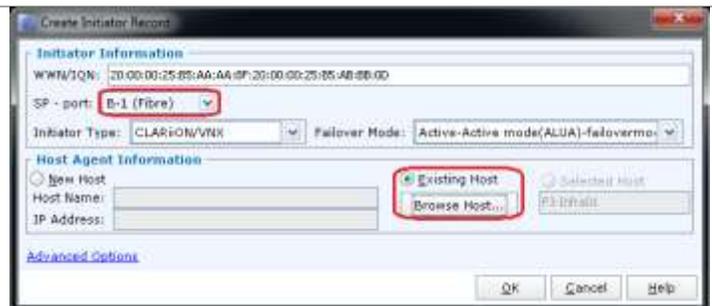
```

EMC VNX5400

When the zones and zonesets have been updated to reflect the multiple paths to the LUN, it is necessary to configure the EMC VNX5400 SAN to present the boot LUN to the additional paths.

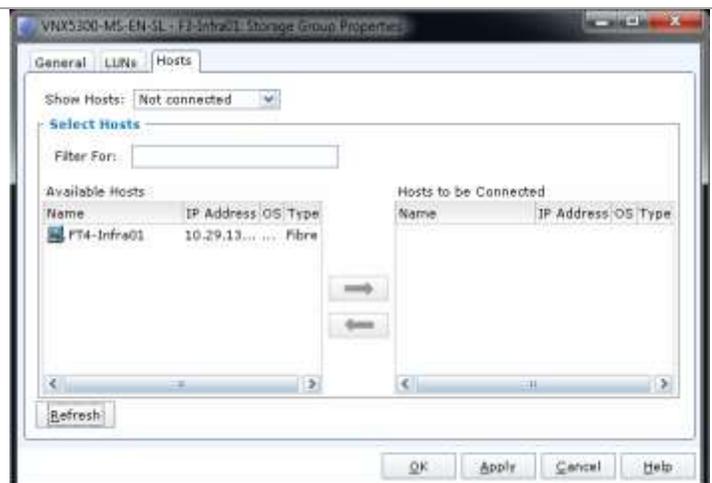
Power off the server before starting.

In Unisphere navigate to **Hosts > Initiators** and click the **Create** button to add a new initiator. The goal is to create an initiator to each port on the EMC VNX5400. You will have two initiator records for each WWNN and WWPN combination for the server. Select **CLARiiON/VNX** as the Initiator Type. Select the appropriate **SP-Port**. Select **Existing Host** then select the proper host.



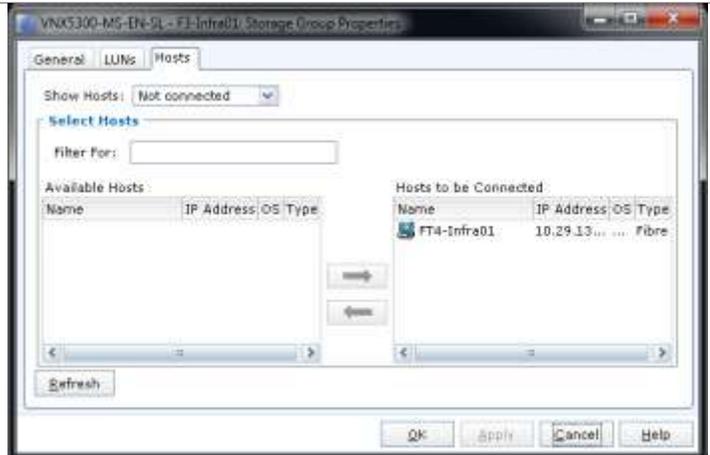
When all initiators are defined and registered, select **Hosts > Storage Groups**. Select the storage group for this server. Select the server from the **Hosts to be Connected** column and move it to the **Available Hosts** column. Click **Apply** to move the host to the Available Hosts column.

Note: When changing the number of paths available to a host, moving the host back and forth refreshes Unisphere to recognize the path changes.



Select the server from **Available Hosts** and move it to **Hosts to be Connected**. Click **OK** to continue.

Boot the server and log into the console.



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

```
PS C:\Users\Administrator> mpclaim -s -d 0
MPIO Disk0: 04 Paths, Round Robin with Subset, Implicit and Explicit
Controlling DSM: Microsoft DSM
SN: 6061602AD1310FCCF48945DABE211
Supported Load Balance Policies: F00 RRWS LQD WF LB

Path ID      State          SCSI Address      Weight
-----
0000000077020001 Active/Unoptimized 002|000|001|000  0
  TPG_State : Active/Unoptimized, TPG_Id: 2, : 12
0000000077020000 Active/Optimized  002|000|000|000  0
  * TPG_State : Active/Optimized, TPG_Id: 1, : 2
0000000077010001 Active/Optimized  001|000|001|000  0
  * TPG_State : Active/Optimized, TPG_Id: 1, : 1
0000000077010000 Active/Unoptimized 001|000|000|000  0
  TPG_State : Active/Unoptimized, TPG_Id: 2, : 11

PS C:\Users\Administrator>
```

Configure Other Common Criteria

In order to enable complete remote management of the server by using RSAT from another system, it is necessary to enable a number of firewall rules and configure some services. The following PowerShell script performs this function. Additionally, it enables the server to be accessed through a Remote Desktop Connection over the Remote Desktop Protocol.

Since these settings are affecting security settings, you should check with your security team to Make sure you these settings are allowed in your environment.

```

##### Make sure Server Manager remoting is enabled
Configure-SMRemoting.exe -Enable
##### Set some firewall rules
##### Enable ping requests in and out
Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-In" -Enabled True -Profile Any
Set-NetFirewallRule -Name "FPS-ICMP6-ERQ-In" -Enabled True -Profile Any
Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-Out" -Enabled True -Profile Any
Set-NetFirewallRule -Name "FPS-ICMP6-ERQ-Out" -Enabled True -Profile Any
##### Enable remote volume management - firewall rules need to be set on both
##### source and destination computers
##### ***NOTE*** Policy must also be set on system to "Allow remote access
##### to the Plug and Play interface"
##### This is done with gpedit.msc locally or gpedit for domain policy
Set-NetFirewallRule -Name "RVM-VDS-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RVM-VDSLDR-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RVM-RPCSS-In-TCP" -Enabled True -Profile Any
##### Enable DCOM management requests in
Try
{
    Set-NetFirewallRule -Name "ComPlusNetworkAccess-DCOM-In" -Enabled True -Profile Any
}
Catch
{
    Write-Host "ComPlusNetworkAccess-DCOM-In not set; assuming core installation"
}
##### Enable remote service management
Set-NetFirewallRule -Name "RemoteSvcAdmin-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteSvcAdmin-NP-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteSvcAdmin-RPCSS-In-TCP" -Enabled True -Profile Any
##### Enable Remote Event Log Management
Set-NetFirewallRule -Name "RemoteEventLogSvc-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteEventLogSvc-NP-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteEventLogSvc-RPCSS-In-TCP" -Enabled True -Profile Any
##### Enable Remote Scheduled Tasks Management
Set-NetFirewallRule -Name "RemoteTask-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteTask-RPCSS-In-TCP" -Enabled True -Profile Any
##### Enable Windows Firewall Remote Management
Set-NetFirewallRule -Name "RemoteFwAdmin-In-TCP" -Enabled True -Profile Any
Set-NetFirewallRule -Name "RemoteFwAdmin-RPCSS-In-TCP" -Enabled True -Profile Any
##### Enable WMI management requests in
Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP" -Enabled True -Profile Any
##### Enable Remote Shutdown
Set-NetFirewallRule -Name "Wininit-Shutdown-In-Rule-TCP-RPC" -Enabled True -Profile Any
##### Enable Network Discovery on the Domain Network
Set-NetFirewallRule -Name "NETDIS-FDPMHOST-In-UDP" -Enabled True -Profile Domain
Set-NetFirewallRule -Name "NETDIS-FDPMHOST-Out-UDP" -Enabled True -Profile Domain
##### Set some services to automatically start and start them.
Set-Service -Name PlugPlay -StartupType Automatic
Start-Service PlugPlay
Set-Service -Name RemoteRegistry -StartupType Automatic
Start-Service RemoteRegistry
Set-Service -Name vds -StartupType Automatic
Start-Service vds
##### Enable Remote Desktop
(Get-WmiObject Win32_TerminalServiceSetting -Namespace
root\cimv2\TerminalServices).SetAllowTsConnections(1,1) | Out-Null

```

```
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace root\cimv2\TerminalServices -Filter "TerminalName='RDP-tcp']").SetUserAuthenticationRequired(0) | Out-Null
##### Enable Remote Desktop rules for all profiles
Set-NetfirewallRule -Name "RemoteDesktop-UserMode-In-TCP" -Enabled True -Profile Any
Set-NetfirewallRule -Name "RemoteDesktop-UserMode-In-UDP" -Enabled True -Profile Any
```

At this time you should implement any standard configuration items that are required by the organization to be on all servers. This may be an anti-malware product or a management agent or other system settings. They will vary from one organization to another.

Sysprep the Image

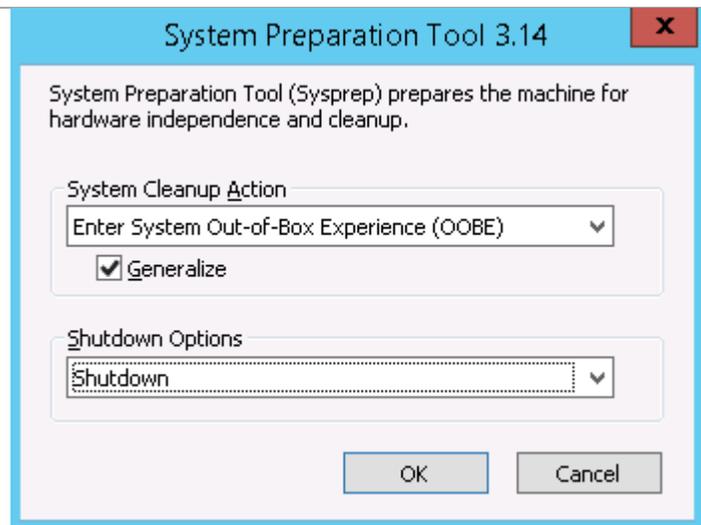
When the image is configured with all the base components that should be included in each image, Microsoft's sysprep utility is run to create an image to be used for cloning to quickly provision physical hosts needed in the private cloud environment.

From an elevated command window, enter the command
c:\windows\system32\sysprep\sysprep.exe.

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

Select **Enter System Out-of-Box Experience (OOBE)** from the System Cleanup Action drop down menu. Select the **Generalize** box. Select **Shutdown** from the Shutdown Options drop down menu. Click **OK** to perform the system preparation.

When the KVM console shows the physical server has shut down, LUN clones can be made for use by other physical servers.

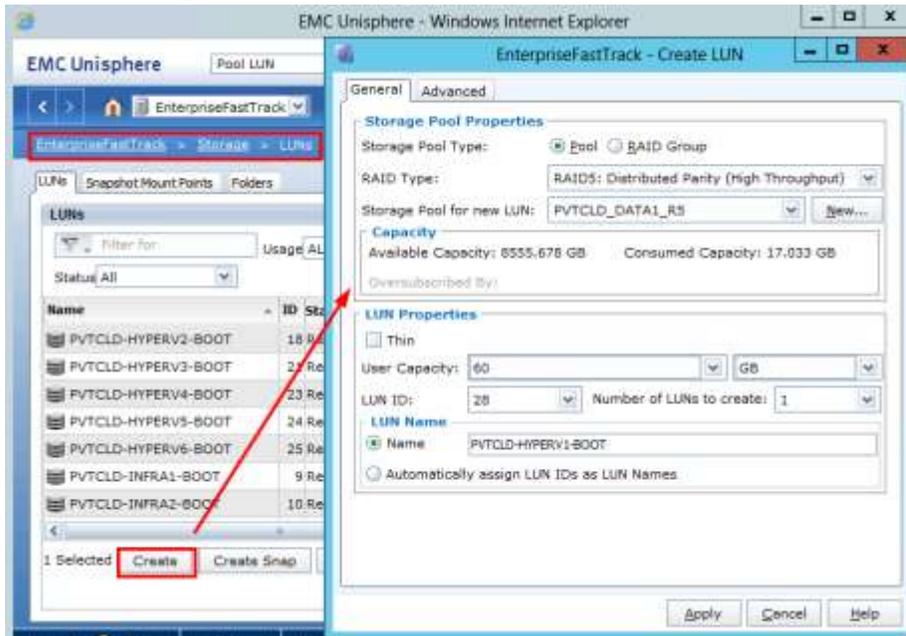


Clone Newly Created Image

After installation of the Windows Server instance and execution of the sysprep process, it is necessary to remove the source LUN from the Service Profile that was used to build the image. To remove the LUN from the Service Profile, use Unisphere to remove the Master_Boot LUN and the assigned host from its storage group. You may also want to remove the host initiator entries for the Master_Boot if you are using a different naming convention for production servers.

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

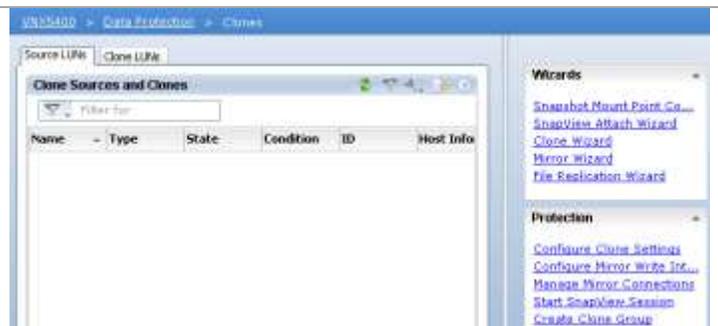
Create Target LUNs



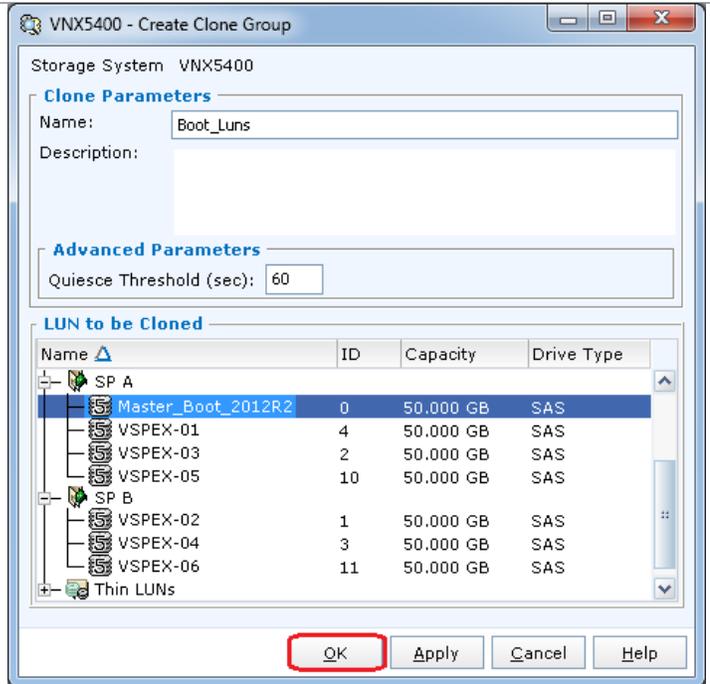
Create Clone LUNs

The following procedure can be performed from EMC Unisphere to create the clone relationship and copy the data from the master LUN to the boot target LUNs.

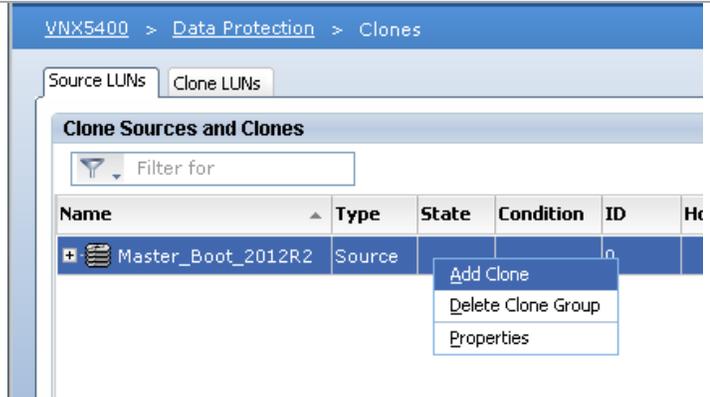
Navigate to **Data Protection > Clones** within Unisphere. Select **Create Clone Group** from the Protection side-bar.



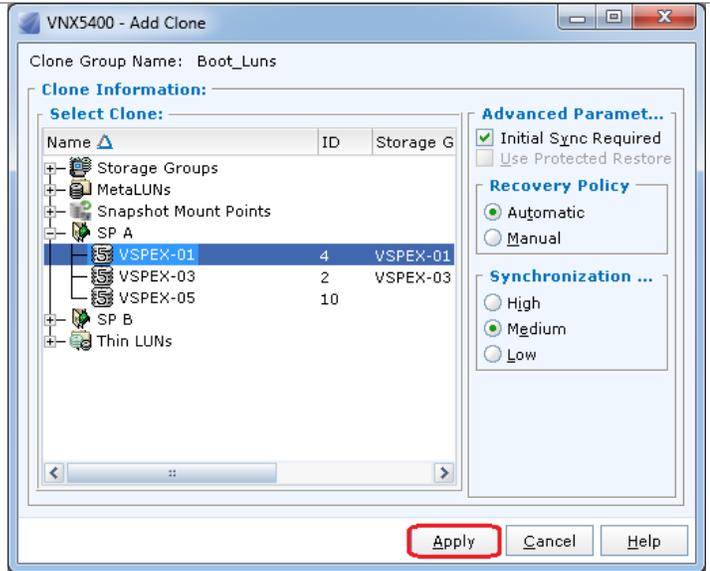
Provide a name for the Clone Group and select the master boot image LUN as the **LUN to be Cloned**. Select **OK**. After reviewing the confirmation page, select **Yes** and **OK** after the group creation returns with success.



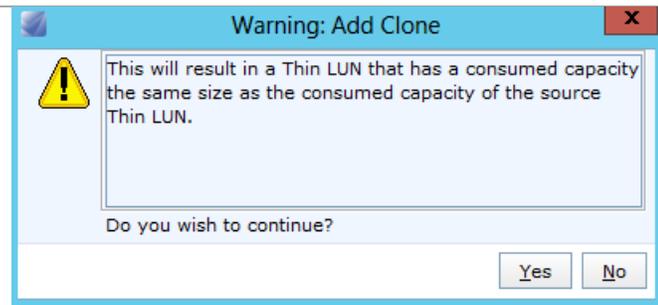
Right-click the newly created **Clone Source** and select **Add Clone**.



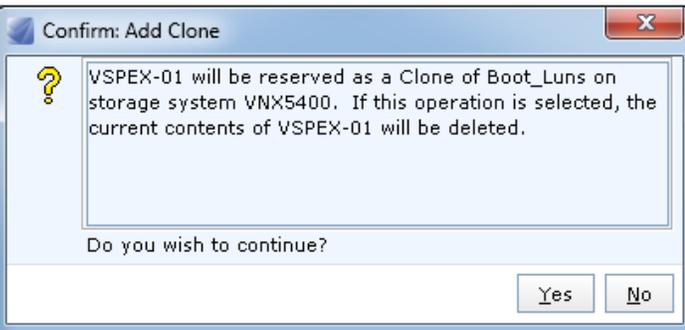
Select the appropriate clone target LUN intended for boot from SAN and select **Apply**.



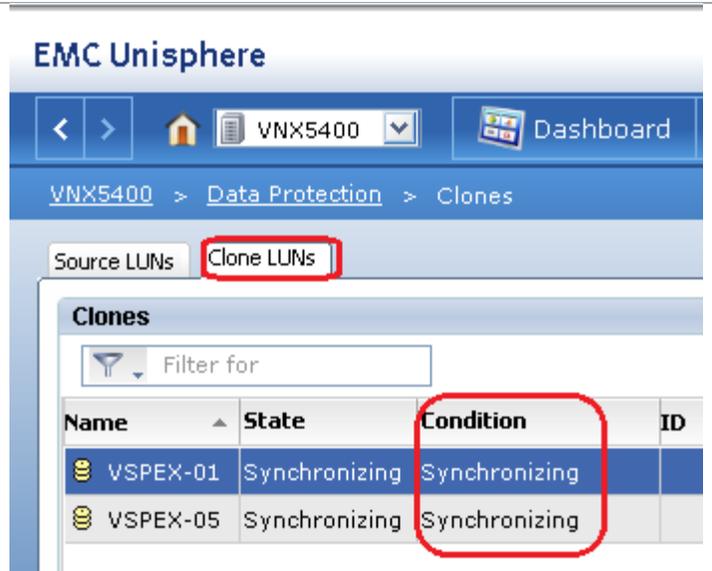
When replicating between LUNs, the following warning will pop up. Select **Yes**.



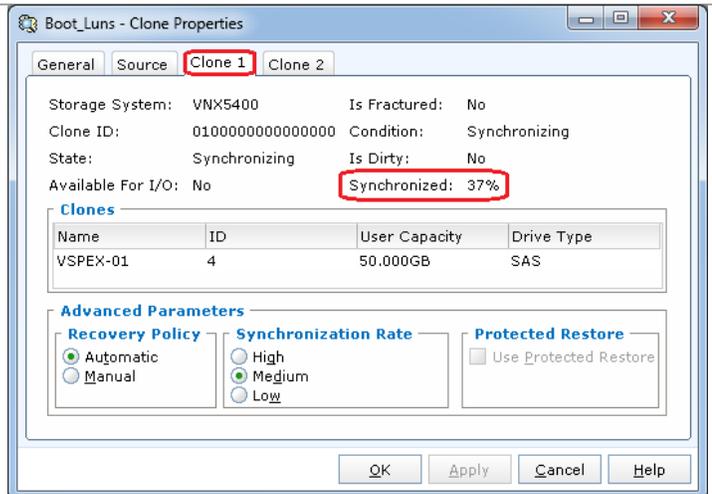
Confirm the target LUN will be overwritten by selecting **Yes**. Select **OK** after the successful addition of the clone. Repeat the previous steps to add the desired number of clone copies. Up to 8 can be added concurrently.



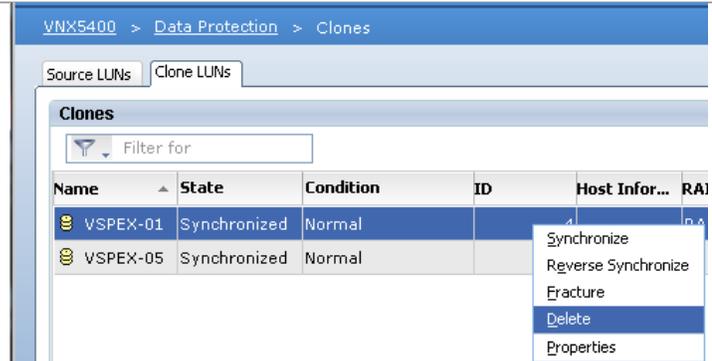
Verify the clones are synchronizing from the **Clone LUNs** tab.



To get more detail on synchronization, Right-click a clone LUN and select **Properties**. Each clone will have its own tab. Within each tab will be a **Synchronized** percentage. Wait for all clones to get to a **Synchronized** state before continuing.

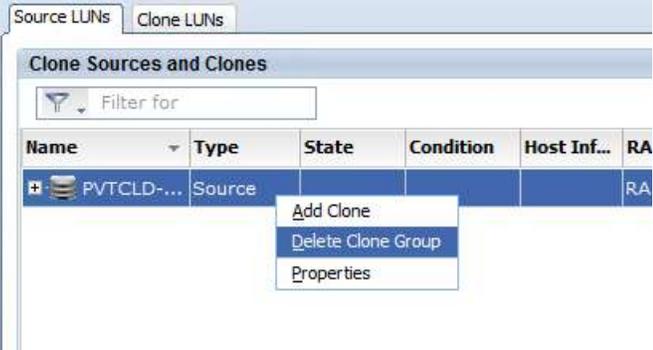


Delete each fractured clone. Select one clone at a time, right-click, and select **Delete**. Select **OK** following the successful deletion.



Optionally delete the clone group from the **Source LUNs** tab, right-click the group and select **Delete Clone Group**. Confirm the deletion by selecting **Yes** on the following screen. This completes the cloning process.

Note: It is recommended to keep this clone group to speed deployment of subsequent servers as your needs expand.



Build Infrastructure Servers

When a clone of the sysprepped LUN has been created for each physical server to be built, you need to zone and mask the LUN before completing a build from the cloned, sysprepped image.

Configure Zoning and Masking

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

Zoning

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

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

```
sjc2-151-E21-5548-A(config)# sho zoneset name VSPEX
zoneset name VSPEX vsan 1
  zone name VSPEX-02 vsan 1
    pwwn 20:00:00:25:b5:99:00:43 [VSPEX-02-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]

  zone name VSPEX-03 vsan 1
    pwwn 20:00:00:25:b5:99:00:45 [VSPEX-03-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]

  zone name VSPEX-04 vsan 1
    pwwn 20:00:00:25:b5:99:00:47 [VSPEX-04-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]

  zone name VSPEX-05 vsan 1
    pwwn 20:00:00:25:b5:99:00:49 [VSPEX-05-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]

  zone name VSPEX-06 vsan 1
    pwwn 20:00:00:25:b5:99:00:4b [VSPEX-06-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]

  zone name VSPEX-01 vsan 1
    pwwn 20:00:00:25:b5:99:00:41 [VSPEX-01-A]
    pwwn 50:06:01:65:08:60:06:a1 [VNX5400-SPA-A-5]
    pwwn 50:06:01:6d:08:60:06:a1 [VNX5400-SPB-B-5]
sjc2-151-E21-5548-A(config)#
```

Masking

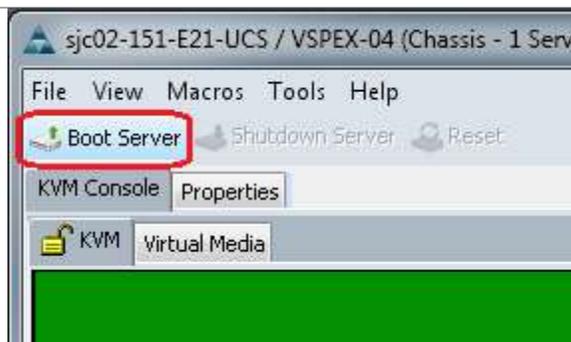
Following the cloning and zoning processes, the boot LUNs can be presented to their respective service profiles. Use the Unisphere management GUI as outlined previously in the “Mask Boot LUN with EMC Unisphere” section. Following the masking operations, start each host and complete the mini-setup to tailor each node with things like name, IP addressing (if fixed IP addresses are used), and join to the domain.

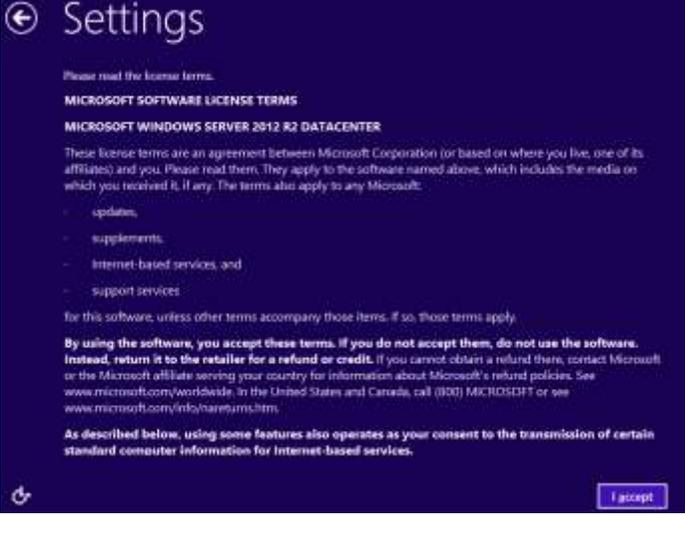
Complete Mini-Setup

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

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

Use the Cisco UCS Manager console to connect to the selected server using **KVM**. Select the option to **Boot Server**.



<p>Make any necessary changes to the Region and Language settings. Click Next to continue.</p>	
<p>Click the box next to I accept the license terms for using Windows. Click Accept to continue.</p>	
<p>Enter a complex password and re-enter it to validate its proper entry. Click Finish to complete the mini-setup.</p>	

At this point, you will have a complete base image. This means you will need to perform several items that will vary from site to site.

- Activate Windows – if using Microsoft’s Key Management Service (KMS) this can happen automatically. If using non-volume media or Microsoft’s Multiple Activation Key (MAK), manual steps are required.
- Rename the computer and join the computer to the Active Directory Domain (sample PowerShell below)
- Any other company-specific required tailoring

As these are not unique to the private cloud, they are not covered in this document.

The following is a sample PowerShell script to rename computer and join to domain:

```
#Rename the server and join it to the domain
$creds = Get-Credential -Message "Provide credentials to join this server to the domain"
Add-Computer -DomainName <domain> -Credential $creds -NewName <new-name> -Force
Write-Host "The server will reboot in 5 seconds to finish the configuration. If the server
doesn't reboot, press Ctrl-c"
Sleep -Seconds 5
Write-Host "      Rebooting..."
#Rebooting the server
Restart-Computer -Force -Confirm:$false
```

Configure Networks and Virtual Switches

Networks

It is recommended that you rename the network adapters from the Windows default values of “Ethernet #x” to match the vNIC name from the UCS Service Profile. You can use the manual procedure defined earlier in the document, or you can use the sample PowerShell script that follows. This script requires that the target machine is domain-joined and the script is run from a configuration workstation in the same domain that has the Cisco UCS PowerTool installed. The script makes use of a variable to define the address of the UCS Manager console. It must be modified to reflect the customer environment.

```

# Import required modules
If ((Get-Module |where {$_.Name -ilike "CiscoUcsPS"}).Name -ine "CiscoUcsPS")
{
    Write-Host "Loading Module: Cisco UCS PowerTool Module"
    Import-Module CiscoUcsPs
}

$trash = set-ucspowertoolconfiguration -supportmultipledefaultucs $false

##### Variables to be tailored to customer environment ###
$UcsmAddress = "192.168.10.100"

# Connect to UCSM
Write-Host -ForegroundColor DarkYellow "`nEnter credentials for UCS Manager`n"
$ucsCreds = Get-Credential
$UCSMHandle = Connect-Ucs $UcsmAddress $ucsCreds

# Get Name of server to work on
Write-Host "Enter server on which to rename default NIC names"
Write-Host "The name of the server and the name of the UCS Service Profile must be the same"
$Srvr = Read-Host "`nNOTE: Case must be EXACTLY the same as the UCS Service Profile"
$Org = Read-Host "`nEnter Sub-Organization name of Service Profile, or 'root'"
If ($org.Length -eq 0) {$org = "root"}
$OrgLevel = Get-UcsOrg -Name $Org
$SrvrProfile = $OrgLevel.DN + "/" + $Srvr

# Retrieve table of NICs from the UCS Profile
$ucsAdapters = Get-UcsVnic -ServiceProfile $SrvrProfile
$remAdapters = Invoke-Command -ComputerName $Srvr {Get-NetAdapter}

ForEach ($ucsA in $ucsAdapters) {
    $ucsMac = $ucsA.Addr -replace ":", "-"
    ForEach ($remA in $remAdapters) {
        If ($ucsMac -eq $($remA.MacAddress))
        {
            If ($ucsA.Name -ne $remA.name)
            {
                $tmp = $($remA.ifDesc).Contains("Hyper-V Virtual Ethernet")
                If ($tmp -eq $false)
                {
                    $old = $remA.Name; $new = $ucsA.Name
                    Write-Host "Changing NIC $old to be named $new - MAC $($remA.MacAddress)"
                    Invoke-Command -ComputerName $Srvr {param($old, $new)Rename-NetAdapter -Name
$old -NewName $new} -args $old,$new
                    break
                }
            }
        }
    }
}

Disconnect-Ucs

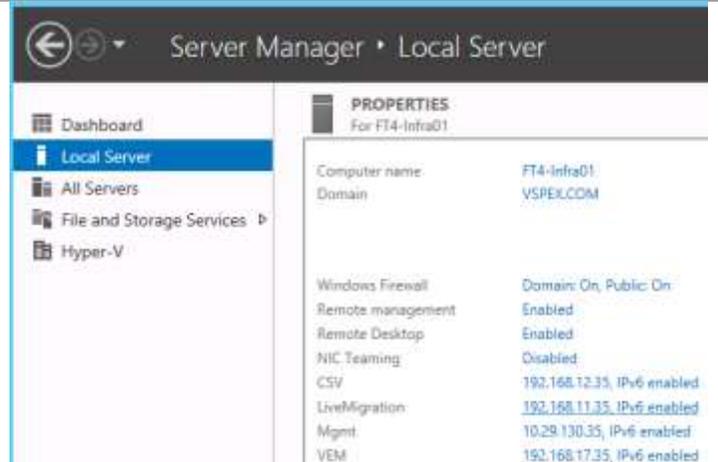
```

This document assigned static IP addresses to all NICs, but Microsoft products will work with all systems using DHCP addresses.

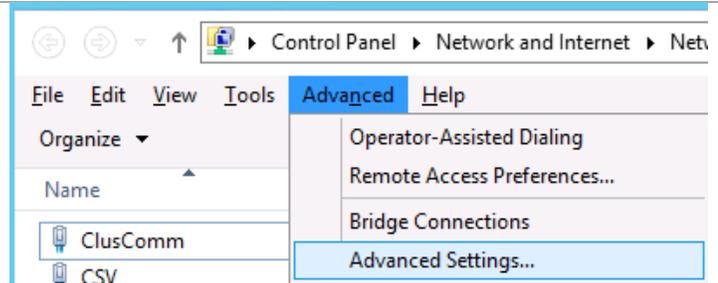
You should make the management network, the network on which domain communications occur, the first network in the network binding order. This procedure is run locally on each server.

Note: If using a Windows Server 2012 R2Core installation, either use the nvspsbind tool to change the order with this command line tool, or temporarily add the GUI to the 2012 R2 installation in order to use the following steps.

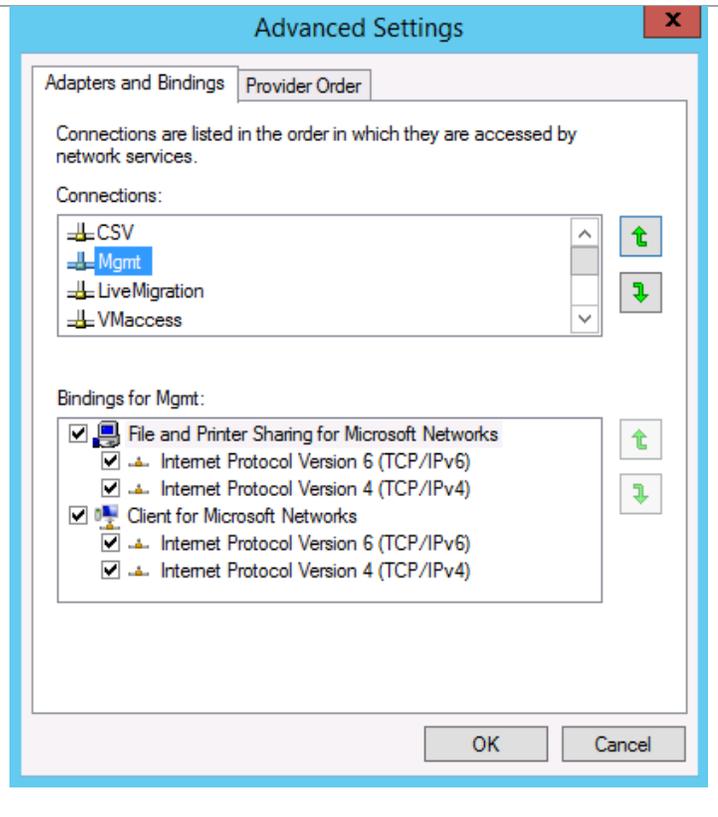
On the **Server Manager** console, clicke of the networks to launch the **Network Connections** control panel.



On the **Network Connections** window, depress the **Alt** key to bring up the menu. Select **Advance > Advanced Settings...**



Select the network you want to be first in the binding order and use the up arrow key on the right to move the network to the top of the list. Click **OK** to continue.



Hyper-V Virtual Switches

Hyper-V virtual switches can be configured either through the Hyper-V Manager console or by using PowerShell. The following PowerShell script assumes that you have previously renamed all the vNICs to match the names in the service profile. It is also designed to be executed from the configuration workstation, so it asks for the system which will be targeted.

```
$srvr = Read-Host "Enter name of host on which to create virtual switches"
New-VmSwitch -Name "ClusComm" -NetAdapterName "ClusComm" -Computername $srvr
New-VmSwitch -Name "VEM" -NetAdapterName "VEM" -Computername $srvr
New-VmSwitch -Name "VMaccess" -NetAdapterName "VMaccess" -Computername $srvr
```

Use the Hyper-V Manager console to create virtual switches. These instructions assume you are running the from the configuration workstation.

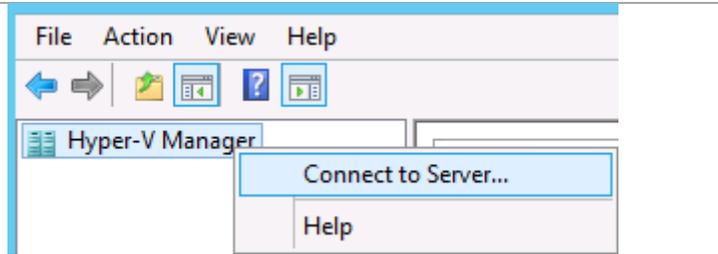
Determine the network adapter name and descriptions on the target computer by executing the following PowerShell cmdlets:

```
$sess = New-CimSession -Computername <server>
Get-NetAdapter -CimSession $sess
```

```
PS C:\Users\Administrator.VSPEX> $sess = New-CimSession -ComputerName FT4-Infra01
PS C:\Users\Administrator.VSPEX> Get-NetAdapter -CimSession $sess
```

Name	InterfaceDescription	ifIndex	Status
LiveMigration	Cisco VIC Ethernet Interface #6	20	Up
VMaccess	Cisco VIC Ethernet Interface #5	19	Up
VEM	Cisco VIC Ethernet Interface #1	18	Up
ClusComm	Cisco VIC Ethernet Interface #2	16	Up
CSV	Cisco VIC Ethernet Interface #4	12	Up
Mgmt	Cisco VIC Ethernet Interface	15	Up

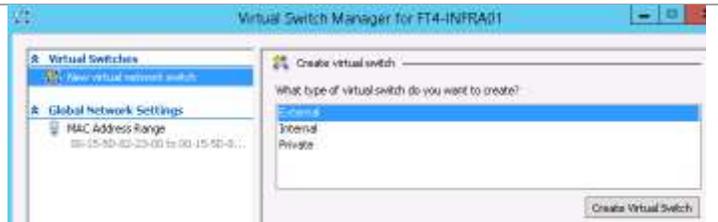
Launch the Hyper-V Manager console. Right-click Hyper-V Manager and select **Connect to Server...** Add the hosts on which you will be creating virtual switches.



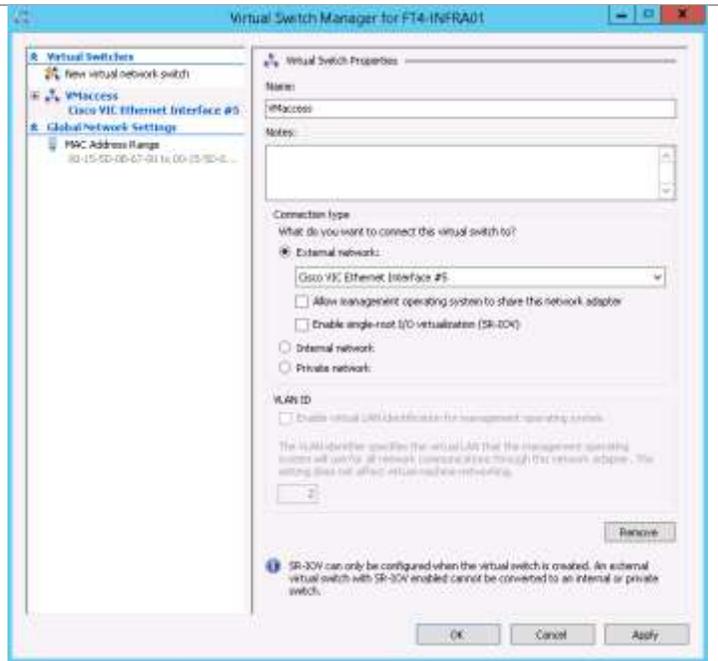
Select the server for which you have previously executed the Get-NetAdapter cmdlet. Select **Virtual Switch Manager...** under **Actions**.



On the **Virtual Switch Manager** page, Make sure you have select **New virtual network switch** under Virtual Switches and **External** under Create Virtual Switch. Click the **Create Virtual Switch** button.



On the **Properties** of the virtual switch, enter a **Name** – recommended to name it the same as the vNIC name. Make sure the radio button for **External network** is selected. From the drop down list, select the description of the vNIC on which you are creating this virtual switch. Uncheck the box for **Allow management operating system to share this network adapter**.



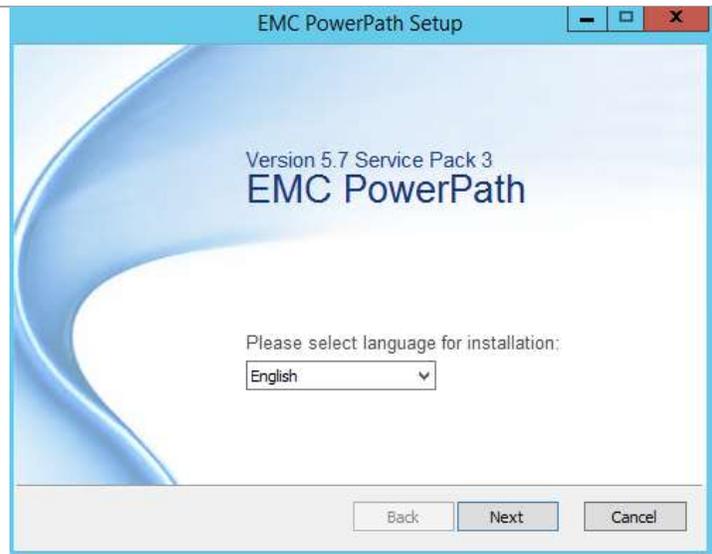
Repeat previous step and this step for all virtual switches. When complete, click **OK** to create all the switches.

Install EMC PowerPath

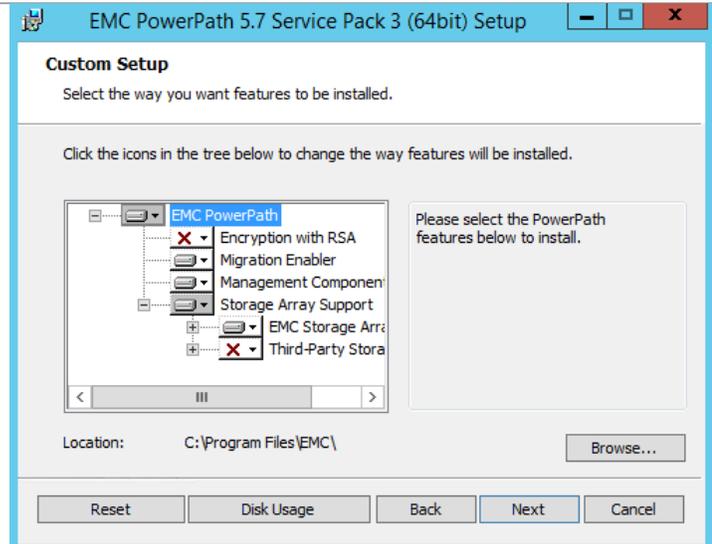
Each system should have EMC PowerPath installed for enhanced multi-pathing capabilities. EMC PowerPath for Windows version 5.7 SP2 or higher should be used. This process must be performed on each host.

► Perform this installation on each Hyper-V host server.

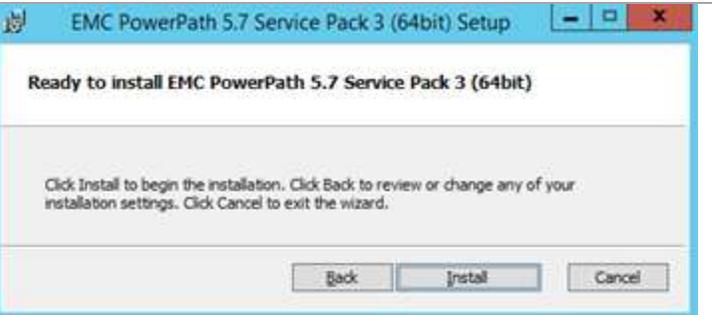
Launch the EMC PowerPath installer, EMCPower.X64.signed.5.7.b223.exe. Click **Next** to continue. Click **Next** on the following copyright information screen.



Accept the default feature installation options and click **Next**.

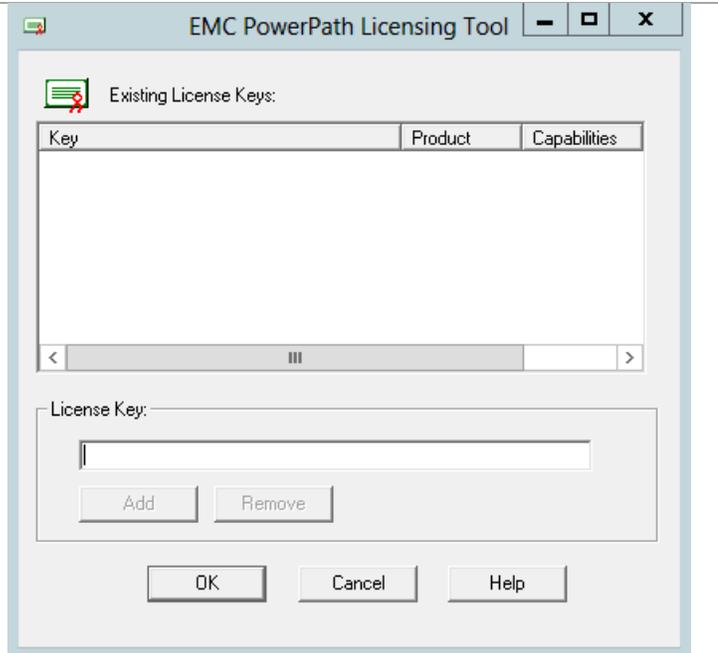


On the **Ready to install EMC PowerPath 5.7 (64-bit)** page click **Install**.

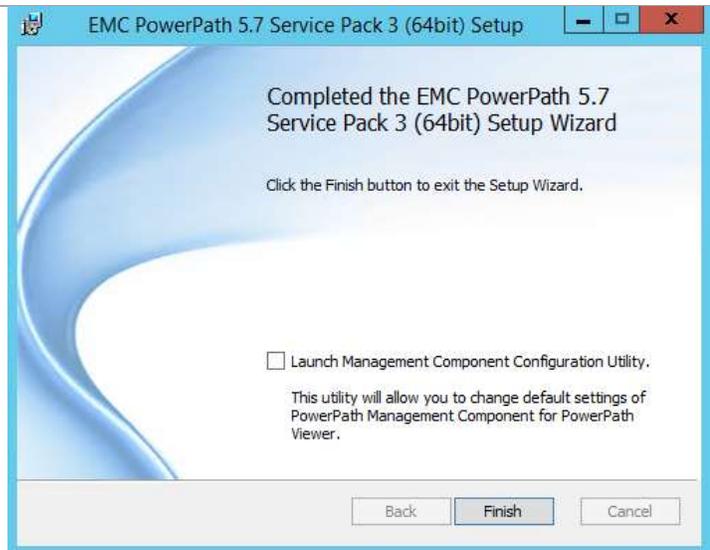


On the **EMC PowerPath Licensing Tool** page, enter the appropriate license key for your environment and select **OK**. If an appropriate license is not installed, PowerPath should not be installed and Microsoft's MPIO should be used.

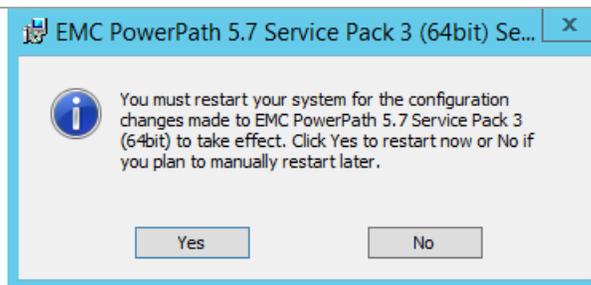
Note: If no license key is entered, PowerPath will be unlicensed and will run in a "basic failover" mode, which allows two storage port connections to one HBA. The other HBA will be marked as unlicensed.



On the completion page, click **Finish** to complete the installation.



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



Install EMC Unisphere Host Agent

The Unisphere Host Agent allows for host specific information to be sent to management applications, like Unisphere, for ease of administration. LUN mapping and Operating System information as well as initiator information can be forwarded from a server to the VNX through the agent. Follow the procedure below to install the Unisphere Host Agent on either a physical Windows Server 2012 R2 server.

Note: Unisphere can also be installed within virtual machines that are using the virtual HBA capability of Hyper-V. This solution does not use virtual HBA, so this notice is for information purposes.

► **Perform this installation on each Hyper-V host server.**

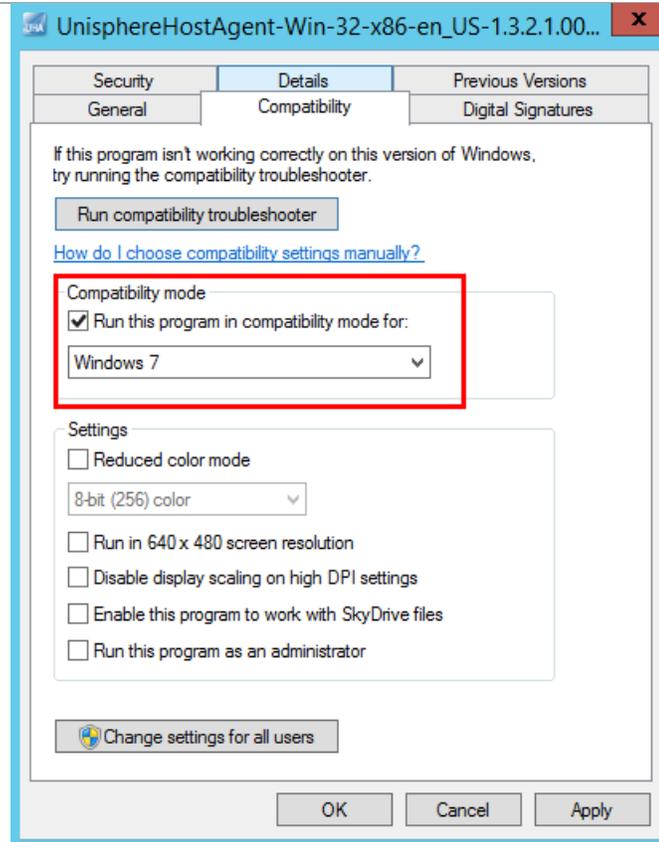
Run the following PowerShell cmdlet from an elevated PowerShell window to open the required firewall port for the Unisphere host agent.

```
New-NetFirewallRule -Name UniAgent-TCP  
-DisplayName UniAgent-TCP -Action Allow  
-Direction Inbound -Protocol TCP -  
LocalPort 6389
```

Right-click the Unisphere Host Agent installer and select **Properties**

Go to the **Compatibility** tab and choose to run the installer in a **Compatibility mode** of **Windows 7**.

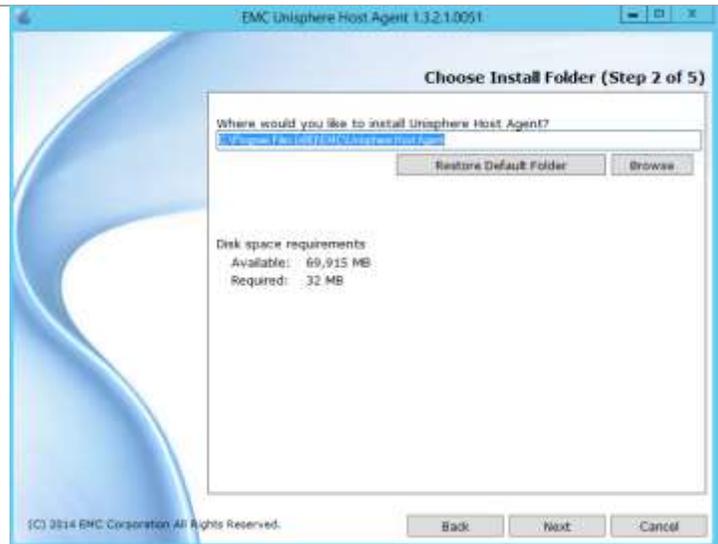
Select **OK**



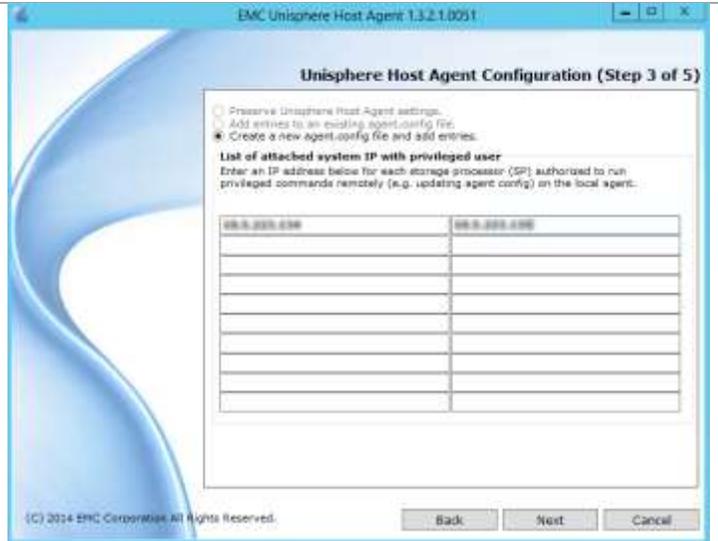
Launch the EMC Unisphere Host Agent installer UnisphereHostAgent-Win-32-x86-en_US-1.3.2.1.0051-1.exe. Click **Next** to continue.



Accept the default installation location. Click **Next** to continue.



Enter the **IP address** of each block service processor (SPA and SPB). Click **Next** to continue.

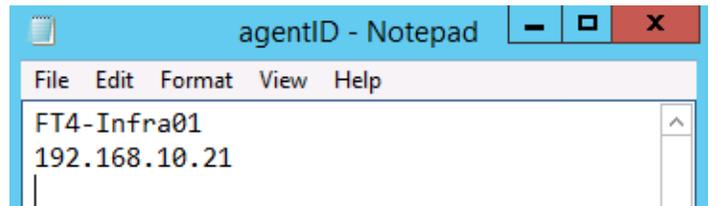
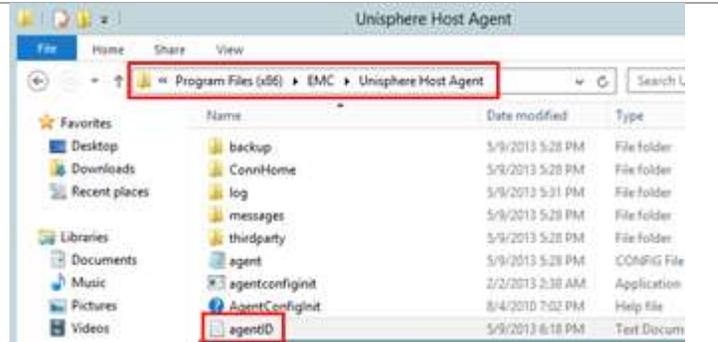


Review the summary information and click **Next** to continue. Click **Finish** on the Installation Complete page.



The Unisphere Host Agent will bind to the first NIC within the binding order on the host. This needs to be a NIC which can communicate with the VNX SP IP addresses. If this ends up being the incorrect NIC, use the agentID.txt file to set the correct interface.

In the installation directory for Unisphere Host Agent (default = C:\Program Files (x86)\EMC\Unisphere Host Agent) create a file called agentID.txt. Within the file, place the server name on the first line, press enter, and then place the IP address of the desired management interface on the second line.



Create Infrastructure Hyper-V Cluster

When you have completed the build of three servers to boot from SAN in a multipath IO environment, have all the network adapters configured the same on each host, and all hosts are joined to the Active Directory domain, you will create the cluster on which all the System Center 2012 R2 infrastructure virtual machines will be deployed. It is recommended that the Fabric Management cluster remain a separately managed cluster and that it not be used for tenant VMs, but Windows does provide enough security to isolate different VMs, so it is totally acceptable to use the nodes of the Fabric Management cluster for running VMs, if that is desired. This document demonstrates two clusters – one for Fabric Management and the other for Tenant virtual machines.

Create Shared Storage

Microsoft Failover Clusters use shared storage for storing the VMs. A minimum of five shared LUNs is recommended for the Fabric Management cluster. The witness disk is used exclusively by the cluster. The Cluster Shared Volumes can be made larger, if desired.

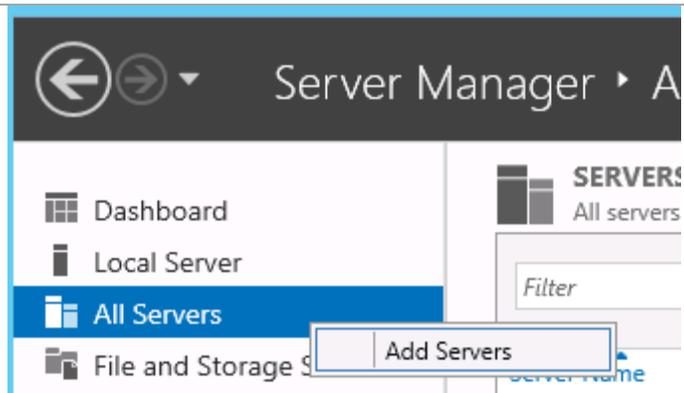
- Witness Disk – 1 GB
- Cluster Shared Volume 1 – 2 TB (recommended minimum), used for storage of VM disks
- Cluster Shared Volume 2 – 2 TB (recommended minimum), used for storage of VM disks
- Cluster Shared Volume 3 – 4 TB (recommended minimum), used for storing SQL DBs
- Cluster Shared Volume 4 – 2 TB (recommended minimum), used for storing SQL logs

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

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

► Perform these steps on only ONE of the Hyper-V servers that will be part of the cluster.

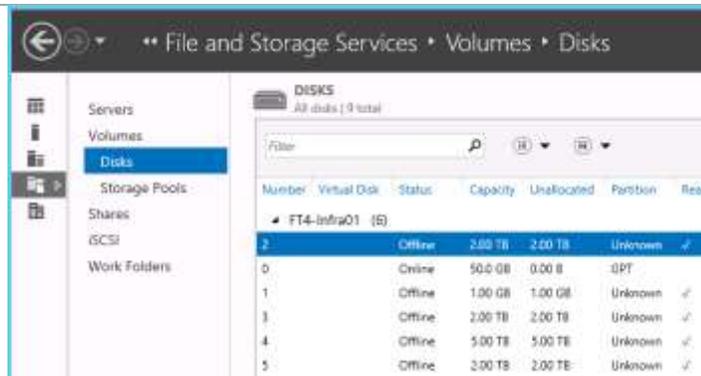
From the **Server Manager** window, right-click **All Servers** and select **Add Servers**.



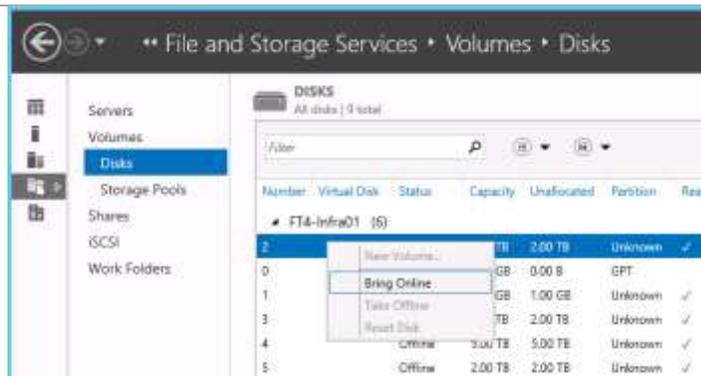
On the **Add Servers** page, enter the name of one of the Hyper-V hosts into **Name (CN)**. Select the server then click the arrow in the middle of the screen to move it to the **Selected** portion of the screen. Click **OK** to continue.



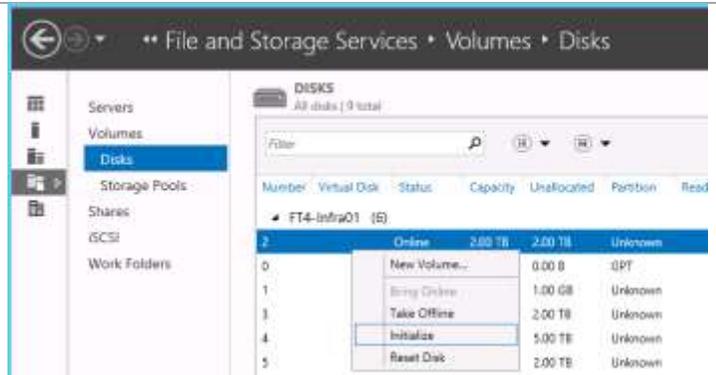
Click the arrow at the end of **File and Storage Services**, Make sure you have high-lighted the server you want to work on, and click **Disks**.



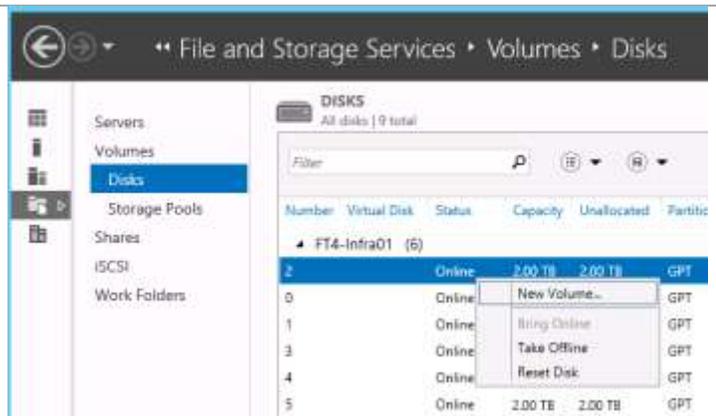
Right-click each disk that is listed as **Offline** and select **Bring Online**. You will receive a warning message about potential data loss if this disk is online on another server. Click **Yes** to acknowledge the warning and bring the disk online.



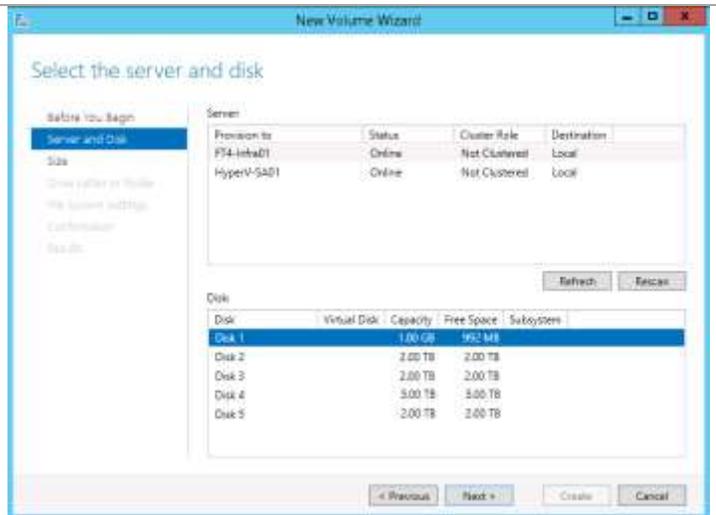
Right-click the first **Unknown** disk and select **Initialize**. You will receive a warning message about initialization erasing all data. Click **Yes** to acknowledge the warning and start the initialization. Repeat for all the disks labeled **Unknown**. When complete, all disks should show a Partition of **GPT**.



Right-click the first disk and select **New Volume**. Click **Next** on the **New Volume Wizard** splash screen.



On the **Select the server and disk** page, first click the server owning the disk and then click a disk. Click **Next** to continue.



On the **Specify the size of the volume**, accept the default (maximum) and click **Next** to continue.



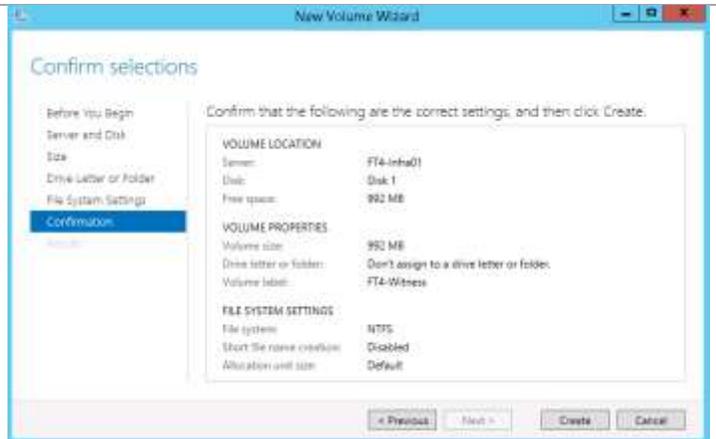
On the **Assign to a drive letter or folder** page, select **Don't assign to a drive letter or folder** radio button. Due to the nature of how these disks will be used, none should have a drive letter. Click **Next** to continue.



On the **Select file system settings** page, leave File system as NTFS. For the volume to be used for SQL databases, make the Allocation unit size the maximum. All others leave a Default. Enter a meaningful Volume label which can be useful in debugging. Click **Next** to continue.



On the **Confirm selections** page, review the settings to Make sure they are correct. Click **Create** to create the volume.

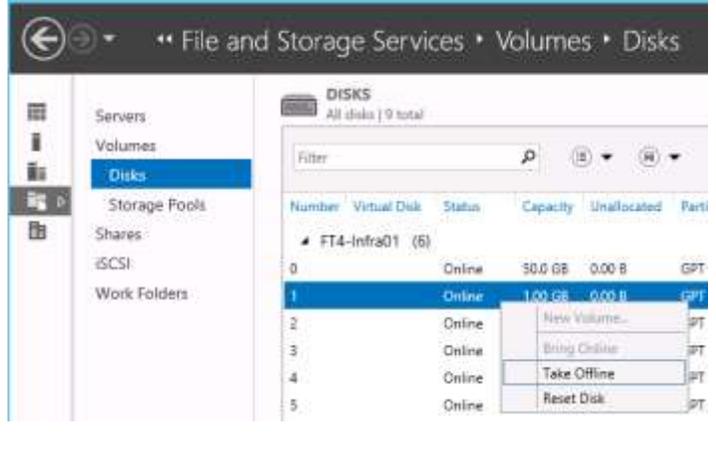


On the **Completion** page, click **Close** when the creation is complete.

Repeat the volume creation steps for all disks.



When volumes have been created on all the disks, right-click each data disks and select **Take Offline**.

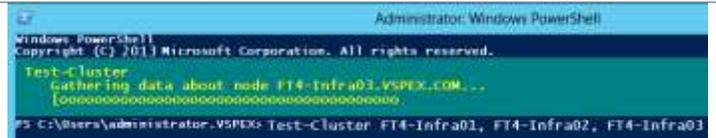


When the disks have been initialized and formatted, it is a good practice to go through each server that will be part of the cluster to make sure the disks can be brought online on each node. If you cannot bring the disks online on every server that will be part of the cluster, check your zoning and masking.

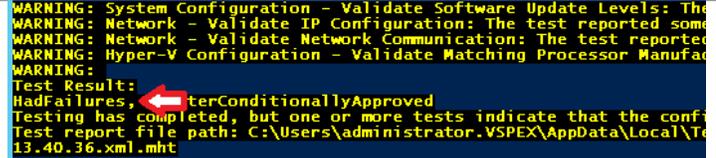
Run Cluster Validation Wizard

Run the Cluster Validation Wizard by issuing the following PowerShell cmdlet:

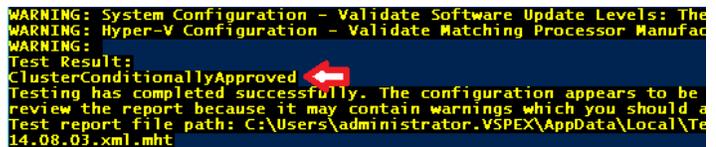
```
Test-Cluster FT4-Infra01, FT4-Infra02, FT4-Infra03
```



It is not uncommon to have errors or warnings. The first run in the screen shot at the right shows a message of **HadFailures**. Failures must be fixed before creating the cluster.

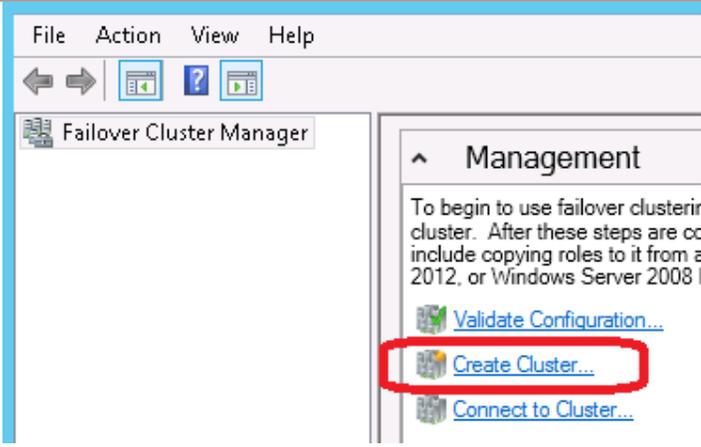


The second run shows a test run with no failures, but there were some warnings. Upon investigatin, it was determined that the warnings were expected and the cluster can be created.



In both cases, the last line of the report shows the name of the file that contains the complete output from the validation wizard.

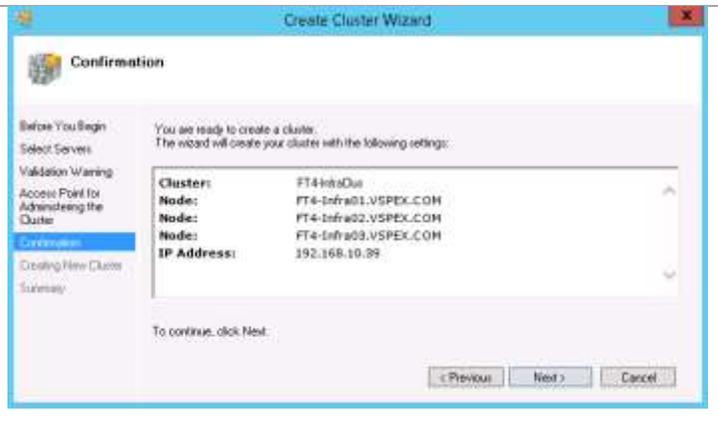
Create Fabric Management Cluster

<p>From Server Manager, launch the Failover Cluster Manager from Tools Failover Cluster Manager. Or, from PowerShell, issue the command Cluadmin.</p>	
<p>In the Management section of the Failover Cluster Manager, select Create Cluster... This launches the Create Cluster Wizard. On the Before You Begin window, click Next to continue.</p>	 <p>The screenshot shows the Failover Cluster Manager console. The 'Management' section is expanded, showing instructions: 'To begin to use failover clusterin cluster. After these steps are cc include copying roles to it from a 2012, or Windows Server 2008'. Below the instructions are three links: 'Validate Configuration...', 'Create Cluster...' (highlighted with a red rectangle), and 'Connect to Cluster...'.</p>
<p>On the Select Servers page, enter either the FQDN or NetBIOS names of the servers to form the cluster. Click Next to continue.</p>	 <p>The screenshot shows the 'Select Servers' step of the 'Create Cluster Wizard'. The 'Before You Begin' section contains the instruction: 'Add the names of all the servers that you want to have in the cluster. You must add at least one server.' The 'Select Servers' section has an 'Enter server name:' field with a 'Browse...' button and a 'Selected servers:' list box containing three entries: 'FT4-Infra01.VSPEX.COM', 'FT4-Infra02.VSPEX.COM', and 'FT4-Infra03.VSPEX.COM'. There are 'Add' and 'Remove' buttons next to the list box. At the bottom are 'Previous', 'Next', and 'Cancel' buttons.</p>
<p>On the Access Point for Administering the Cluster page, enter a name in the Cluster Name field. (The name must be 15 characters or less in length). If you are not using DHCP for address assignment, you will be prompted to enter an IP address for the Cluster Name Object. The cluster name and IP address will be registered in DNS and the cluster name will be registered in Active Directory.</p>	 <p>The screenshot shows the 'Access Point for Administering the Cluster' step of the 'Create Cluster Wizard'. The 'Before You Begin' section contains the instruction: 'Type the name you want to use when administering the cluster.' The 'Access Point for Administering the Cluster' section has a 'Cluster Name:' field with the value 'FT4-InfraClus'. Below this is a warning icon and text: 'The NetBIOS name is limited to 15 characters. One or more IP+ addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.' Below the warning is a table with columns 'Networks' and 'Address'. The first row has a checked checkbox, '192.168.10.0/24', and '192.168.10.39'. At the bottom are 'Previous', 'Next', and 'Cancel' buttons.</p>

Check your answers on the **Confirmation** page. Click **Next** to create the cluster. Click **Finish** on the Summary window. If any errors occurred, they would be listed on the Summary window. They would need to be resolved before continuing.

The cluster can also be created with the following PowerShell cmdlet:

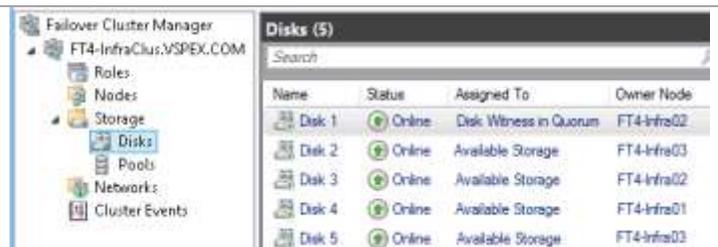
```
New-Cluster -Name <ClusterName>
-Node <node1>, <node2>,
<node3>, -StaticAddress
<clusterIP>
```



Configure Disks

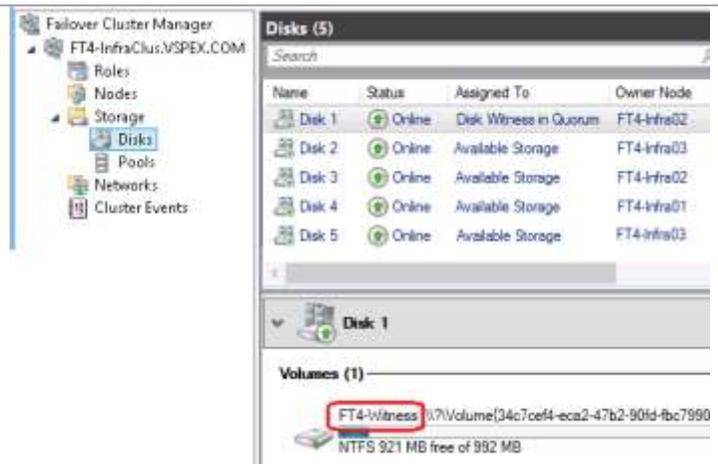
The disks are added into the cluster as Available Storage, meaning they have not been assigned to any specific role or resource group within the cluster. Additionally, the disks have generic names of Disk 1, Disk 2, Disk 3, etc. Using the Failover Cluster Manager console, the disk names can be changed to something meaningful and the data disks can be assigned as Cluster Shared Volumes for use by the virtual machines.

From the **Failover Cluster Manager** console, expand the cluster, expand the Storage, and click **Disks**.



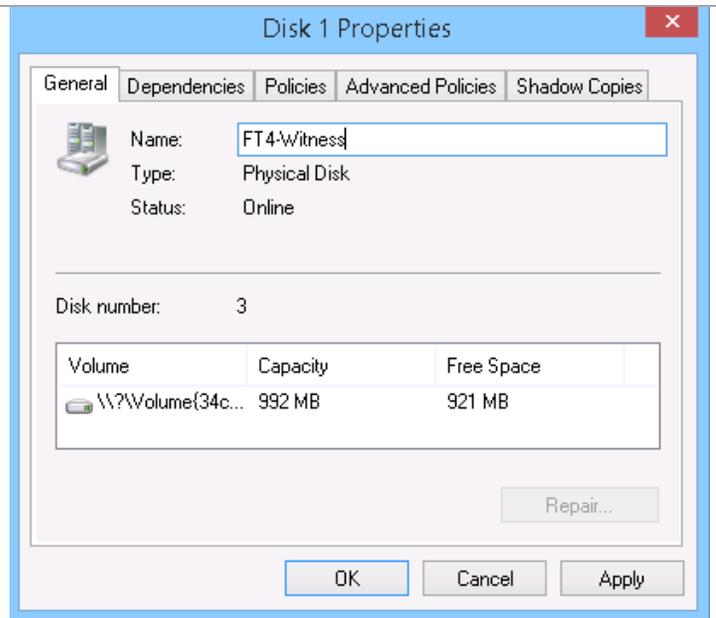
Click the first disk. Under the list of disks, you will see information about the selected disk, including the name you assigned when you formatted the disk.

Note: The cluster will automatically add the smallest NTFS formatted disk as the witness disk.

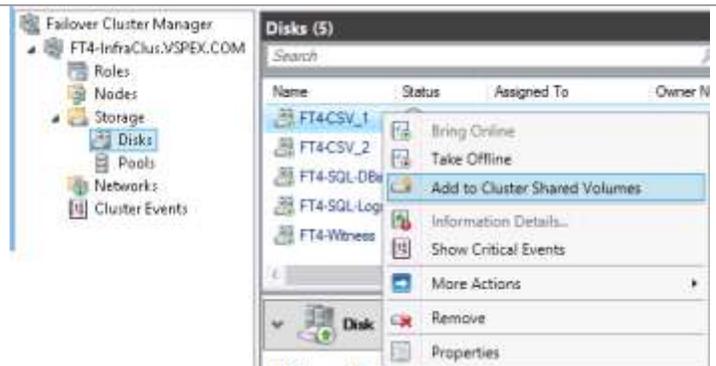


Right-click the disk and select **Properties**. Change the name to reflect the name you assigned when you formatted the disk. Click **OK** to continue.

Repeat on all other disks to rename them.



Right-click the first **Available Storage** volume and select **Add to Cluster Shared Volumes**. Repeat for the other Available Storage volumes.



Configure Networks

Multiple networks have been defined for specific usage within the cluster – Mgmt, CSV, and Live Migration. The cluster has different capabilities that can be assigned to each network, and during the creation of the cluster, the cluster attempts to assign the appropriate capabilities. But those do not always match. We need to make sure the capabilities are properly assigned.

The cluster build process assigns default names to the NICs. For documentation and debugging purposes it is recommended to assign meaningful names to the NICs.

All networks are available for Live Migration in a default configuration, and we want to make sure the network we defined for Live Migration is the only one configured.

The Cluster Shared Volume network has a special requirement. By default, the cluster could assign CSV traffic to the wrong NIC, so we need to make sure the cluster uses the NIC we defined for CSV.

Though the first three changes can be handled through the Failover Cluster Manager console, setting the CSV network is done through PowerShell. The following sample script shows how to take care of all the above steps using a few PowerShell cmdlets.

```

# Rename cluster NICs based upon IP address
(Get-ClusterNetwork -Cluster FT4-InfraClus | ? {$_.Address -like "192.168.177.*"}).Name = "Mgmt"
(Get-ClusterNetwork -Cluster FT4-InfraClus | ? {$_.Address -like "192.168.11.*"}).Name =
"LiveMigration"
(Get-ClusterNetwork -Cluster FT4-InfraClus | ? {$_.Address -like "192.168.12.*"}).Name = "CSV"

# Set cluster network roles based on cluster NIC names set in previous step
(Get-ClusterNetwork -Cluster FT4-InfraClus -Name "Mgmt").Role = 3
(Get-ClusterNetwork -Cluster FT4-InfraClus -Name "LiveMigration").Role = 0
(Get-ClusterNetwork -Cluster FT4-InfraClus -Name "CSV").Role = 1

# Set the Live Migration network by excluding all other networks
Get-ClusterResourceType -Name "Virtual Machine" | Set-ClusterParameter -Name
MigrationExcludeNetworks -Value ([String]::Join(";",(Get-ClusterNetwork | Where-Object {$_.Name -
ne "LiveMigration"}).ID))

# Set cluster metric on CSV network to Make sure it is used exclusively for CSV traffic
(Get-ClusterNetwork -Cluster FT4-InfraClus -Name "CSV").Metric = 900

```

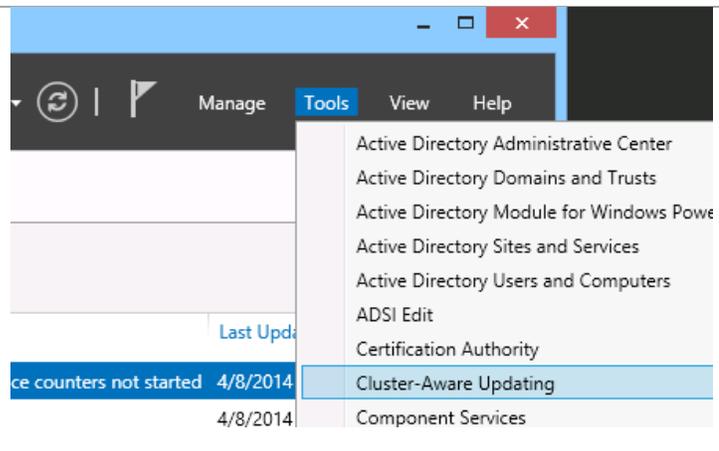
Configure Cluster Aware Updating

Cluster Aware Updating (CAU) allows you to update clustered servers with little or no loss in availability during the update process. During an Updating Run, CAU transparently puts each node of the cluster into node maintenance mode, temporarily fails over the clustered roles off it to other nodes, installs the updates and any dependent updates on the first node, performs a restart if necessary, brings the node back out of maintenance mode, fails back the original clustered roles back onto the node, and then proceeds to update the next node.

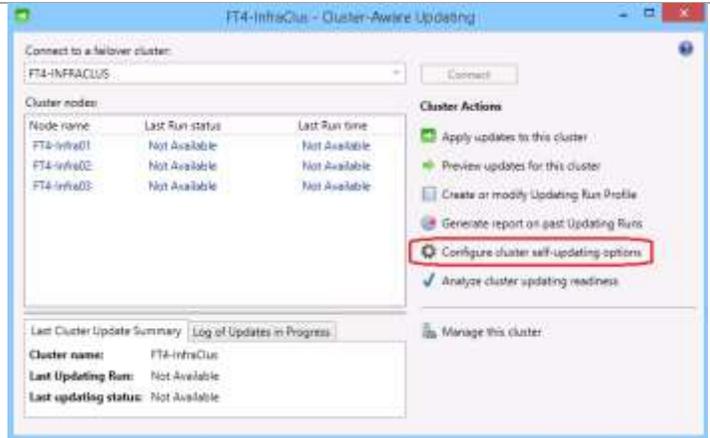
CAU is one of the Failover Clustering tools that is installed with the Failover Clustering feature. Therefore, after you have configured the cluster, all that is left is to configure CAU. Configuration can be accomplished either through the GUI or through PowerShell. The following steps illustrate how to configure the tool through the GUI. The last step shows the PowerShell command.

For this example, the CAU is configured to be self-updating, meaning that it will automatically update itself based on the schedule created. Since Microsoft publishes patches on the second Tuesday of each month, this schedule is being configured to run on the third Tuesday of each month, providing time for the patches to be tested before they are automatically applied.

From **Server Manager** start by selecting **Tools > Cluster Aware Updating**.



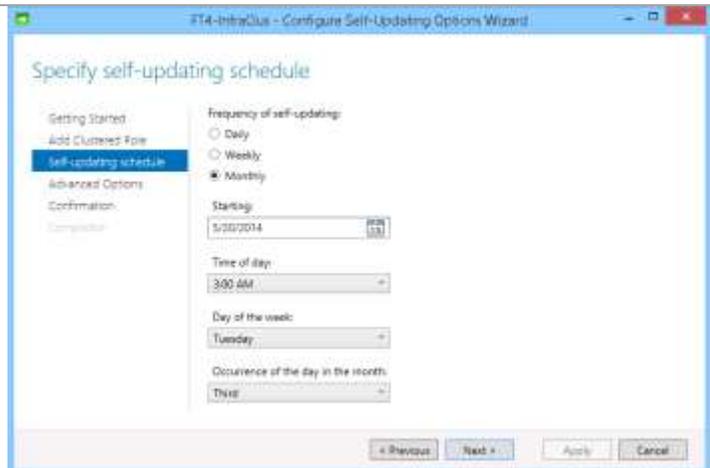
On the **Connect to a failover cluster** page, enter the name of the infrastructure cluster and click the **Connect** button. It will list the nodes of the cluster and show that none of the nodes has run CAU. Click **Configure cluster self-updating options**. Click **Next** on the **Getting Started** page.



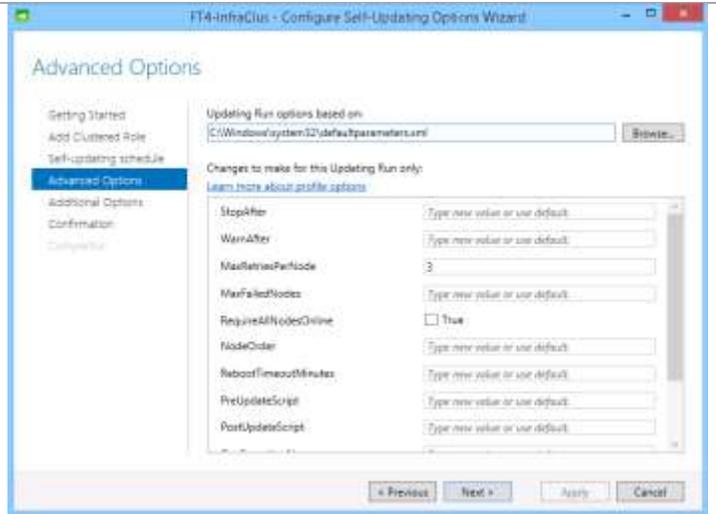
On the **Add CAU Clustered Role with Self-Updating Enabled** page, click the check box by **Add the CAU clustered role, with self-updating mode enabled to this cluster**. Click **Next** to continue.



On the **Specify self-updating schedule** page, select the radio button by **Monthly**. Enter a **Starting** date that begins on a third Tuesday of the month sometime in the future. You can leave the other default entries unless you want to change them. Click **Next** to continue.



On the **Advanced Options** page you have the option to alter how to apply patches. Click **Next** to continue.

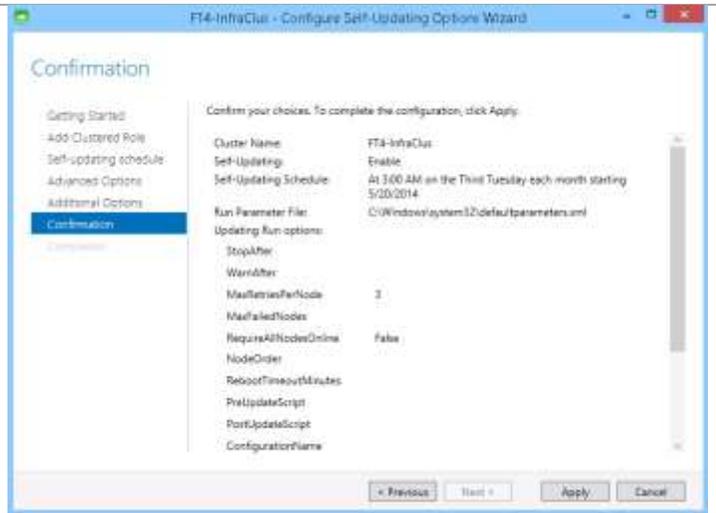


On the **Additional Update Options** page, select the check box by **Give me recommended updates the same way that I receive important updates** if that is the policy in your organization. Click **Next** to continue.



On the **Confirmation** page, review your entries. If satisfied with the entries, click **Apply** to continue.

The clustered role will be added to the cluster with the settings you provided. On the **Completion** page, click **Close** upon successful completion.



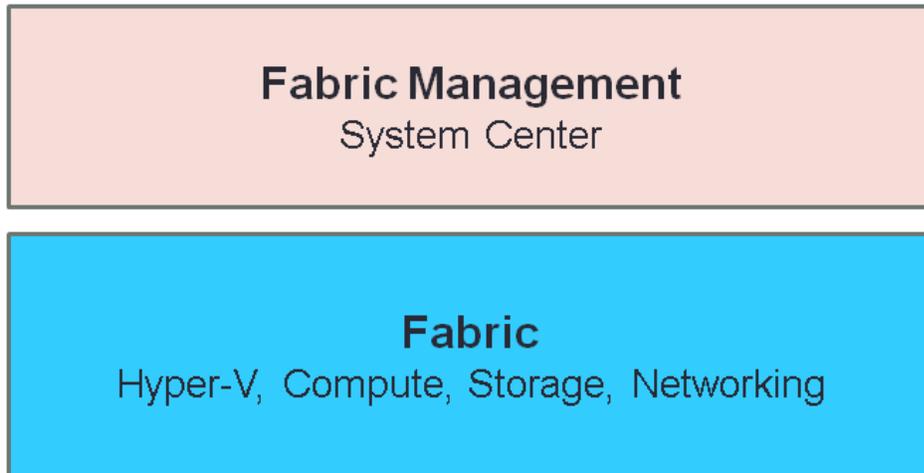
The PowerShell command to the right shows the command to accomplish the same steps as shown above.

```
Add-CauClusterRole -ClusterName FT4-InfraClus -Force -CauPluginName Microsoft.WindowsUpdatePlugin -MaxRetriesPerNode 3 -CauPluginArguments @{ 'IncludeRecommendedUpdates' = 'True' } -StartDate "5/20/2014 3:00:00 AM" -DaysOfWeek 4 -WeeksOfMonth @(3) -verbose
```

Fabric Management

The PLA patterns at a high level include the concept of a compute, storage, and network Fabric. This is logically and physically independent from components such as System Center, which provide Fabric Management.

Figure 8. Components of the Microsoft Private Cloud



Fabric

The Fabric is typically the entire compute, storage, and network infrastructure, consisted of one or more capacity clouds (sometimes referred as Fabric resource pools) that carry characteristics like delegation of access and administration, SLAs, and cost metering. The Fabric is usually implemented as Hyper-V host clusters or stand-alone hosts managed by the System Center infrastructure.

For private cloud infrastructures, a Fabric capacity cloud constitutes of one or more scale units. In a modular architecture, the concept of a scale unit refers to the point to which a module in the architecture can be consumed (i.e. scale) before another module is required. A scale unit can be as small as an individual server because it provides finite capacity, and CPU and random access memory (RAM) resources can be consumed up to a certain point. However, once it is consumed up to its maximum capacity, an additional server is required to continue scaling.

Each scale unit also has an associated amount of physical installation and configuration labor. With larger scale units, like a preconfigured full rack of servers, the labor overhead can be minimized. Thus larger scale units may be more effective from the standpoint of implementation costs. However, it is critical to know the scale limits of all components, both hardware and software, when determining the optimum scale units for the overall architecture.

Scale units allow the documentation of all the requirements (for example, space, power, heating, ventilation and air conditioning (HVAC), and connectivity) that are needed for implementation.

Fabric Management

Fabric management is the concept of treating discrete capacity clouds as a single Fabric. Fabric Management allows centralizing and automating complex management functions that can be carried out in a highly standardized, repeatable fashion to increase availability and lower operational costs.

Provisioning Fabric Management Hosts

In order to properly size Fabric Management host systems, the following table outlines the virtual machines (and their default configurations) that are deployed to compose the fabric management component architecture. These virtual machines are hosted on a dedicated three node Hyper-V failover cluster.

These virtual machines serve as the basis for fabric management operations. The following table summarizes the fabric management virtual machine requirements by the System Center component that supports the product or operating system role.

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

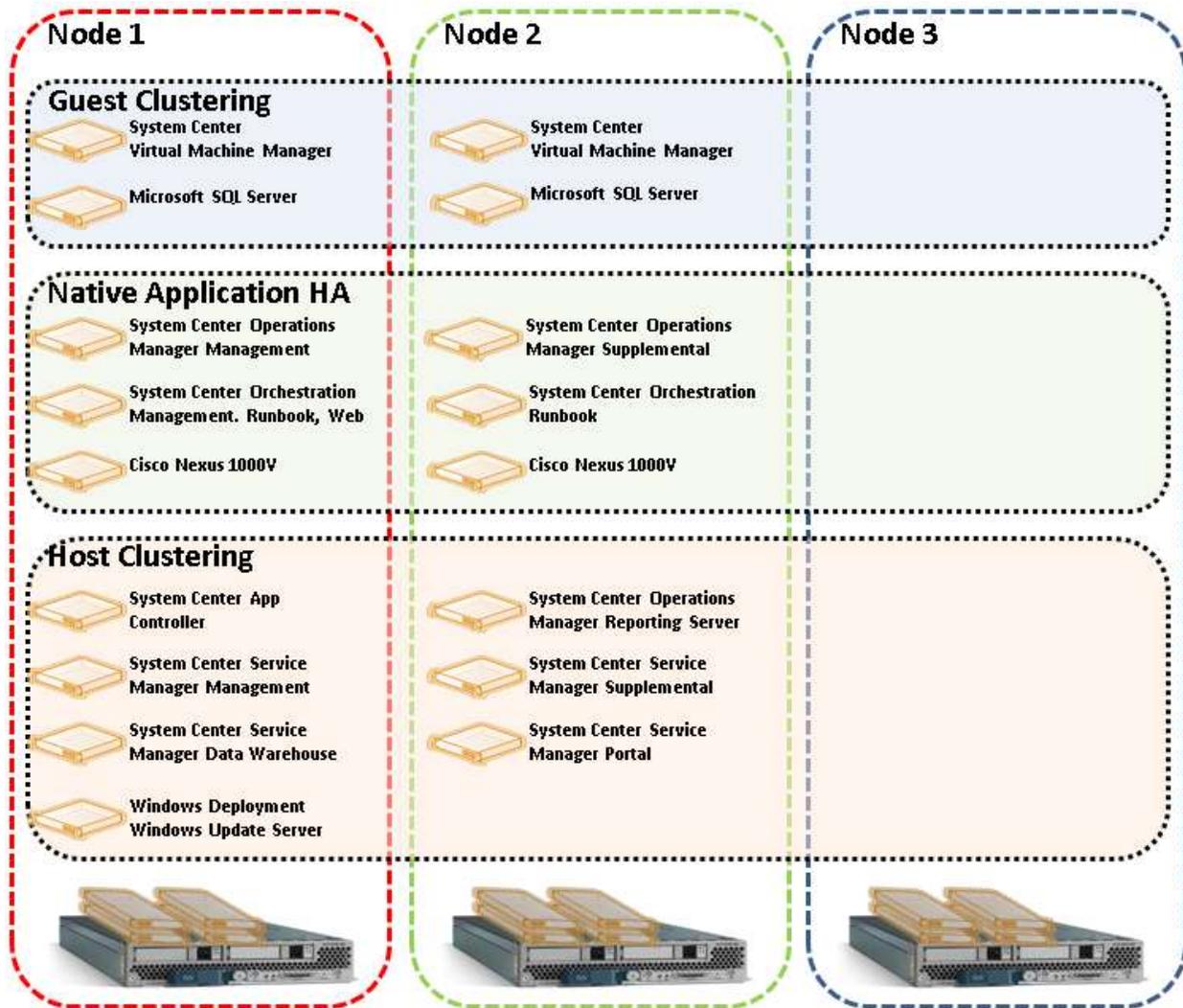
Table 15: VM Configuration Summaries

Component Roles	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
SQL Server Cluster Node 1	16	16	50
SQL Server Cluster Node 2	16	16	50
Virtual Machine Manager	4	8	50
Virtual Machine Manager	4	8	50
App Controller Server	4	8	50
Operations Manager Management Server	8	16	50
Operations Manager supplemental Management Server	8	16	50
Operations Manager Reporting Server	8	16	50
Orchestrator Server (Management, Runbook, Web)	4	8	50
Orchestrator supplemental Runbook Server	4	8	50
Service Manager Management Server	4	16	50
Service Manager supplemental Management Server	4	16	50
Service Manager portal (Windows Server 2008 R2 SP1)	8	16	50
Service Manager Data Warehouse	8	16	50
Windows Deployment Services/Windows Server Update Services	2	4	50
Cisco Nexus 1000V	2	4	
Cisco Nexus 1000V	2	4	
Totals	106	206 GB	750 GB

One of the features of Windows Server 2012 Failover Clustering is dynamic quorum. This gives the administrator the ability to automatically manage the quorum vote assignment for a node, based on the state of the node. When a node shuts down or crashes, the node loses its quorum vote. When a node successfully rejoins the cluster, it regains its quorum vote. By dynamically adjusting the assignment of quorum votes, the cluster can increase or decrease the number of quorum votes that are required to keep running. This enables the cluster to maintain availability during sequential node failures or shutdowns.

It is critical the Fabric Management cluster be available at all times. Therefore, this design includes a minimum of three nodes for the Fabric Management cluster. This Make sures that even if a node is down for maintenance, for example, applying a patch, the remaining nodes will continue to provide a highly available environment with the remaining two nodes. Therefore, should an unexpected hardware or software failure occur while one node is down due to planned maintenance, the remaining components of the cluster will continue their operations. The following picture shows a typical configuration of the cluster just before taking the third node down for maintenance.

Figure 9. Fabric Management Cluster



Fabric Management Cluster



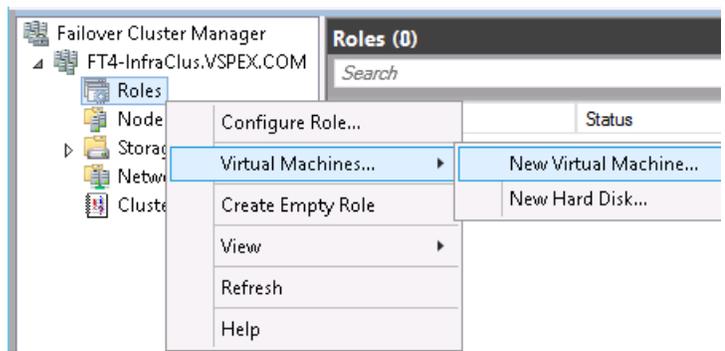
Following the steps in the previous chapter, you created a three-node Windows Server Failover Cluster using the EMC VNX5400 for shared storage.

Create Sysprepped Virtual Hard Disk

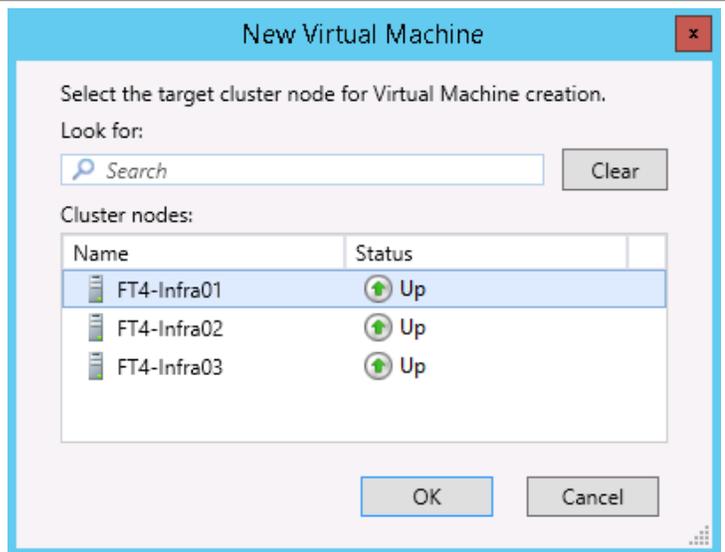
Just as with the physical hosts, much time can be saved by creating a master image for the virtual machines and then using copies, or clones, of this image for building each of the required infrastructure servers running as virtual machines. When the master image is created, additional virtual machines can be created by making copies of this master image. Either the Failover Cluster Manager console or PowerShell can be used to create the additional virtual machines.

The following instructions detail how to create the first VM that will be sysprepped for use in creating all the VMs.

Open the **Failover Cluster Manager** console. Right-click **Roles**, select **Virtual Machines...**, and then select **New Virtual Machine...**



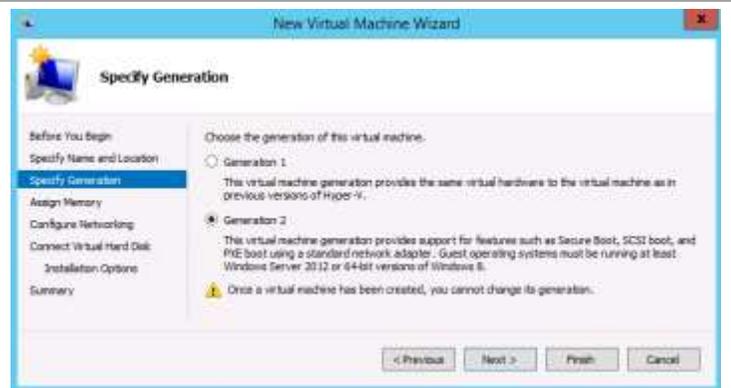
Select one of the nodes as the target for the VM. Click **Next** to continue, and click **Next** on the Before You Begin page.



On the **Specify Name and Location** page, enter a **Name** for the master virtual machine. Select the check box for **Store the virtual machine in a different location**. In the Location field, browse to **C:\ClusterStorage\Volume1** location for storing the VM's files. Click **Next** to continue.



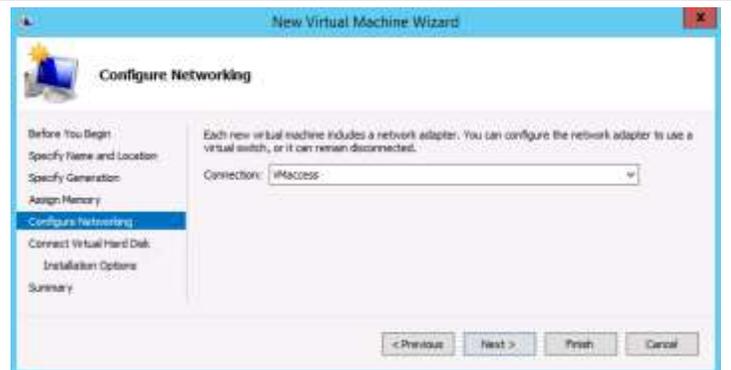
On the **Specify Generation** page, select the radio button by **Generation 2**. Click **Next** to continue.



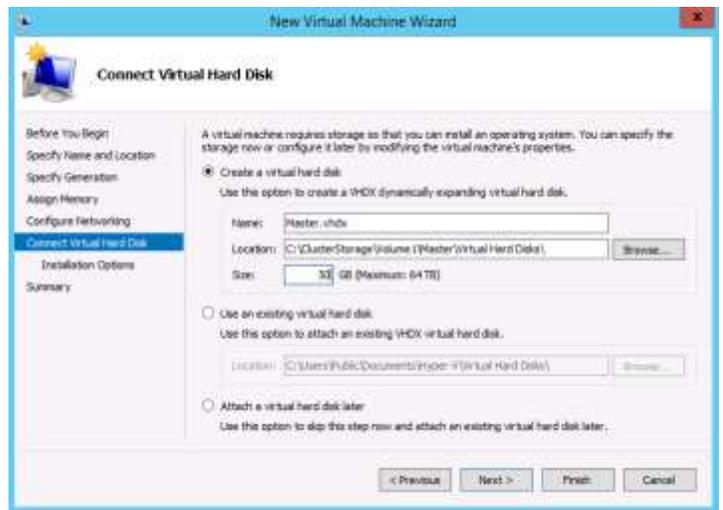
On the **Assign Memory** page, enter 2048 as the amount of memory. Click **Next** to continue.



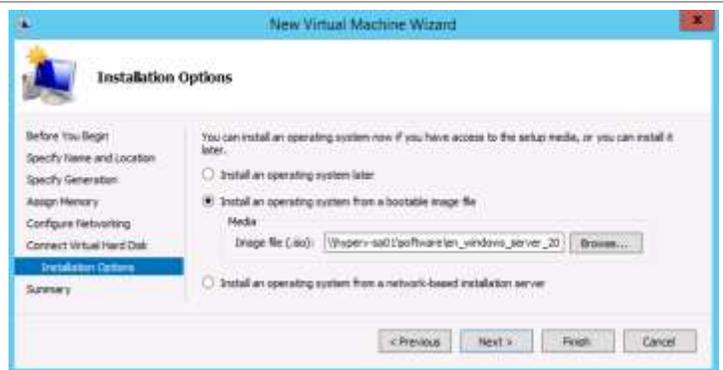
On the **Configure Networking** page, select the appropriate network that will allow access to the internet for updating. Click **Next** to continue.



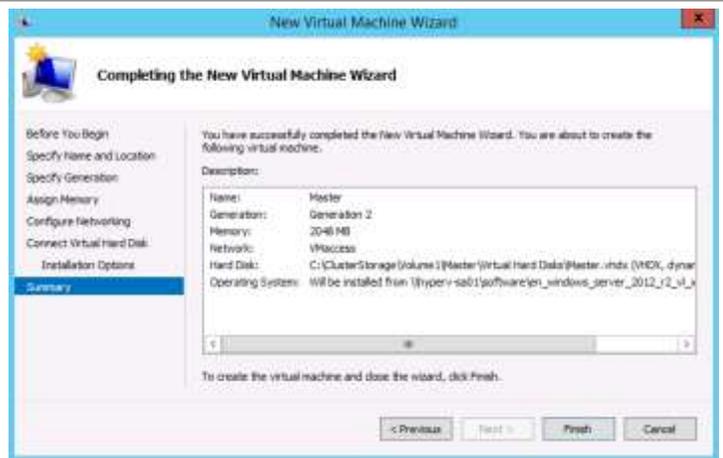
On the **Connect Virtual Hard Disk** page, enter 50 as the size of the virtual hard disk. Click **Next** to continue.



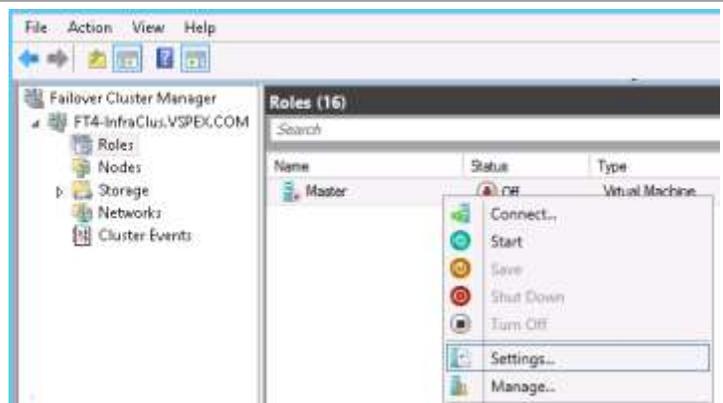
On the **Installation Options** page, select the radio button by **Install an operating system from a bootable image file**. Browse to the location where you have stored the Windows installation media and select it. Click **Next** to continue.



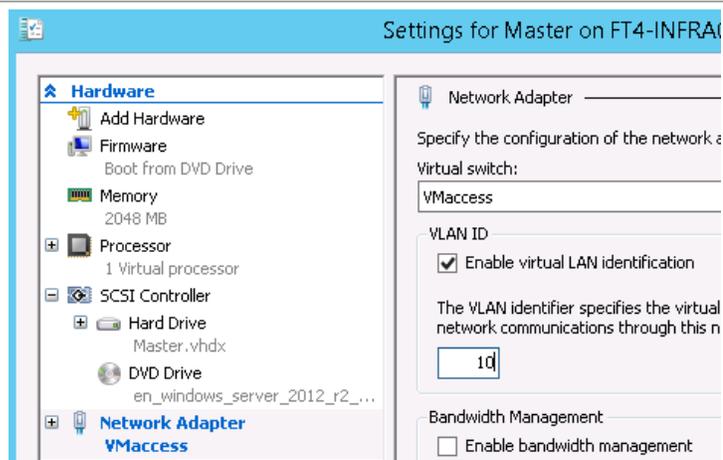
On the **Completing the New Virtual Machine Wizard**, review your entries. If satisfied, click **Finish** to create the VM. Click **Finish** on the Summary page that appears after successful completion.



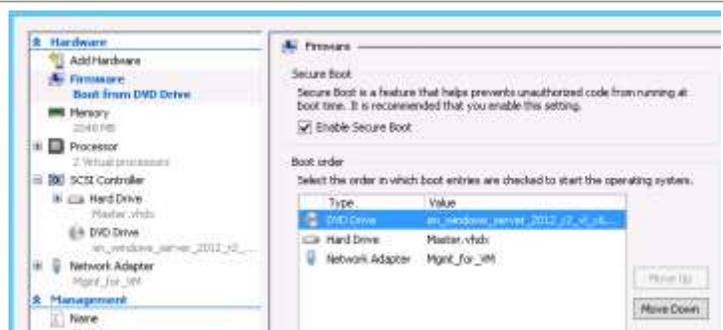
In the **Failover Cluster Manager** console, right-click the virtual machine and select **Settings...**



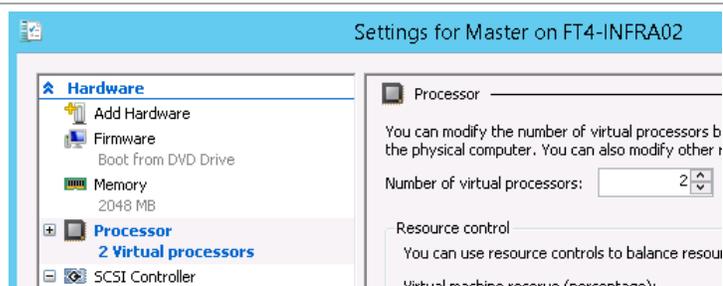
On the **Settings** page, click the network connection under **Hardware**. Select the check box for **VLAN ID** and enter the appropriate VLAN tag. Click **Apply** to save the change.



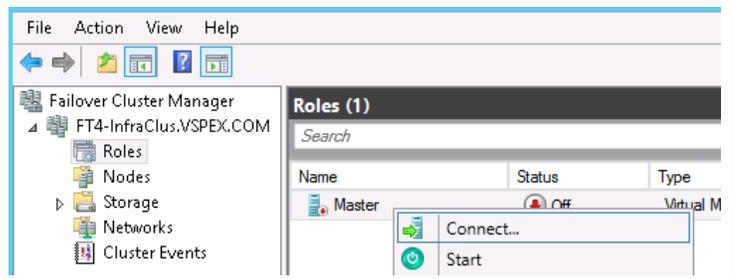
Click the **Firmware** selection. Under **Boot order**, select **DVD Drive** and move it to the top of the list by clicking on the **Move Up** button. Click **Apply** to save the change.



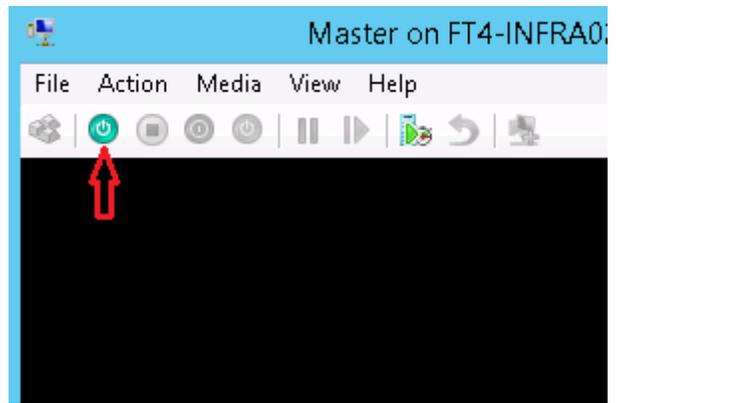
Optional. The build process will run faster if you increase the number of virtual processors to 2. Click **Processor** and change the number of virtual processors to 2. Click **OK** to save the changes.



In the **Failover Cluster Manager** console, right-click the virtual machine and select **Connect...**

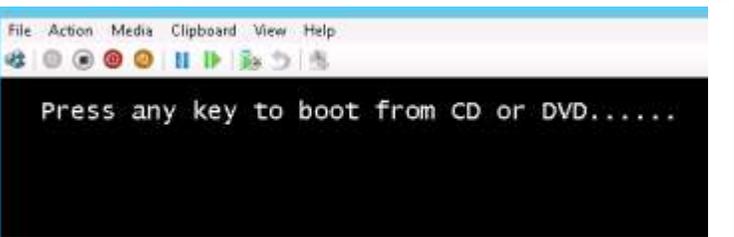


In the **Connection** window, click the **Start** icon to start the installation.



When the **Press any key to boot from CD or DVD** message appears, press any key to have the system boot.

Note: The virtual machine is created as a Generation 2 VM, which means that it is going to perform a UEFI boot. The **Press and key** message does not display very long; you have to get it quickly. If you miss, stop and start the VM again.



The installation of Windows Server 2012 R2 will begin.

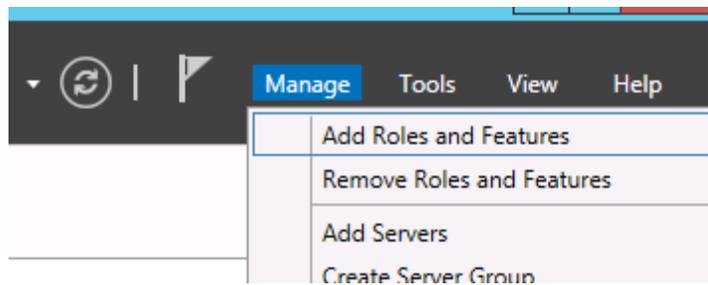
When the installation completes, you should follow procedures similar to those provided earlier for the physical host, including updating with latest patches, configuring for remote management, and installing any customer-specific utilities and tools. This machine does not have to be joined to the domain. It is going to be sysprepped, and sysprepped machines cannot be domain members.

Several of the infrastructure servers require the .NET Framework 3.5 Features. The following steps demonstrate how to add this feature to the image before sysprepping it. This will save time while configuring the VMs that require this feature as you will not have to install it each time it is needed. This is not required, but it can be a time-saver.

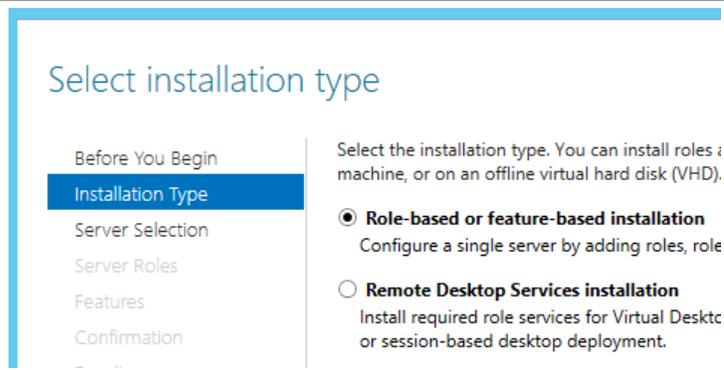
From the **Failover Cluster Manager** console, make sure the Windows installation media is still mounted to the VM. Log into the VM.



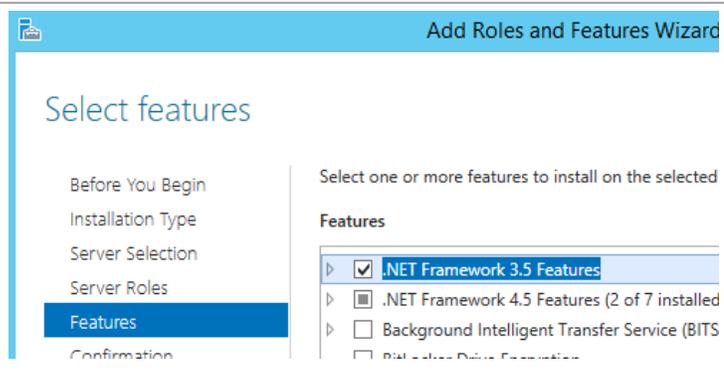
From the **Server Manager** console, select **Manage > Add Roles and Features**. Click **Next** on the **Before You Begin** page.



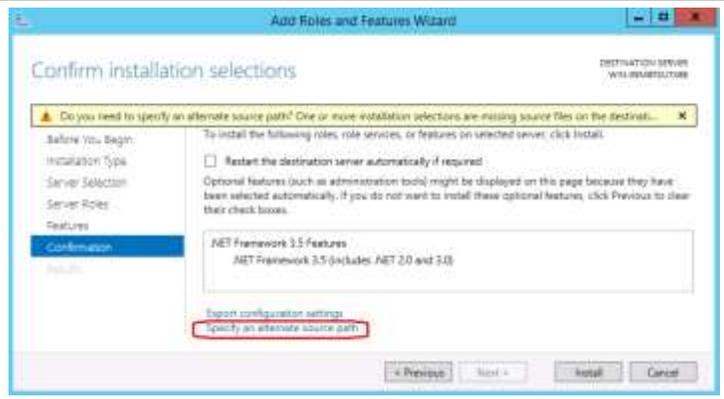
On the **Select installation type** page, click the radio button to select **Role-based or feature-based installation**. Click **Next** to continue. Click **Next** on subsequent pages until you get to the **Select Features** page.



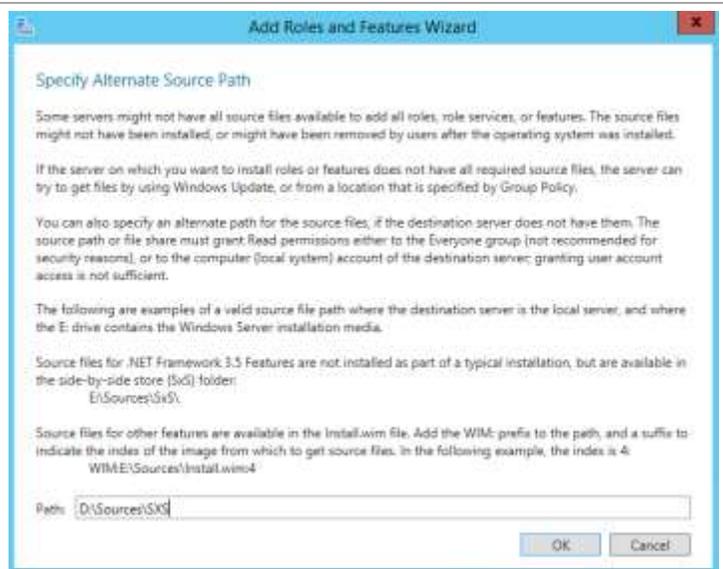
On the **Select Features** page, select the check box by **.NET Framework 3.5 Features**. Click **Next** to continue.



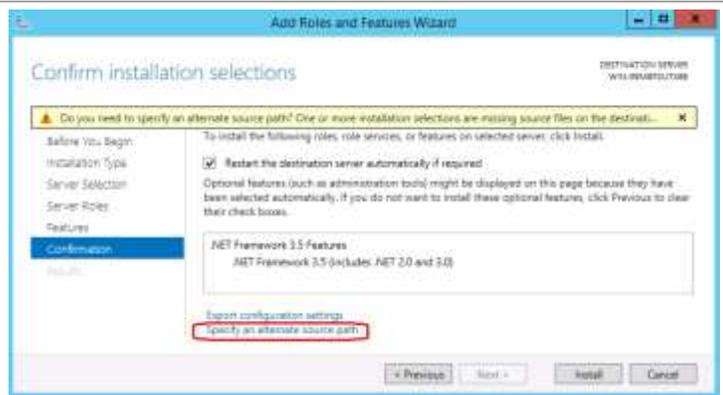
On the **Confirm installation selections** page, click **Specify and alternate source path**.



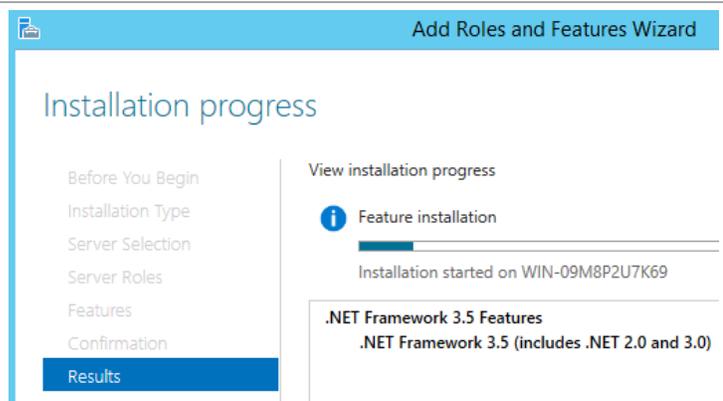
On the **Specify Alternate Source Path** page, enter the path to the location on the Windows installation media where the sources for .NET Framework 3.5 can be found. These are found in the \Sources\SXS directory on the installation media. Click **OK** when the proper path has been entered.



Back on the **Confirm installation selections** page, click the check box for **Restart the destination server automatically if required**. Click **OK** on the informational window that display. Click **Install** to in



An **Installation progress** page will display to show the progress. Click the **Close** button when the installation is complete.



When the above preparations have been completed, it is possible to sysprep the VM. Then the VM hard disk file can be copied and used as the basis for configuring the rest of the infrastructure server VMs (except for the Service Manager Portal, which requires Windows Server 2008 R2 SP1).

Start a PowerShell window and enter the following command:

```
\Windows\System32\sysprep\sysprep /generalize /oobe /shutdown
```

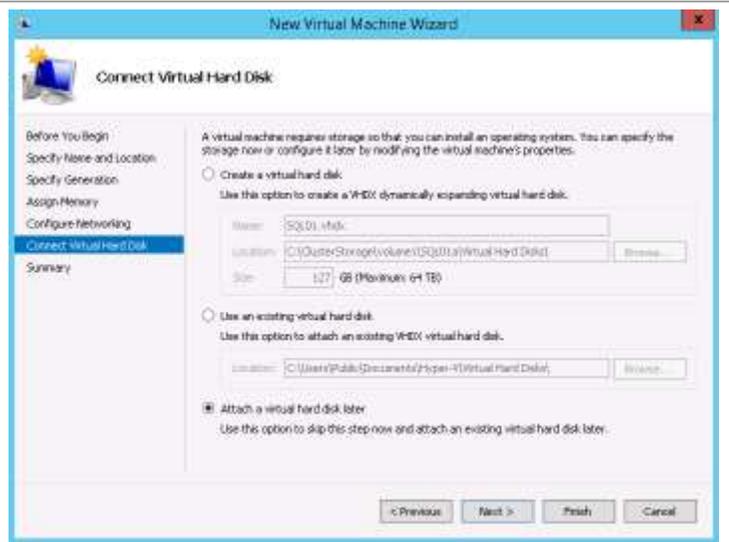
This will sysprep the image and shut it down so the virtual hard disk can be copied for new machines.

Create Infrastructure Virtual Machines From Sysprepped Image

Below are abbreviated instructions, very similar to above, for creating the infrastructure virtual machines by using the Failover Cluster Manager console. Following these instructions for creating a virtual machine from the sysprepped image are the PowerShell commands that perform the same function.

Note: It is recommended to place store the VMs on both Cluster Shared Volumes created on the infrastructure cluster.

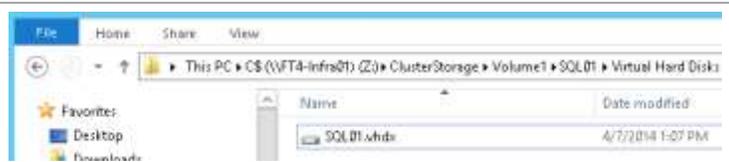
Follow the above steps 1-6 for creating a virtual machine within the Failover Cluster Manager console. Use the memory and CPU values from the table to size the VMs correctly. On the **Connect Virtual Hard Disk** page, select the radio button by **Attach a virtual hard disk later**. Click **Finish** to create the virtual machine. Click **Finish** on the Summary page when the machine is built.



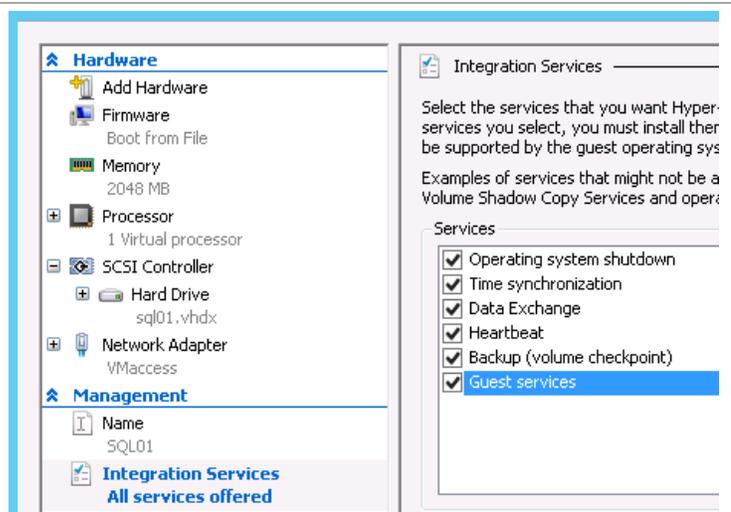
In **Windows Explorer**, open the directory of the newly created VM. Create a new directory and name it **Virtual Hard Disks**.



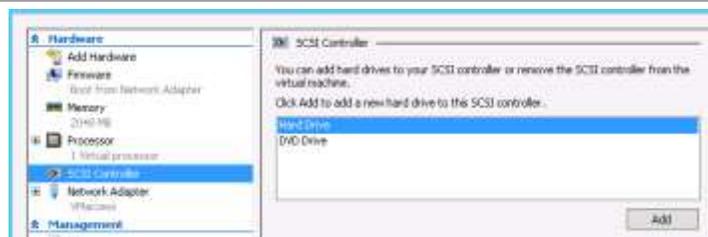
Copy the sysprepped virtual hard disk into the **Virtual Hard Disks** directory and rename it to be the same as the name of the VM you are creating.



In the **Failover Cluster Manager** console, open the **Settings...** of the VM. Under **Management** click **Integration Services**. Check the box by **Guest Services**. Click **Apply** to accept the change.



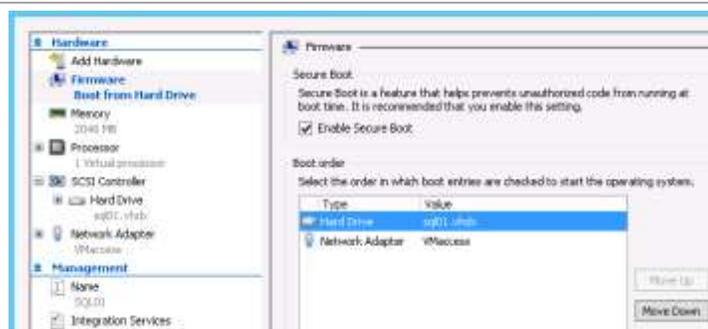
Under Hardware click **SCSI Controller**. From the right-hand side, select **Hard Drive** and click **Add**.



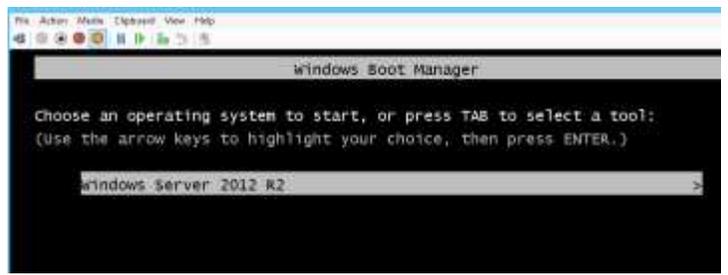
Click the new created **Hard Drive**. Browse to the location you just saved and renamed the copy of the sysprepped image and select the file. Click **Apply**.



Click **Firmware**. Under **Boot** order, select the **Hard Drive** and move it to the top using the **Move up** button. Click **OK** to apply the changes.



In the **Failover Cluster Manager** console, right-click the newly create virtual machine and select **Connect**. **Start** the virtual machine. Strike the **Enter** key to boot into the sysprep mini-setup.



When the mini-setup completes, you have a virtual machine to be used for the infrastructure servers. Repeat to complete all required VMs.

Instead of using the GUI to create all the infrastructure VMs, PowerShell can perform the same tasks. The following script has been used to create infrastructure VMs in a cluster. It must be modified to reflect each customer's environment. The script is supplied as a sample. Neither support nor warranty is implied.

```

<#

Build the VM definitions for the Private Cloud VMs

    W A R N I N G
    W A R N I N G
    W A R N I N G

Make sure that all the Cluster Shared Volumes are owned by the host on which this runs.

This script MUST be run from an elevated PowerShell environment.

The variables in this script should be modified to reflect the customer environment.

#>

# Variables to be edited for the customer environment

# Virtual Switch Names and VLAN IDs

$vNIC1 = "VMaccess"
$vNIC2 = "ClusComm"
$vNICnull = $null
$vLAN1 = "10"
$vLAN2 = "13"
$vLANnull = $null

$templateSource = "C:\ClusterStorage\Volume1\Master\Virtual Hard Disks\Master.vhdx"
$VHD = "\Virtual Hard Disks\"

$vmHost1 = "FT4-Infra01"
$vmHost2 = "Ft4-Infra02"
$vmCluster = "FT4-InfraClus"

# Since good practice would have the sysprepped disk read-only,
# this variable is used to reset the file after copying.

New-Variable -Name read_only -Value 1 -Option readonly

# Virtual Machine information
# Name, Memory, vCPUs, vNIC1, vLANtag1, vNIC2, vLANtag2, lor2)

$VMArray = @()
$VMArray += ("SQL01", 16384MB, 16, $vNIC1, $vLAN1, $vNIC2, $vLAN2, 1)
$VMArray += ("SQL02", 16384MB, 16, $vNIC1, $vLAN1, $vNIC2, $vLAN2, 2)
$VMArray += ("VMM01", 8192MB, 4, $vNIC1, $vLAN1, $vNIC2, $vLAN2, 1)
$VMArray += ("VMM02", 8192MB, 4, $vNIC1, $vLAN1, $vNIC2, $vLAN2, 2)
$VMArray += ("Orch01", 8192MB, 4, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)
$VMArray += ("Orch02", 8192MB, 4, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 2)
$VMArray += ("SM01", 16384MB, 4, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)
$VMArray += ("SM02", 16384MB, 4, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 2)
$VMArray += ("SMDW", 16384MB, 8, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)
$VMArray += ("AC01", 8192MB, 4, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)
$VMArray += ("WDS", 4096MB, 2, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)
$VMArray += ("OM01", 16384MB, 8, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)

```

```

$VMArray +=, ("OM02", 16384MB, 8, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 2)
$VMArray +=, ("OMRS", 16384MB, 8, $vNIC1, $vLAN1, $vNICnull, $vLANnull, 1)

#Import required modules

if ((Get-Module | Where {$_.Name -ilike "FailoverClusters"}).Name -ine "FailoverClusters")
{
    Write-Host "Loading Module: FailoverClusters"
    Import-Module FailoverClusters
}
if ((Get-Module | Where {$_.Name -ilike "ServerManager"}).Name -ine "ServerManager")
{
    Write-Host "Loading Module: ServerManager"
    Import-Module ServerManager
}
if ((Get-Module | Where {$_.Name -ilike "Hyper-V"}).Name -ine "Hyper-V")
{
    Write-Host "Loading Module: Hyper-V"
    Import-Module Hyper-V
}

#####
# Process all VMs in array
#####

For ($i = 0; $i -lt $VMArray.length; $i++)
{
    $element = $VMArray[$i]
    $vmName = $element[0]
    $vmMem = $element[1]
    $vmCpu = $element[2]
    $vmVnic1 = $element[3]
    $vmVlan1 = $element[4]
    $vmVnic2 = $element[5]
    $vmVlan2 = $element[6]
    $lor2 = $element[7]

    $vmHost1VMs = Get-VM -Computer $vmHost1
    $vmHost2VMs = Get-VM -Computer $vmHost2

    Write-Host "`n*****`n* Creating:" $vmName "at" (Get-Date) "`n*****"

    $clusterStorage = "C:\ClusterStorage\Volume1\"
    $vmHost = $vmHost1
    If ($lor2 -eq "2")
    {
        $clusterStorage = "C:\ClusterStorage\Volume2\"
        $vmHost = $vmHost2
    }
    $vhDir = $clusterStorage + $vmName + $VHD
    $dest = $vhDir + $vmName + ".vhdx"

    $vmInfo = New-VM -Name $vmName -Path $clusterStorage -MemoryStartupBytes $vmMem -NoVhd -
    Generation 2 -ComputerName $vmHost
    $trash = New-Item -Path $vhDir -ItemType Directory

```

```

copy $templateSource $dest
Get-ChildItem -Path $dest | Where-Object { $_.attributes -match 'readonly' } |
    ForEach-Object { $_.attributes = $_.attributes -Bxor $read_only }
$vmInfo | Add-VMHardDiskDrive -ControllerType SCSI -ControllerNumber 0 -Path $dest
$vmInfo | Remove-VMNetworkAdapter -Name "Network Adapter"
$vmInfo | Add-VMNetworkAdapter -Name $vNIC1 -SwitchName $vNIC1
If ($vmVlan1 -ne $null)
{
    $vmInfo | Set-VMNetworkAdapterVlan -Access -VlanId $vmVlan1 -VMNetworkAdapterName $vmNic1
}
If ($vmVnic2 -ne $null)
{
    $vmInfo | Add-VMNetworkAdapter -Name $vNIC2 -SwitchName $vNIC2
    If ($vmVlan2 -ne $null)
    {
        $vmInfo | Set-VMNetworkAdapterVlan -Access -VlanId $vmVlan2 -VMNetworkAdapterName
$vmNic2
    }
}

$vmInfo | Set-VM -ProcessorCount $vmCpu
$vmInfo | Add-ClusterVirtualMachineRole -Cluster $vmCluster
$vmInfo | Set-VMFirmware -FirstBootDevice ($vmInfo | Get-VMHardDiskDrive -ControllerLocation
0 -ControllerNumber 0)
$vmInfo | Enable-VMIntegrationService "Guest Service Interface"
}

Write-Host "Completed at:" (Get-Date)

```

Configure Cluster Preferred Owners and Priority

The fabric management components have some machines that back up each other. For example, there are at least two SQL virtual machines and two SCVMM machines. These machines also happen to be configured in a failover cluster configuration for high availability. Machines that have a relationship like this you will generally want to make sure are running on separate nodes in the cluster. If both nodes of the SQL cluster were running on a single node of the Hyper-V cluster, and that node failed, SQL would become temporarily unavailable while the VMs are restarted on a surviving node of the cluster. If each VM of the SQL cluster is running on different nodes in the Hyper-V cluster, the loss of a Hyper-V node will have a lesser impact on SQL's availability because there will be a surviving SQL VM to continue serving the SQL instances.

To implement this capability requires that you assign preferred owners to those VMs you want to keep separated. It is not required that all VMs be configured with preferred owners; primarily those that are serving the same role. Setting preferred owners is accomplished from within the Failover Cluster Manager console.

In addition, it is possible to make sure that some VMs are started before others by assigning a priority to those VMs. For example, SQL is used by many of the other VMs. Therefore, it makes sense that SQL be given a higher priority when it is starting. Other applications, such as a report server, most likely will not be needed as quickly, so it can be configured with a lower priority. Since the settings for preferred owners and priority are located in the same window, examples will be provided here for setting some priorities.

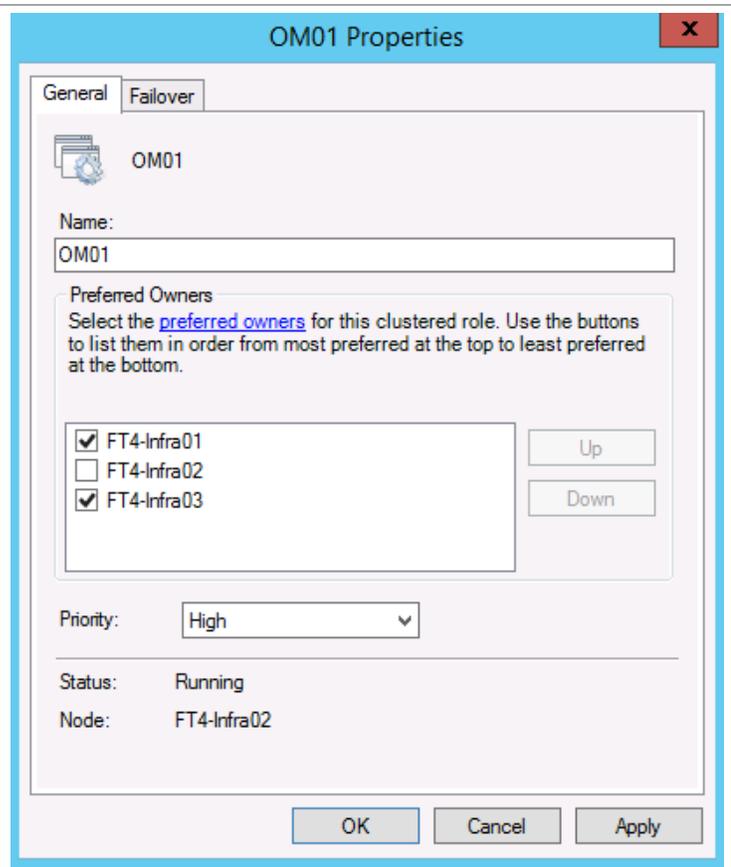
Table 16: lists the recommendations about how to configure preferred owners and priorities.

Table 16: Preferred Owners

Virtual Machine	Preferred Owners	Priority
SQL01	Node1, Node3	High
SQL02	Node2, Node3	High
VMM01	Node1, Node3	High
VMM02	Node2, Node3	High
OM01	Node1, Node3	High
OM02	Node2, Node3	High
Orch01	Node1, Node3	Medium
Orch02	Node2, Node3	Medium
SM01	Node1, Node3	Medium
SM02	Node2, Node3	Medium

The configuration of preferred owners and priority is accomplished within the Failover Cluster Manager console.

Right-click a virtual machine and select **Properties**. In the **Properties** page, select the appropriate preferred owners by clicking the check box by the preferred owner's name. Also select the appropriate priority by making a selection from the drop down list when you click **Priority**. Click **OK** to accept the changes.



Create Required User Accounts and Security Groups

While each System Center 2012 R2 component installation section in this document outlines the individual accounts and groups required for each installation and operation, a short summary is provided in the tables below.

Active Directory Domain User Accounts

The following Active Directory user accounts are required for the Fast Track System Center 2012 R2 installation:

Table 17: Active Directory User Accounts

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

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

Active Directory Domain Security Groups

The following Active Directory security groups are required for the Fast Track System Center 2012 R2 installation:

Table 18: Active Directory Domain Security Groups

Component	Group	Name	Group notes
System Center 2012	System Center Administrators	FT-SC-Admins	This group's members are full Admins on all System Center components.
SQL Server	SQL Server Administrators	FT-SQL-Admins	This group's members are sysadmins on all SQL Server instances and local administrators on all SQL Server nodes.
Operations Manager	Operations Manager Administrators	FT-SCOM-Admins	This group's members are administrators for the Operations Manager installation and hold the Administrators role in Operations Manager.
Virtual Machine Manager	Virtual Machine Manager Administrators	FT-SCVMM-Admins	This group's members are administrators for the Virtual Machine Manager installation and hold the Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Delegated Administrators	FT-SCVMM-FabricAdmins	This group's members are delegated administrators for the Virtual Machine Manager installation and hold the Fabric Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Read Only Admins	FT-SCVMM-ROAdmins	This group's members are read-only administrators for the Virtual Machine Manager installation and hold the Read-Only Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Tenant Administrators	FT-SCVMM-TenantAdmins	This group's members are administrators for Virtual Machine Manager Self-Service users and hold the Tenant Administrators role in Virtual Machine Manager.
Virtual Machine Manager	Virtual Machine Manager Self-Service users	FT-VMM-AppAdmins	This group's members are self-service users in the Virtual Machine Manager and hold the Application Administrators role in Virtual Machine Manager.
Orchestrator	Orchestrator Administrators	FT-SCO-Admins	This group's members are administrators for the Orchestrator installation.
Orchestrator	Orchestrator Operators	FT-SCO-Operators	This group's members gain access to Orchestrator through membership in the Orchestrator Operators group. Any user account added to this group is granted permission to use the Runbook Designer and Deployment Manager tools.
Service Manager	Service Manager Admins	FT-SCSM-Admins	This group is added to the Service Manager Administrators user role and the Data Warehouse Administrators user role.

SQL Server 2012 Failover Cluster Installation

A minimum of two virtual machines running SQL Server 2012 SP1 must be deployed as a guest failover cluster to support the solution, with an option to scale to a four-node cluster. This multi-node SQL Server failover cluster contains all the databases for each System Center product in discrete instances by product and function. This separation of instances allows for division by unique requirements and scale-over time as the needs of each component scales higher.

Should the needs of the solution exceed what two SQL Server virtual machines are able to provide, additional virtual machines can be added to the virtual SQL Server cluster, and each SQL Server instance can be distributed across nodes of the failover cluster.

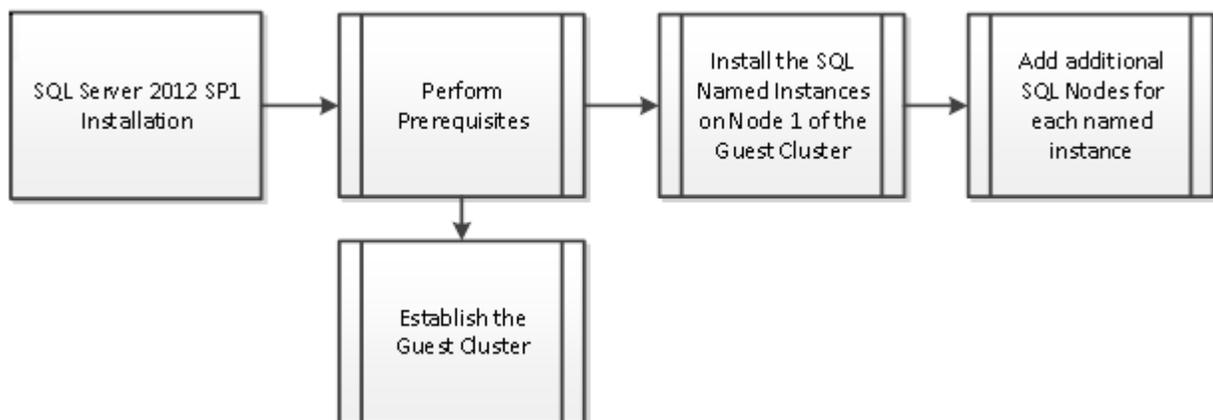
Not all features are supported for failover cluster installations, some features cannot be combined on the same instances, and some allow configuration only during the initial installation. Specifically this applies to database engine services and analysis services. As a general rule, database engine services and analysis services are hosted in separate instances within the failover cluster. SQL Server Reporting Services (SSRS) is not a cluster aware SQL Server service and if deployed within the cluster, it can only be deployed to the scope of a single node. For this reason SSRS will be installed on the respective System Center component server (virtual machine). This installation is “files only”, and the SSRS configuration provisions reporting services databases to be hosted on the component’s corresponding database instance in the SQL Server failover cluster. The exception to this is the System Center Operations Manager Analysis Services and Reporting Services configuration. For this instance, Analysis Services and Reporting Services must be installed with the same server and with the same instance to support Virtual Machine Manager and Operations Manager integration. Similarly, SQL Server Integration Services is also not a cluster-aware SQL Server service and if deployed within the cluster, it can only be deployed to the scope of a single node. For this reason the Service Reporting SQL services functionality will be installed on the Service Reporting virtual machine.

Note: All instances are required to be configured with Windows authentication.

In System Center 2012 R2, the App Controller and Orchestrator components can share an instance of SQL Server with a SharePoint farm, which provides additional consolidation of the SQL Server instance requirements. That shared instance can be considered as a general System Center instance, while other instances are dedicated per individual System Center component.

The SQL Server 2012 SP1 failover cluster installation process includes the high-level steps shown in the following figure.

Figure 10. SQL: Server Failover Cluster Installation Steps



Overview

There is a decision 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
 - Shared VHDX
 - iSCSI
 - Fibre Channel

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

A high-level walkthrough on how to install SQL Server 2012 SP1 is provided below. The following assumptions are made prior to installation:

- Two to four base virtual machines running Windows Server 2012 R2 have been provisioned for SQL Server.
- 15 Shared VHDX LUNs have been assigned to the virtual machine guests.
 - One LUN for quorum (1 GB)
 - Two LUNs for each fabric management component database (14 LUNs for all components)

As discussed in the Infrastructure-as-a-Service Fabric Management Architecture Guide, virtual machines running SQL Server are 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 is installed on the hosting System Center component server (for example, the Operations Manager reporting server). However, this installation is “Files only,” and the SQL Server Reporting Services configuration configures remote Reporting Services databases that are hosted on the component instance on the SQL Server cluster. All instances are required to be configured with Windows Authentication. The following table outlines the options required for each instance.

Table 15. Database Instances and Requirements

Fabric Management Component	Instance Name (Suggested)	Components	Collation	Storage Requirements
Virtual Machine Manager Windows Server Update Services	SCVMMDB	Database Engine	Latin1_General_100_CI_AS	2 LUNs
Operations Manager	SCOMDB	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs
Operations Manager Data Warehouse	SCOMDW	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs
Service Manager	SCSMDB	Database Engine, Full-Text Search	Latin1_General_100_CI_AS	2 LUNs

Service Data Warehouse	Manager	SCSMDW	Database Engine, Full-Text Search	Latin1_General_100_CI_ AS	2 LUNs
Service Data Warehouse	Manager	SCSMAS	Analysis Services	Latin1_General_100_CI_ AS	2 LUNs
Service Web Parts and Portal (SharePoint Foundation), Orchestrator, Controller	Manager App	SCDB	Database Engine	Latin1_General_100_CI_ AS	2 LUNs

Prerequisites

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

Accounts

Verify that the following accounts have been created:

Table 16. SQL Server Accounts

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

Groups

Verify that the following security groups have been created:

Table 17. SQL Server Security Groups

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

Establish the SQL Server Guest Cluster

This section assumes that storage with the Shared VHDX is available and the customer is implementing a SQL Server guest cluster. The following steps create the SQL Server guest cluster.

Notes

- The SQL Server guest cluster can also use Fibre Channel storage for clustering the virtual Fibre Channel adapter, or iSCSI LUNs for Hyper-V in Windows Server 2012 R2.
- Although SMB shares can be used for SQL Server failover clusters, SQL Server Analysis Services is a requirement for the IaaS PLA design, and it is not compatible with SMB shares.

Create Shared VHDX

The first step in installing SQL Server is to create the guest cluster by using Shared VHDX. Access to Shared VHDX is required to allow each guest virtual machine in the cluster to access shared storage. Prior to completing the following steps, the Shared VHDX should be provisioned and presented to the nodes, but not yet made online, initialized, or formatted. The following table provides example sizing of the required .vhdx files:

Table 18. Sample VHDX Design

VHDX	Component(s)	Instance Name	Purpose	Size
VHDX 1	Service Manager Management	SCSMDB	Instance Database	145 GB
VHDX 2	Service Manager Management	SCSMDB	Instance Logs	70 GB
VHDX 3	Service Manager Data Warehouse	SCSMDW	Instance Database	1 TB
VHDX 4	Service Manager Data Warehouse	SCSMDW	Instance Logs	500 GB
VHDX 5	Service Manager Analysis Service	SCSMAS	Analysis Services	8 GB
VHDX 6	Service Manager Analysis Service	SCSMAS	Analysis Logs	4 GB
VHDX 7	Service Manager SharePoint Farm, Orchestrator, App Controller	SCDB	Instance Database	10 GB
VHDX 8	Service Manager SharePoint Farm, Orchestrator, App Controller	SCDB	Instance Logs	5 GB
VHDX 9	Virtual Machine Manager, Windows Server Update Services	SCVMMDB	Instance Database	6 GB
VHDX 10	Virtual Machine Manager, Windows Server Update Services	SCVMMDB	Instance Logs	3 GB
VHDX 11	Operations Manager	SCOMDB	Instance Database	130 GB
VHDX 12	Operations Manager	SCOMDB	Instance Logs	65 GB
VHDX 13	Operations Manager Data Warehouse	SCOMDW	Instance Database	1 TB
VHDX 14	Operations Manager Data Warehouse	SCOMDW	Instance Logs	500 GB
VHDX 15	N/A	N/A	SQL Server Failover Cluster Disk Witness	1 GB

During the provisioning process, two to four virtual machines were built to the specifications outlined in the Infrastructure-as-a-Service Fabric Management Architecture Guide to support SQL Server operations for fabric management. After they are created, the Shared VHDXs must be configured within each virtual machine to make them accessible by each candidate cluster node.

Prior to installing the SQL Server cluster, information must be compiled to provide a point of reference for the steps required during setup. The following table provides an example.

Table 19. Sample System Center Component Database Worksheet

Component	Service Manager management server	Service Manager data warehouse server	Service Manager analysis server	App Controller, Orchestrator, SharePoint Services farm, and WSUS	Virtual Machine Manager	Operations Manager	Operations Manager data warehouse
SQL Server Instance Name	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance Failover CNO	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance DATA Cluster Disk Resource	SCSMDB	SCSMDW	SCSMAS	SCDB	SCVMMDB	SCOMDB	SCOMDW
SQL Server Instance LOG Cluster Disk Resource	SCSMDBlog	SCSMDWlog	SCSMASlog	SCDBlog	SCVMMDBlog	SCOMDBlog	SCOMDWlog
SQL Server Instance Install Drive	E:	G:	I:	K:	M:	O:	Q:
SQL Server Instance DATA Drive	E:	G:	I:	K:	M:	O:	Q:
SQL Server Instance LOG Drive	F:	H:	J:	L:	N:	P:	R:
SQL Server Instance TEMPDB Drive	F:	H:	J:	L:	N:	P:	R:
Cluster Service Name	SQL Server (SCSMDB)	SQL Server (SCSMDW)	SQL Server (SCSMAS)	SQL Server (SCDB)	SQL Server (SCVMMDB)	SQL Server (SCOMDB)	SQL Server (SCOMDW)
Clustered SQL Server Instance IP Address	192.168.10.80	192.168.10.81	192.168.10.82	192.168.10.83	192.168.10.84	192.168.10.85	192.168.10.86
Host Cluster Public Network Interface Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Host Cluster Public Network Interface Name	VMaccess	VMaccess	VMaccess	VMaccess	VMaccess	VMaccess	VMaccess
SQL Server Instance Listening TCP/IP Port	10480	10481	10482	10483	10484	10485	10486
SQL Server Instance Preferred Owners	Node2, Node1	Node2, Node1	Node2, Node1	Node1, Node2	Node1, Node2	Node1, Node2	Node2, Node1

Assign Users and Groups to Local Administrators Group

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

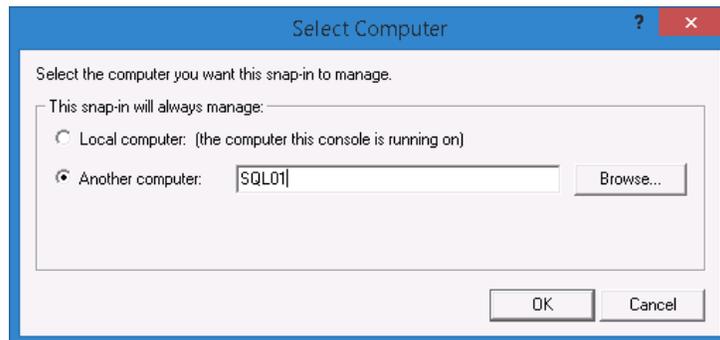
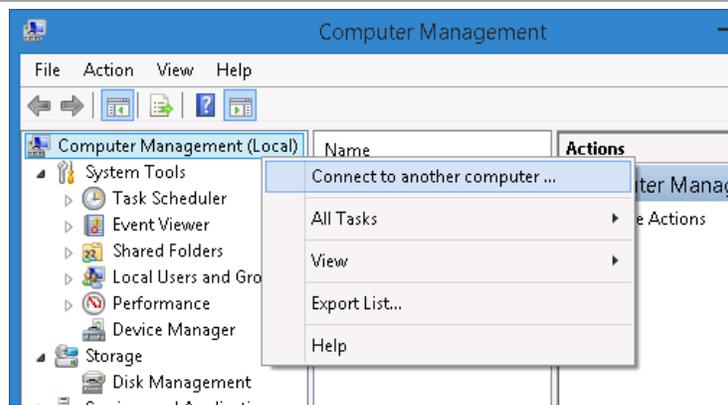
It is possible to accomplish the management functions from the management workstation by using the proper RSAT tool.

Launch the **Computer Management** console. Right-click **Computer Management** and select **Connect to another computer ...**

Enter the name of the computer you want to manage and click **OK**.

Similar to above, you can manage the cluster from the management workstation.

The following steps assume you are logging into each server, but the same steps can be handled remotely in the exact same manner.

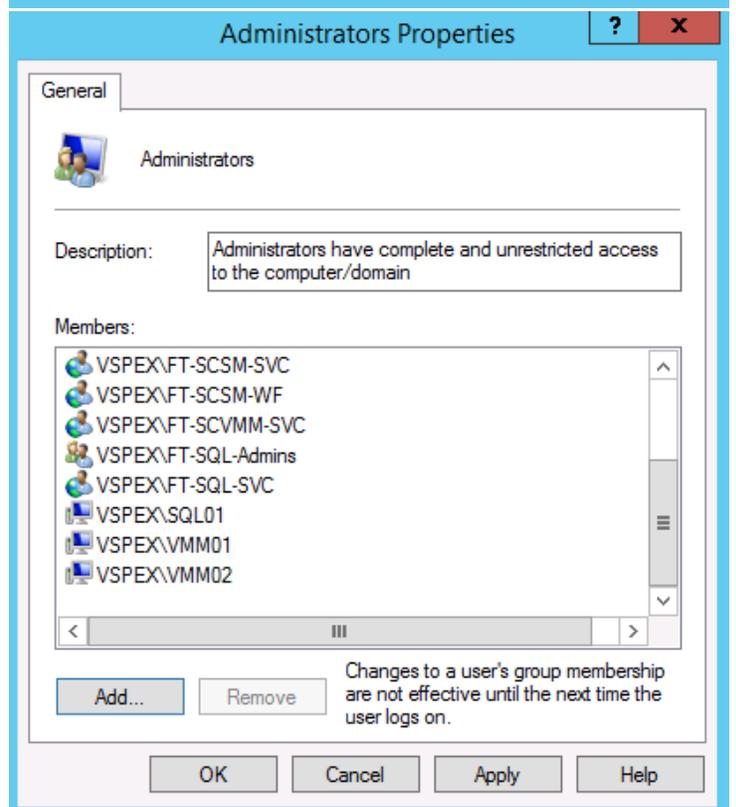
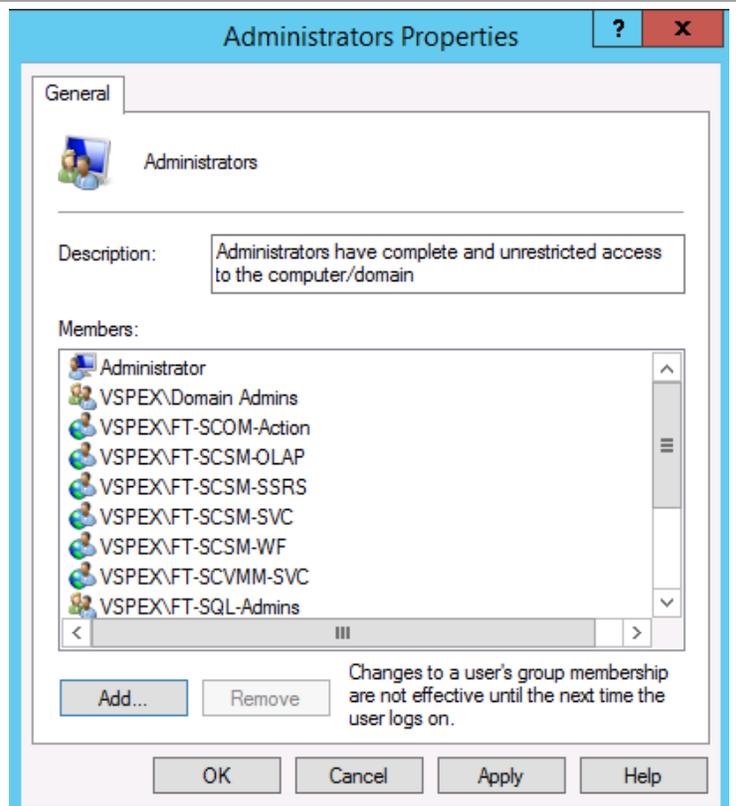


Log on to the first node in the SQL Server cluster as a user with local Administrator rights.

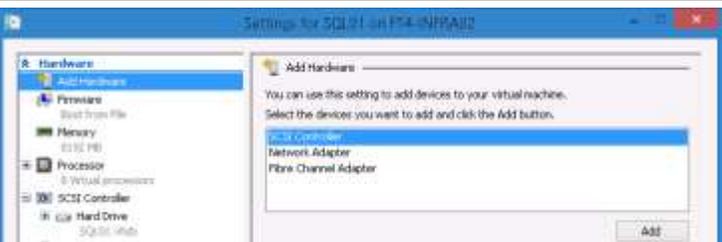
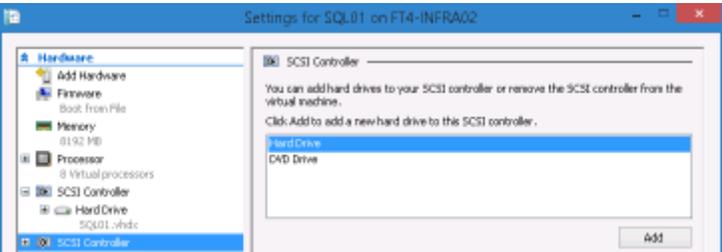
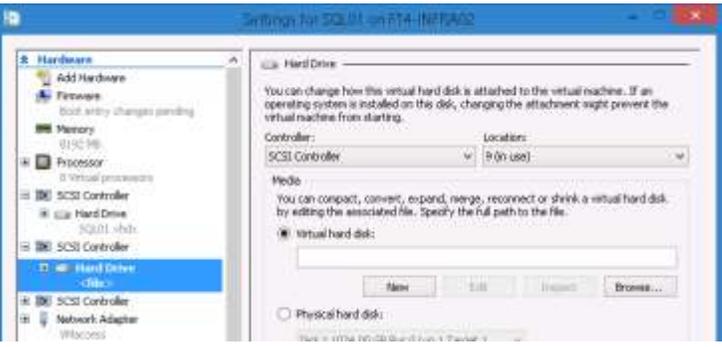
Verify that the following accounts and/or groups are members of the local Administrators group on the first and second SQL Server nodes:

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

Repeat on the other node of the SQL Server cluster.



Create and Add Shared VHDX to VM

<p>Open Failover Cluster Manager, click Roles, right-click SQL01, select Shut Down.</p> <p>Right-click SQL01 and select Settings.</p> <p>Select Add Hardware. Make sure SCSI Controller is selected and click Add.</p> <p>Repeat to add a second SCSI controller. All shared VHDX files will be connected to these additional SCSI controllers</p>	
<p>Select SCSI Controller, click Hard Drive, and click Add.</p> <p>Note: As you add drives to the VM, you will want to alternate them between the two new SCSI controllers.</p>	
<p>Select Virtual Hard Disk, and click New.</p>	
<p>On the Before You Begin page, select Next.</p>	

On the **Choose Disk Type** page, select the radio button by **Fixed Size** and click **Next**.



On the **Specify Name and Location** page, specify the following:

Name: See Component Database Worksheet

Location: Location of Cluster Shared Volumes where VHDXs will reside

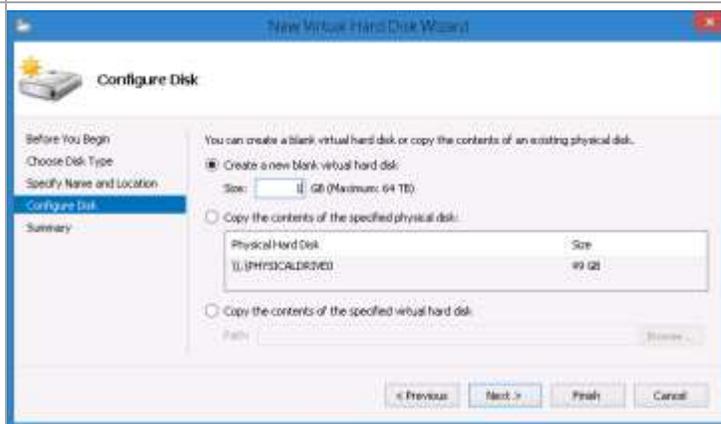
Click **Next**.



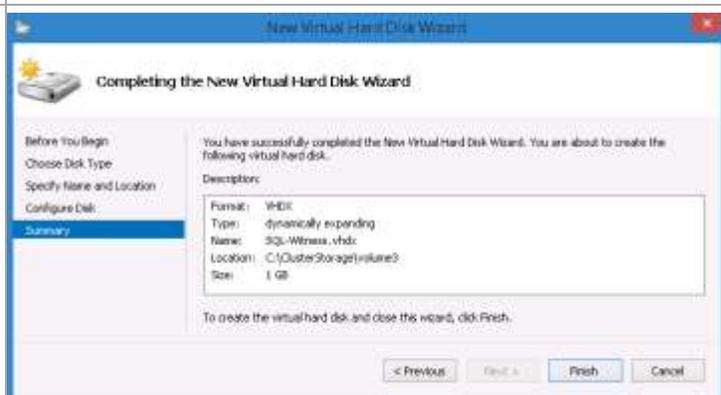
On **Configure Disk** page, specify the following:

Size: See Component Database Worksheet

Click **Next**.

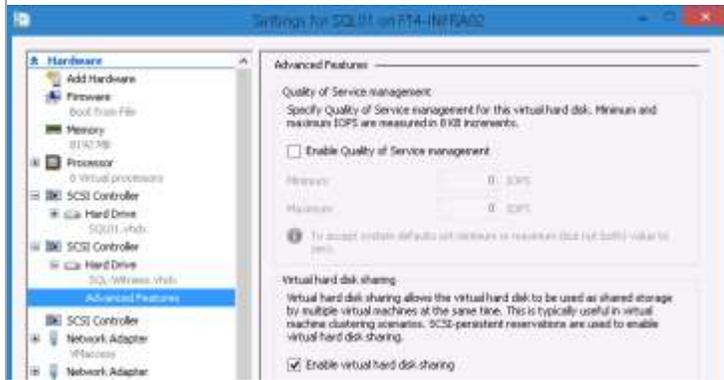


Click **Finish**.



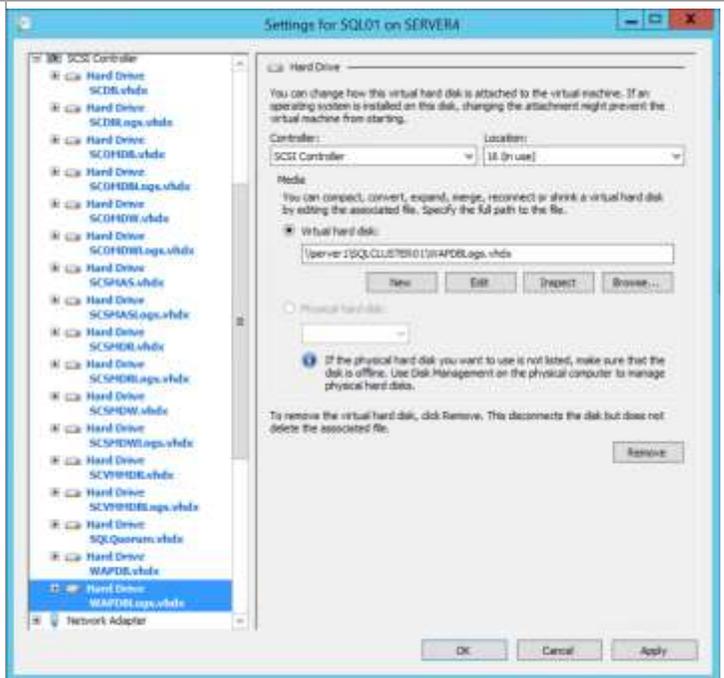
Expand the newly added Hard Drive, select **Advanced Features**, and check **Enable virtual hard disk sharing**.

Repeat steps 4-12 for each disk represented in Sample VHDX Design table.



When all the disks have been added, select **Ok**.

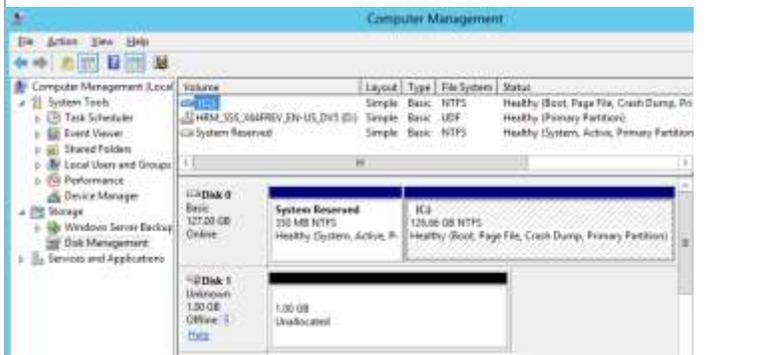
Repeat the steps 1-16 for SQL02.



Initialize and Format VHDX

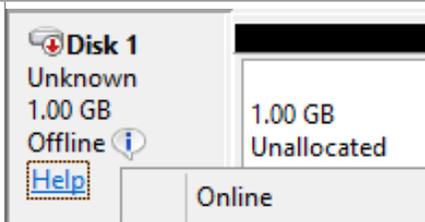
- ▶ Perform the following steps on the **first** fabric management SQL Server virtual machine. Perform these operations on a single node prior to creating the failover cluster.

Within **Computer Management**, navigate to the **Storage** node and click **Disk Management**. The SCSI LUNs should be visible, and they should appear offline.



Right-click each disk and click **Online** in the context menu. This step must be completed for each attached VHDX.

Note: Perform this action on the first node of the SQL cluster.

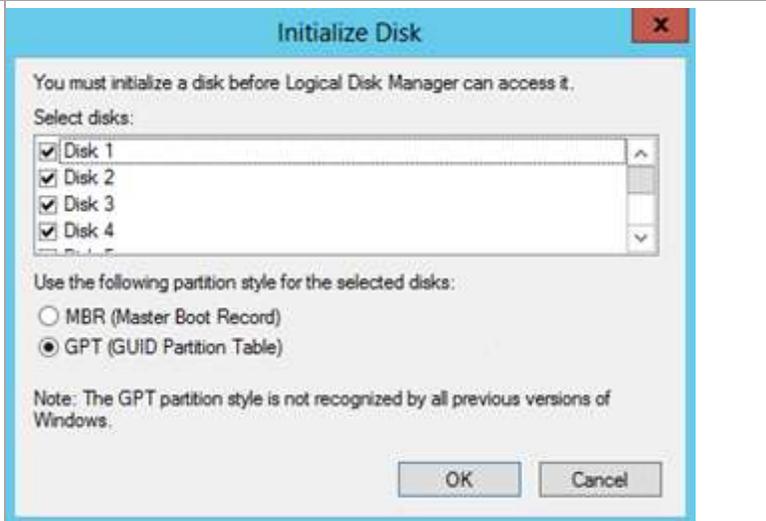


When each disk is online, right-click the first disk and click **Initialize Disk** in the context menu.

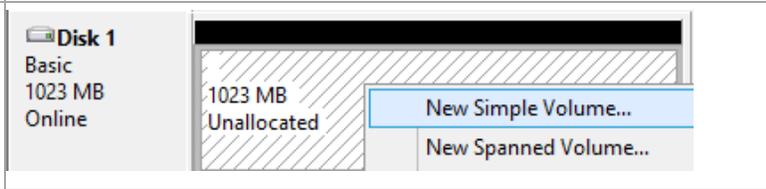
Note: Perform this action on the first node of the SQL cluster.



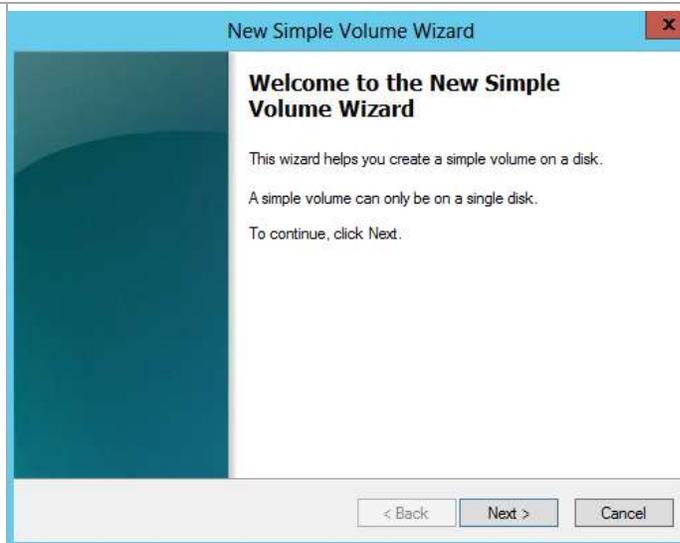
The **Initialize Disk** page appears. Verify that each VHDX check box is selected in the **Select disks** section. Verify that the GPT (GUID Partition Table) option is selected, and then click **OK** to initialize the disks.



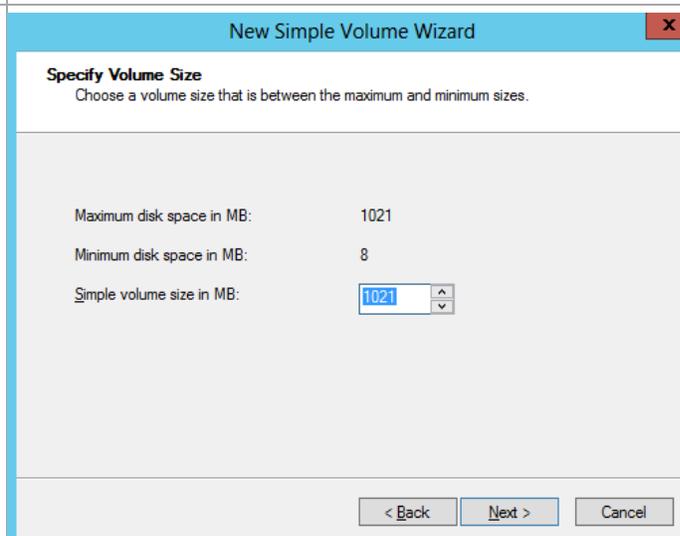
After they are initialized, on the first node, right-click each disk, and click **New Simple Volume...** in the context menu.



When the **New Simple Volume Wizard** appears, click **Next** to continue.

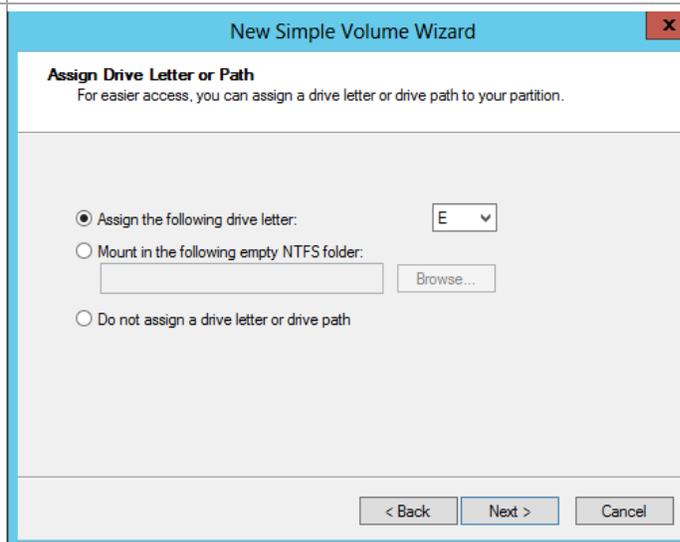


In the **Specify Volume Size** text box, specify the maximum disk space value in the **Simple volume size in MB** text box. Click **Next** to continue.

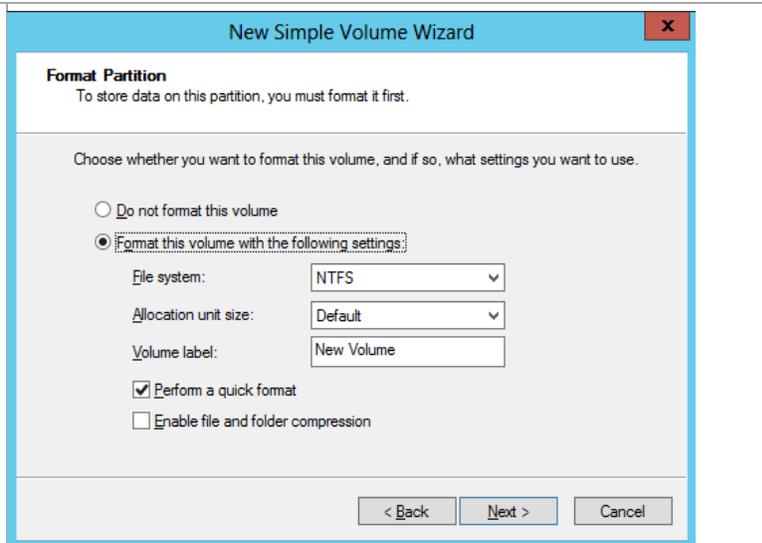


In the **Assign Drive Letter or Path** text box, select **Assign the following drive letter**, and specify a path in the text box. Click **Next** to continue.

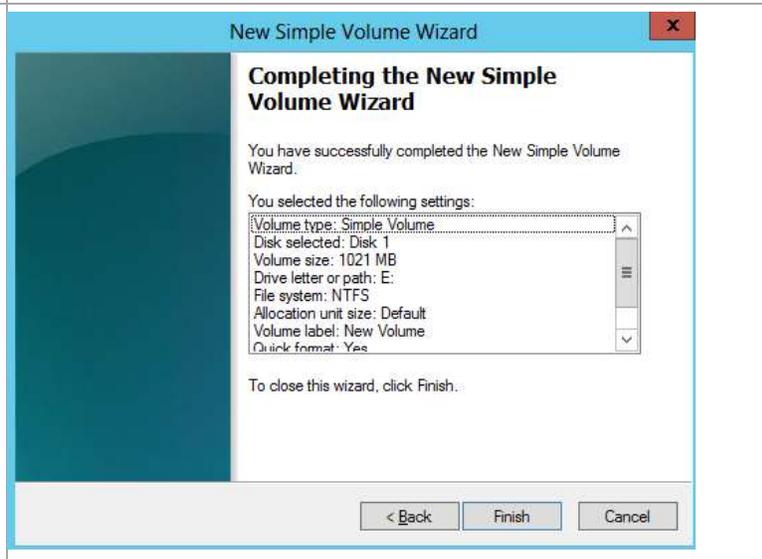
Note: There is no need to assign a drive letter to the witness disk.



On the **Format Partition** page, select **Format this volume with the following settings**. In the **File system** drop-down list, select **NTFS**. In the **Allocation unit size** drop-down list, select **Default**. Optionally, type a descriptive label in the **Volume Label** text box. Verify that the **Perform a quick format** check box is selected, and click **Next** to format the partition.



When the **Completing the New Simple Volume Wizard** page appears, click **Finish** to complete the operation, and then repeat the steps for each disk.



Organizations should configure the interfaces according to their specific deployment characteristics. If separate physical networks are used for VHDXs and inter-cluster private communications (also known as heartbeat), you should reconnect the virtual network adapters appropriately.

When these steps are complete, each disk should be brought online one at a time, initialized, and formatted on the first candidate cluster node. Specifying meaningful volume labels while formatting the disks can help in the future if one or more of the disks lose their assignment to the cluster or virtual machines and they need be identified.

Important: The installation of a SQL Server cluster creates computer accounts in AD DS, called cluster name objects, for each instance in the cluster. By default, these objects are created in the default Computers container of the target Active Directory domain. The account that is used to perform the installation of the SQL Server cluster requires rights in AD DS to create the associated cluster name objects for each SQL Server instance. This occurs as a standard part of the SQL Server installation process.

There are several approaches to mitigate this process, including using a higher privileged account for installation, delegating rights in AD DS for the account that is used for installation, or pre-creating 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 *Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory*.

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

Open an elevated Windows PowerShell prompt within each guest virtual machine (Node 1, Node 2, and additional nodes such as Node 3 and Node 4, if desired). Or perform remotely with the Invoke-Command cmdlet.

Note: The Failover Clustering feature can be installed from an elevated Windows PowerShell® prompt by using the following command:
 Add-WindowsFeature –Name Failover-Clustering – IncludeManagementTools

```
PS C:\Scripts> Invoke-Command -ComputerName SQL01 -Add-WindowsFeature Failover-Clustering -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result                                PSComputerName
-----
True      No          Success          Ifailover-Clustering, Remote Server Admin... SQL01
PS C:\Scripts>
```

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

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

If successful, the **Test-Cluster** cmdlet provides a validation report that can be opened in a local browser from %TEMP% as outlined in Step 3. It is not uncommon to have warnings. For example, if you have a non-routed network for cluster communication, it may fail to communicate with other networks, which is acceptable.

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

```
PS C:\Users\Administrators> Test-Cluster SQL01, SQL02
WARNING: Network - validate network connectivity. The test reported some warnings...
WARNING:
Test Result:
ClusterConditionallyApproved
Testing has completed successfully. The configuration appears to be suitable for clustering. However, you should review the report because it may contain warnings which you should address to obtain the highest availability.
Test report file path: C:\Users\Administrators\AppData\Local\Temp\validation-report-2014-01-10 at 14:31:39.xml.txt
ComputerName : SQL01/2014-01-10 14:31:39 PM
Length       : 4520B
Name         : validation-report-2014-01-10 at 14:31:39.xml.txt
PS C:\Users\Administrators>
```

Navigate to %TEMP% and review the **Failover Cluster Validation Report** for errors and warnings. Perform any required remediation and perform the cluster tests described in Step 2 as required.

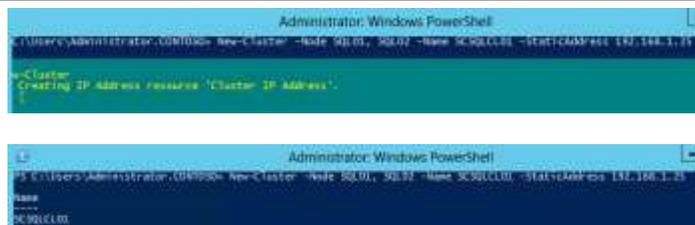


The next step is to create the cluster. From the same elevated Windows PowerShell prompt, run the following command to create the cluster:

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

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

Note: If you are using Dynamic Host Configuration Protocol (DHCP) for the cluster nodes, the `-StaticAddress` parameter should not be used.



After the cluster creation is complete, verify that the correct LUN was assigned as the quorum disk. If the incorrect disk was assigned, the correct assignment can be made by running the following Windows PowerShell command:

`Set-ClusterQuorum -NodeAndDiskMajority <ClusterQuorumDisk>`

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



Verify that all cluster networks are assigned properly. Take care to document which cluster network names are assigned to public and private network interfaces.

Name	Status	Cluster Use
Cluster Network 1	Up	Internal
Cluster Network 2	Up	Enabled

Document all disk assignments in the cluster. Create a mapping table of available storage (by name) to drive letters or mount points. This information will be used during the SQL Server installation.

Name	Status	Assigned To	Owner Node	Disk Number
Cluster Disk 1	Online	Disk Witness in Quorum	SQL01	9
Cluster Disk 2	Online	Available Storage	SQL01	10
Cluster Disk 3	Online	Available Storage	SQL01	11
Cluster Disk 4	Online	Available Storage	SQL01	12
Cluster Disk 5	Online	Available Storage	SQL01	13
Cluster Disk 6	Online	Available Storage	SQL01	14
Cluster Disk 7	Online	Available Storage	SQL01	15
Cluster Disk 8	Online	Available Storage	SQL01	1
Cluster Disk 9	Online	Available Storage	SQL01	2
Cluster Disk 10	Online	Available Storage	SQL01	3
Cluster Disk 11	Online	Available Storage	SQL01	4
Cluster Disk 12	Online	Available Storage	SQL01	5
Cluster Disk 13	Online	Available Storage	SQL01	6
Cluster Disk 14	Online	Available Storage	SQL01	7
Cluster Disk 15	Online	Available Storage	SQL01	8

Note that as an optional step, cluster disks can be renamed and provided with more friendly versions to keep track of which cluster disks are associated with each System Center SQL Instance.

Name	Status	Assigned To	Owner Node
SCDB	Online	Available Storage	SQL01
SCDBlog	Online	Available Storage	SQL01
SCOMDB	Online	Available Storage	SQL01
SCOMDBlog	Online	Available Storage	SQL01
SCOMDW	Online	Available Storage	SQL01
SCOMDWlog	Online	Available Storage	SQL01
SCSMAS	Online	Available Storage	SQL01
SCSMASlog	Online	Available Storage	SQL01
SCSMDB	Online	Available Storage	SQL01
SCSMDBlog	Online	Available Storage	SQL01
SCSMDW	Online	Available Storage	SQL01
SCSMDWlog	Online	Available Storage	SQL01
SCVMMDB	Online	Available Storage	SQL01
SCVMMDBlog	Online	Available Storage	SQL01
SQL-Witness	Online	Disk Witness in Quorum	SQL01
VMMlibrary	Online	Available Storage	SQL01

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

Install First Instance in Cluster

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

The IaaS PLA installation requires separate instances for each System Center product. The instances associated with these products are:

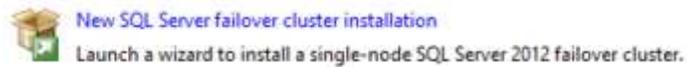
- SCSMDB (Service Manager database)
- SCSMDW (Service Manager data warehouse)
- SCSMAS (Service Manager SQL Analysis Services)
- SCDB (Shared App Controller, Orchestrator, Service Provider Foundation, Services Management Automation, Service Manager self-service portal, Microsoft SharePoint® Foundation 2010 services, and WSUS database)
- SCVMMDB (Virtual Machine Manager database and optional WSUS database)
- SCOMDB (Operations Manager database)
- SCOMDW (Operations Manager data warehouse)

For multi-instance failover clusters, installation of SQL Server 2012 SP1 must be performed when for each instance. As such, these steps must be performed for each instance sequentially.

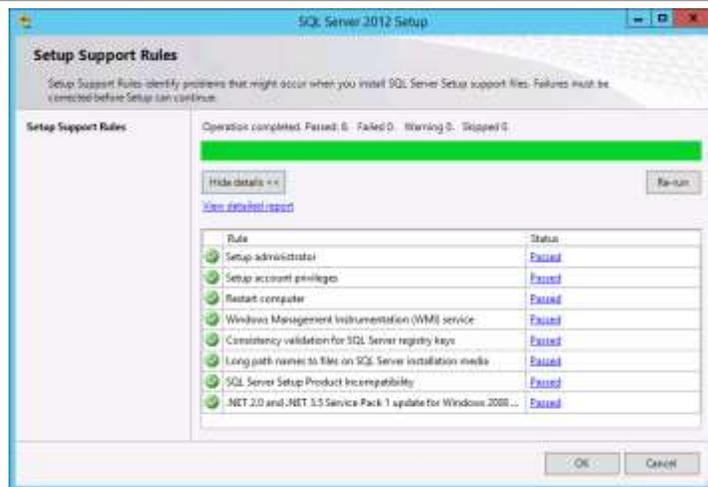
From the SQL Server 2012 SP1 installation media source, right-click setup.exe and click **Run as administrator** to begin setup. The **SQL Server Installation Center** will appear. Click **Installation** in the left pane.



Click **New SQL Server failover cluster installation**.



The SQL Server 2012 Setup Wizard will appear. On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **OK** to continue.



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

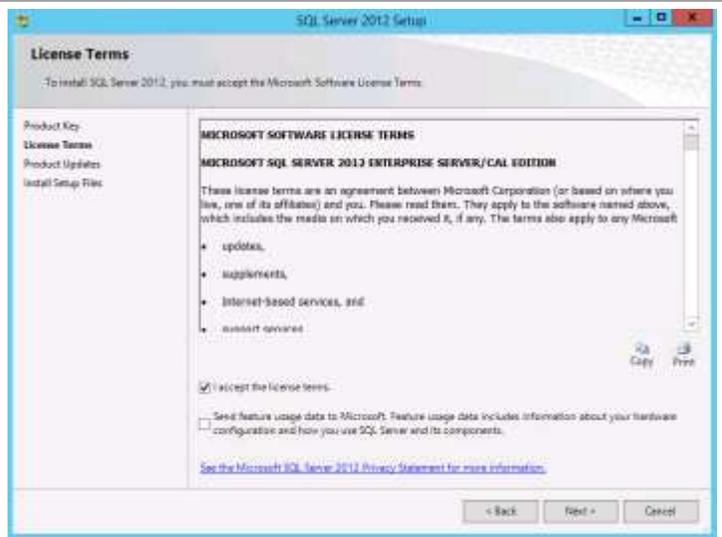


On the **Product Key** page, select the **Enter the product key** option and enter the associated product key in the provided text box. Click **Next** to continue.

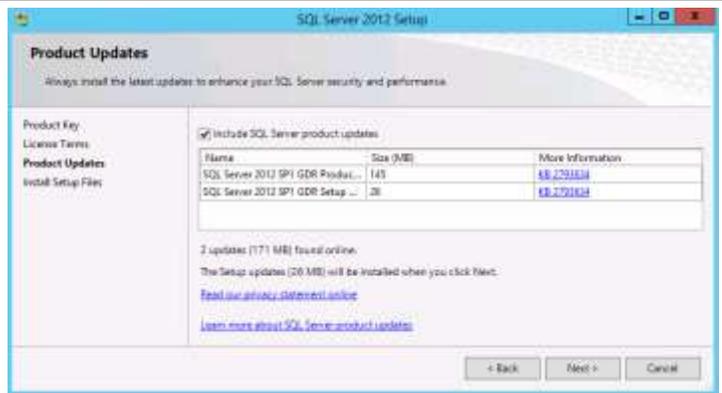
Note: If you do not have a product key, select the **Specify a free edition** option, and then click **Evaluation** from the drop-down list for a 180-day evaluation period.



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



On the **Product Updates** page, select the **Include SQL Server product updates** check box, and click **Next** to continue.

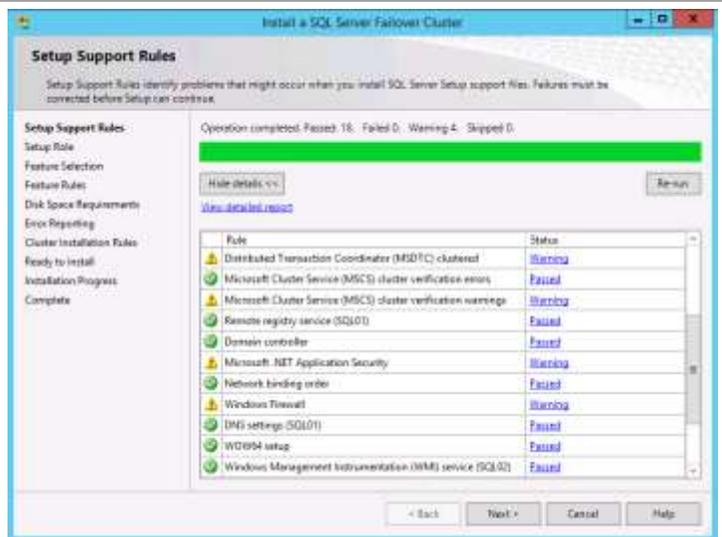


On the **Install Setup Files** page, click **Install Setup Files** and allow the files to install.



On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.

Note: Common issues include MSDTC, MSCS, and Windows Firewall warnings. The use of MSDTC is not required for the System Center 2012 R2 environment.



On the **Setup Role** page, select **SQL Server Feature Installation**, and click **Next** to continue.

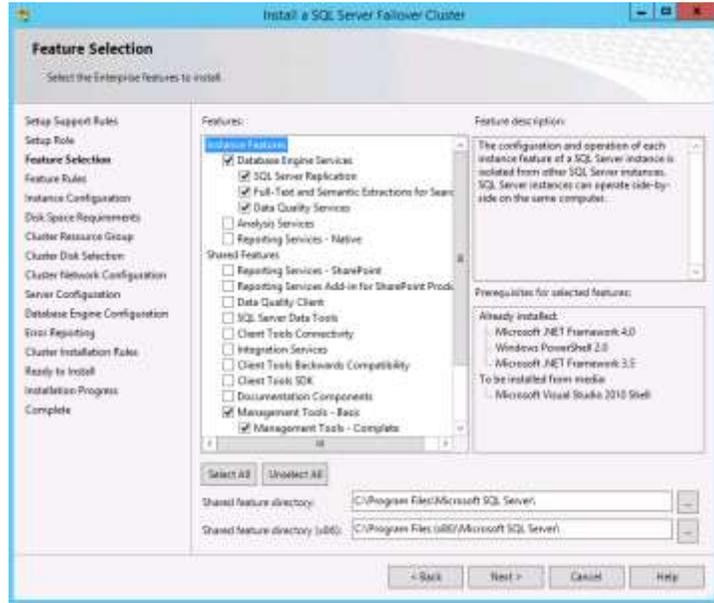


On the **Feature Selection** page, features for the various instances will be selected. **Note:** Not all features are supported for failover cluster installations, so the features for the IaaS PLA are limited to the features in the following list. SQL Server with failover clusters requires the selection of the **SQL Server Replication** check box and **Full-Text Search** check box with every instance. The following additional selections are required for each instance:

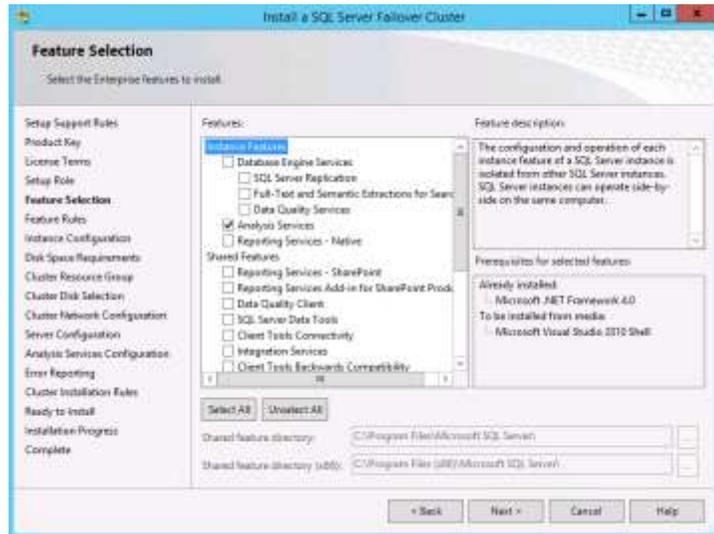
- SCDB - Database Engine Services
- SCOMDB - Database Engine Services
- SCOMDW - Database Engine Services
- SCSMAS - Analysis Services
- SCSMDB - Database Engine Services
- SCSMDW - Database Engine Services
- SCVMMDB - Database Engine Services

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

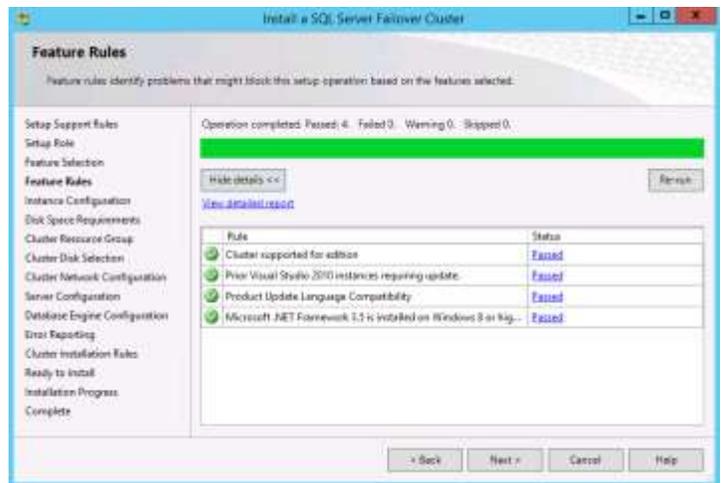
Database Engine Services (all instances except SCSMAS):



Analysis Services (SCSMAS instance only):



On the **Feature Rules** page, click **Next** to continue. **Show details** and **View detailed report** can be viewed if required.

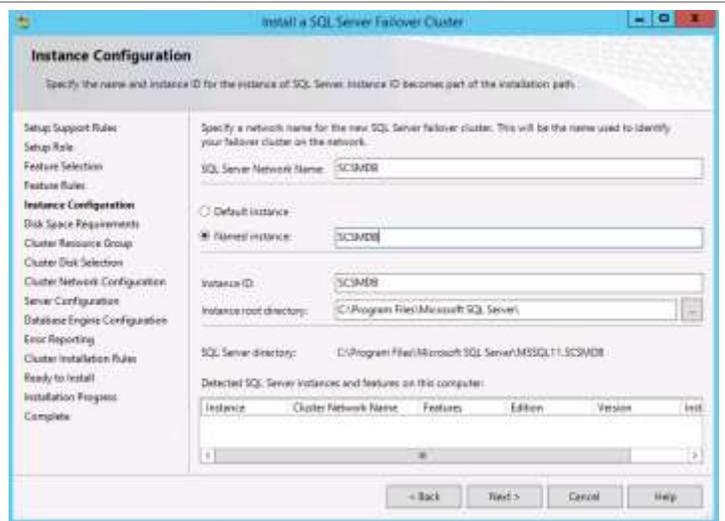


On the **Instance Configuration** page, make the following selections (refer to the worksheet that you created earlier):

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

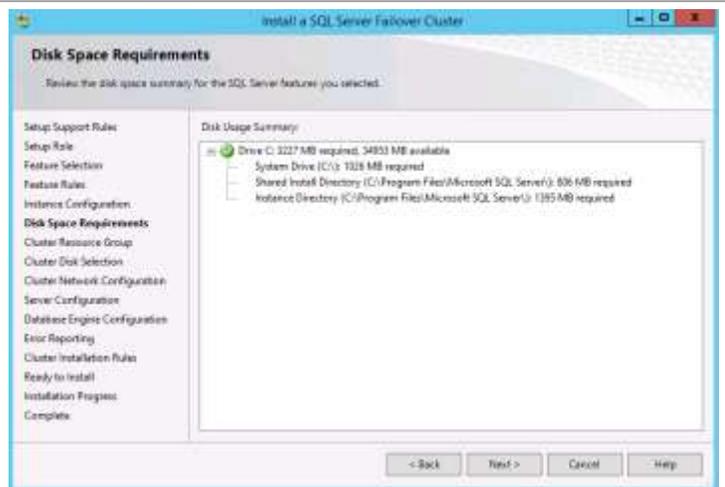
Select the **Named instance** option. In the provided text box, specify the instance name being installed:

- **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.

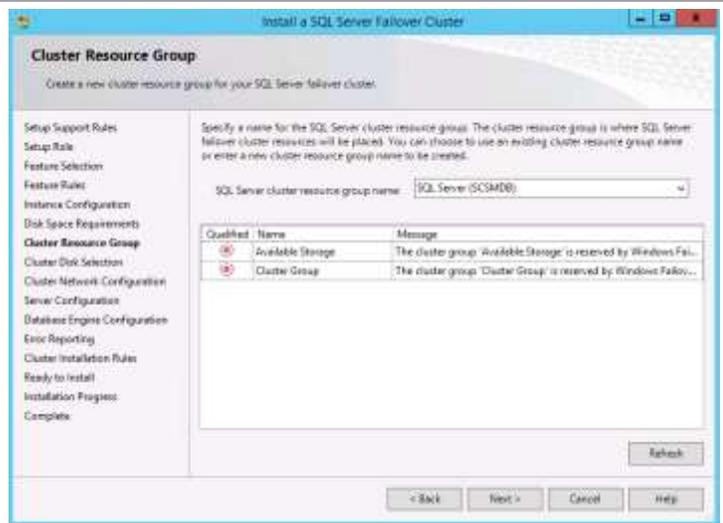


Click **Next** to continue.

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

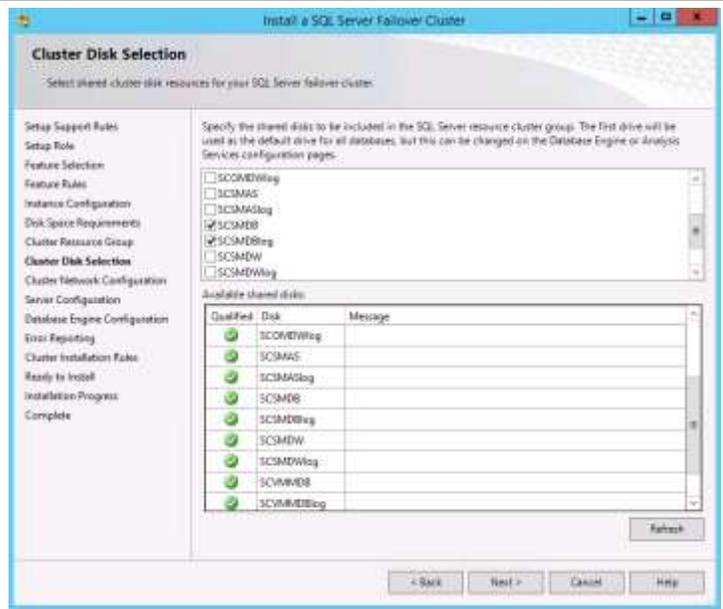


On the **Cluster Resource Group** page, in the **SQL Server cluster resource group name** drop-down list, accept the default value of **SQL Server (<InstanceName>)**. Click **Next** to continue.



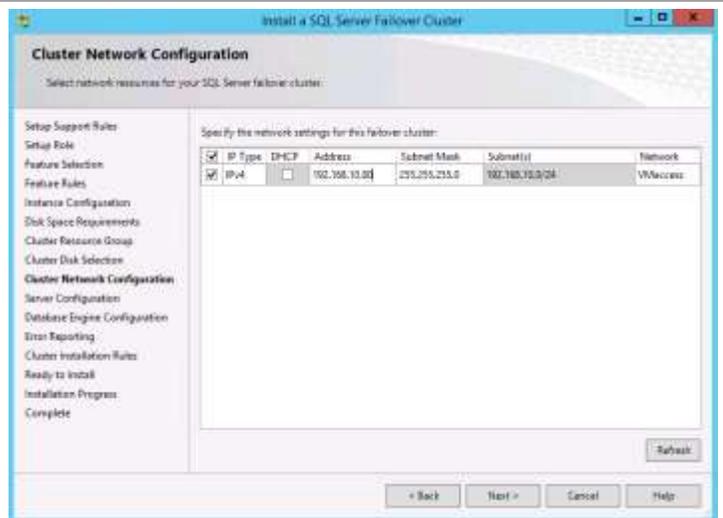
On the **Cluster Disk Selection** page, refer to the worksheet that you created earlier to make the proper disk selections. Two cluster disks will be selected to support separation of databases and logs for each database instance. Make the selections by selecting the appropriate **Cluster Disk** check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

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



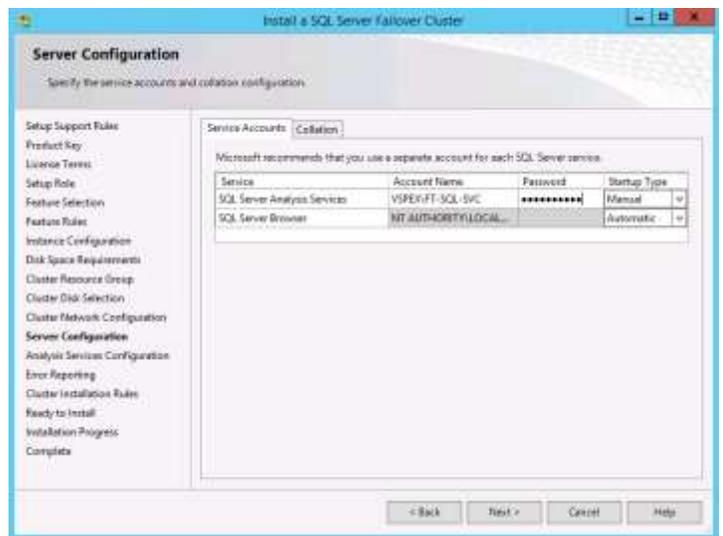
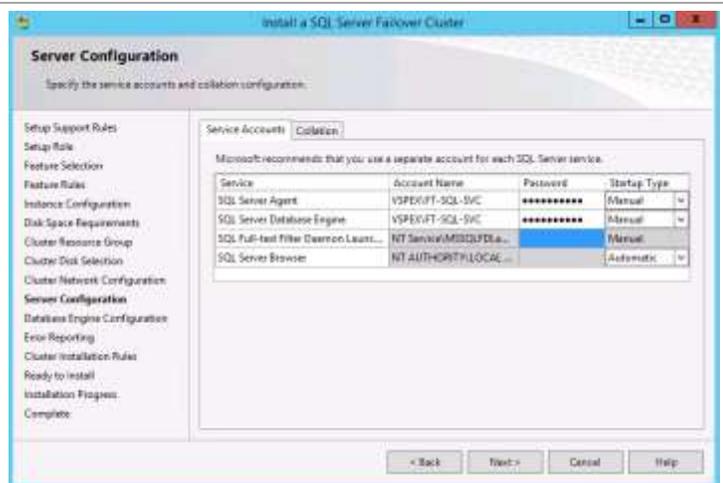
On the **Cluster Network Configuration** page, refer to the worksheet that you created earlier to assign the correct IP address for each instance. Clear the **DHCP** check box if you are using static addressing, and enter the IP address in the **Address** field text box.

Click **Next** to continue.

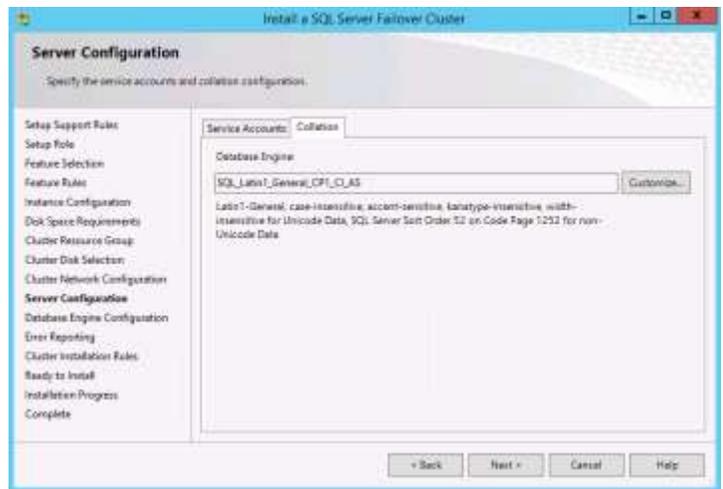


On the **Server Configuration** page, click the **Service Accounts** tab. Specify the SQL Server Service account and associated password for the **SQL Server Agent** and **SQL Server Database Engine** services.

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

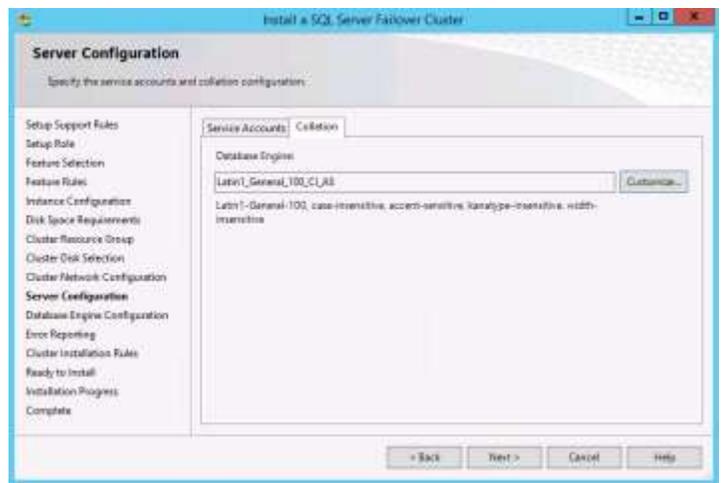
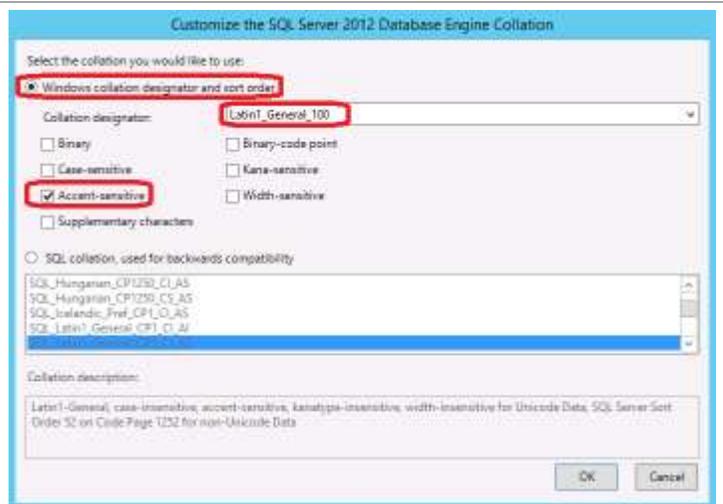


On the same **Server Configuration** page, click the **Collation** tab. Click the **Customize...** button to change the collation.

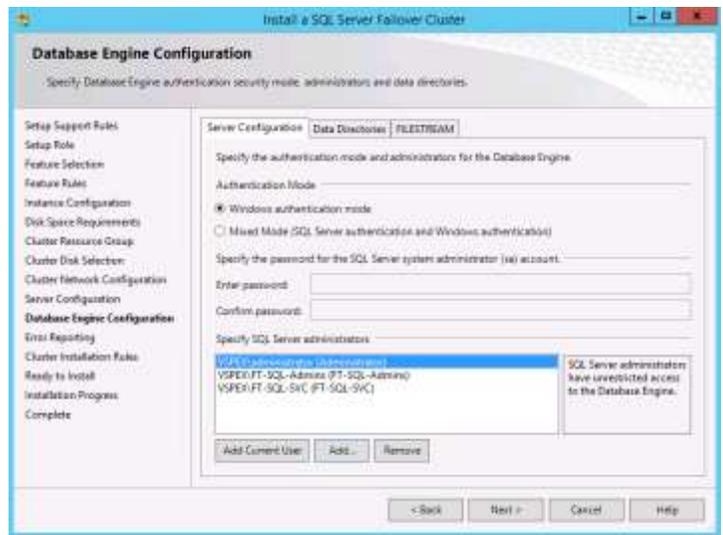


Select the radio button by **Windows collation designator and sort order**. From the drop down list, select **Latin1_General_100**. Check the box by **Accent-sensitive**. This sets the value to Latin1_General_100_CI_AS. Do this for all instances. Click **OK** to continue. Then click **Next** back on the Server Configuration page to continue.

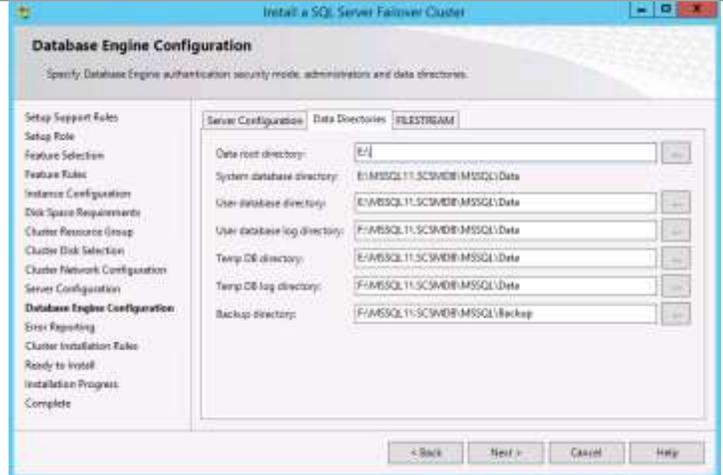
Note: If it is required to use a collation other than English, please contact Microsoft for assistance in properly configuring collation.



On the **Database Engine Configuration** page, **Server Configuration** tab, in the **Authentication Mode** section, select the **Windows authentication mode** option. In the **Specify SQL Server administrators** section, click the **Add Current User** button to add the current installation user. Click the **Add...** button to select the previously created SQL Server Admins group and the SQL service account from the object picker. You can also add any application specific service accounts and groups at this point or add them later.



On the same **Database Engine Configuration** page, click the **Data Directories** tab. The proper drive letter or mount point associated with the Cluster Disk resource for SQL Server data should be specified. If not, verify that the proper Cluster Disk resource check boxes were selected earlier and enter the proper drive letter in the **Data root directory** text box.



To redirect log files by default to the second Cluster Disk resource, change the drive letter in the **User databaselog directory** and **Temp DB log directory** text boxes.

It is also recommended to change the **Backup Directory** to a separate drive such as the log drive. Do not change the folder structure unless your organization has specific standards for this. When complete, click **Next** to continue.

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

In instances that contain Analysis Services, on the **Analysis Services Configuration** page, click the **Server Configuration** tab. In the **Specify which users have administrative permissions for Analysis Services** section, click **Add Current User** to add the current installation user.

Click **Add...** to select the following groups:

Service Manager instance:

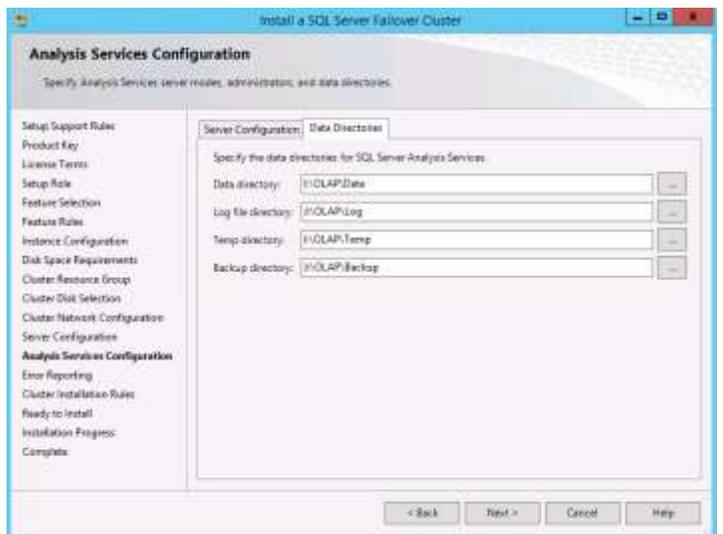
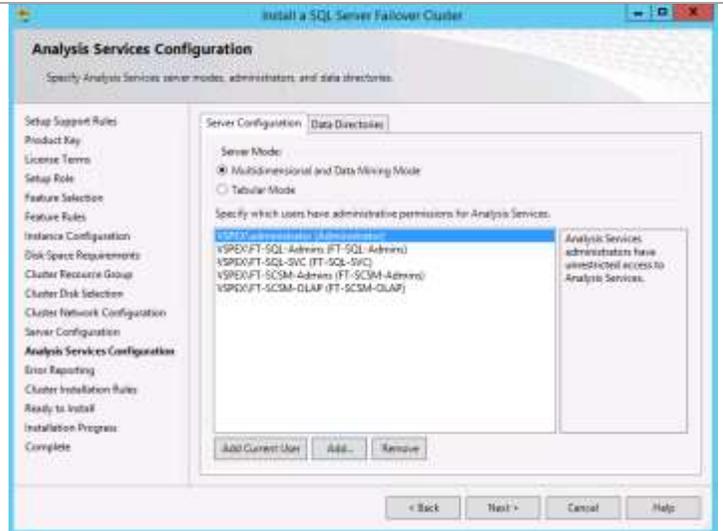
- SQL Server Admins group
- SQL Server Service account
- SM Admins group
- SM OLAP account

On the **Data Directories** tab, use the following configuration

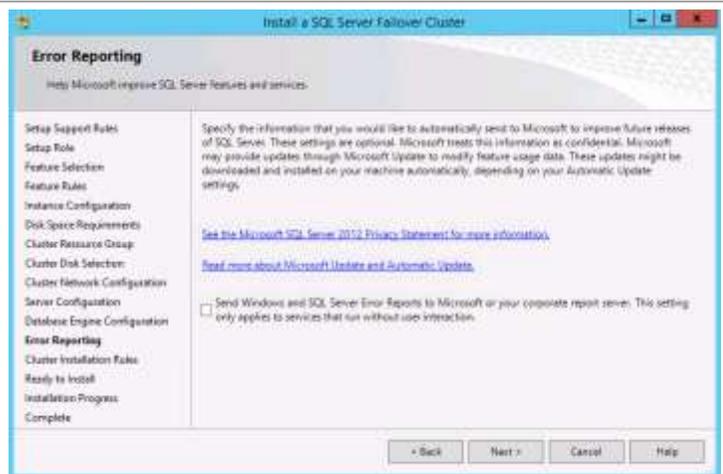
Set the **Data directory**, and **Temp directory** to the cluster disk that is configured for the database files.

Set the **Log file directory** and the **Backup directory** to the cluster disk that is configured for the log files.

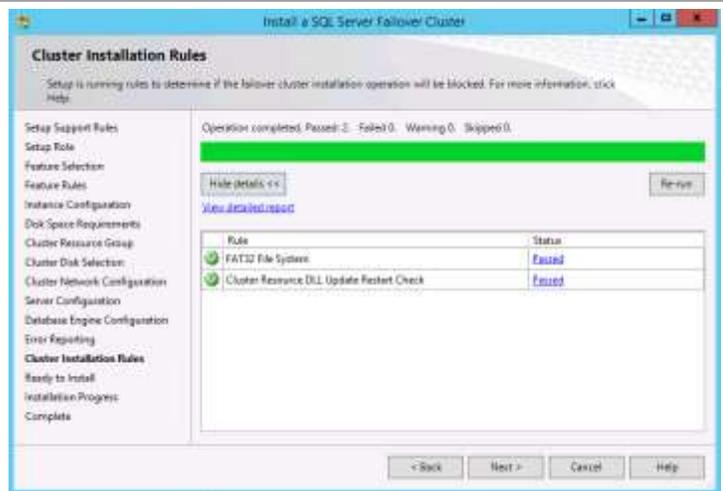
Do not change the folder structure unless your organization has specific standards for this. Click **Next** to continue.



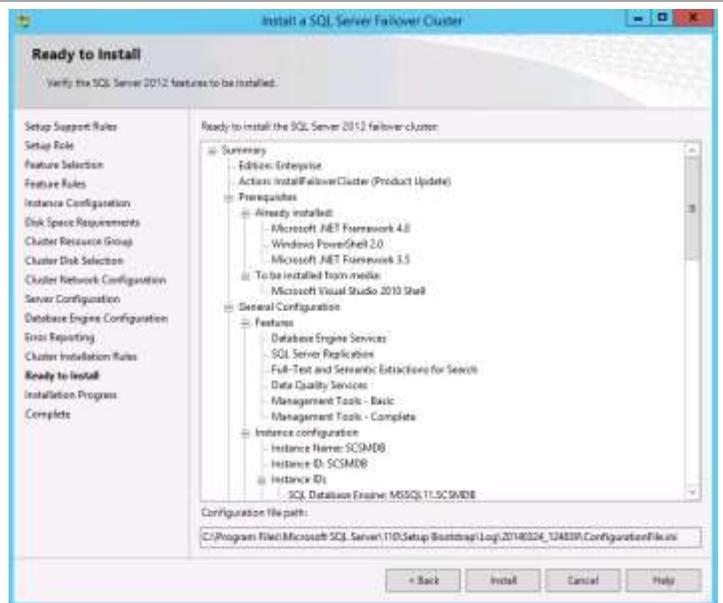
On the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies, and click **Next** to continue.



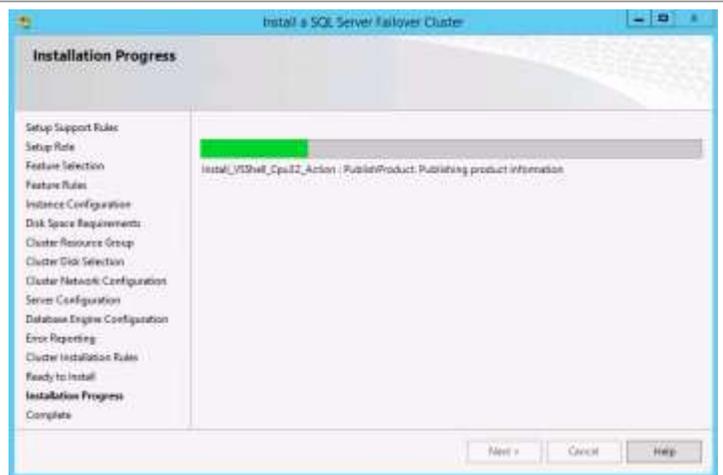
On the **Cluster Installation Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



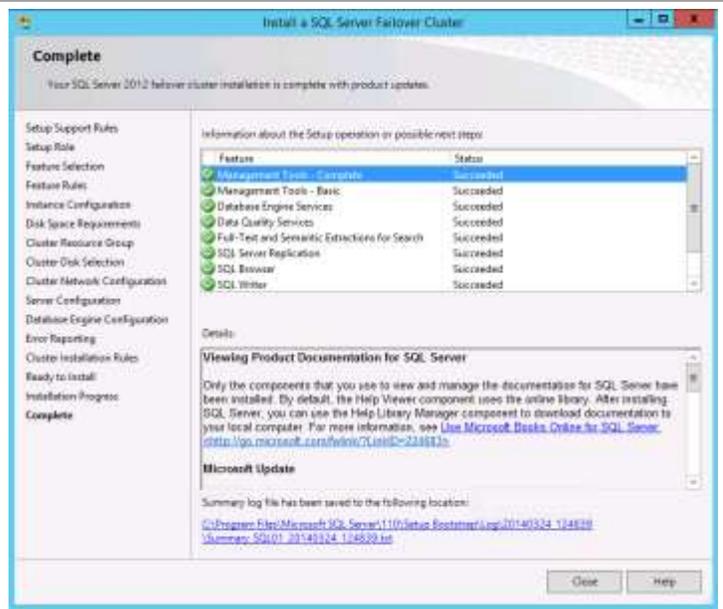
On the **Ready to Install** page, verify all of the settings that were entered during the setup process, and click **Install** to begin the installation of the SQL Server instance.



On the **Installation Progress** page, the installation progress will be displayed.



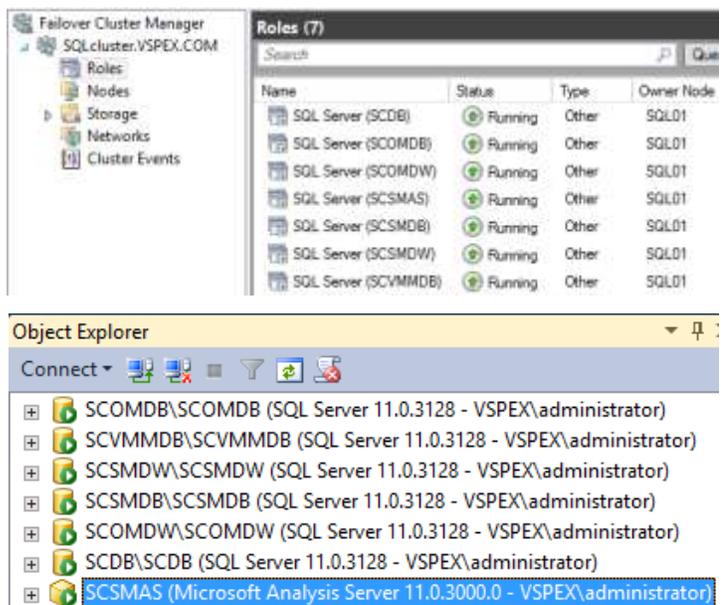
When the installation is complete, the **Complete** page will appear. Click **Close**.



Repeat these steps for each associated SQL Server instance that is required for the IaaS PLA fabric management installation (seven instances total).

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

NOTE: The default value for Analysis Services is **SCSMAS\SCSMAS** and needs to be changed to **SCSMAS**



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

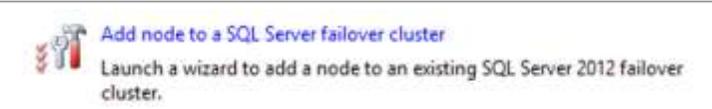
After the creation of all required SQL Server instances on Node 1 is complete, additional nodes (Node 2 is required and additional nodes are optional) can be added to each instance of the cluster. Follow these steps to begin the installation of additional nodes of the cluster.

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

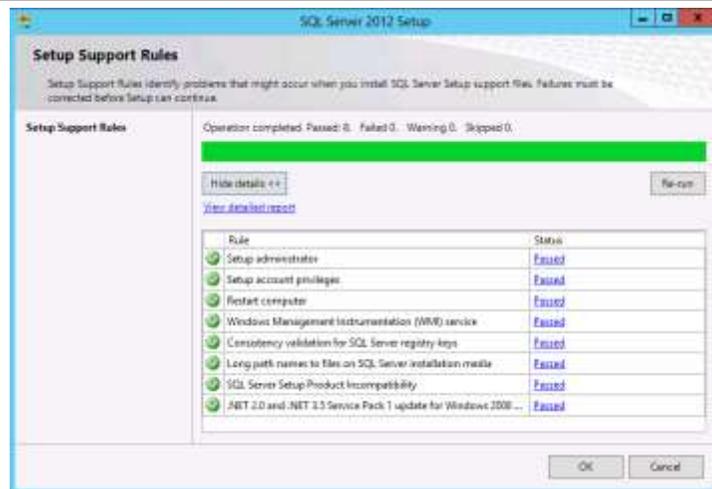
From the SQL Server 2012 SP1 installation media source, right-click setup.exe and click **Run as administrator** to begin setup. The **SQL Server Installation Center** will appear.



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

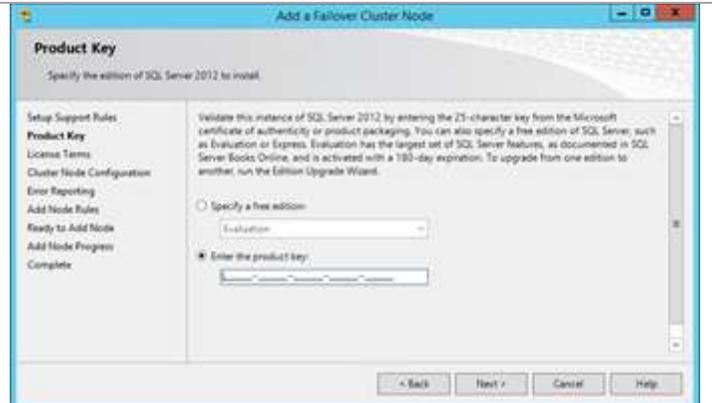


The SQL Server 2012 Setup Wizard will appear. On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **OK** to continue.



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

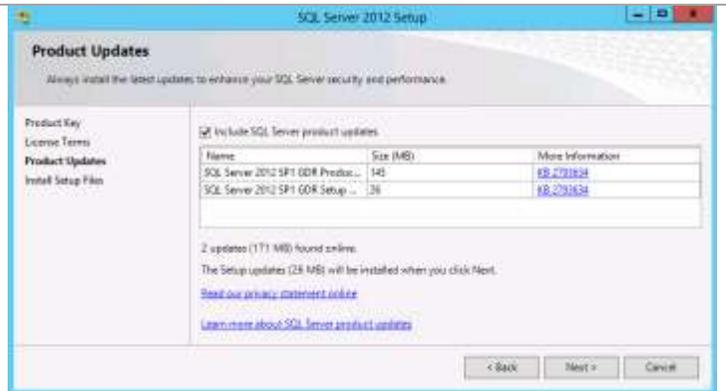
Note: If you do not have a product key, select the **Specify a free edition** option, and select **Evaluation** from the drop-down list for a 180-day evaluation period.



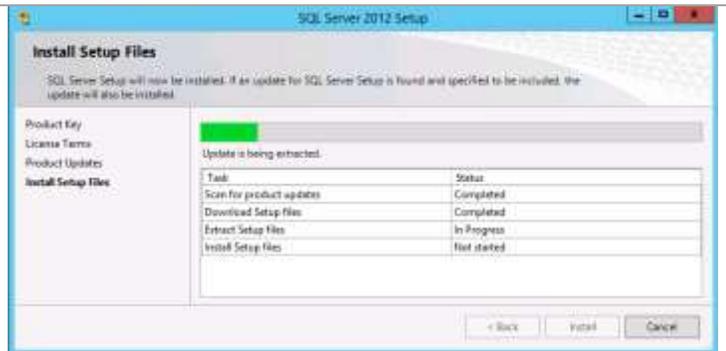
On the **License Terms** page, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft**, based on your organization's policies, and click **Next** to continue.



On the **Product Updates** page, select the **Include SQL Server product updates** check box, and click **Next** to continue.

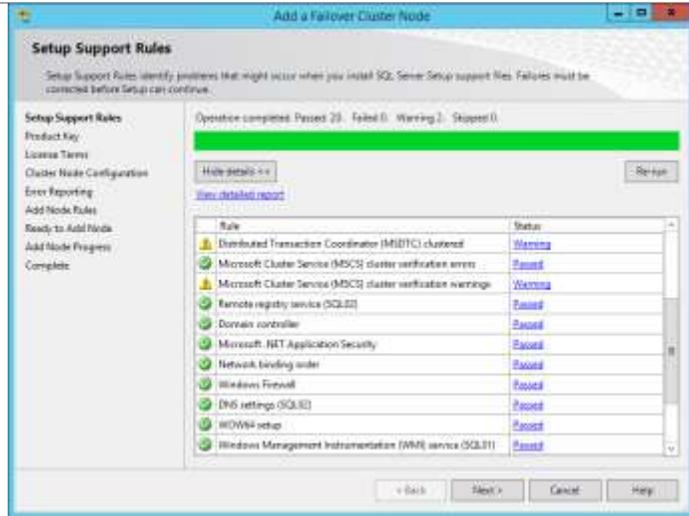


On the **Install Setup Files** page, click **Install**, and allow the support files to install.

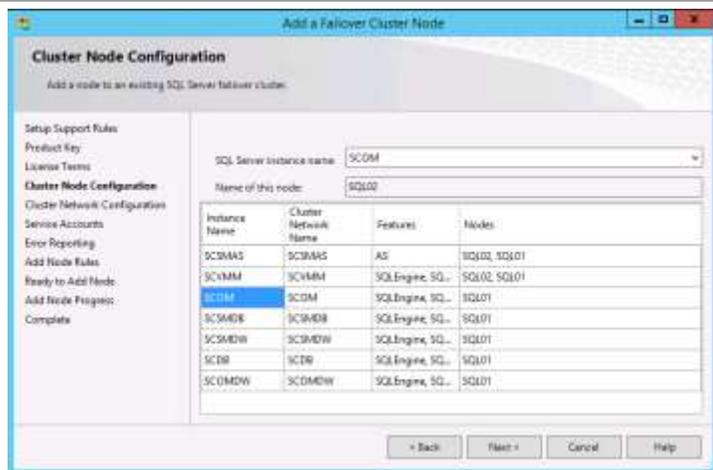


On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.

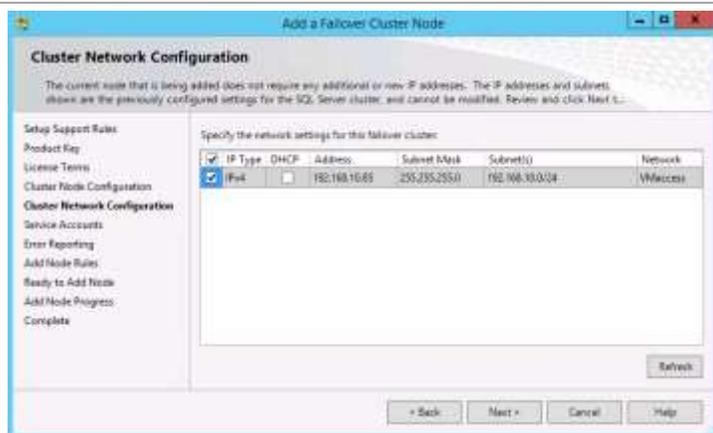
Note: Common issues include MSDTC, MSCS, and Windows Firewall warnings. The use of MSDTC is not required for the System Center 2012 R2 environment.



On the **Cluster Node Configuration** page, select the desired instance name from the **SQL Server instance name** drop-down list. Each instance will be listed along with the nodes that are currently assigned to each instance. Click **Next** to continue.

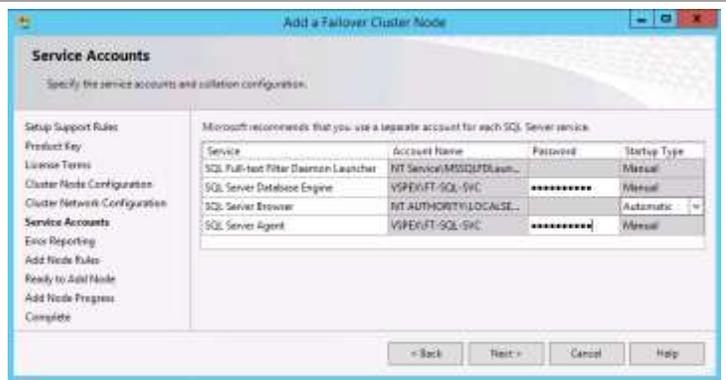


On the **Cluster Network Configuration** page, the network configuration values are displayed and set based on the existing failover cluster instance values from the first node. They cannot be modified. Click **Next** to continue.



On the **Service Accounts** page, specify the SQL Server Service Account and an associated password for the **SQL Server Agent** and **SQL Server Database Engine** services. Click **Next** to continue.

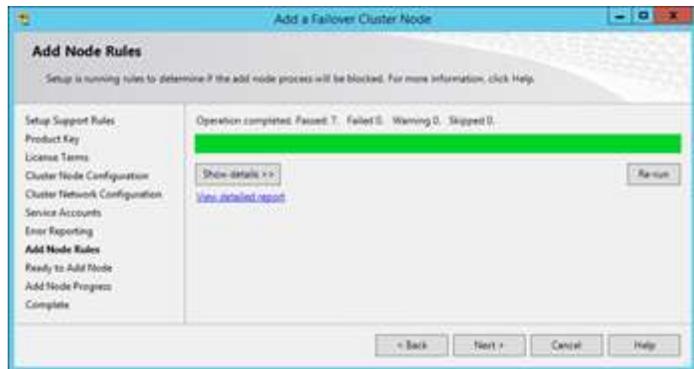
Note: For the SCSMAS instance only, an additional password must be supplied for the **SQL Server Analysis Services** service account.



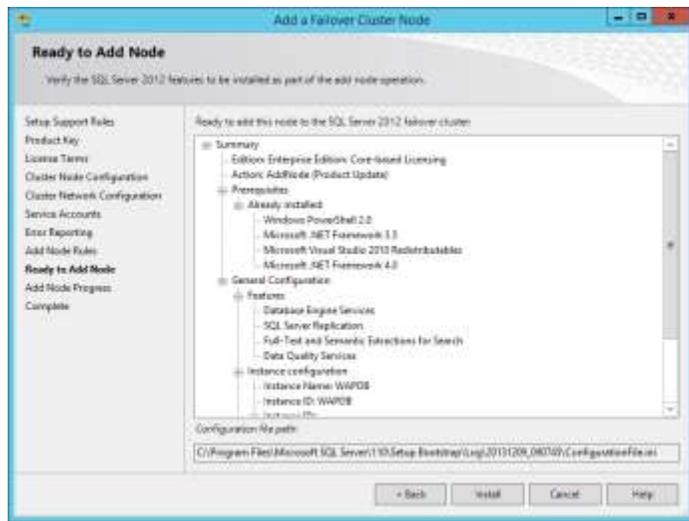
On the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies, and click **Next** to continue.



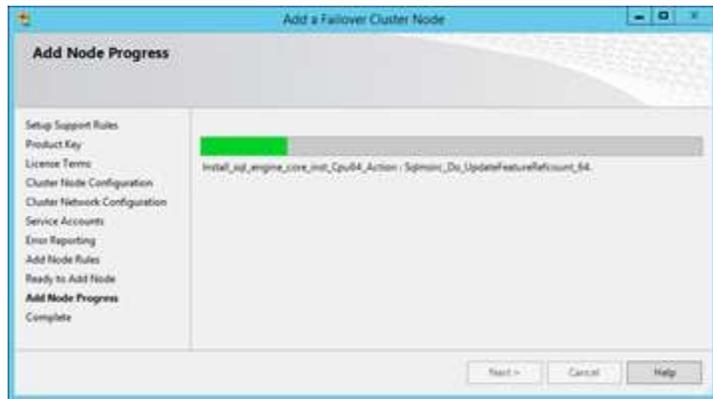
On the **Add Node Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



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



The **Add Node Progress** screen will display real-time progress for the operation.

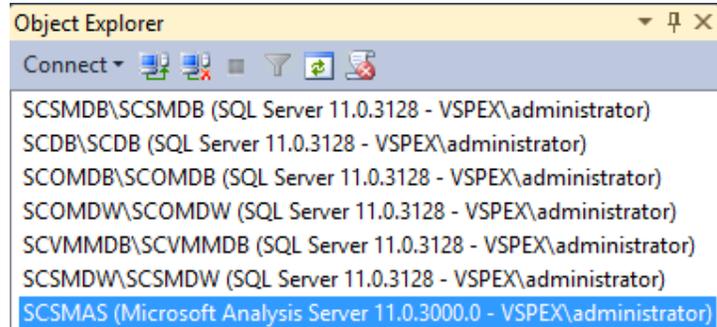
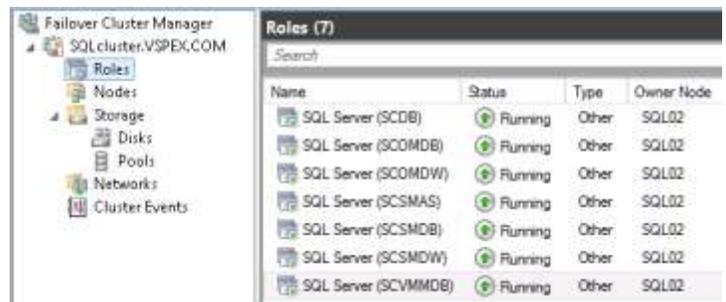


When the installation is complete, the **Complete** page will appear. Click **Close** to complete the installation of this SQL Server database instance.

Repeat these steps for each associated SQL Server instance that is required for IaaS PLA fabric management installation (seven instances total).

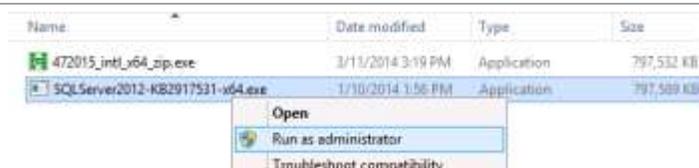
Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server 2012 Management Studio prior to moving to the next step of installation. Move all instances to the node.

NOTE: The default value for Analysis Services is **SCSMAS\SCSMAS** and needs to be changed to **SCSMAS**



When complete, install the latest cumulative update for SQL Server 2012 SP1 on each node of the SQL cluster. To avoid warnings during the installation, move all instances off the node being patched. Note that at the time of writing, the latest is Cumulative Update 8. Integration with initial install can be achieved using the following command line during setup:

```
\Setup.exe /Action=Install /UpdateSource=[PATH]
```



Post-Installation Tasks

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

Configure Windows Firewall Settings for SQL Server Named Instances

To support the multi-instance cluster, you must configure each SQL Server instance to use a specific TCP/IP port for the database engine or analysis services. The default instance of the database engine uses port 1433, and named instances use dynamic ports. To configure the firewall rules to allow access to each named instance, static listening ports must be assigned.

Use the following procedure to configure the TCP/IP port. For more information, see [Configure a Server to Listen on a Specific TCP Port \(SQL Server Configuration Manager\)](#)¹.

¹ Additional information for configuring the Windows Firewall to support SQL Server can be found at <http://technet.microsoft.com/library/cc646023.aspx> and <http://technet.microsoft.com/library/ms174937.aspx>.

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

Open an administrative **Command Prompt** by searching for and selecting **CMD.EXE**, then right-click and select **Run as Administrator**. Within the command prompt type the following command:

netstat -b

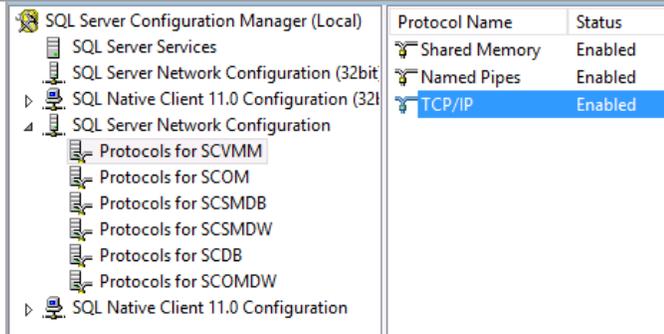
The existing dynamic ports used by the SQLSERVER.EXE sessions will appear.

```
TCP 192.168.10.80:58428 SQL01:65305 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.80:58428 SQL01:65314 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.80:58428 SQL01:65315 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.81:59699 SQL01:65363 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.81:59699 SQL01:65371 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.81:59699 SQL01:65372 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.83:61968 SQL01:65407 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.83:61968 SQL01:65415 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.83:61968 SQL01:65417 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.84:54950 SQL01:65153 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.84:54950 SQL01:65161 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.84:54950 SQL01:65163 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.85:50094 SQL01:65197 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.85:50094 SQL01:65206 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.85:50094 SQL01:65207 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.86:62650 SQL01:65509 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.86:62650 SQL01:65517 ESTABLISHED
[sqlservr.exe]
TCP 192.168.10.86:62650 SQL01:65518 ESTABLISHED
[sqlservr.exe]
```

On the first SQL Server node, open **SQL Configuration Manager**.



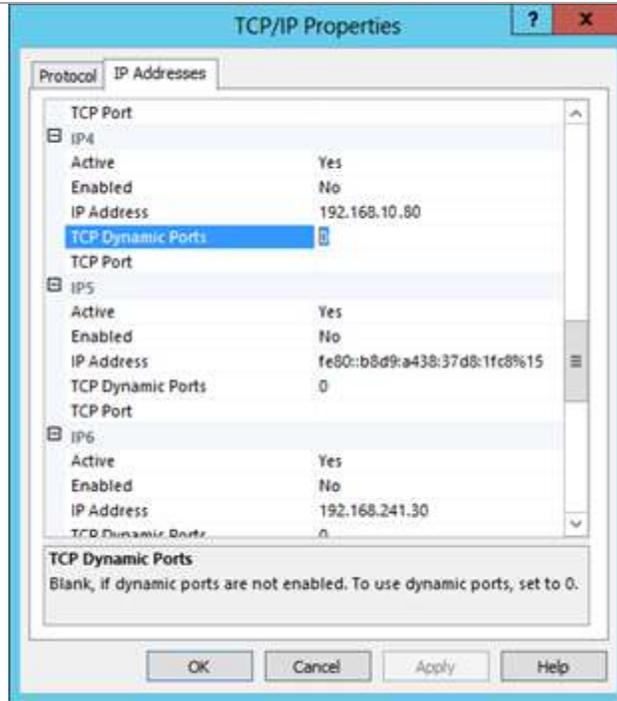
In the **SQL Server Configuration Manager** console pane, expand the **SQL Server Network Configuration** node and then click **Protocols for the <instance name>**. Double-click **TCP/IP** from the available protocol names to observe its properties.



On the **TCP/IP Properties** page, click the **IP Addresses** tab. Several IP addresses appear in the format IP1, IP2, up to IPAll. Each address will include several values:

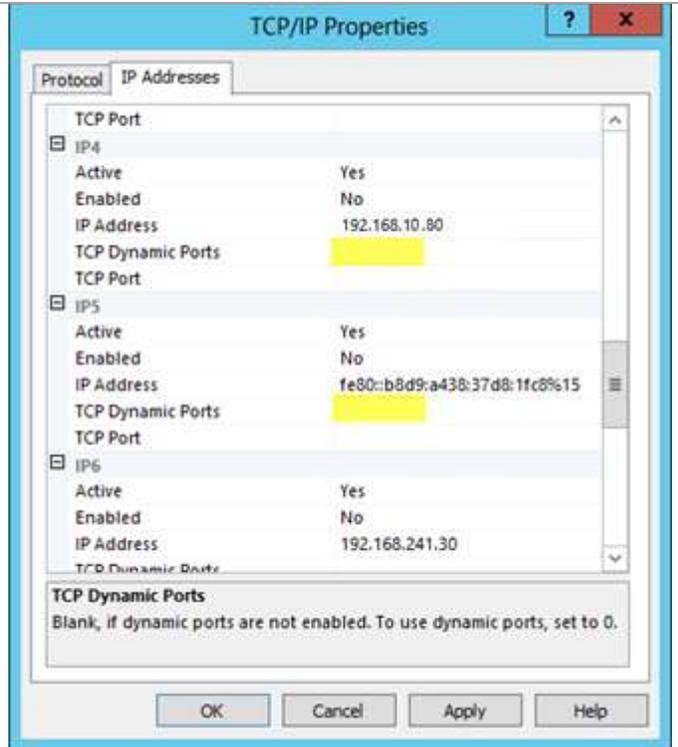
- **Active** - Indicates that the IP address is active on the computer. Not available for IPAll.
- **Enabled** - If the **Listen All** property in **TCP/IP Properties** (on the **Protocol** tab) is set to **No**, this property indicates whether SQL Server is listening on the IP address. If the **Listen All** property in **TCP/IP Properties** (on the **Protocol** tab) is set to **Yes**, the property is disregarded. Not available for IPAll.
- **IP Address** - View or change the IP address used by this connection. Lists the IP address that is used by the computer and the IP loopback address, 127.0.0.1. Not available for IPAll. The IP address can be in IPv4 or IPv6 format.
- **TCP Dynamic Ports** - Blank if dynamic ports are not enabled. To use dynamic ports, set to 0. For IPAll, displays the port number of the dynamic port used.
- **TCP Port** - View or change the port on which SQL Server listens. By default, the default instance of Database Engine listens on port 1433.

SQL Server Database Engine can listen on multiple ports on the same IP address. List the ports separated by commas in the format 1433, 1500, 1501. This field is limited to 2047 characters. To configure a single IP address to listen on multiple ports, the **Listen All** parameter must also be set to **No** in the **TCP/IP Properties** on the **Protocols** tab.

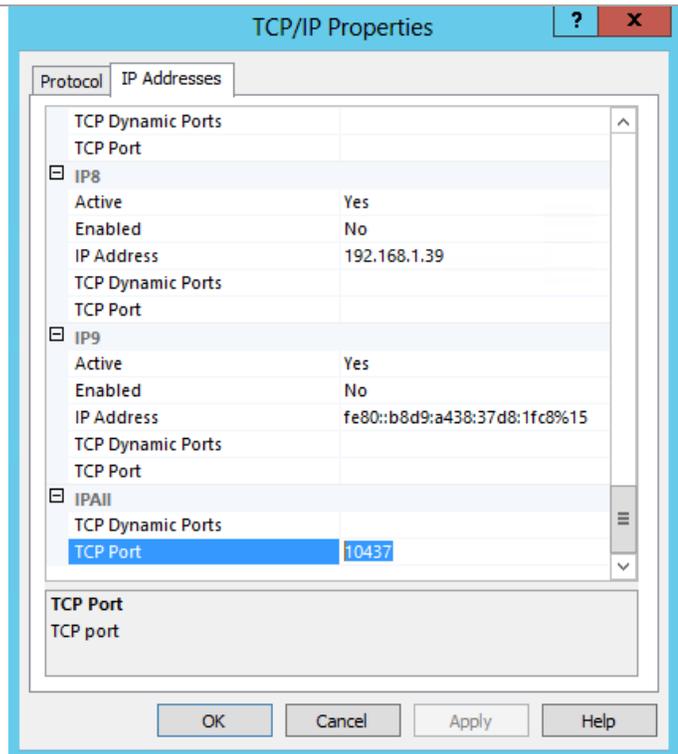


For more information see [How to: Configure the Database Engine to Listen on Multiple TCP Ports](#).

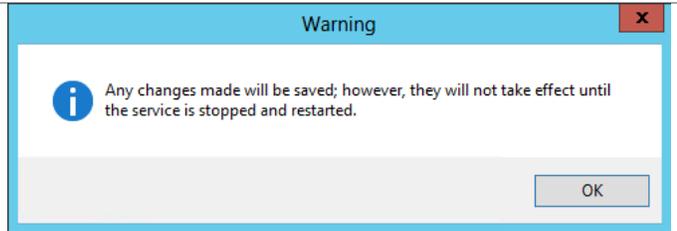
Within the dialog box, browse to each IP address section for the instance, and delete the numerical value (0) from the **TCP Dynamic Ports** field.



Scroll down to the **IPAll** section, and delete the existing dynamic port value from **TCP Dynamic Ports** property. Assign a static port value under **TCP Port** that is appropriate for the instance. For this example, port 10437 was specified. Click **Apply** to save the changes.



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



Repeat these steps to set a static port for each database service instance. Reference the SQL Server settings table at the beginning of this section for the default values that are used in this guide.

When all of the database instances are configured, close **SQL Server Configuration Manager** and continue to the next steps to change the SSAS instance listening port.

SQL Instance	Listening Port
SCSMDB	10480
SCSMDW	10481
SCSMAS	10482
SCDB	10483
SCVMMDB	10484
SCOMDB	10485
SCOMDW	10486

Open **SQL Server Management Studio**.

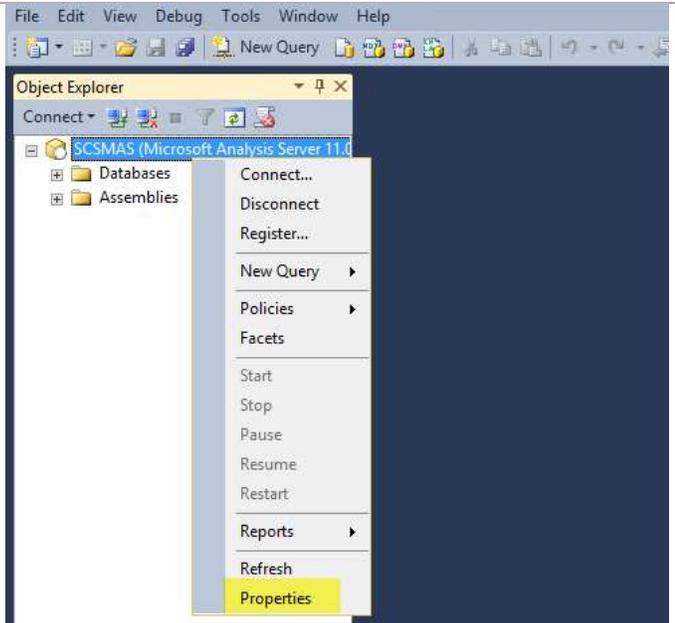


On the **Connect to Server** page, input the connection values for the SSAS instance.

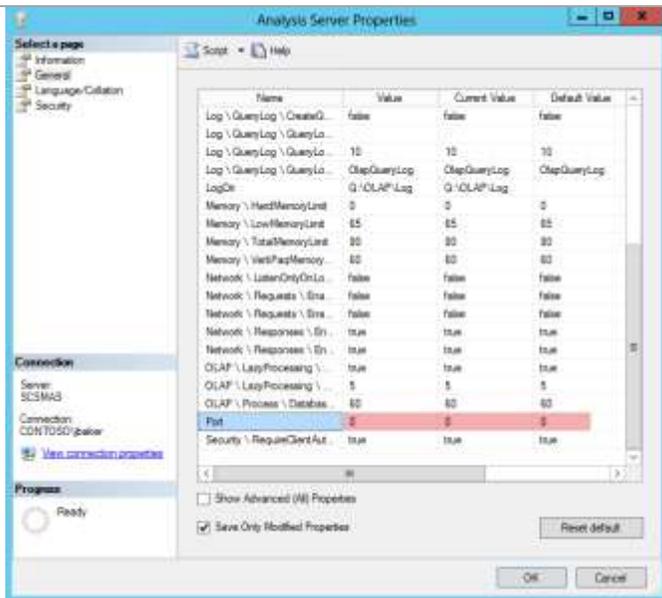
Connect to connect to the instance.



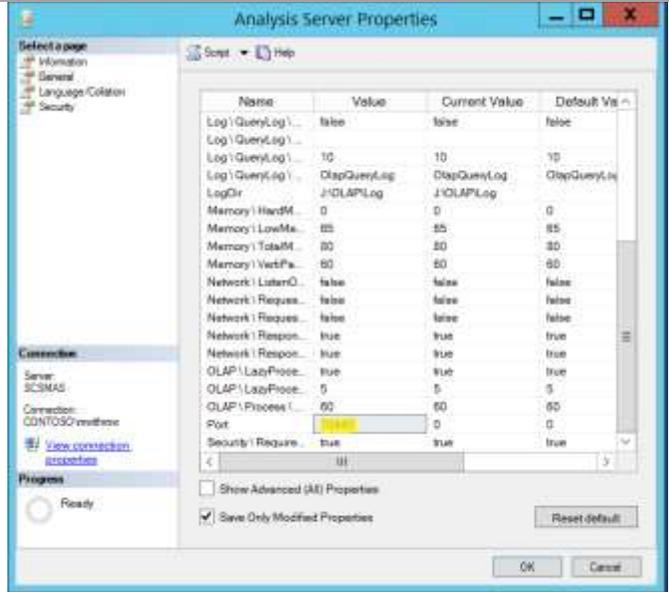
When you are connected to the instance in **SQL Management Studio**, right-click the SSAS instance and click **Properties**.



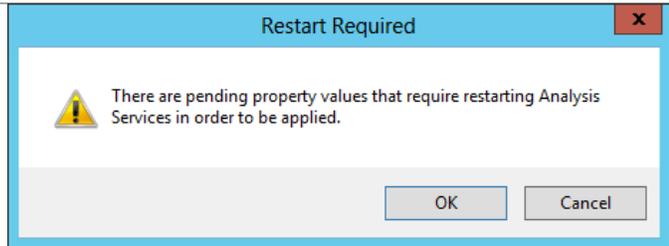
On the **Analysis Server Properties** page, click the **General** tab, and in the **Name** column, click **Port**. By default the value will be set to “0” (zero) to specify a dynamic port.



On the same page, in the **Value** column, specify an appropriate static port value, then click **OK** to save the changes.



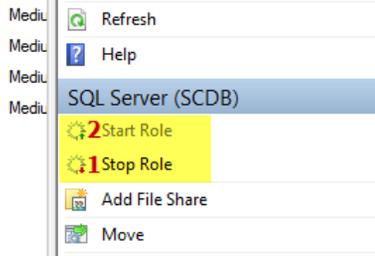
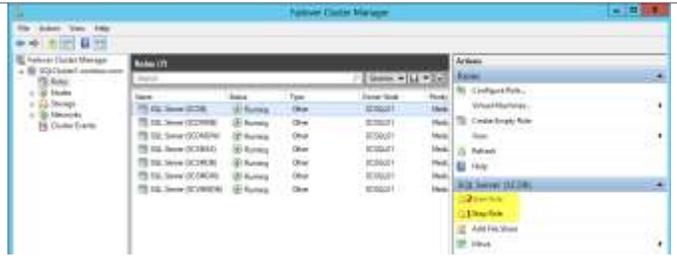
A message will appear outlining that a restart is required. Click **OK** and close SQL Management Studio.



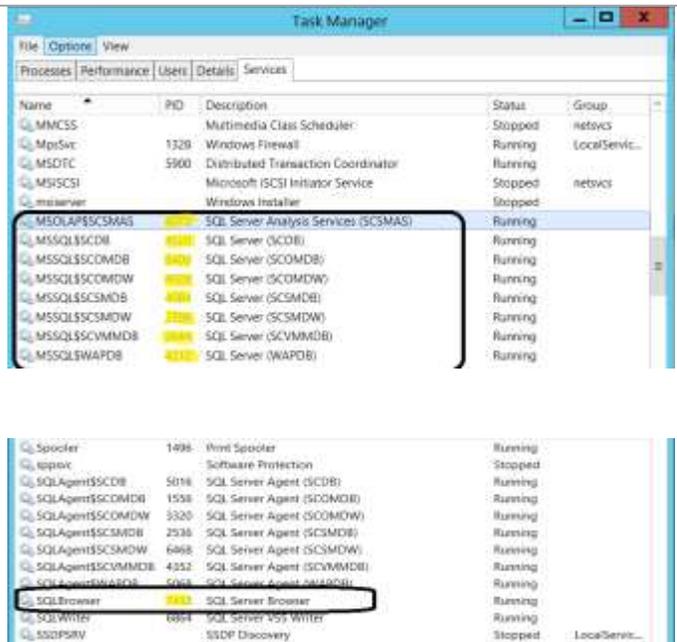
Open **Failover Cluster Manager** and expand the **Roles** node.



To apply the new port settings, in **Failover Cluster Manager**, select each SQL Server instance (this must be repeated per instance). In the Action pane, select **Stop Role** to stop the service for each instance. Restart each instance by selecting **Start Role** from the Action pane. Close the **Failover Cluster Manager** console.



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



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



Import the CSV file into Excel to then format the data into a spreadsheet.

Locate the PIDs you documented from the Task Manager previously. Then filter on the state column to identify the listening and blank values.

The resulting table should confirm that all of the SQL instances are listening on only the static ports assigned previously.

In addition to the static ports for each instance, the 2382 TCP/UDP and 1434 TCP/UDP ports for the SQL Server Browser are also listed. You must open them in the firewall settings to support the Analysis and Database Engine instances.

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING	1876
TCP	192.168.10.80:10480	0.0.0.0:0	LISTENING	5172
TCP	192.168.10.81:10481	0.0.0.0:0	LISTENING	7656
TCP	192.168.10.82:10482	0.0.0.0:0	LISTENING	7956
TCP	192.168.10.83:10483	0.0.0.0:0	LISTENING	8760
TCP	192.168.10.84:10484	0.0.0.0:0	LISTENING	3596
TCP	192.168.10.85:10485	0.0.0.0:0	LISTENING	5148
TCP	192.168.10.86:10486	0.0.0.0:0	LISTENING	1228
TCP	[::]:2382	[::]:0	LISTENING	1876
UDP	0.0.0.0:1434	*:*		1876
UDP	[::]:1434	*:*		1876

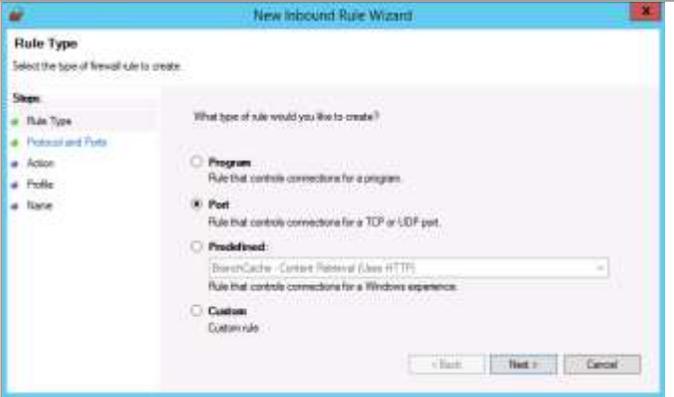
When completed, configure the Windows Firewall rule for the SQL Server Browser. To perform this action, on each node in the Windows Failover Cluster that will host SQL Server instances, open the **Windows Firewall with Advanced Security** MMC console.



In the **Windows Firewall with Advanced Security** MMC console, click the **Inbound Rules** node, and click **New Rule...** in the Action pane.



In the New Inbound Rule Wizard, on the **Rule Type** page, select the **Port** button, and click **Next** to continue.



On the **Protocol and Ports** page, select the **UDP** button. Select the **Specific local ports** button and type 1434 in the text box. This enables access to the SQL Server Browser for Database Engine instances. Click **Next** to continue.



On the **Action** page, select the **Allow the connection** button, and click **Next** to continue.

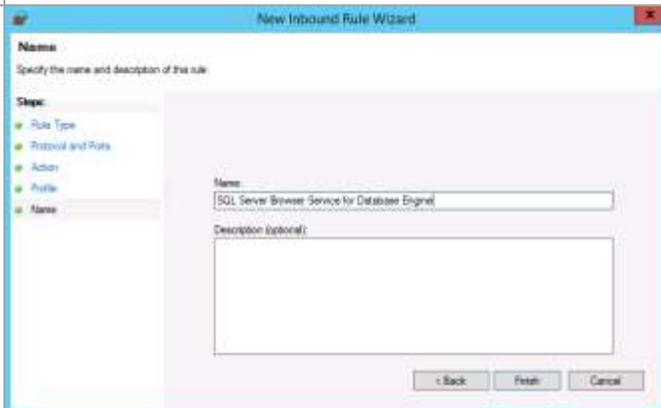


On the **Profile** page, leave the **Domain**, **Private**, and **Public** check boxes selected, and click **Next** to continue.

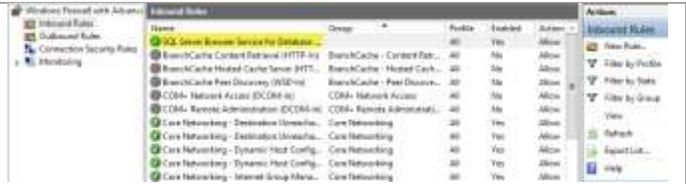
Note: Allowing the Private and Public network types enables this rule to support other scenarios such as the SQL Server AlwaysOn Multisite Failover Cluster Instance for database availability groups when replication may take place on a network other than the domain network.



Specify a name for the new rule, such as **SQL Server Browser Service for Database Engine**, and click **Finish**.



Note the new rule listed in under **Inbound Rules**. Click **New Rule** again from the Action pane to create the **SQL Server Browser Service for Analysis Server** rule.

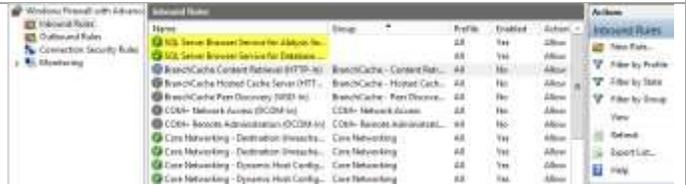


On the **Protocol and Ports** page, select the **TCP** and the **Specific local ports** buttons. In the **Specific local ports** text box, type **2382** to enable access to the **SQL Server Browser** for the Analysis Server instance.

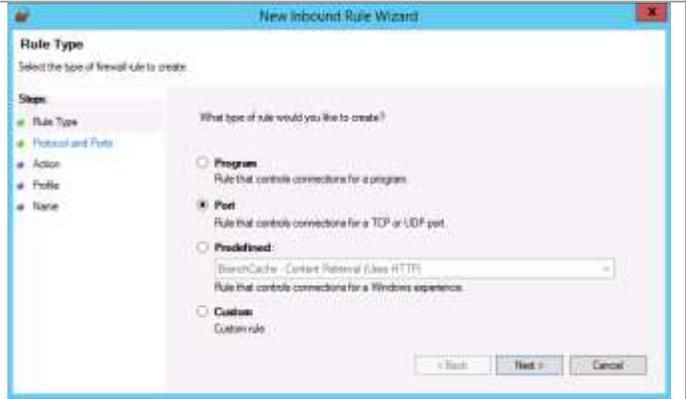


Note the additional new rule listed in the **Inbound Rules** pane.

Next, create and configure the inbound Windows Firewall rule for each SQL Server instance. In the same window, click **New Rule** in the Action pane to create the firewall rule for the first named instance.



In the New Inbound Rule Wizard, on the **Rule Type** page, select the **Port** button, and click **Next** to continue.



On the **Protocol and Ports** page, select the **TCP** button. Select the **Specific local ports** button and type the specific local TCP/IP port to enable access to the first named SQL Server instance. In this example, to enable access to the SQL Server instance, SCDB, the port specified is 10433.

Click **Next** to continue.



On the **Action** page, select the **Allow the connection** button and click **Next** to continue.

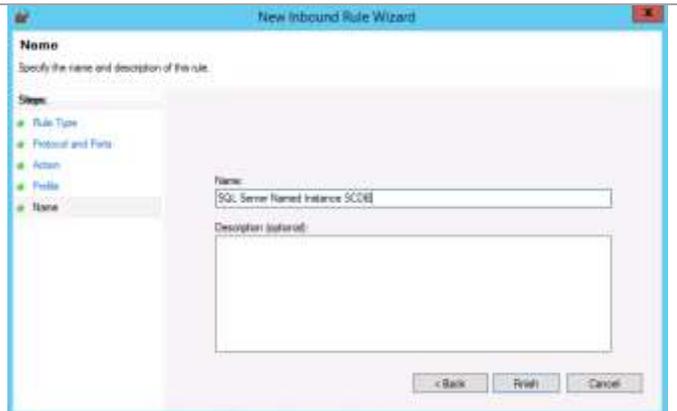


On the **Profile** page, leave the **Domain**, **Private**, and **Public** check boxes selected, and click **Next** to continue.

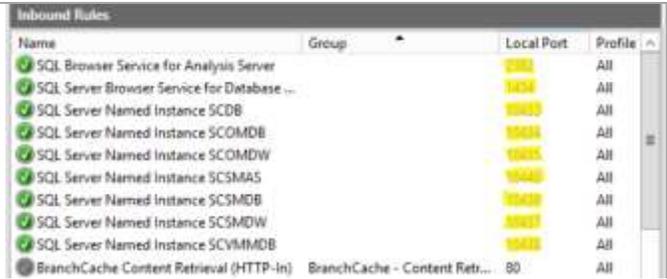
Note: Allowing the Private and Public network types enables this rule to support other scenarios such as the SQL Server AlwaysOn Multisite Failover Cluster Instance for database availability groups when replication may take place on a network other than the domain network.



Specify a name for the new rule, such as **SQL Server Named Instance SCDB**, and click **Finish**.



Create an additional rule for each SQL Server instance. This screenshot provides an example for how the rule set for the SQL Server architecture and instances would be configured.



Name	Group	Local Port	Profile
SQL Browser Service for Analysis Server		1356	All
SQL Server Browser Service for Database Engine		1434	All
SQL Server Named Instance SCODB		15433	All
SQL Server Named Instance SCOMDB		15434	All
SQL Server Named Instance SCOMDW		15435	All
SQL Server Named Instance SCSMAS		15436	All
SQL Server Named Instance SCSMDB		15437	All
SQL Server Named Instance SCSMDW		15438	All
SQL Server Named Instance SCVIMMDB		15439	All
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	80	All

Alternatively, firewall rules can be created through Windows PowerShell on the local server as shown in this example. Be sure to replace the port number value with the correct value for your environment.

`New-NetFirewallRule -DisplayName "SQL Server Browser Service for Database Engine" -LocalPort 1434 -Protocol UDP -Action Allow`

These commands provide an example for using Windows PowerShell to create rules on remote nodes.

```
$RemoteSession = New-CimSession -  
ComputerName SQL02
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Browser Service for Database Engine" -LocalPort  
1434 -Protocol UDP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Browser Service for Analysis Server" -  
LocalPort 2382 -Protocol TCP -Action Allow -  
CimSession $RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCDB" -LocalPort 10483 -Protocol  
TCP -Action Allow -CimSession $RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCVMMDB" -LocalPort 10484 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDB" -LocalPort 10485 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCOMDW" -LocalPort 10486 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDB" -LocalPort 10480 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMDW" -LocalPort 10481 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

```
New-NetFirewallRule -DisplayName "SQL Server  
Named Instance SCSMAS" -LocalPort 10482 -  
Protocol TCP -Action Allow -CimSession  
$RemoteSession
```

Assign Preferred Owners for SQL Server Instances in Failover Cluster Manager

To support the proper distribution of SQL Server instances across the multi-instance SQL Server cluster, you must configure failover clustering in Windows to assign preferred owners for each SQL Server instance. The following steps are provided to assist with this configuration. With a two node cluster, what the following steps make sure is that the SQL instances will generally run on the node specified first in the preferred owner list. For larger installations, it may make sense to have a third or fourth node added to the cluster. Then one node could be specified as the primary and specific node as the secondary preferred owner. This does not prevent the SQL instance from failing over to a different node than those specified in the preferred owner list, but it does make sure the instances remain balanced when preferred nodes are available.

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

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



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

To better control failover behavior and distribution of the instances, the **Preferred Owners** list must be modified and the owner node must be assigned by failing over the SQL Server instance to that node. To start this process, you need the list that you created previously.

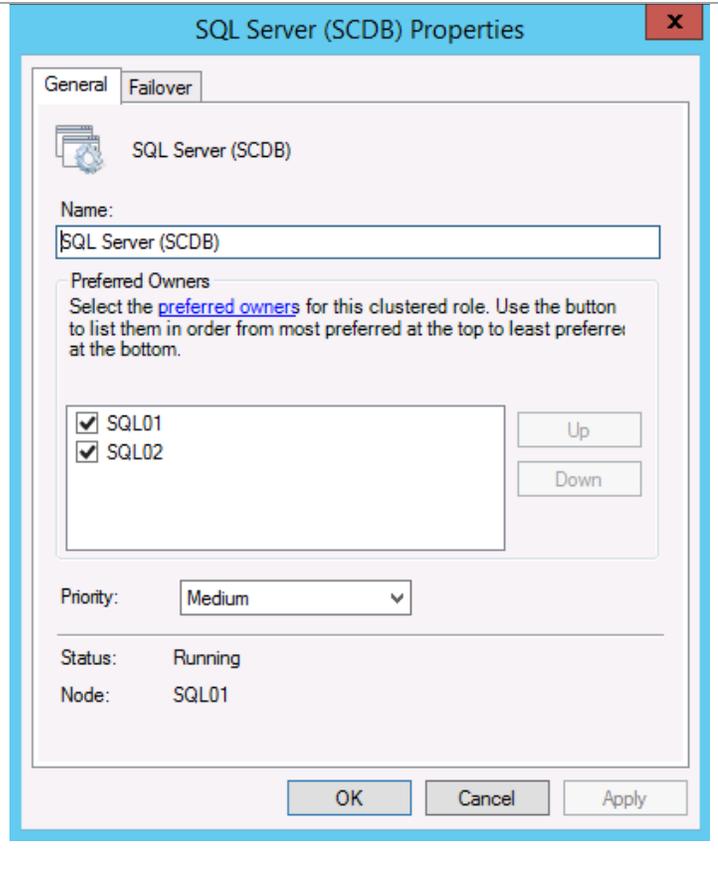
To perform this configuration, select the first SQL Server instance under the **Roles** node, then click the **Any Node** link next to **Preferred Owners**.

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL01
SQL Server (SCOM)	Running	Other	SQL01
SQL Server (SCOMDW)	Running	Other	SQL01
SQL Server (SCSMAS)	Running	Other	SQL01
SQL Server (SCSMDB)	Running	Other	SQL01
SQL Server (SCSMDW)	Running	Other	SQL01
SQL Server (SCVMM)	Running	Other	SQL01

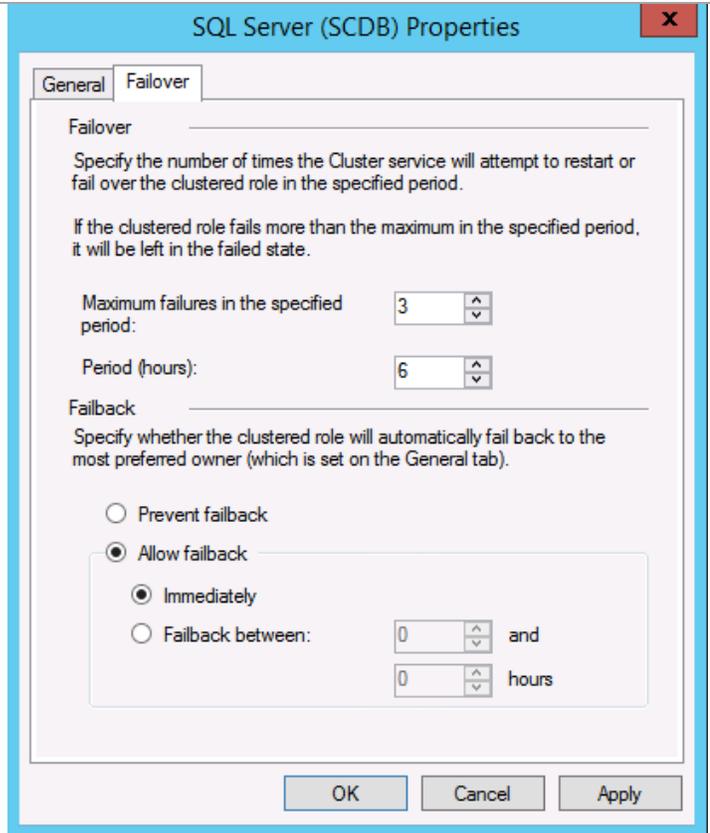
SQL Server (SCDB)	Preferred Owners: Any node
-------------------	--

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

On the **SQL Server Properties** page, click the **General** tab, and select the two preferred nodes for the instance. The order will be automatically adjusted when the process is completed.



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



Note: The value for the **Preferred Owners** link now displays a value of **User Settings** if all nodes are not selected as preferred owners. If all available nodes are selected for the VM, the value will remain as **Any node**.

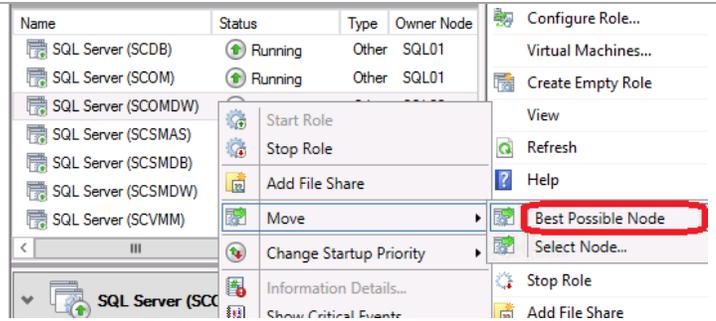
Repeat this process for each SQL Server instance.

Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL02
SQL Server (SCOMDB)	Running	Other	SQL02
SQL Server (SCOMDW)	Running	Other	SQL02
SQL Server (SCSMAS)	Running	Other	SQL02
SQL Server (SCSMDB)	Running	Other	SQL02
SQL Server (SCSMDW)	Running	Other	SQL02
SQL Server (SCVMMDB)	Running	Other	SQL02

Below the table, a summary bar shows 'SQL Server (...)' with 'Preferred Owners: [User Settings](#)'. A red arrow points to the 'User Settings' link.

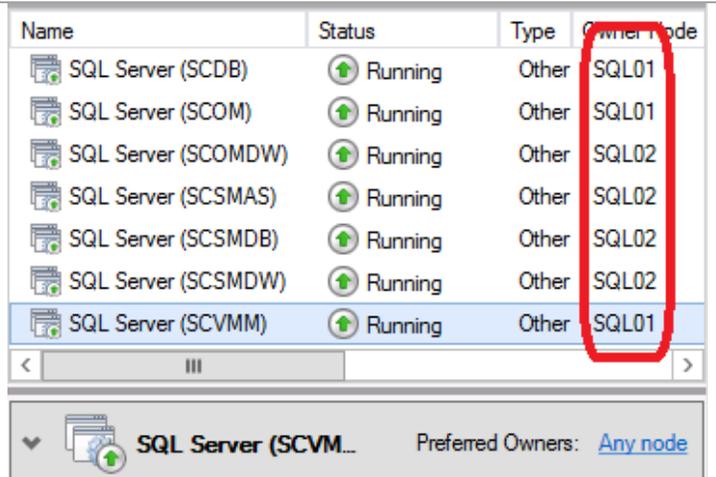
After all instances have been configured correctly for **Preferred Owners**, you must initiate a planned failover to balance the SQL Server instances across nodes.

In **Failover Cluster Manager**, select the roles for each of the SQL Server instances that should not run on Node1 (In this example, these are: SCOMDB, SCOMDW, SCSMDB, SCSMDW, SCSMAS). Right-click the selection of SQL Server instances, click **Move**, and then click **Best Possible Node**.



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

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



Virtual Machine Manager

Two servers running Virtual Machine Manager Management Server role are deployed and configured in a failover cluster that uses a dedicated SQL Server instance in the virtualized SQL Server cluster.

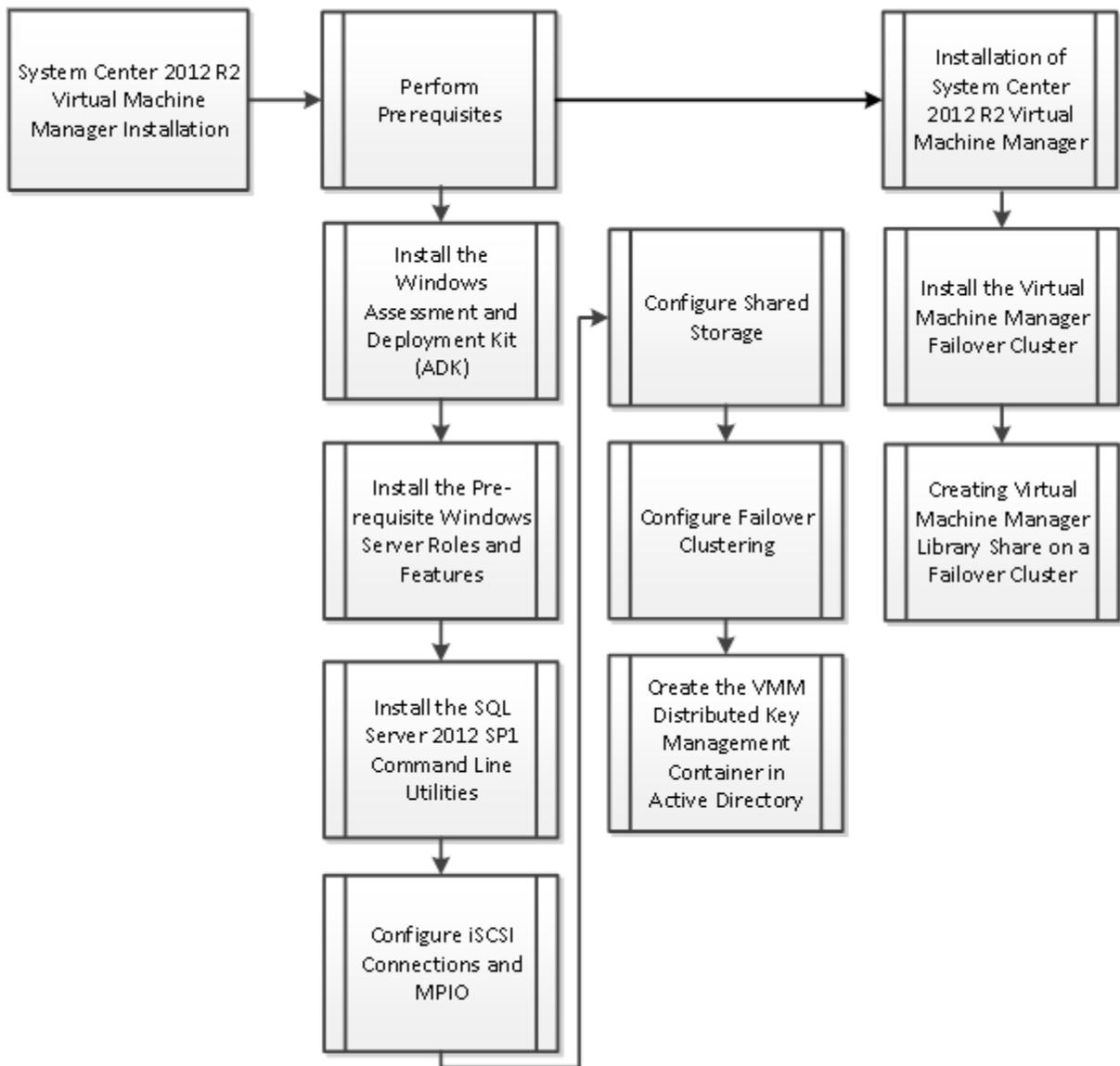
One library share is used for Virtual Machine Manager library. Provisioning the Library Share on a File Server cluster instead of a stand-alone server is recommended. Additional library servers can be added as needed.

Note: In this deployment, the library file share is created on the SQL Server cluster. This was done simply from a convenience standpoint to avoid setting up a clustered file service for a single share. If the customer already has a highly available file service available, it can be used for the VMM library.

Virtual Machine Manager and Operations Manager integration is configured during the installation process.

The installation process for System Center 2012 R2 Virtual Machine Manager includes the high-level steps shown in the following figure.

Figure 7. Virtual Machine Manager Installation Process



Overview

This section provides a high-level walkthrough for deploying Virtual Machine Manager into the IaaS PLA fabric management architecture. The following assumptions are made prior to the installation:

- Two base virtual machines running Windows Server 2012 R2 have been provisioned and configured as a Windows Failover Cluster, which includes:
 - The selected operating system installation type must be Full Installation.
 - At least two shared storage LUNs or one shared storage LUN and a file share witness disk.
 - A dedicated virtual network adapter for cluster communication.
 - At least one dedicated virtual network adapter for iSCSI communications (if using iSCSI).
- The target virtual machines must have the Windows Assessment and Deployment Kit (ADK) for Windows 8 and Windows Server 2012 R2 installed.
- The target virtual machine must have the Windows Server Update Services (WSUS) 4.0 console installed (available in Windows Server 2012 R2).
 - Virtual Machine Manager can use a WSUS root server or a downstream WSUS server. Virtual Machine Manager does not support using a WSUS replica server. The WSUS server can be dedicated to Virtual Machine Manager or it can be a WSUS server that is already in use.
- A Microsoft SQL Server instance dedicated to Virtual Machine Manager as outlined in previous steps must be available.
 - The Virtual Machine Manager SQL Server instance must be case-insensitive (this is the default in SQL Server 2012).
 - The SQL Server name must not exceed 15 characters.
 - The account used to install Virtual Machine Manager must have the rights needed to connect to the remote SQL Server instance and create databases.
- The installation account must have rights to create the distributed key management container in AD DS, or this container must already exist prior to running the Virtual Machine Manager setup.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following service accounts have been created:

Table 21. Virtual Machine Manager Accounts

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

Groups

Verify that the following security groups are created:

Table 22. Virtual Machine Manager Security Groups

Security group name	Group scope	Members
<DOMAIN>\FT-SCVMM-Admins	Global	FT-SCVMM-SVC
<DOMAIN>\FT-SCVMM-FabricAdmins	Global	Virtual Machine Manager delegated administrators
<DOMAIN>\FT-SCVMM-ROAdmins	Global	Virtual Machine Manager Read-only administrators
<DOMAIN>\FT-SCVMM-TenantAdmins	Global	Virtual Machine Manager tenant administrators who manage self-service users
<DOMAIN>\FT-VMM-AppAdmins	Global	Virtual Machine Manager self-service users

For more information, see [Creating User Roles in VMM](#) on Microsoft TechNet.

Install the Windows Assessment and Deployment Kit

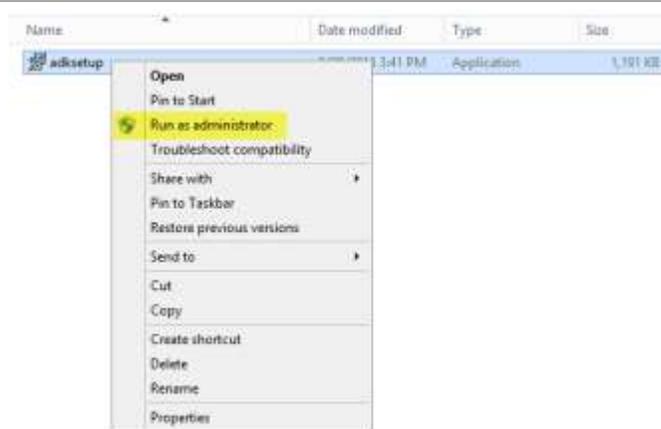
The Virtual Machine Manager installation requires that the Windows Assessment and Deployment Kit (ADK) is installed on the Virtual Machine Manager management server. To download this kit, see [Windows Assessment and Deployment Kit for Windows 8 in the Microsoft Download Center](#).

During installation, only the Deployment Tools and the Windows Pre-installation Environment features will be selected. This installation also assumes the Virtual Machine Manager servers have Internet access. If that is not the case, an offline installation can be performed. For more information for this installation option and complete installation details, see [Installing the Windows ADK](#).

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

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

From the Windows ADK installation media source, right-click **adksetup.exe** and select **Run as administrator** to begin setup. If prompted by User Account Control, click **Yes** to allow the installation to make changes to the computer.



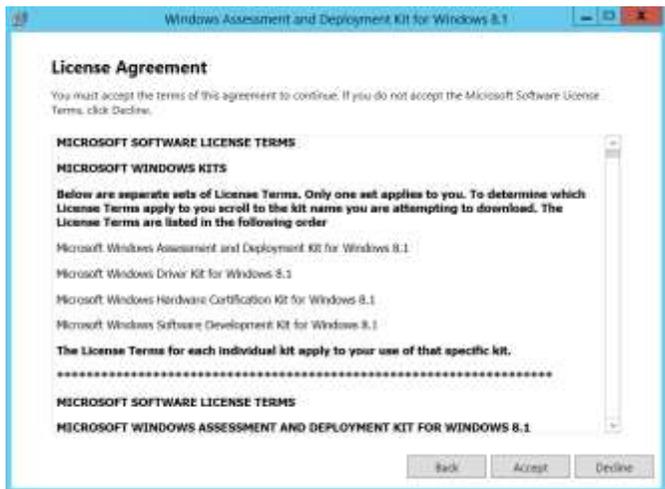
The Assessment and Deployment Kit Wizard appears On the **Specify Location** page, accept the default folder location of *%ProgramFiles%\Windows Kits\8.1*, and click **Next** to continue.



On the **Join the Customer Experience Improvement Program (CEIP)** page, choose to participate or to not participate by providing selected system information. Click **Next** to continue.



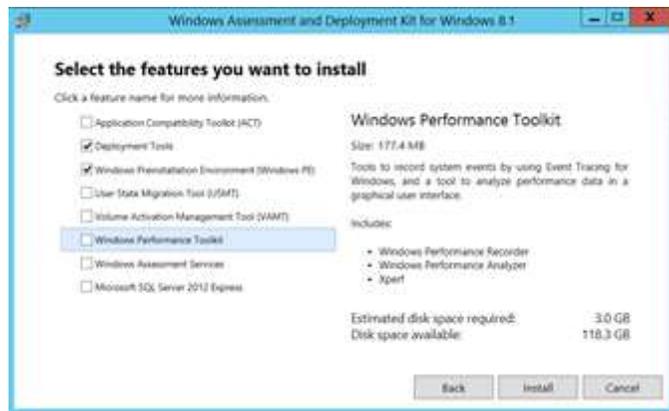
On the **License Agreement** page, click **Accept** to continue.



On the **Select the features you want to install** page, select the following option check boxes:

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

Make sure all other option check boxes are cleared. Click **Install** to begin the installation.



After the installation is complete, clear the **Launch the Getting Started Guide** check box, and click **Close**.



Install the Prerequisite Windows Server Roles and Features

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

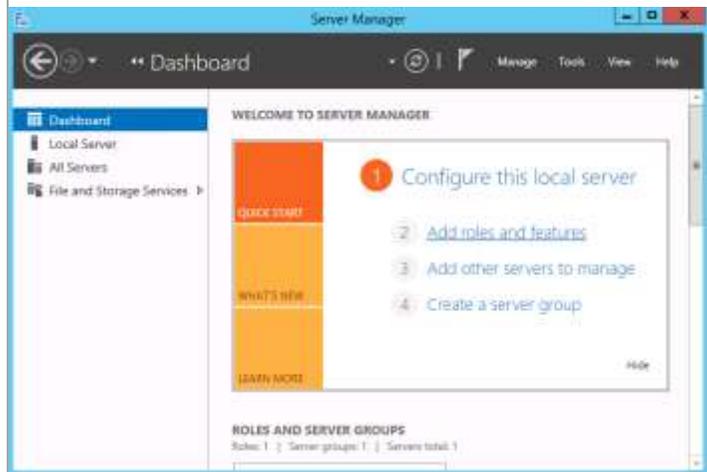
► Perform the following steps on each Virtual Machine Manager virtual machine.

Although this installation can be performed interactively, the installation of roles and features can be automated by using the Server Manager module for Windows PowerShell. Either use the PowerShell cmdlets to the right, or use the GUI with the following instructions.

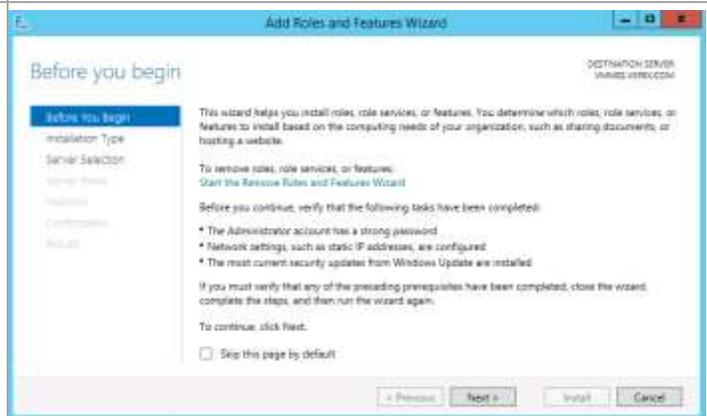
```
Add-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

```
Add-WindowsFeature -Name UpdateServices-RSAT
```

Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, click **Add roles and features**.



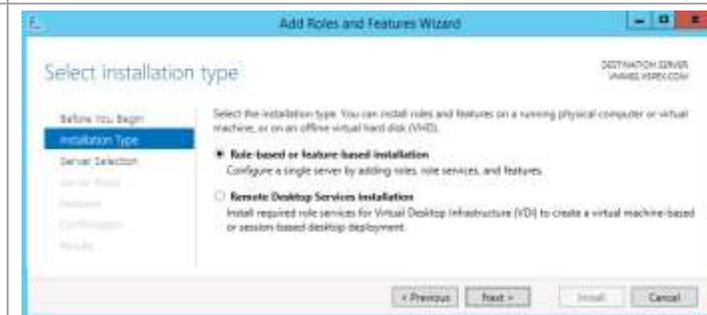
The **Add Roles and Features Wizard** appears. On the **Before You Begin** page, click **Next** to continue.



On the **Select Installation Type** page, you are presented with two options:

- **Role-based or feature-based installation.** This is a traditional installation of roles and features to enable discrete functionality on the operating system.
- **Remote Desktop Services installation.** This installs a predetermined combination of roles, features, and configurations to support a Remote Desktop (Session Virtualization) or VDI scenario.

Select the **Role-based or feature-based installation** button, and click **Next** to continue.

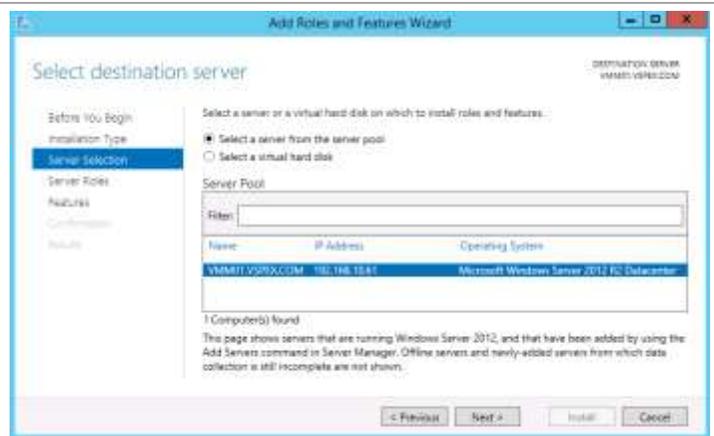


On the **Select destination server** page, you are presented with two options:

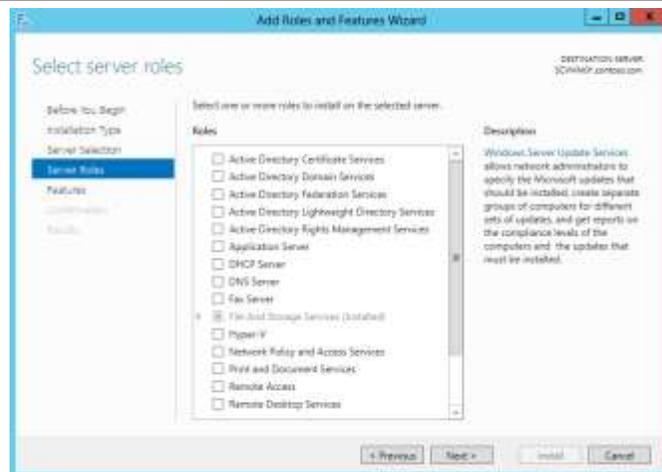
- **Select a server from the server pool.** This option allows you to select a server from the managed pool of systems defined within Server Manager.
- **Select a virtual hard disk.** This option allows for roles to be installed to staged VHD files for offline servicing purposes.

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

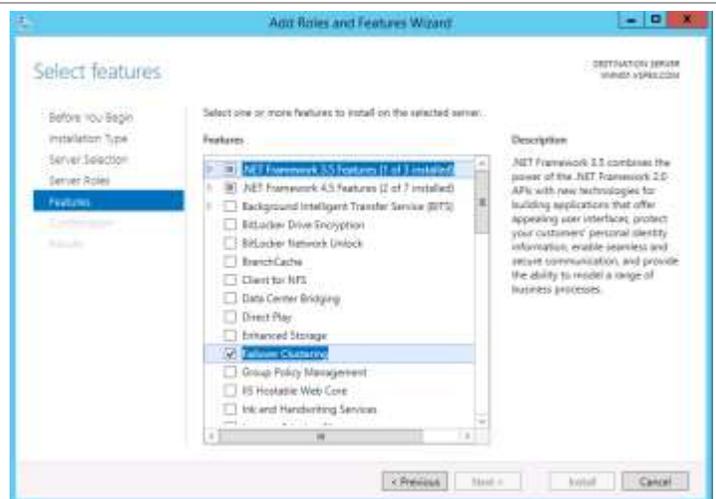
Note: Although many servers may be presented in the **Select a server from the server pool option**, only one can be selected at a time for role and feature installation operations. To enable installations across multiple hosts, the configuration can be saved at the end of the wizard and applied to multiple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



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



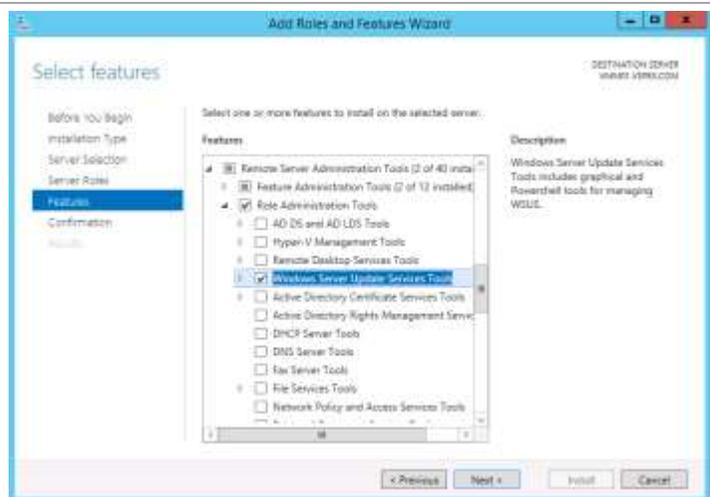
On the **Features** page, select **Failover Clustering**.



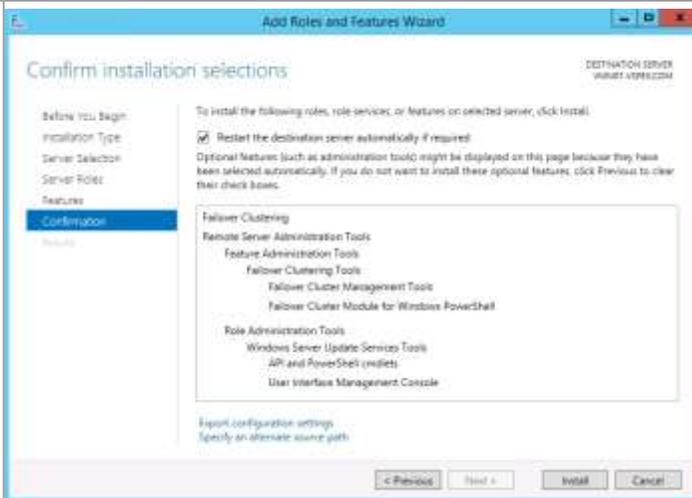
The **Add features that are required for Failover Clustering?** page appears. Select the **Include management tools (if applicable)** check box, then click the **Add Features** button.



Expand Remote Server Administration Tools, then expand Role Administration Tools, and select the **Windows Server Update Services Tools** features. Click **Next** to continue.

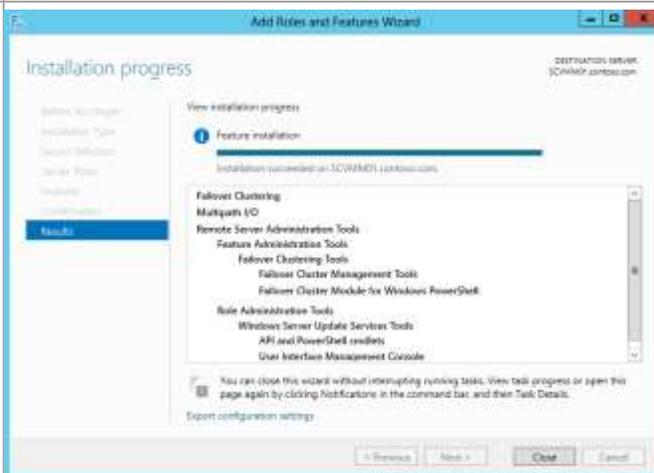


On the **Confirm installation selections** page, verify that the Windows Server Update Services Tools and Failover Clustering features are selected. Make sure that **Restart each destination server automatically if required** is selected. This is especially important for remote role and feature installation. Click **Install** to begin installation.



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

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

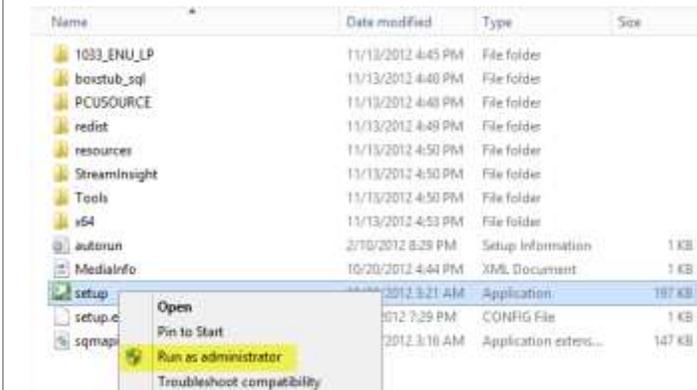


Install the Command-Line Utilities in SQL Server 2012 with SP1

The Virtual Machine Manager installation requires that the command-line utilities and management tools in SQL Server 2012 with SP1 are installed on the Virtual Machine Manager management server. Use the following procedure to install the command-line utilities and management tools on the Virtual Machine Manager management server.

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

From the SQL Server 2012 with SP1 installation media source, right-click **setup.exe**, and select **Run as administrator** to begin setup.



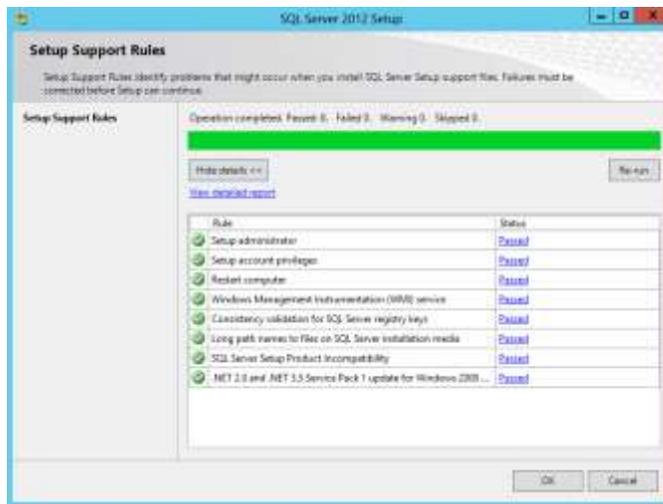
The SQL Server Installation Center appears. In the left pane, click **Installation**.



Click the **New SQL Server stand-alone installation or add features to an existing installation** link.

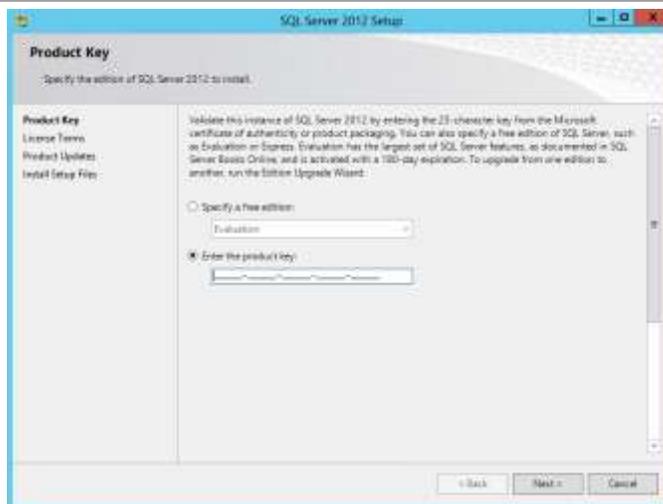


The SQL Server 2012 Setup Wizard appears. On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **OK** to continue.

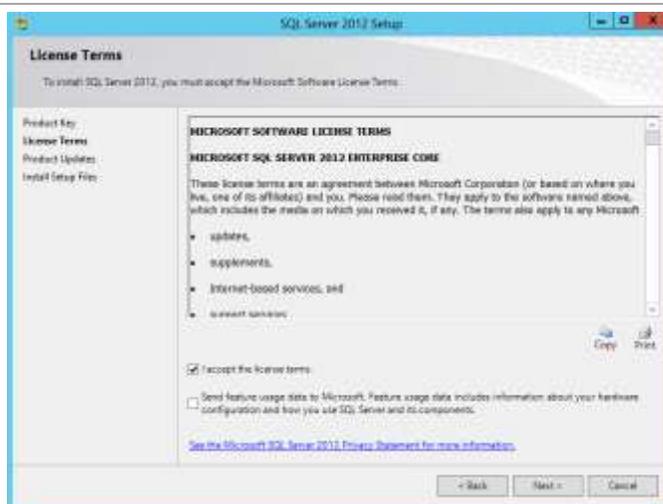


On the **Product Key** page, select the **Enter the product key** option and type the associated product key in the text box. Click **Next** to continue.

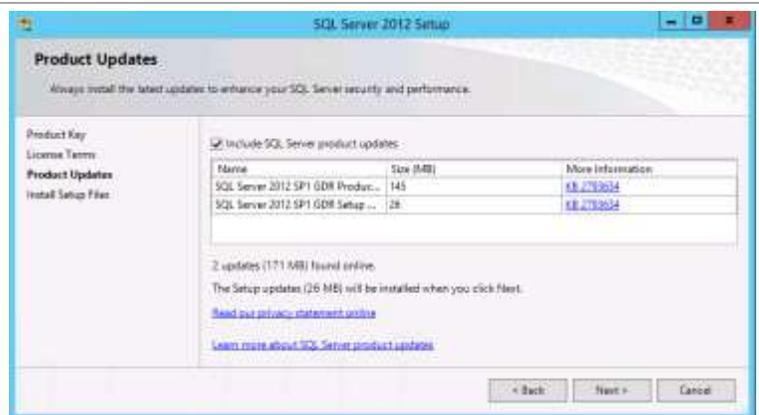
Note: If you do not have a product key, select the **Specify a free edition** option, and select **Evaluation** from the drop-down list for a 180-day evaluation period.



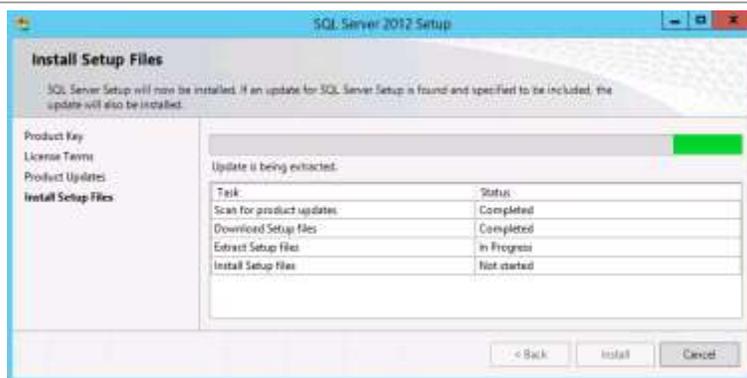
On the **License Terms** page, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft**, based on your organization's policies, and click **Next** to continue.



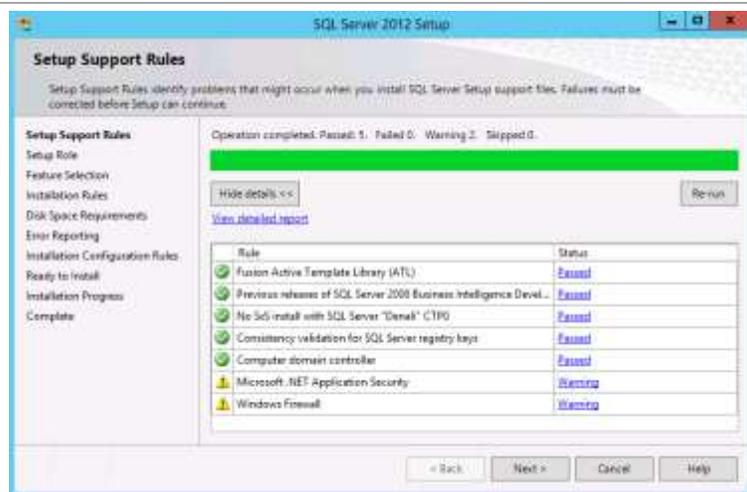
On the **Product Updates** page, leave the **Include SQL Server product updates**, selection selected, and click **Next**.



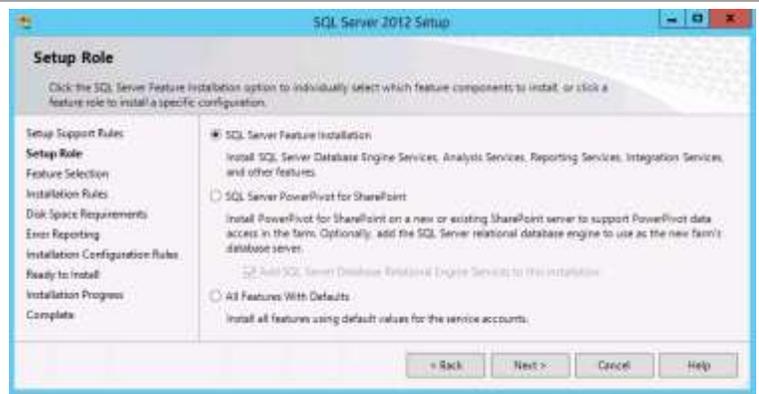
On the **Install Setup Files** page, the update and installation process will be displayed.



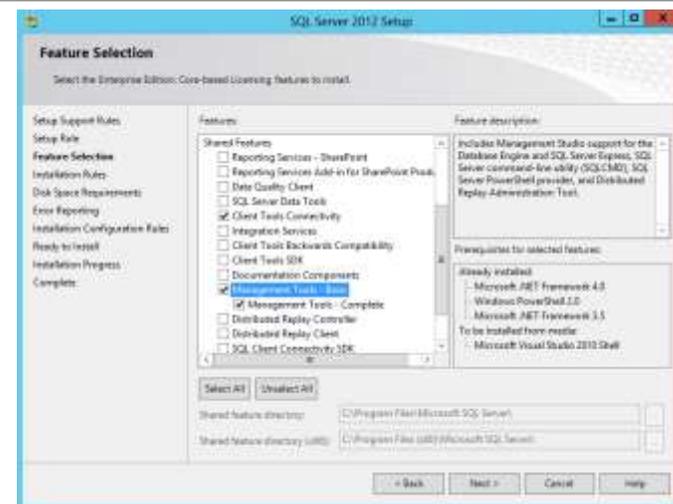
On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



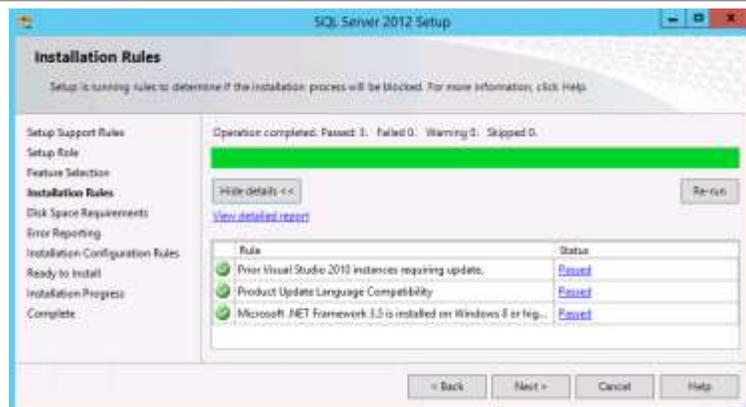
On the **Setup Role** page, select the **SQL Server Feature Installation** option, and click **Next** to continue.



On the **Feature Selection** page, select the **Client Tools Connectivity**, **Management Tools – Basic** and **Management Tools – Complete** check boxes, then click **Next** to continue.



On the **Installation Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



On the **Disk Space Requirements** page, verify that the installation has enough space on the target drive, and click **Next** to continue.



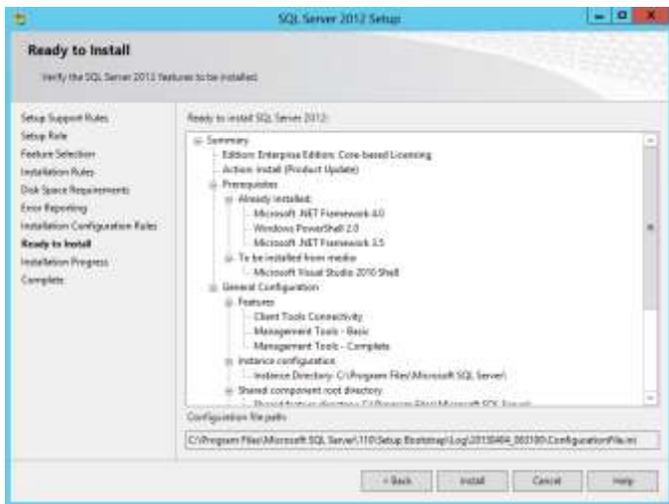
on the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies, and click **Next** to continue.



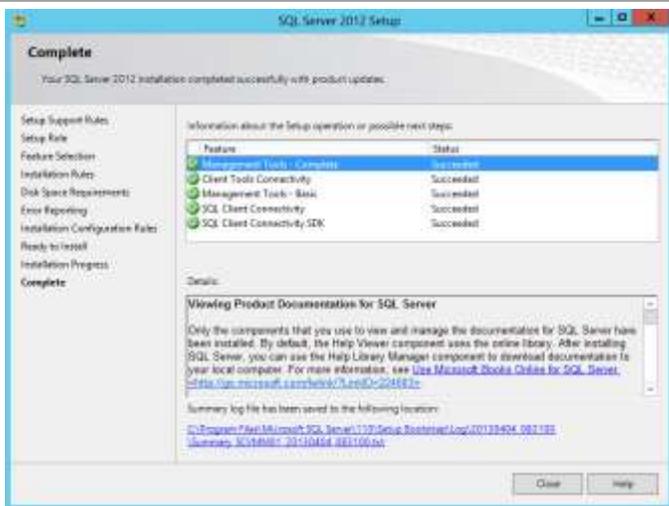
On the **Installation Configuration Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



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



When the installation completes, the **Complete** page will appear. Click **Close** to complete the installation of command-line tools in SQL Server.



Configure Shared VHDX files

The Virtual Machine Manager Failover cluster installation requires a quorum model. That model can be a disk witness or a file share witness. If a disk witness is selected for the quorum model, you need to connect both Virtual Machine Manager management servers to shared storage. If a file share witness will be used, you can skip this section.

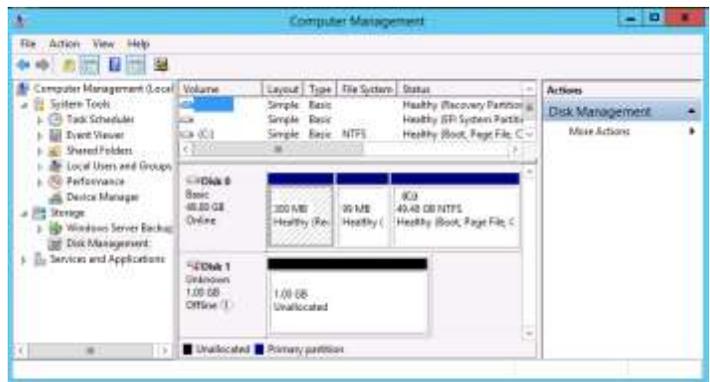
This section assumes Shared VHDX files are in use.

Configure Shared Storage

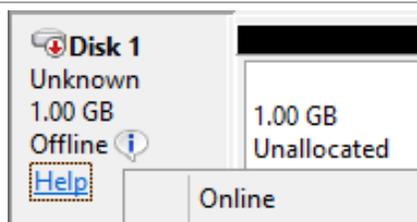
- ▶ Perform the following steps on the **first** Virtual Machine Manager virtual machine. These operations must occur on a single node prior to creating the failover cluster.

Refer to the section in SQL Server 2012 Failover Cluster Installation that demonstrates the creation of a VHDX file and configuring it in the settings of the VMs to enable sharing.

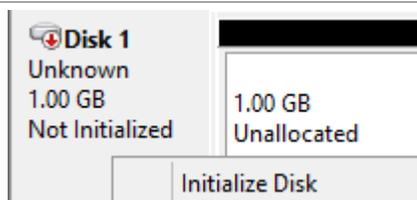
Within **Server Manager**, navigate to the **Storage** node and expand the **Disk Management** snap-in. The LUN should be visible in the snap-in, but should appear offline.



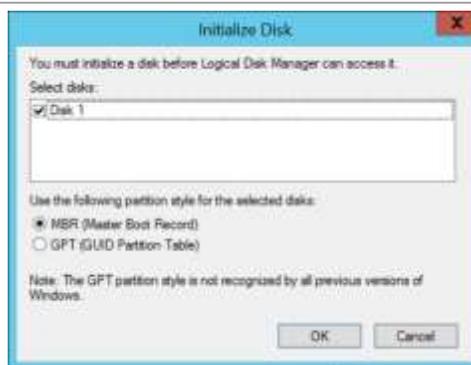
Right-click the disk and select **Online**. Perform this action on a single node of the cluster.



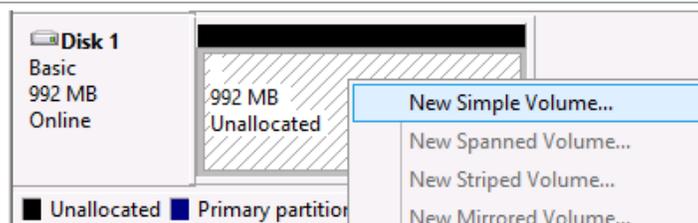
When the disk is online, right-click and select **Initialize Disk**. Perform this action on the first node of the cluster.



The **Initialize Disk** page appears. In the **Select disks** section, verify that the check box is selected. Verify that the **MBR (Master Boot Record)** option is selected, and click **OK** to initialize the disk.



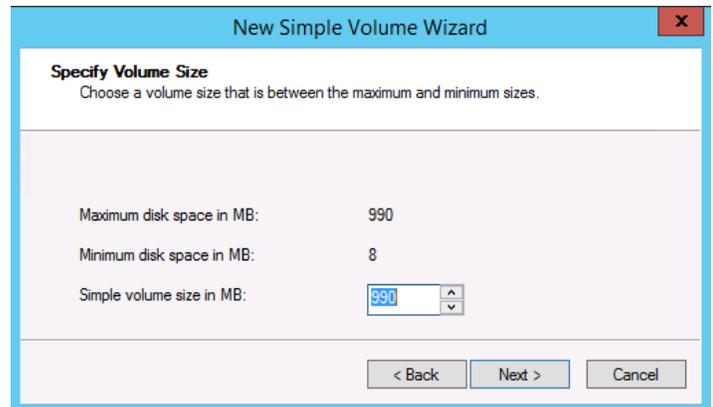
After they are initialized, on the first node, right-click the disk and click **New Simple Volume...**



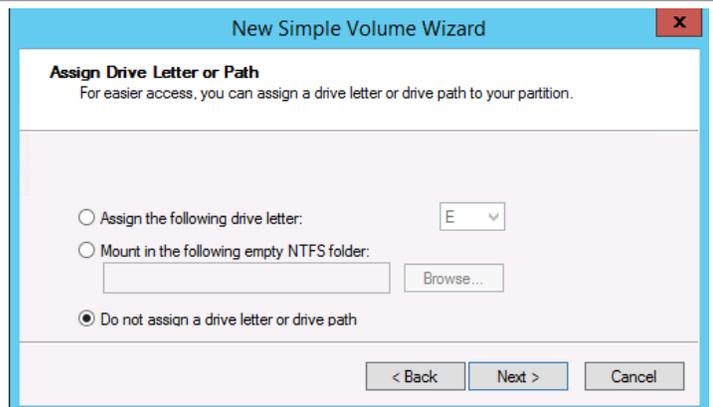
The New Simple Volume Wizard appears. Click **Next** to continue.



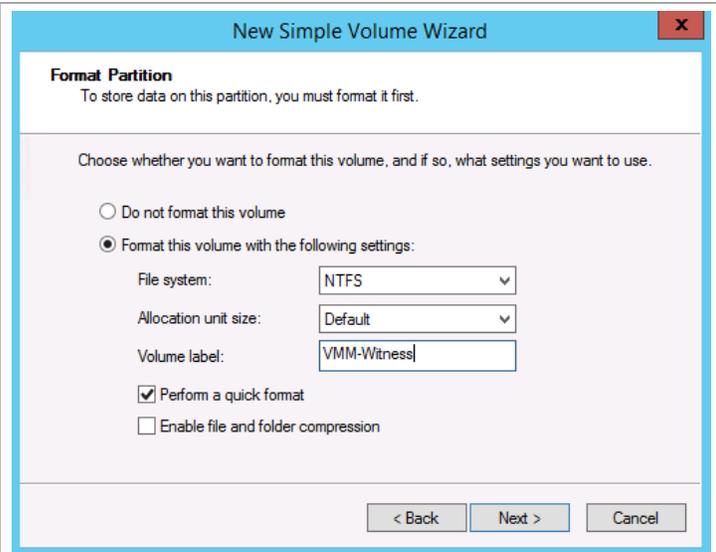
On the **Specify Volume Size** page, specify the maximum disk space value in the **Simple volume size in MB** text box. Click **Next** to continue.



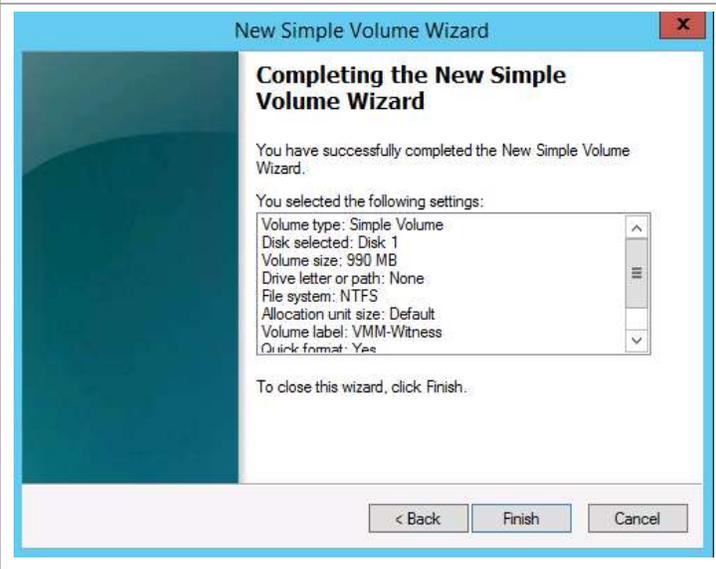
On the **Assign Drive Letter or Path** page, select the **Do not assign the following drive letter** option. Click **Next** to continue.



On the **Format Partition** page, select the **Format this volume with the following settings** option. In the **File system** drop-down list, click **NTFS**. In the **Allocation unit size** drop-down list, click **Default**. Optionally, type a descriptive label in the **Volume label** text box, for example, “WitnessDisk.” Verify that the **Perform a quick format** check box is selected, and click **Next** to format the partition.



When the **Completing the New Simple Volume Wizard** page appears, click **Finish** to complete the operation.



Create the Failover Cluster

During the provisioning process, two virtual machines were built to the specifications outlined in the IaaS PLA Fabric Management Architecture Guide to support a high availability Virtual Machine Manager for fabric management. After the shared storage was created, it was configured within each virtual machine to make them accessible to each candidate cluster node.

- ▶ Perform the following steps on the **first** Virtual Machine Manager virtual machine with an account that has both local Administrator rights and permissions in AD DS to create the Virtual Machine Manager CNOs.

From an elevated command prompt in Windows PowerShell, on the first VMM Server node, run the following commands to test the cluster configuration:

Import-Module FailoverClusters

Test-Cluster <Node1>, <Node2>

If successful the **Test-Cluster** cmdlet will display a validation report.

Note: You may get a warning message on the cluster communication network. It is a non-routed network, so it will not be able to reach the access network. This is expected.

Test-Cluster VMM01,VMM02

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Test-Cluster SCVMM01,SCVMM02

Test-Cluster
Trying to write to sector 11 on Test Disk D from node SCVMM01.contoso.com.
[ooooooooooooooooooooo]
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Test-Cluster SCVMM01,SCVMM02

Node:          SCVMM01
LastWriteTime: 3/3/2013 4:33 PM
Length: 398359
Name: Validation Report_2013.03.03_AT_16.31.50_x61.mht
```

```
PS C:\Users\Administrator_VSPEX> Test-Cluster -node vmm01,vmm02
WARNING: System Configuration - Validate Software Update Levels: The test reported some warnings...
WARNING: Network - Validate Network Communication: The test reported some warnings...
WARNING:

Test Results:
ClusterConfigurationApproved:
Testing has completed successfully. The configuration appears to be suitable for clustering. However, you should review the report for possible warnings, which you should address to attain the highest availability.
Test report file path: C:\Users\Administrator_VSPEX\AppData\Local\Temp\1\ValidationReport_2014.03.25_AT_11.49.51_x61.mht

Node:          VMM01
LastWriteTime: 3/25/2014 11:51 AM
Length: 403912
Name: Validation Report_2014.03.25_AT_11.49.51_x61.mht
```

Navigate to %TEMP% and review the **Failover Cluster Validation Report** for errors and warnings. Perform any required remediation and run the previous cluster test as required.

Microsoft

Failover Cluster Validation Report

Node: SCVMM01.contoso.com Validated
 Node: SCVMM02.contoso.com Validated

Started 3/3/2013 4:31:51 PM
 Completed 3/3/2013 4:33:24 PM

The Validate a Configuration Wizard must be run after any change is made to the configuration of the cluster or hardware. For more information, see <http://go.microsoft.com/fwlink/?linkid=226143>.

Name	Result Summary	Description
Inventory	Success	Success
Network	Success	Success
Storage	Success	Success
System Configuration	Success	Success

Microsoft

Failover Cluster Validation Report

Node: VMM01.VSPEX.COM Validated
 Node: VMM02.VSPEX.COM Validated

Started 3/25/2014 11:54:46 AM
 Completed 3/25/2014 11:56:39 AM

The Validate a Configuration Wizard must be run after any change is made to the configuration of the cluster or hardware. For more information, see <http://go.microsoft.com/fwlink/?linkid=226143>.

Name	Result Summary	Description
Inventory	Success	Success
Network	Warning	Warning
Storage	Success	Success
System Configuration	Success	Success

From the same elevated command prompt in Windows PowerShell, run the following command to create the cluster:

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

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

Note: If you are using DHCP for the cluster nodes, do not use the **-StaticAddress** parameter.

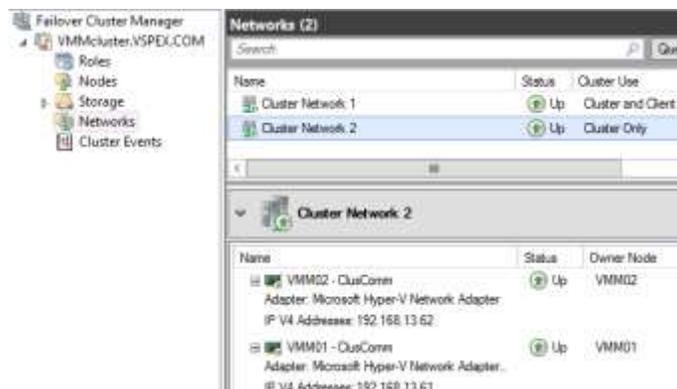
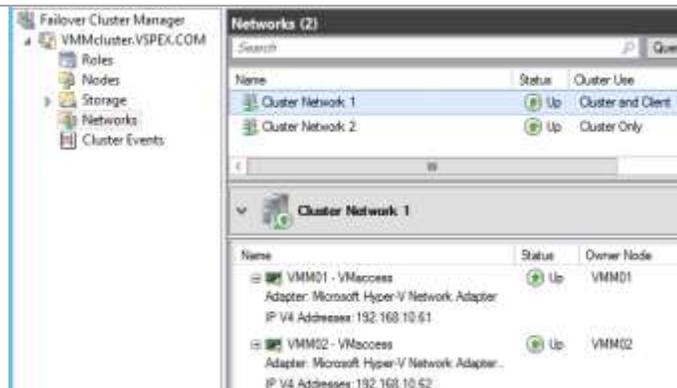
Open **Failover Cluster Manager**.



In the **Failover Cluster Manager** console, select the **Networks** node. Verify that all the cluster networks are assigned properly. Take care to document which cluster network name is assigned to the public and private network interfaces.

Close **Failover Cluster Manager**.

Note: The cluster networks can be renamed to specify the network connection.



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

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

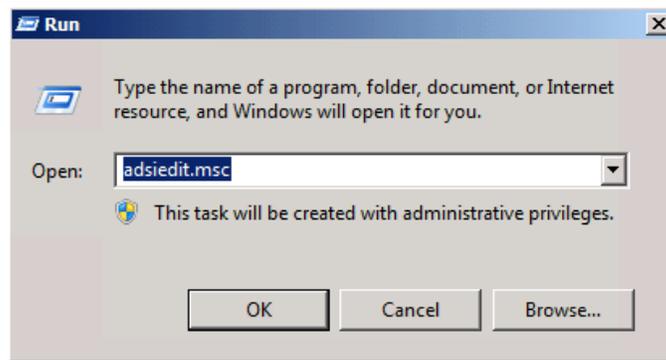
For more information, see [Configuring Distributed Key Management in VMM](#).

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

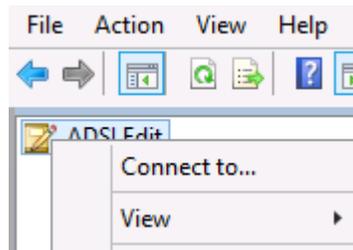
Use the following procedure to create an AD DS container to house the distributed key information. These instructions assume that a domain controller running Windows Server 2008 R2 is in use. Similar steps would be followed for other versions of Active Directory, including versions in Windows Server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

► Perform the following steps on a domain controller in the domain where Virtual Machine Manager is to be installed.

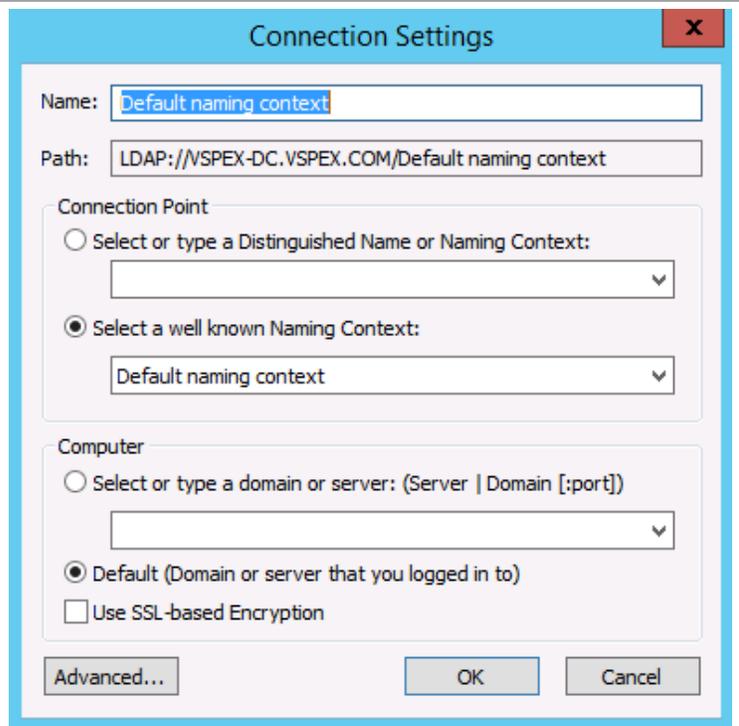
Log on to a domain controller with a user that has Domain Admin privileges, and run **adsiedit.msc**.



Right-click the **ADSI Edit** node, and click **Connect to...**



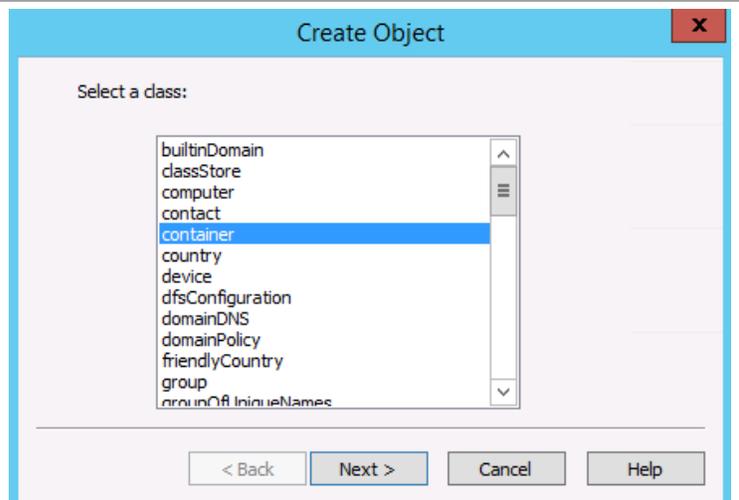
In the **Connections Settings** dialog box, in the **Connection Point** section, select the **Select a well known Naming Context** option. Select **Default naming context** from the drop-down list, and click **OK**.



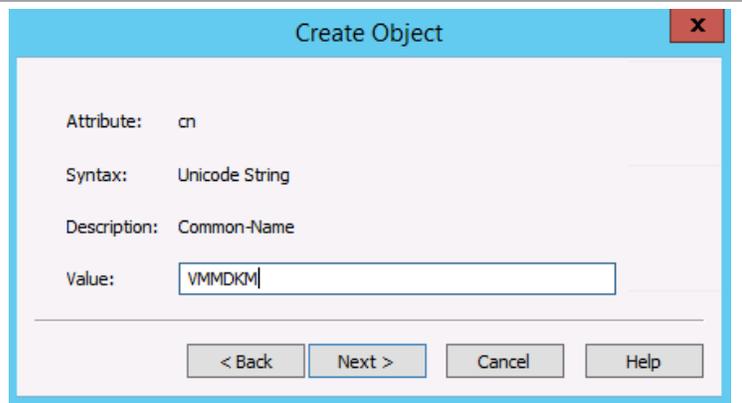
On the ADSI Edit page, click **Default naming context** [*<computer fully qualified domain name>*], expand *<distinguished name of domain>*, right-click the root node. Click **New**, and then click **Object...**



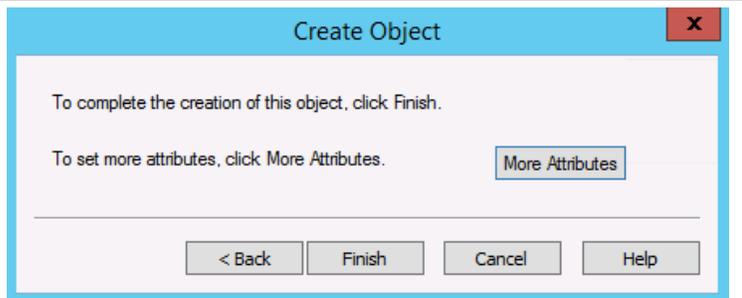
On the **Create Object** page, click **container**, and then click **Next**.



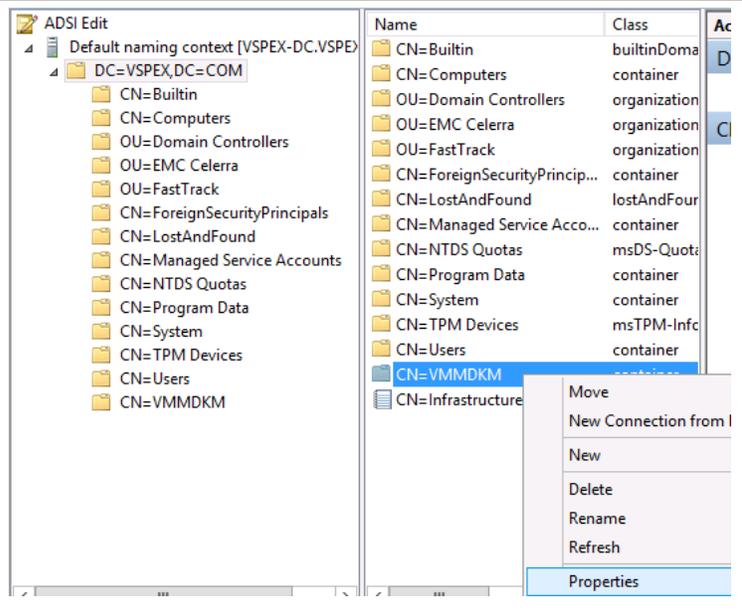
In the **Value** text box, type *VMMDKM*, and then click **Next**.



Click **Finish** to create the container object.

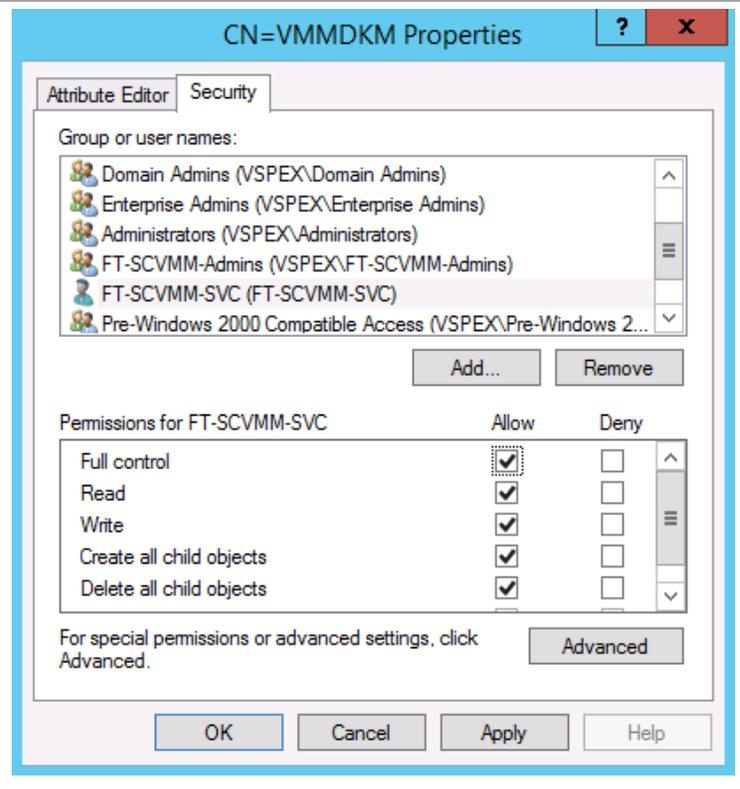


Within **ADSI Edit**, right-click the new **CN=VMMDKM** object, and then click **Properties**.



On the **VMMDKM Properties** page, click the **Security** tab. Click **Add** to add the VMM Service account and VMM Admins group. Grant the security principles **Full Control** permissions.

Click **OK** and close ADSI Edit.



Installation

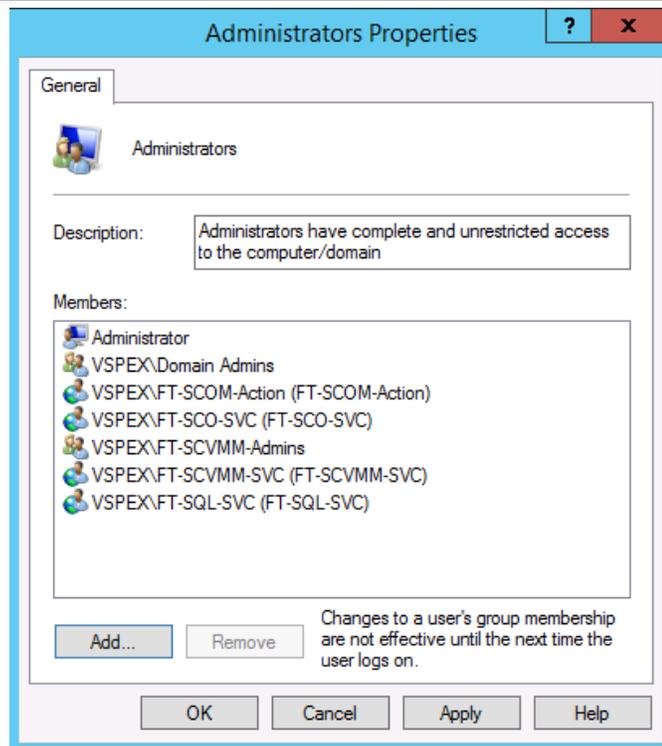
Install the Virtual Machine Manager Failover Cluster

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

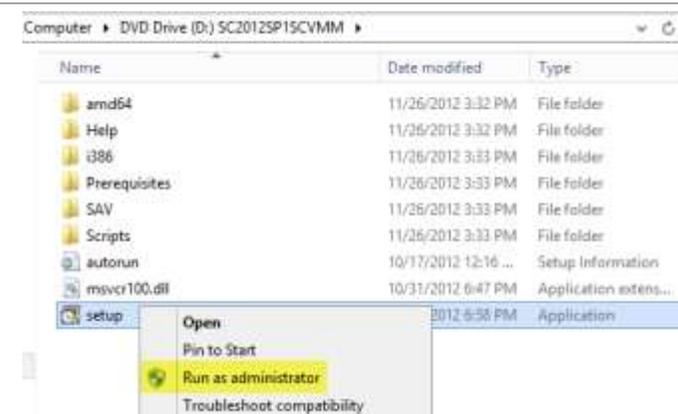
Log on to Virtual Machine Manager virtual machine as a user with local Administrator rights.

Verify that the following accounts or groups are members of the local Administrators group on the Virtual Machine Manager virtual machine:

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



From the Virtual Machine Manager installation media source, right-click **setup.exe** and click **Run as administrator** to begin setup. If prompted by User Account Control, select **Yes** to allow the installation to make changes to the computer.

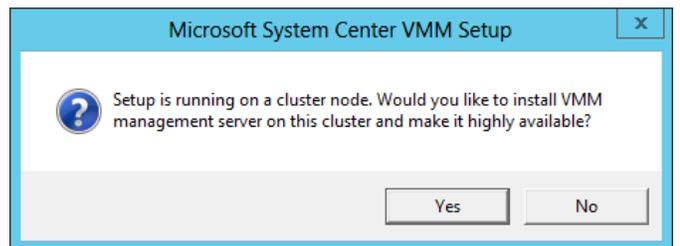
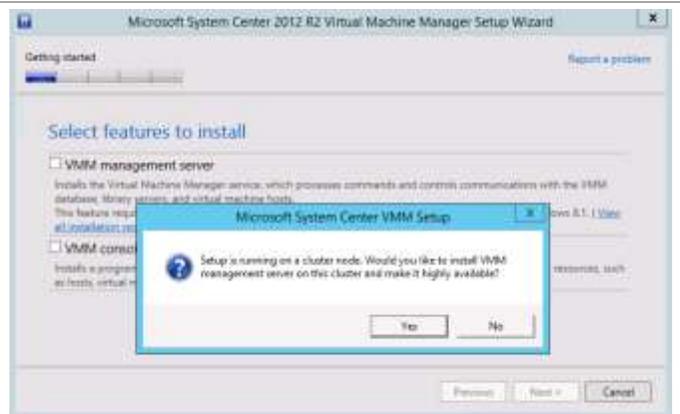


The Virtual Machine Manager installation wizard will appear. Click **Install** to begin the Virtual Machine Manager server installation.

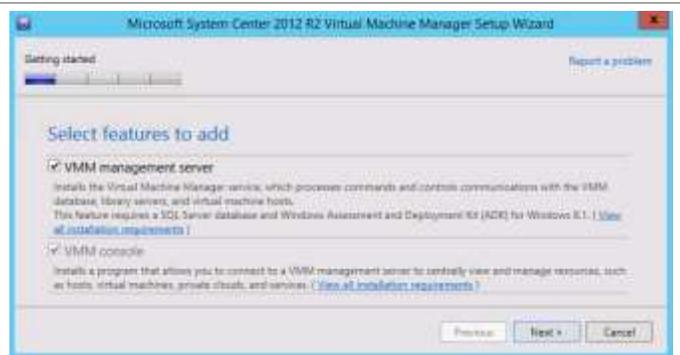


Selecting the VMM Management server feature will cause a Microsoft System Center VMM Setup message to appear.

Click **Yes** to switch to the high availability Virtual Machine Manager Setup Wizard.



On the **Select features to install** page, verify that the **VMM management server** installation option check box is selected. When it is selected, the **VMM console** installation option check box is selected by default. Click **Next** to continue.



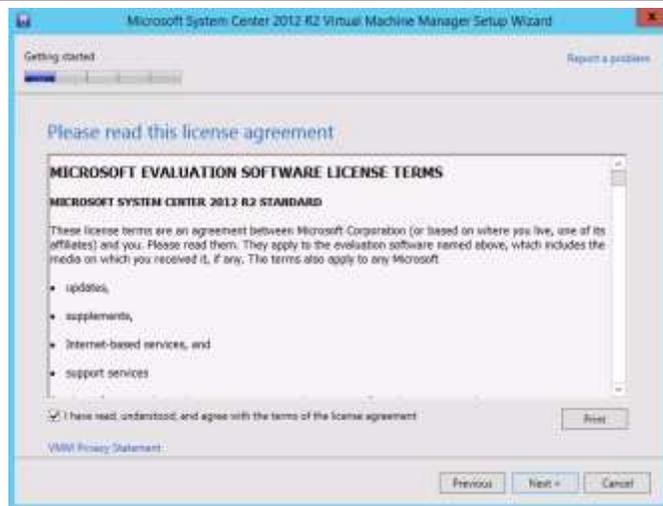
On the **Product registration information** page, type the following information in the provided text boxes:

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

Click **Next** to continue.



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



On the **Join the Customer Experience Improvement Program (CEIP)** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



On the **Select installation location** page, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Virtual Machine Manager for the installation. Click **Next** to continue.



Note: The Virtual Machine Manager Setup Wizard automatically checks for prerequisites. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy. This screenshot provides an example of a discrepancy warning.

If the system passes the prerequisite check, no screen will be displayed and the Setup Wizard will proceed to the **Database configuration** page.



On the **Database configuration** page, type the following information in the provided text boxes:

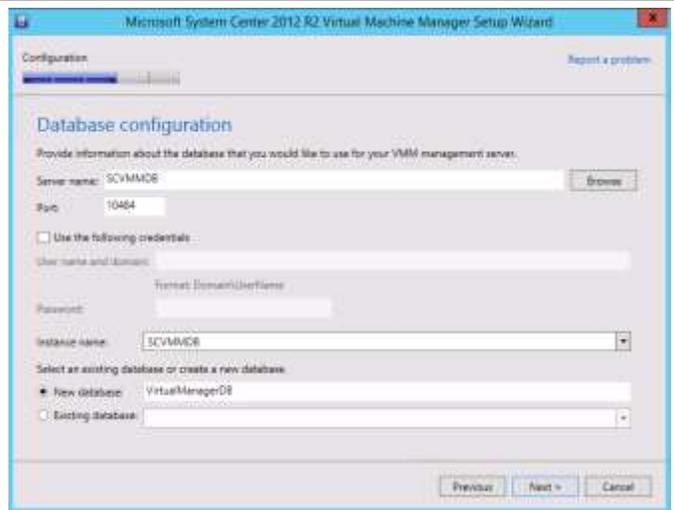
Server name – Specify the name of the SQL Server cluster created in the steps above.

Port - Specify the TCP port used for the SQL Server, as configured in the steps above.

Verify that the **Use the following credentials** check box is clear. In the **Instance name** drop-down list, select the Virtual Machine Manager database instance deployed earlier in the SQL Server cluster.

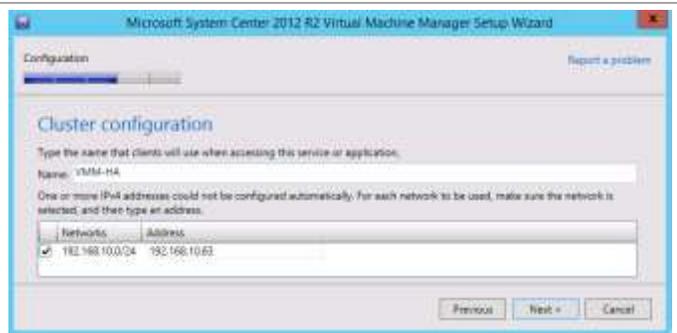
In the **Select an existing database or create a new database** option, select **New database**, and accept the default database name of **VirtualManagerDB**.

Click **Next** to continue.



On the **Cluster Configuration** page, in the **Name** field, provide a name for the Virtual Machine Manager cluster service.

Note: If the cluster node you are installing is configured with static IP addresses, you also need to provide an IP address for the Virtual Machine Manager cluster service. If the cluster node is configured to use DHCP, no additional information is required.



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

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

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

Click **Next** to continue.



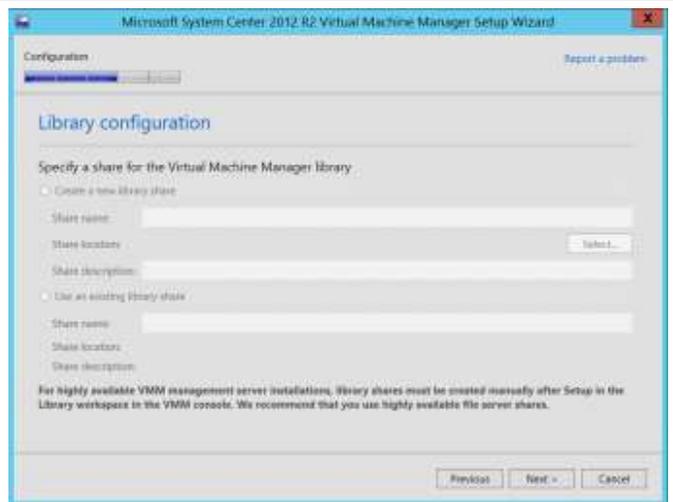
On the **Port configuration** page, accept the default values in the provided text boxes:

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

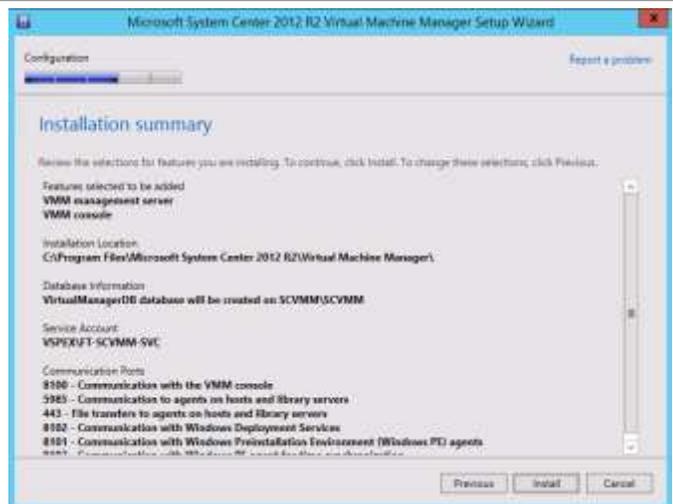
Click **Next** to continue.



On the **Library configuration** page, no options are available for a high availability installation. The Library must be configured separately and it should point to a high availability file share. Click **Next** to continue.



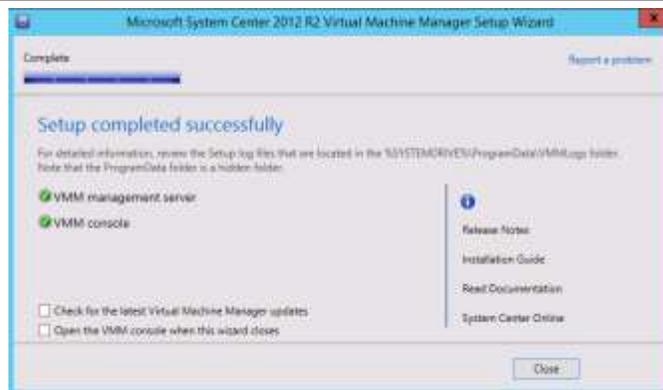
The **Installation summary** page will appear and display the selections you made in the Setup Wizard. Review the options selected and click **Install** to continue.



The wizard will display the progress while installing features.

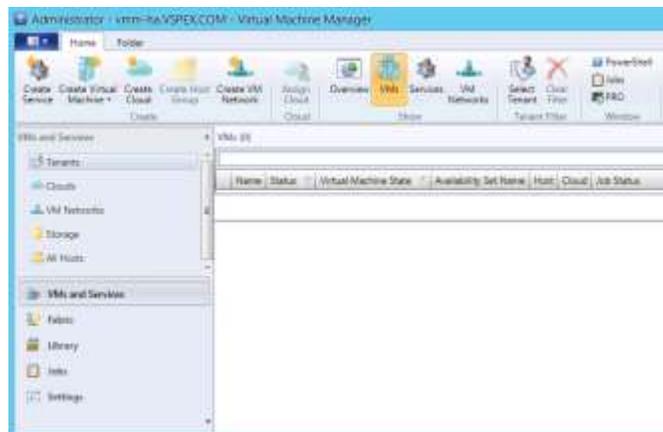


When the installation completes, the wizard will display the **Setup completed successfully** page. Uncheck the boxes to check for updates and launch the console. Click **Close** to complete the installation.



When the installation is complete, open the Virtual Machine Manager console to verify that it installed properly.

- Set the **Server name** value to match the name that was provided for the **Cluster Resource** name during setup (for example, HAVMM: 8100).
- Verify that the console opens and connects to the Virtual Machine Manager instance installed.

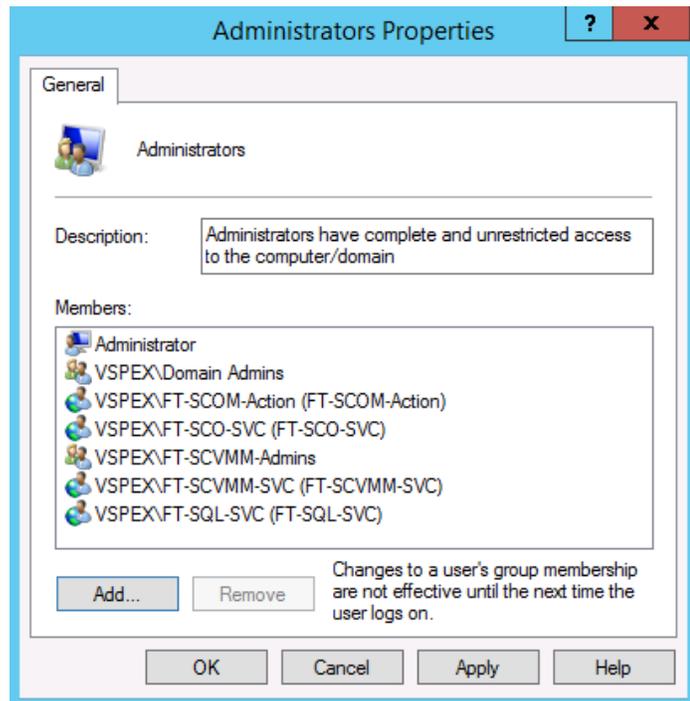


► Perform the following steps on the **second** Virtual Machine Manager virtual machine.

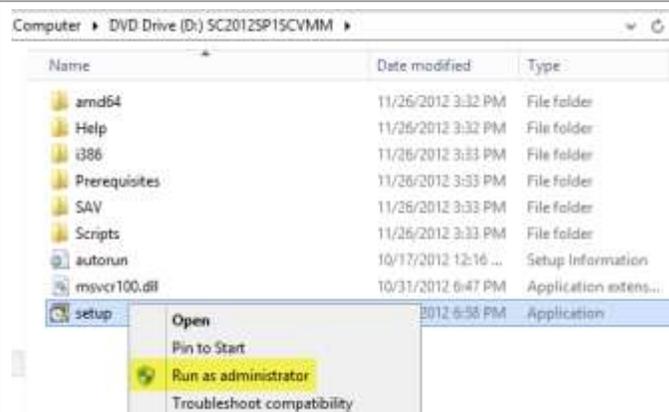
Log on to the **second** Virtual Machine Manager virtual machine as a user with local Administrator rights.

Verify that the following accounts or groups are members of the local Administrators group on the Virtual Machine Manager virtual machine:

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



From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup. If prompted by User Account Control, select **Yes** to allow the installation to make changes to the computer.



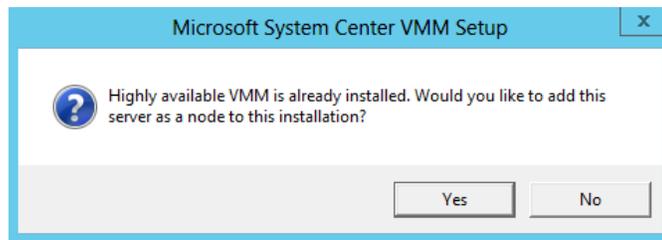
The Virtual Machine Manager installation wizard will begin. Click **Install** to begin the Virtual Machine Manager server installation.



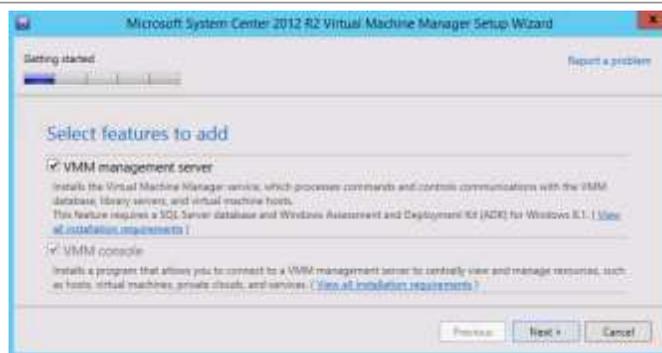
Selecting the VMM management server feature will cause the Microsoft System Center VMM Setup message to appear.

Click **Yes** to switch to the high availability Virtual Machine Manager Setup Wizard and add the second node.

Note: Virtual Machine Manager can be deployed on up to 16 cluster nodes but only a single node can be active at any time.



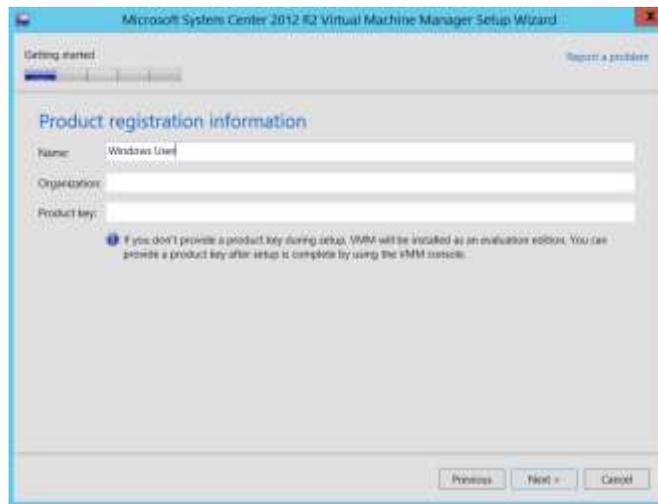
On the **Select features to install** page, verify that the **VMM management server** installation option check box is selected. When it is selected, the **Virtual Machine Manager console** installation option check box is selected by default. Click **Next** to continue.



On the **Product registration information** page, type the following information in the provided text boxes:

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

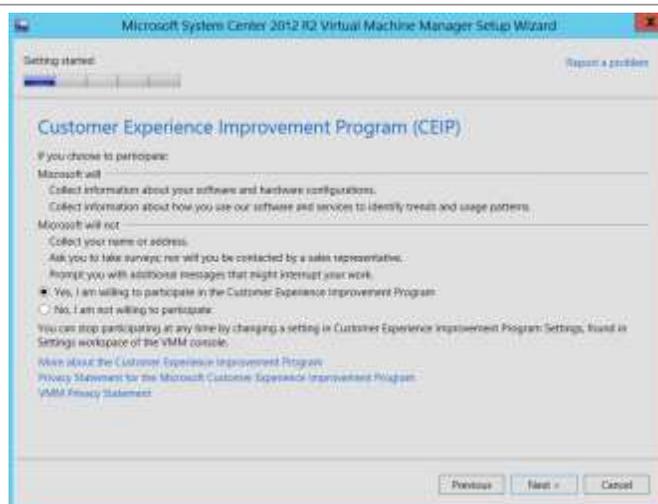
Click **Next** to continue.



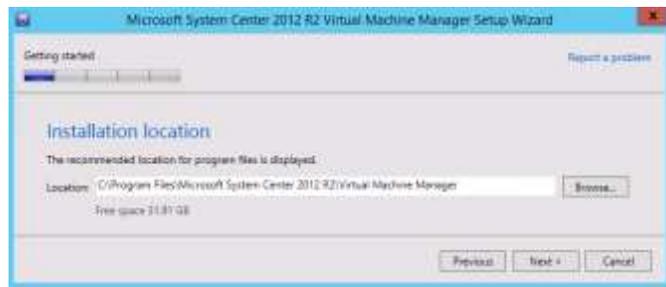
On the **Please read this license agreement** page, verify that the **I have read, understood and agree with the terms of the license agreement** check box is selected, and click **Next** to continue.



On the **Join the Customer Experience Improvement Program (CEIP)** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



On the **Installation location** page, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Virtual Machine Manager for the installation. Click **Next** to continue.



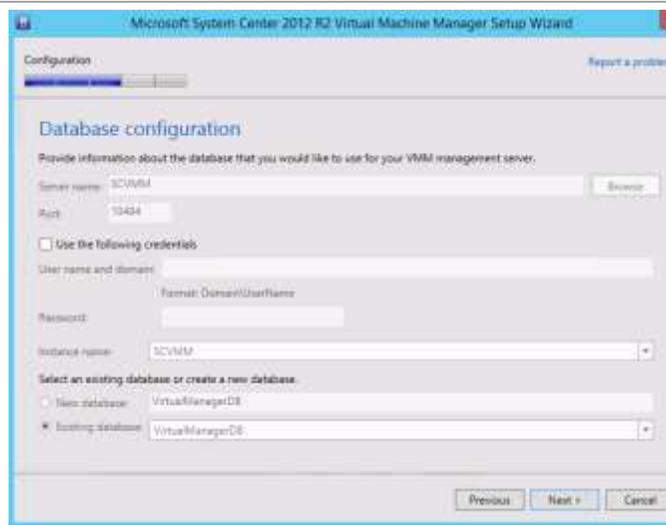
Note: The Setup Wizard automatically checks for prerequisites. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy. This screenshot provides an example of a discrepancy warning.

If the system passes the prerequisite check, no screen will be displayed and the Setup Wizard will proceed to the **Database configuration** page.



On the **Database configuration** page, all options are unavailable when adding an additional node to an existing Virtual Machine Manager cluster.

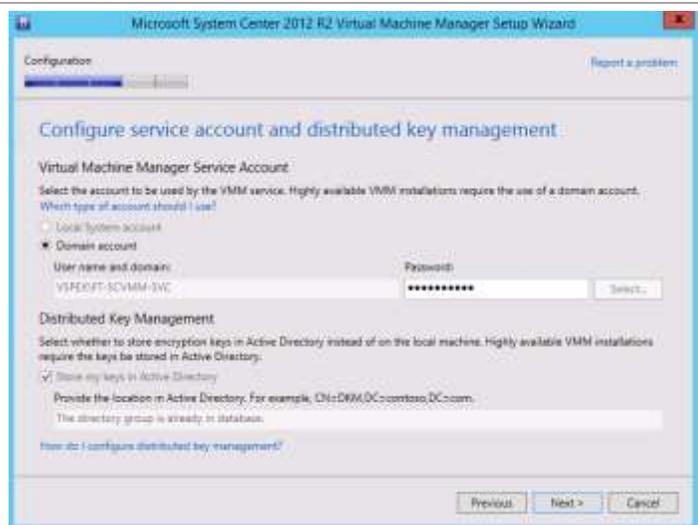
Click **Next** to continue.



On the **Configure service account and distributed key management** page, when deploying additional nodes to a Virtual Machine Manager cluster, all fields other than **Password** are unavailable.

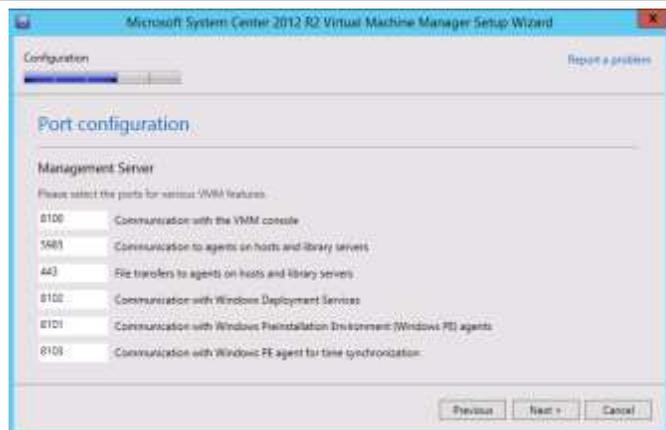
- **Password** – Specify the password for the Virtual Machine Manager service account identified earlier.

Click **Next** to continue.

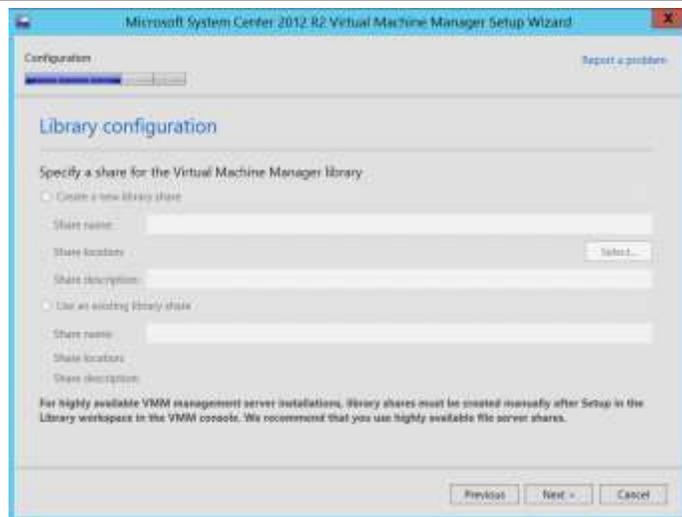


On the **Port configuration** page, when deploying additional nodes to a Virtual Machine Manager cluster, all fields are unavailable.

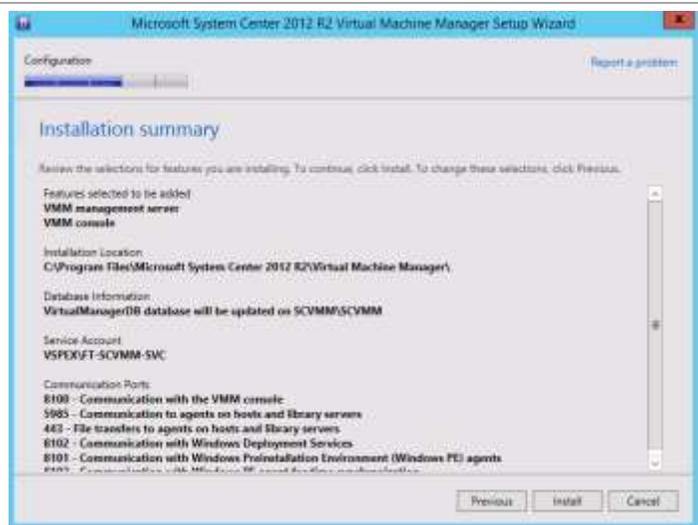
Click **Next** to continue.



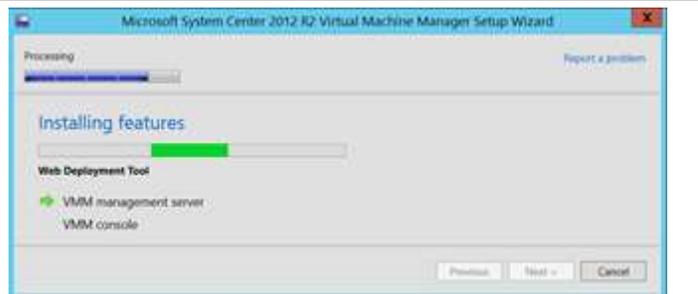
On the **Library configuration** page, no options are available for a high availability installation. The Library must be configured separately and should point to a high availability file share. Click **Next** to continue.



The **Installation summary** page will appear and display the selections you made during the Setup Wizard. Review the options selected and click **Install** to continue.



The wizard will display the progress while installing features.



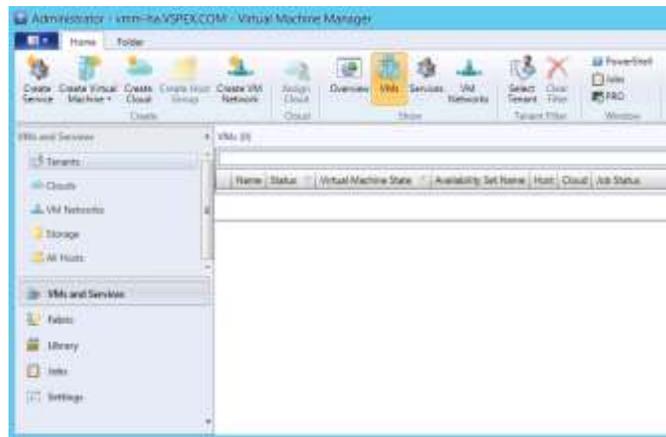
When the installation completes, the wizard will display the **Setup completed successfully** page. Click **Close** to complete the installation.



When complete, open the Virtual Machine Manager console to verify that the installation occurred properly.

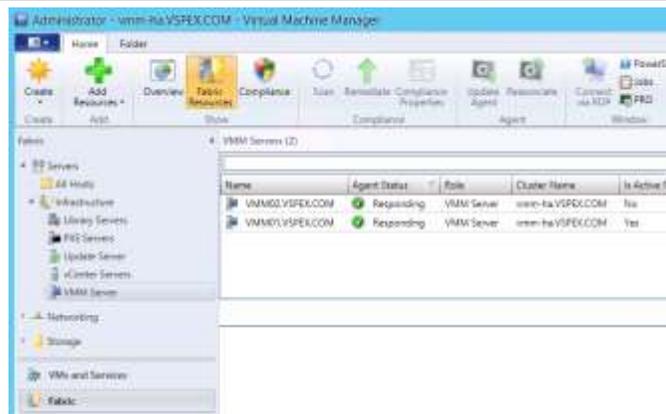
Set the **Server** Name value to match the name that was provided for the **Cluster Resource** name during setup (for example, HAVMM: 8100).

Verify that the console opens and connects to the Virtual Machine Manager instance installed.



In the Virtual Machine Manager Console, select **Fabric** node, then select **Servers**, and then select **Infrastructure**, and then select **VMM Server**.

- In the **Role** column, verify that both cluster nodes are listed as **VMM Servers**.
- In the **Agent Status** column, verify that both nodes are listed as **Responding**.



Creating Virtual Machine Manager Library Share on a Failover Cluster

In a highly available installation of Virtual Machine Manager, the Virtual Machine Manager Library must reside on a Windows Server file share outside the Virtual Machine Manager cluster infrastructure; it is not a supported configuration to reside on the Virtual Machine Manager cluster or its nodes.

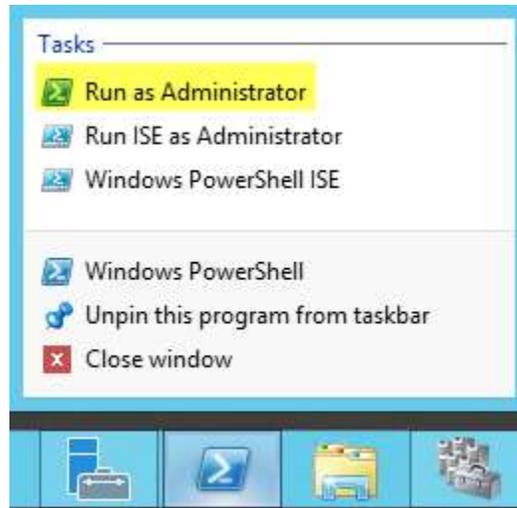
In addition, creating a highly available Virtual Machine Manager Library is a recommended practice given that the Virtual Machine Manager servers are highly available servers.

The Private Cloud IaaS PLA physical architecture makes no recommendations for where the Virtual Machine Manager Library resides, other than that it should have the same high availability as other aspects of the installation. Although any file server cluster will suffice, this document details the steps required to host the Virtual Machine Manager Library on the SQL Server Cluster created in earlier portions of this document as an example.

Note: In general, it is recommended to only run SQL instances on a SQL cluster. In this case, in order to simplify the installation, the share was placed on the SQL cluster rather than creating cluster for this single use. It is expected that customer installations will have highly available file share clusters in their environment for hosting this share.

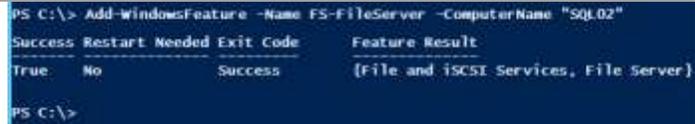
► Perform the following steps on **each** SQL Server virtual machine.

Open a Windows PowerShell session as an administrator.



Run the following command once for each SQL Server cluster node, and change the **ComputerName** value each time to that of a different SQL Server cluster node.

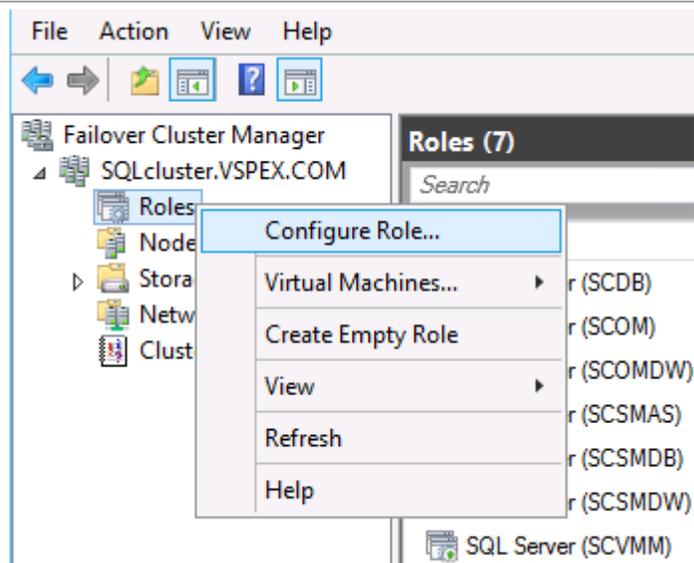
`Add-WindowsFeature -Name FS-FileServer -ComputerName "SQL01"`



Add an additional Shared VHDX and prepare it as described in previous steps. This should appear as available storage in the **Failover Cluster Manager Storage** node.

► Perform the following steps on the **first** SQL Server cluster node.

Within **Failover Cluster Manager**, right-click **Services and applications** and select **Configure Role...**



The **High Availability Wizard** appears. On the **Before You Begin** page, click **Next** to begin the wizard.



On the **Select Role** page, from the available services and applications, click **File Server**, and click **Next** to continue.



On the **File Server Type** page, select the **File Server for general use** button, and click **Next** to continue.



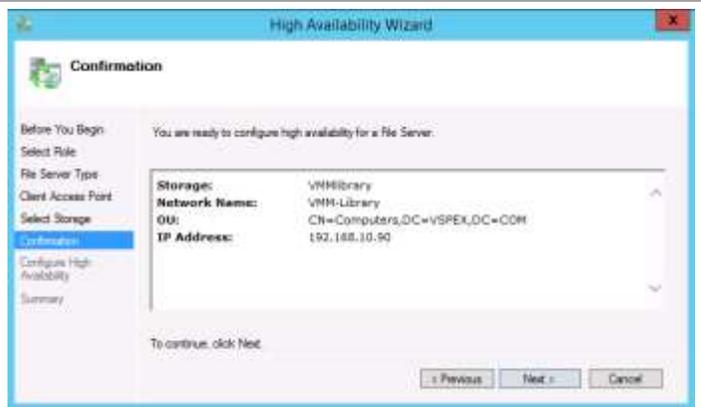
On the **Client Access Point** page, type a unique name for the clustered file server in the **Name** text box. Additionally, for static IP configurations, select the appropriate network and assign a unique IP address to the service. Click **Next** to continue.



On the **Select Storage** page, from the available storage, select the cluster disk that will be used for the Virtual Machine Manager Library, and click **Next** to continue.



On the **Confirmation** page, verify the options selected, and click **Next** to continue.



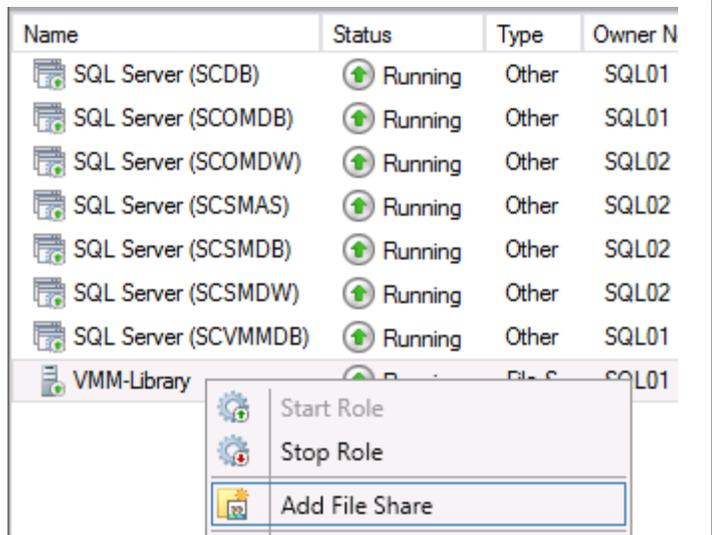
When complete, the **Summary** page will show a report of the actions taken by the wizard. Verify success, and click **Finish** to complete the wizard.



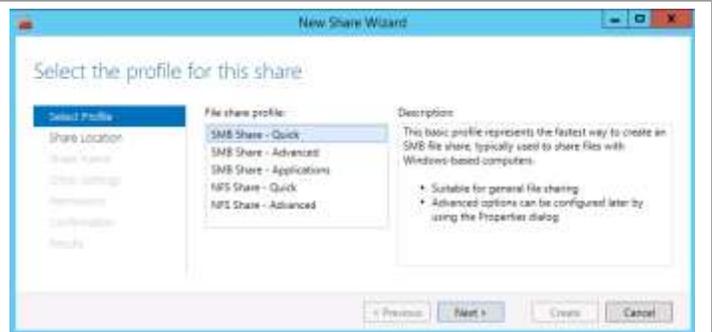
Note: The high availability file server is available as a service in Failover Cluster Manager.

Roles (8)			
Name	Status	Type	Owner Node
SQL Server (SCDB)	Running	Other	SQL01
SQL Server (SCOMDB)	Running	Other	SQL01
SQL Server (SCOMDW)	Running	Other	SQL02
SQL Server (SCSMAS)	Running	Other	SQL02
SQL Server (SCSMDB)	Running	Other	SQL02
SQL Server (SCSMDW)	Running	Other	SQL02
SQL Server (SCVMMDB)	Running	Other	SQL01
VMM-Library	Running	File S...	SQL01

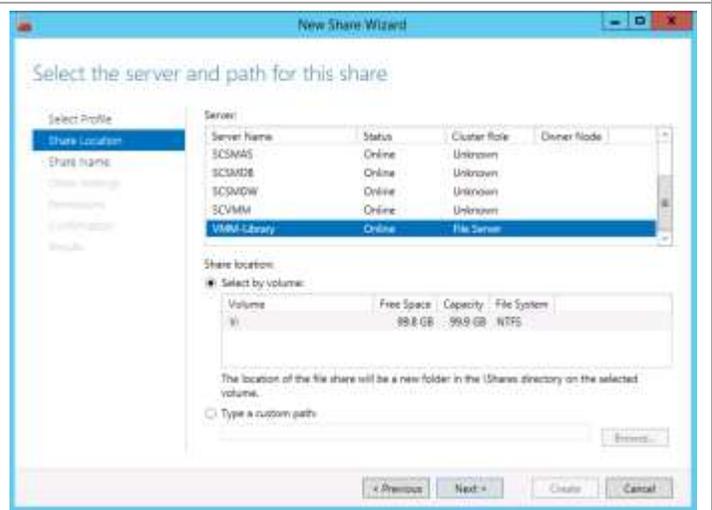
Within **Failover Cluster Manager**, right-click the newly created file server, and click **Add File Share**.



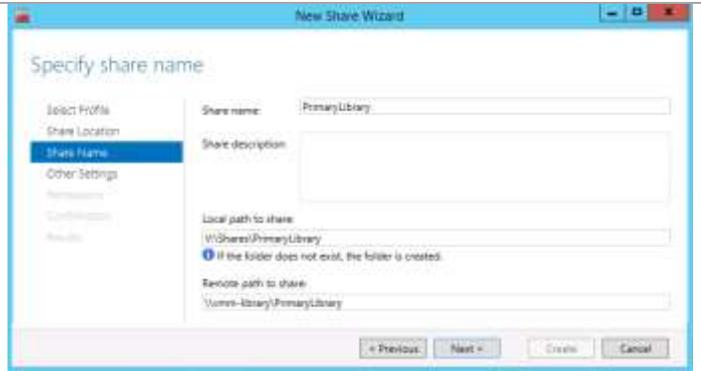
The **New Share Wizard** appears. On the **Select Profile** page, select **SMB Share - Quick**, and click **Next** to continue.



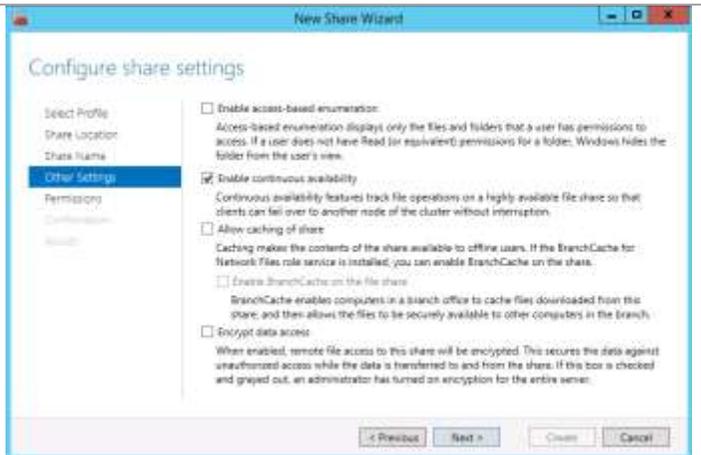
On the **Shared the server and path for this share** page, in the **Server** pane, select the File Server cluster role object name created earlier. In the **Share location** pane, select the **Select by volume** button and click **Next** to continue.



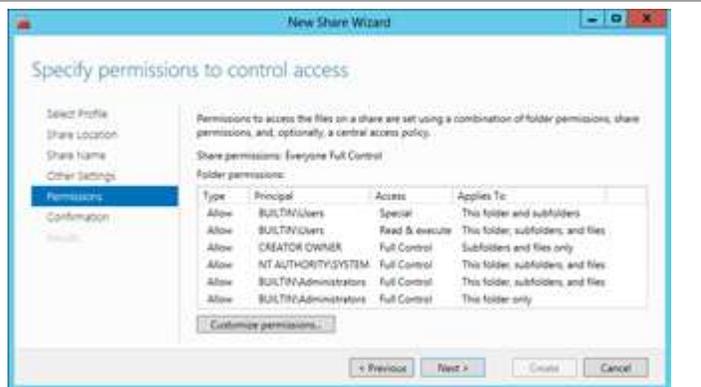
On the **Share Name** page, type the name you wish in the **Share name** field, and then click **Next** to continue.



On the **Other Settings** page, select only the **Enable continuous availability** option, and then click **Next**.



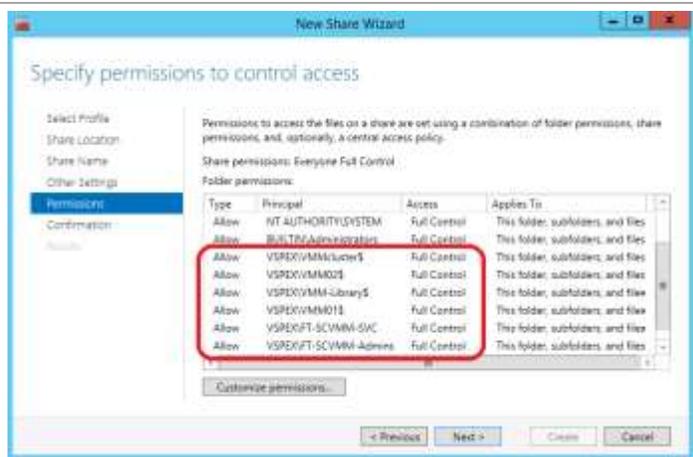
On the **Permissions** page, click **Customize Permissions...**



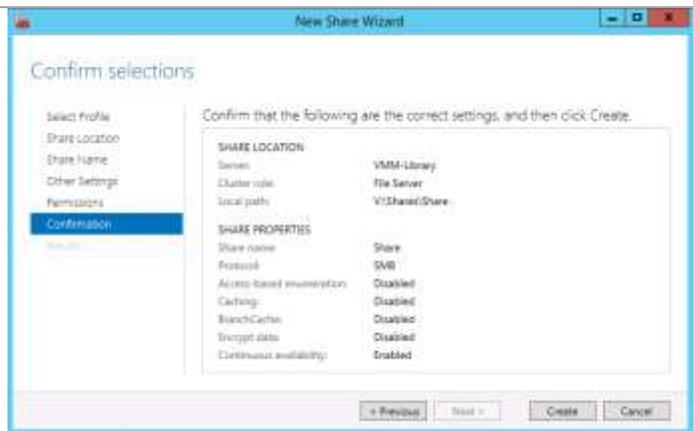
Click the **Customize Permissions** button, and then click **Add**. Add the following accounts with NTFS Full Control permissions:

- VMM service account
- VMM Admins group
- Both VMM computer accounts
- VMM cluster name object computer account
- VMM VCO computer account

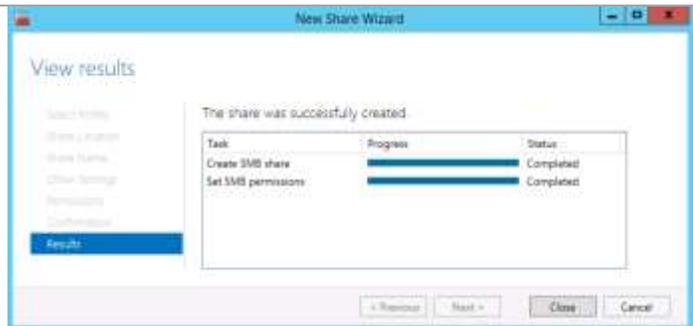
Click **OK** to save the changes, and click **Next** to continue the wizard.



On the **Confirmation** page, review the settings, and then click **Create**.

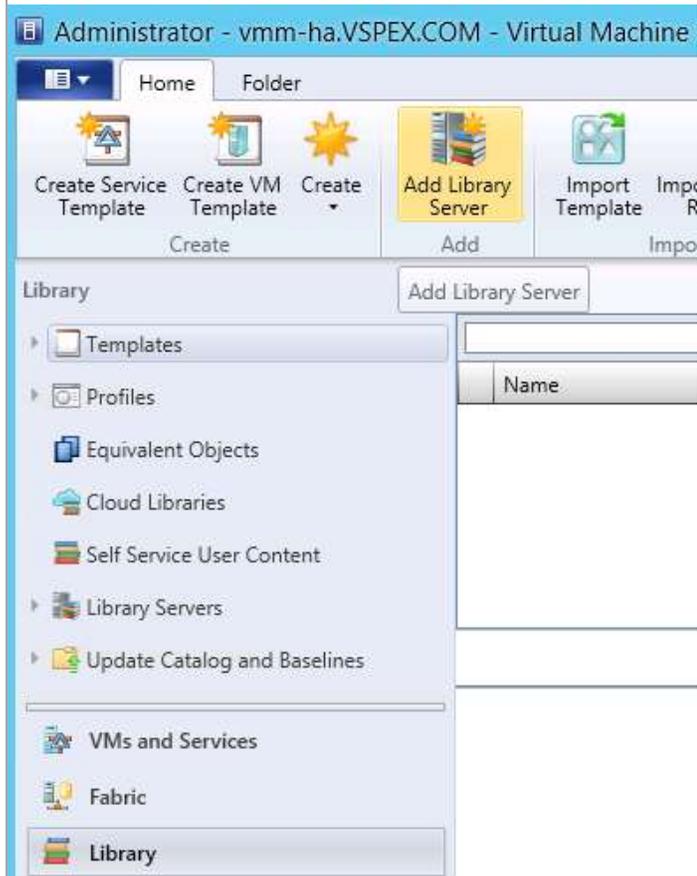


On the **Results** page, verify that the shared folder was provisioned properly, and click **Close**.



► Perform the following steps on the Virtual Machine Manager virtual machine.

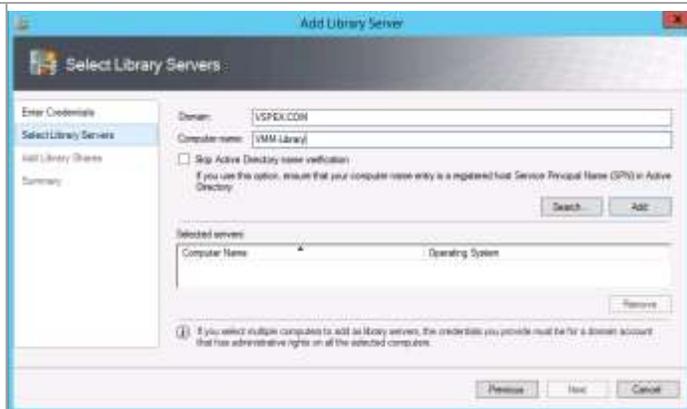
In the **Virtual Machine Manager** console, click the **Library** node. Click the **Home** tab, and then click **Add Library Server** from the ribbon.



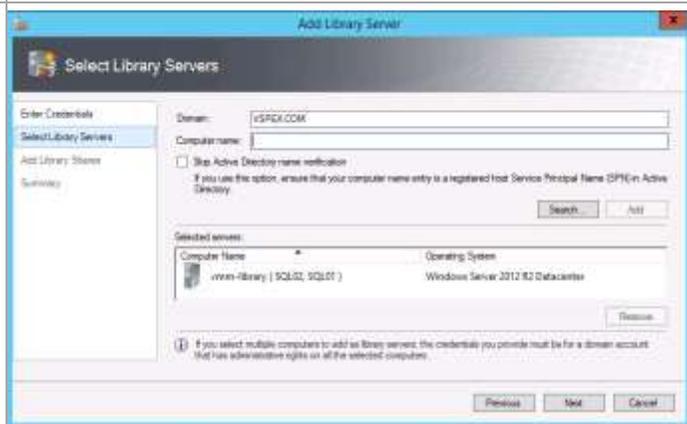
The Add Library Server Wizard appears. On the **Enter Credentials** page, select the **Enter a user name and password** option. In the **User name** and **Password** text boxes, type credentials that have administrative rights over each of the target servers where the new highly-available Virtual Machine Manager Library share will reside. For example, if you placed the share on the SQL cluster, this must be an account with local administrator privileges on those cluster nodes. Click **Next** to continue.



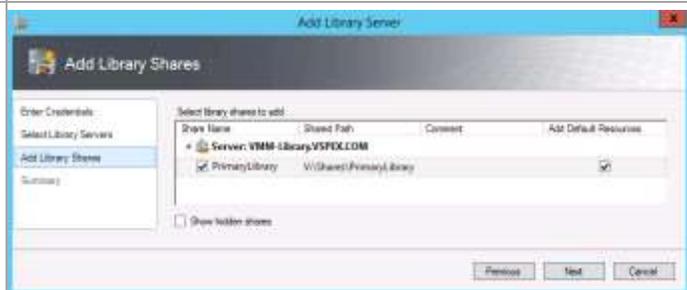
On the **Select Library Servers** page, in the **Domain** text box, specify the FQDN of the target domain. In the **Computer name** text box, type the name of the newly created highly-available File Server cluster name object, and click **Add**.



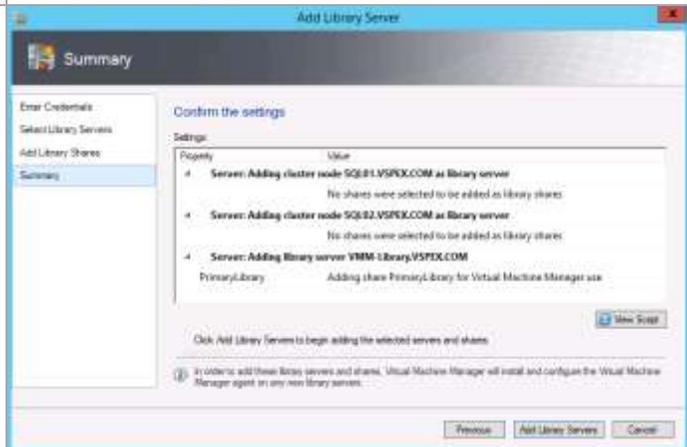
The cluster object will appear in the **Specified Servers** pane. Click **Next** to continue.



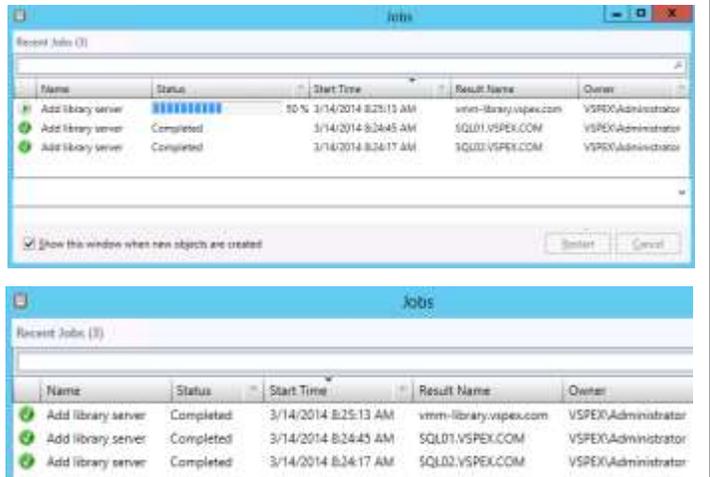
On the **Add Library Shares** page, select the check box associated with the **VMM-Library** share created earlier. Verify that the **Add Default Resources** check box is selected, and click **Next** to continue.



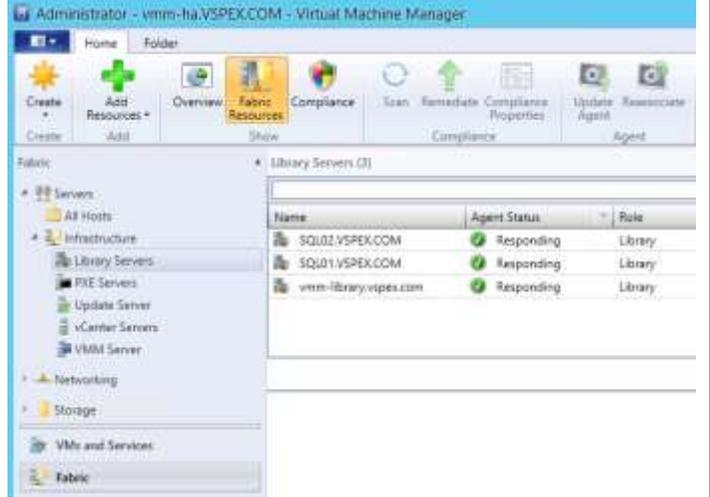
Review the **Summary** page, and click **Add Library Servers** to continue.



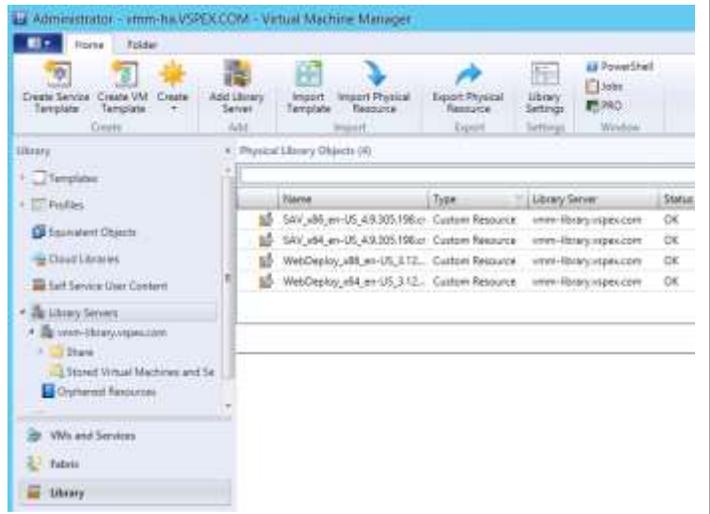
The **Jobs** page will appear showing the progress of the Add Library Server action. Verify that all steps have completed.



In the **Virtual Machine Manager** console, click **Fabric Resources**, and then click **Library Servers** in the left pane. Verify that all cluster nodes are listed with the cluster object name and that all servers are listed as **Responding** under **Agent Status**.



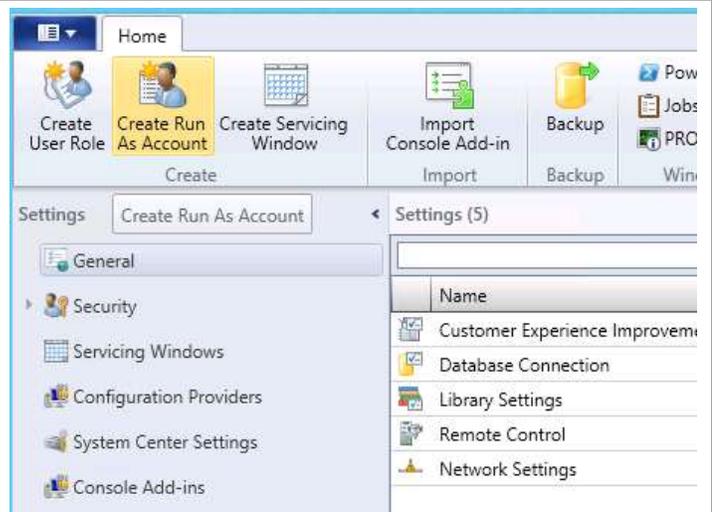
In the **Virtual Machine Manager** console, click **Library Servers** in the left pane, and verify that all of the correct objects are created. When they are verified, exit the console.



Create a Run As Account

SCVMM has implemented a role-based access capability to allow for different individuals to have different levels of access to the functions available within SCVMM. To assign different levels of access, you need to create Run As Accounts. At a minimum, you should create a Run As Account for full administration of the SCVMM installation and start using it for any further configuration of the environment.

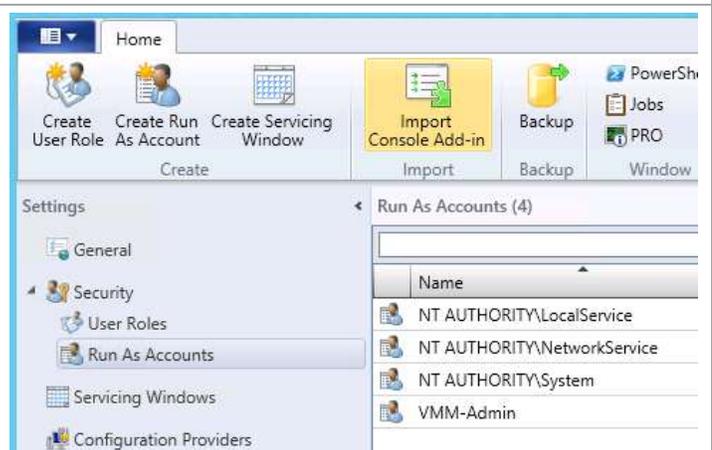
In the **Virtual Machine Manager** console, click **Settings**. From the ribbon, click **Create Run As Account**.



On the **Create Run As Account** page, enter a **Name** for the Run As account. Enter an Active Directory **User Name** with the privileges to accomplish the functions to be done. Enter and confirm the **password**. Make sure the box by **Validate domain credentials** and click **OK** to continue.



Back in the SCVMM console, expand **Security** and select **Run As Accounts**. You will see the newly created account.

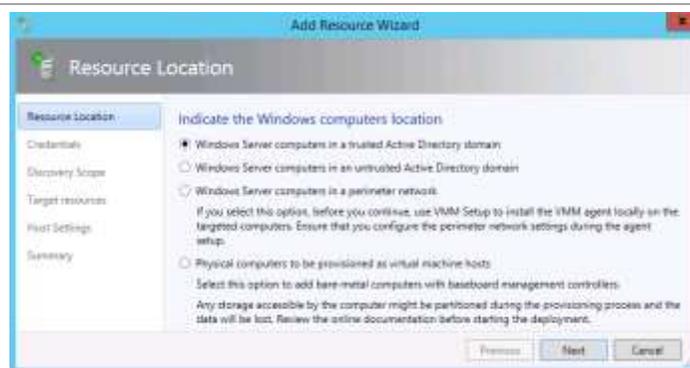


Add Hyper-V Hosts to be Managed by SCVMM

From the SCVMM console select **Fabric** and click the down arrow on **Add Resources** in the menu ribbon. Select **Hyper-V Hosts and Clusters**.



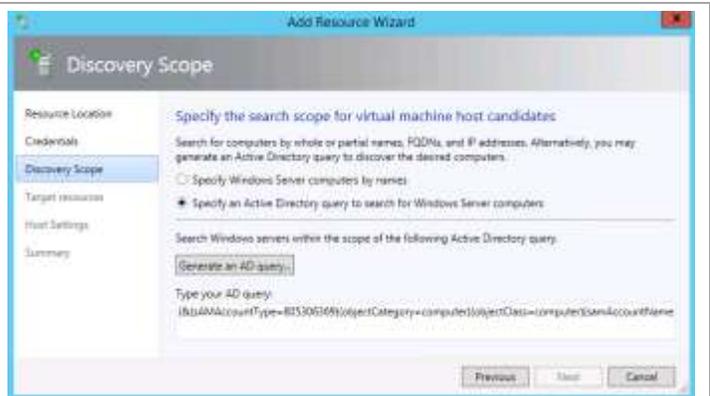
On the **Resource Location** page, select the radio button by **Windows Server computers in a trusted Active Directory domain**. Click **Next** to continue.



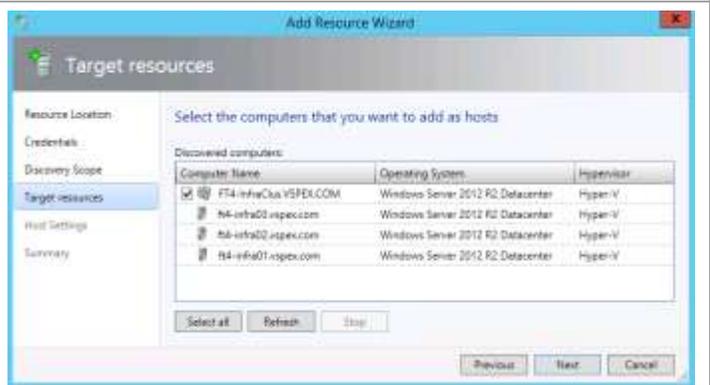
On the **Credentials** page you can enter either the Run As account previously created or manually enter appropriate credentials. In either case, the underlying account must be a local administrator on the host machines being added. Click **Next** to continue.



On the **Discovery Scope** page you can either enter the server names manually or you can create an Active Directory query. After entering the servers name or the Active Directory query, click **Next** to continue.



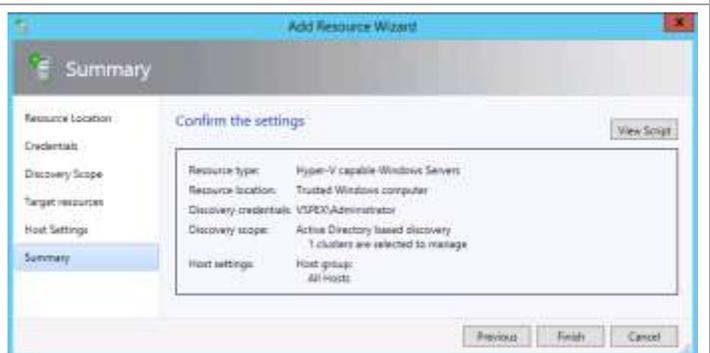
On the **Target Resources** page, click the check box by the cluster name. Click **Next** to continue.



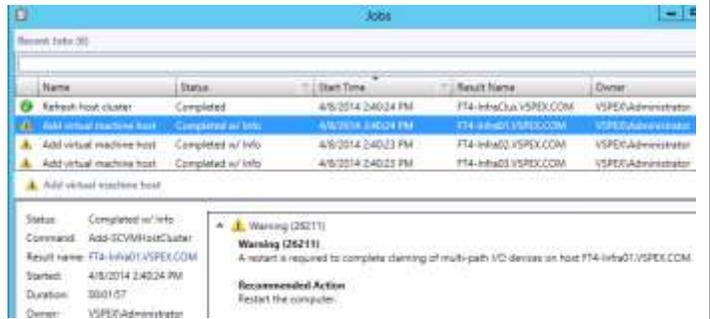
On the **Host Settings** page, specify the **Host Group** in which you wish to place the discovered hosts. If the hosts have ever been associated with a VMM instance in the past, click the check box by Reassociate this host with this VMM environment. Click **Next** to continue.



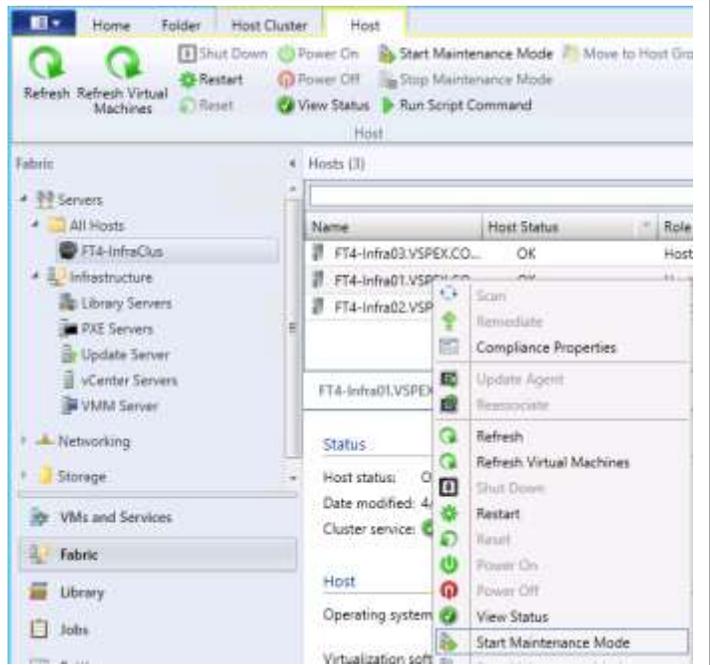
Review your selections on the **Summary** page. Click **Finish** to accept.



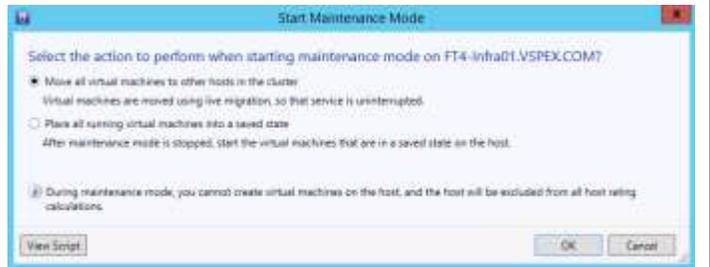
When the job to add the hosts completes, you are likely to see a warning message in regards to MPIO. You can either reboot the servers now, or schedule them for a reboot.



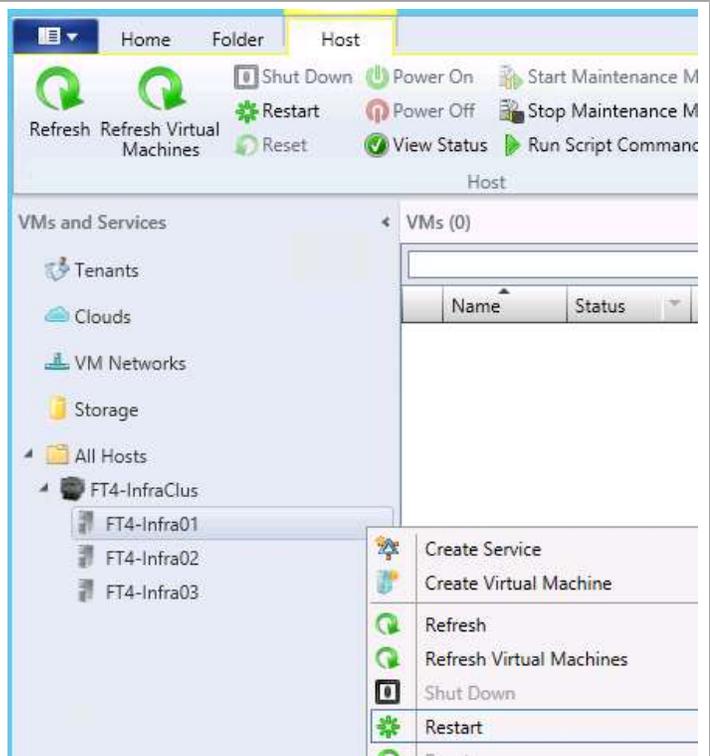
Now that the Hyper-V hosts are managed by SCVMM, you can manage the reboot from the SCVMM console. Right-click the server you wish to restart and select **Start Maintenance Mode** from the menu.



On the **Select the action to perform ...** page, select the radio button to **Move all virtual machines ...** option to live migrate all the VMs to another node in the cluster. Click **OK** to continue.

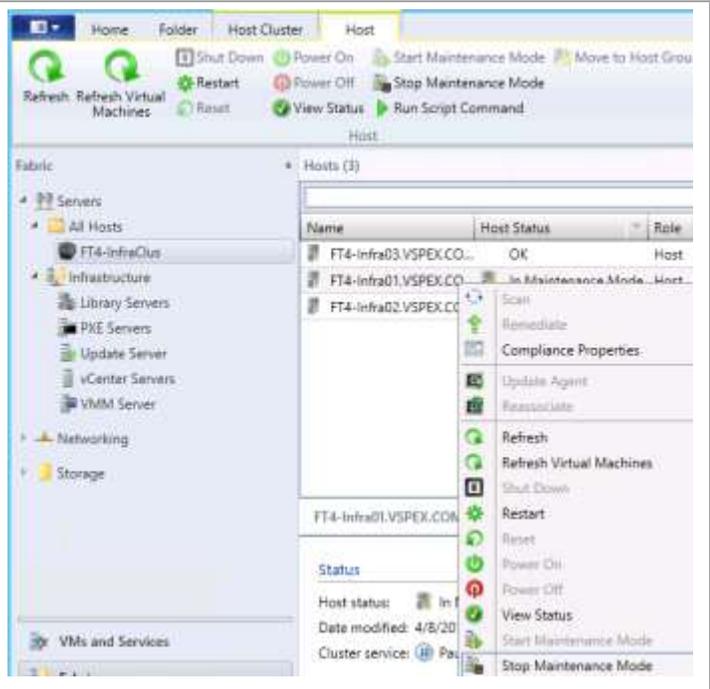


In the **Virtual Machine Manager** console, select the host that was placed in maintenance mode. When no VMs are left on that host, right-click the host and select **Restart**. A warning message about what will happen to VMs on the host will display. Since you have already evacuated the host, click **Yes** to continue.



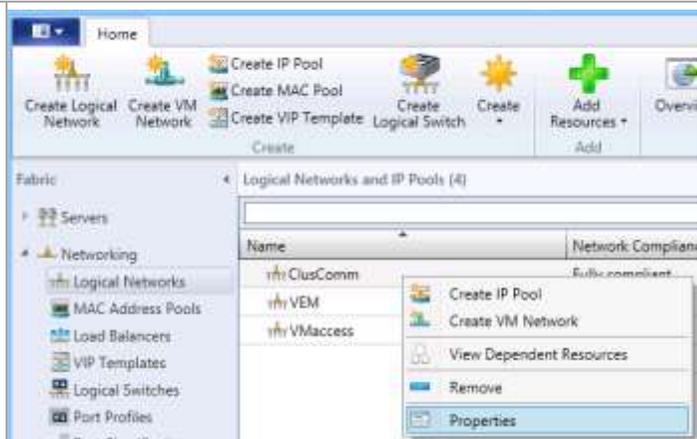
When the host restarts, right-click the host and select **Stop Maintenance Mode** so it will be able to accept VMs being moved to it.

Cycle through the other hosts to restart them.



Configure Logical Networks

Select **Fabric** within the VMM console. Then select **Networking** and **Logical Networks**. Double click one of the networks, except VEM, to open the **Properties**.



On the **Properties** window, click **Network Site**. Click **Add** to start the configuration of the network site.

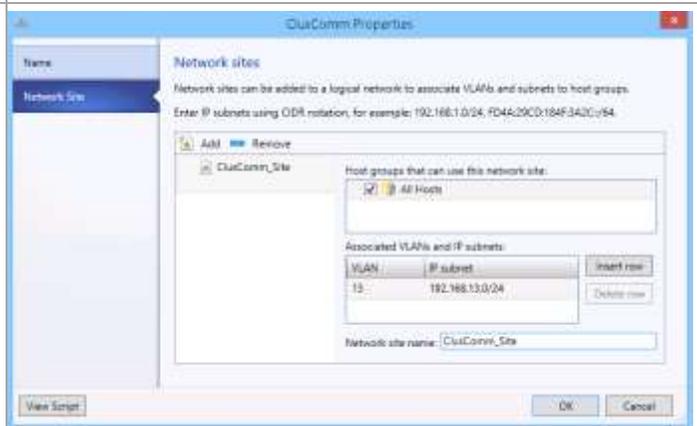
Select the Hyper-V hosts that will be able to offer this network site through a virtual switch definition.

Click **Insert Row** and enter the VLAN tag value for this network. Enter the IP subnet definition in CIDR notation for this network.

Optionally, rename the site name.

Click **OK** to continue.

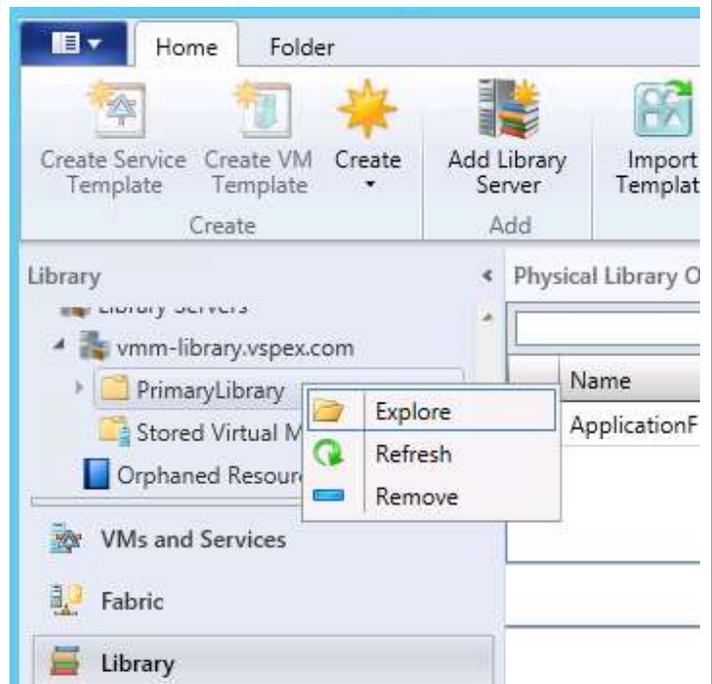
Repeat for all networks except VEM. The VEM network is for use with the Cisco Nexus 1000V



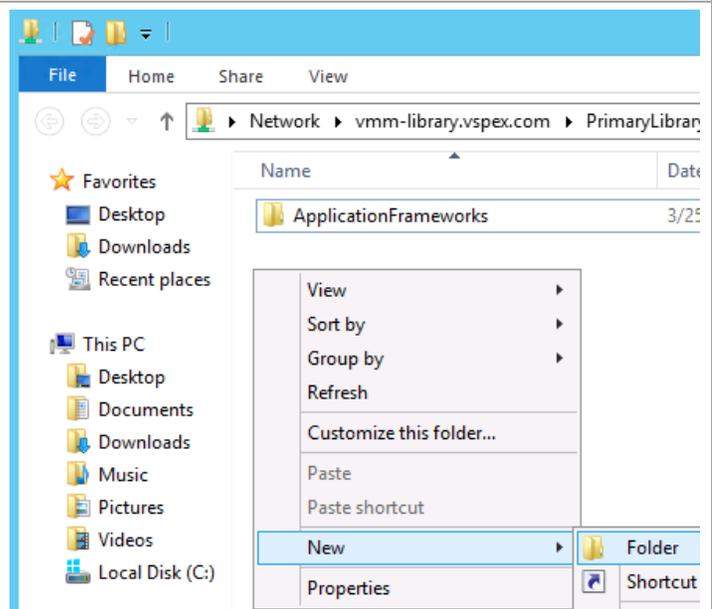
Configure Library Subdirectories (optional)

Having a library as part of VMM provides a handy location for storage of many items that are used regularly in the management and maintenance of the cloud. It can be helpful to create subdirectories within the standard SCVMMlibrary share that was just created for storage of items, such as distribution media in the form of ISO files.

In the **Virtual Machine Manager** console, click **Library**. Right-click the previously created library and select **Explore**.



A Windows Explorer window will display allowing you to create whatever directories you may find using, such as a Software directory to be used for storing ISO files, or a PowerShell directory to store re-usable PowerShell scripts. After the directories are created, they can be used as regular UNC paths under the share created previously, allowing you to copy information into them from any location, as long as the user performing the copy has the proper privileges.

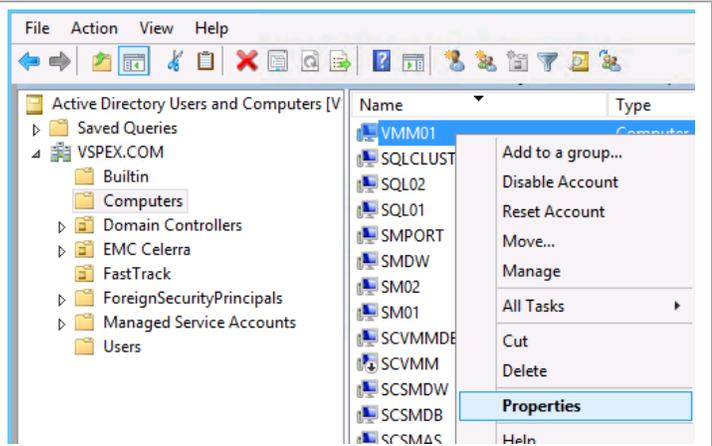


Configure Constrained Delegation (optional)

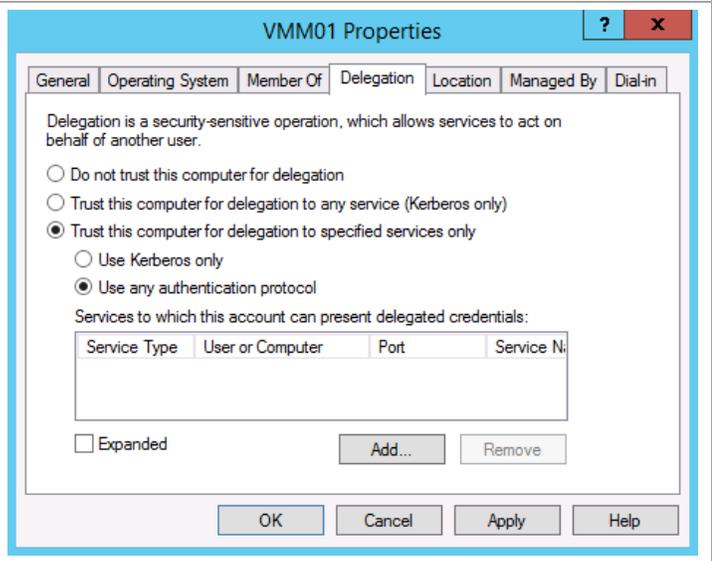
By default, when VMM is creating a virtual machine, and you are using an ISO file from the library for installation purposes, the ISO file is copied and made part of the virtual machine's definition. This wastes time copying the file and it takes extra space. It also means that different versions of installation media may end up getting stored all over. Sharing ISO items across nodes requires additional configuration of the VMM hosts and any system that runs the VMM console. This is called constrained delegation which allows the VMM host to operate on behalf of the virtual machine being created.

This is a security change to a default installation, so it should be reviewed with your security department before deployment.

On your domain controller (or a system that has the proper Remote Server Administration Tools installed), launch **Active Directory Users and Computers**. Expand your domain and expand **Computers**. Right-click your VMM host and select **Properties**.

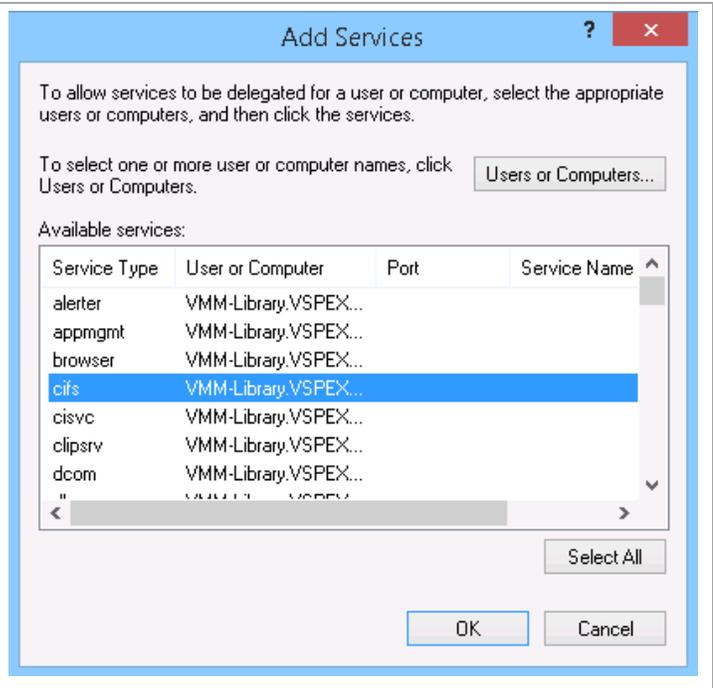


On the **Delegation** tab, click the radio button by **Trust this computer for delegation to specified service only**. Select the radio button by **Use any authentication protocol**. Click the **Add...** button.



On the **Add Services** page, click the **Users or Computers...** button. Select the SCVMM library server in the **Select Users or Computers** window. Click **OK** to show the list of services available for the selected server. Select the **cifs** service and click **OK** to continue. Then click **OK** on the server Property page to update the services

Repeat for each SCVMM server or any server from which you plan to run the VMM console, such as your remote management workstation.



Cisco UCS SCVMM Add-In

The UCS Add-in for Microsoft System Center 2012 R2 Virtual Machine Manager enables management of Cisco UCS from within SCVMM.

Installation of this add-in requires that Cisco UCS PowerTool is already installed on the servers to which the UI extensions add-in will be added. The add-in needs to be installed on any SCVMM console from which you want to use the extensions. The deployment instructions for the Cisco SCVMM Add-in are included in the chapter covering all the Cisco integration components.

Operations Manager

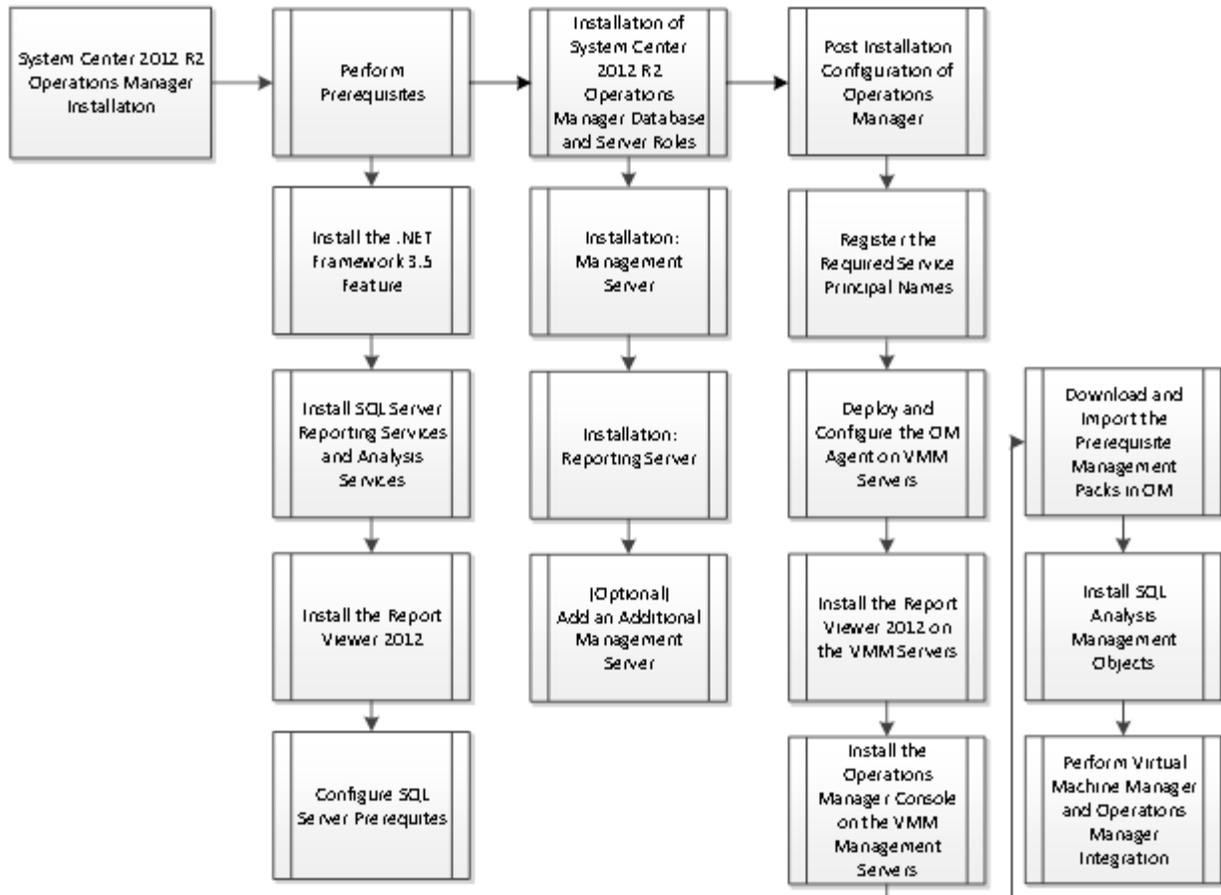
A minimum of two Operations Manager servers are deployed in a single management group that is using a dedicated SQL Server instance in the virtualized SQL Server cluster. An Operations Manager agent is required to be installed on every management host and each scale unit cluster node to support health monitoring functionality. Additionally, agents may be installed on every guest virtual machine to provide guest level monitoring capabilities.

Operations Manager gateway servers and additional management servers are supported for custom solutions; however, for the base reference implementation these additional roles are not implemented. Additionally, if there is a requirement to monitor agentless devices in the solution, such as datacenter switches, additional management servers should be deployed to handle the additional load. These additional management servers should be configured into an Operations manager Resource Pool dedicated to this task (<http://technet.microsoft.com/library/hh230706.aspx>). Deployment of these additional servers is beyond the scope of this CVD.

The Operations Manager installation uses a dedicated SQL Server instance in the virtualized SQL Server cluster. The installation follows a split SQL Server configuration: SQL Server Reporting Services and Operations Manager Management Server components reside on the Operations Manager virtual machines, and the SQL Server Reporting Services and Operations Manager databases utilize a dedicated instance on the virtualized SQL Server cluster. Note that for the IaaS PLA implementation, the Data Warehouse is sized for 90-day retention instead of the default retention period.

The Operations Manager installation process includes the high-level steps shown in the following figure.

Figure 8. Operations Manager Installation Process



Overview

This section provides a high-level walkthrough for deploying Operations Manager into the fabric management architecture. The following assumptions are made:

- A base virtual machine running Windows Server 2012 R2 has been provisioned for Operations Manager.
- A SQL Server 2012 SP1 cluster with dedicated instances has been established in previous steps.
 - The default SQL Server collation settings are SQL_Latin1_General_CP1_CI_AS.
 - SQL Server full text search is required.
- The installation will follow a remote SQL Server configuration with multiple SQL Server instances:
 - SQL Server Reporting Services and SQL Server Analysis Services are installed in one SQL instance locally on the Operations Manager reporting server. The reporting services databases will run on the remote Operations Manager data warehouse SQL FCI and the Analysis Services data will reside locally on the Operations manager reporting server.
 - The Operations Manager databases on will run on a separate SQL Server instance in the Fabric Management SQL Server cluster.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following domain accounts have been created:

Table 23. Operations Manager Accounts

User name	Purpose	Permissions
<DOMAIN>\FT-SCOM-SVC	System Center Configuration service and System Center Data Access service account (sdk_user role)	Domain account with local Administrator permissions on all Operations Manager management servers and all SQL Server nodes, in addition to System Admin rights on all Operations Manager SQL Server instances.
<DOMAIN>\FT-SCOM-Action	Operations Manager action account	This account needs full Administrator permissions on all target systems that will be managed by using the action account.
<DOMAIN>\FT-SCOM-DR	Operations Manager data reader account	Domain account with local Administrator permissions on all Operations Manager management servers and all SQL Server nodes.
<DOMAIN>\FT-SCOM-DW	Operations Manager, data warehouse write account	Domain account with local Administrator permissions on all Operations Manager management servers and all SQL Server nodes.

Note: Specific requirements for Operations Manager are outlined in the Before You Begin section of [Deploying System Center 2012 R2 - Operations Manager](#) in the TechNet Library.

Groups

Verify that the following security groups have been created.

Table 24. Operations Manager Security Groups

Security group name	Group scope	Members
<DOMAIN>\FT-SCOM-Admins	Global	<DOMAIN>\FT-SCOM-Action <DOMAIN>\FT-SCOM-SVC <DOMAIN>\FT-SCOM-DR <DOMAIN>\FT-SCOM-DW Operations Manager Administrators privileged admin account Operations Manager computer account <DOMAIN>\FT-SCVMM-SVC

Security group name	Group scope	Members
<DOMAIN>FT-SCOM-Operators	Global	Operations Manager Operators privileged admin accounts
<DOMAIN>FT-SCOM-AdvOperators	Global	Operations Manager Advanced Operators privileged admin accounts

Add .NET Framework 3.5

The Operations Manager installation requires that .NET Framework 3.5 is enabled to support installation. Use the following procedure to enable .NET Framework 3.5.

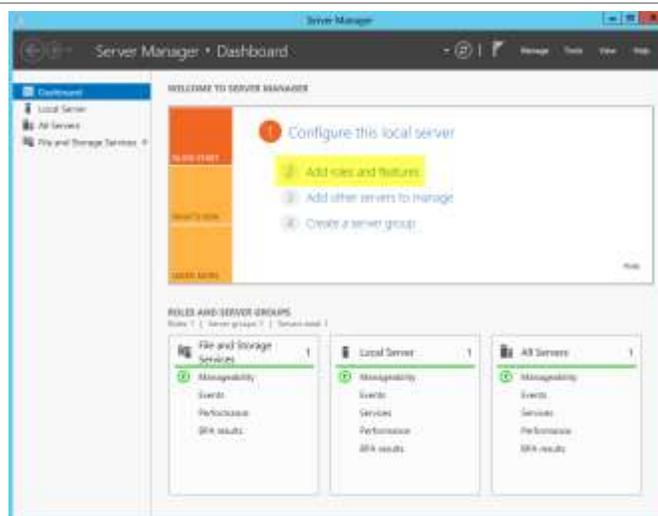
► Perform the following steps on **all** Operations Manager virtual machines.

If you do not have access to the internet to contact Microsoft Update, you will need to have the Windows Installation files mounted locally or on an accessible file share.

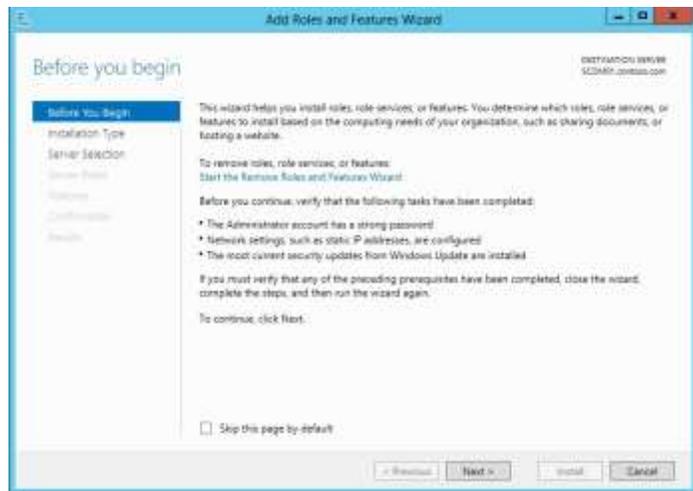
The .NET Framework 3.5 feature can be installed with a PowerShell cmdlet, or the following instructions can be followed for using the GUI. If the VM has access to the internet, the `-Source` parameter should not be needed.

`Install-windowsFeature -Name NET-Framework-Core -Source "E:\Sources\sxs"`

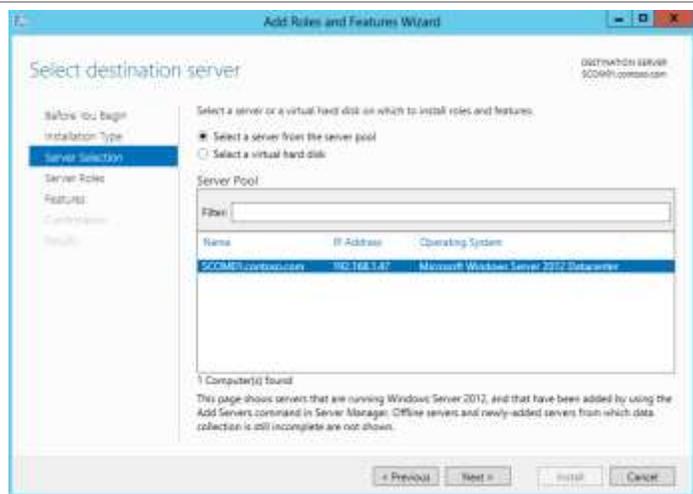
Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, select **Add roles and features**.



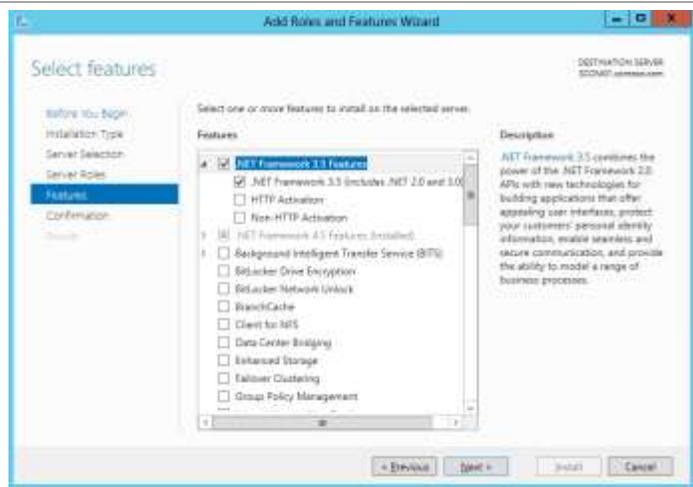
The **Add Roles and Features Wizard** appears. On the **Before You Begin** page, click **Server Selection** in the left pane. (Do not click **Next**.)



On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server and then click **Features** in the left pane. (Do not click **Next**.)



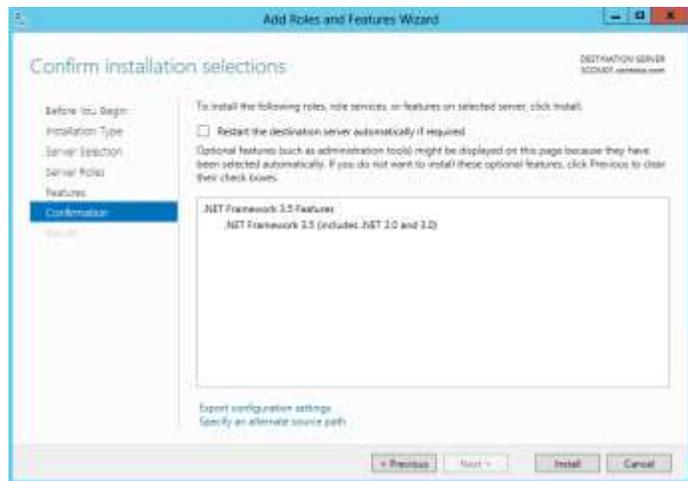
On the **Select Features** page, in the **Features** pane, select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 Features (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



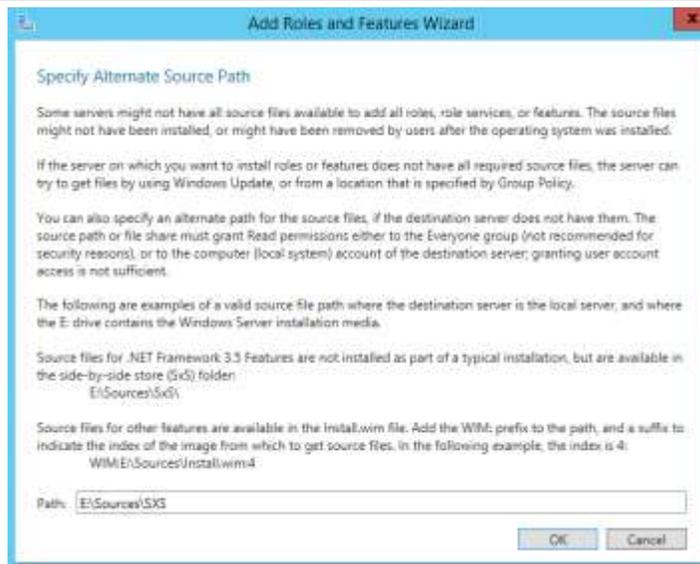
On the **Confirm installation selections** page, verify that **.NET Framework 3.5 Features** is listed. Make sure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

Note: The **Export configuration settings** option is available as a link on this page to export the options selected to XML. When exported, they can be used in conjunction with the Server Manager module for Windows PowerShell to automate the installation of roles and features.

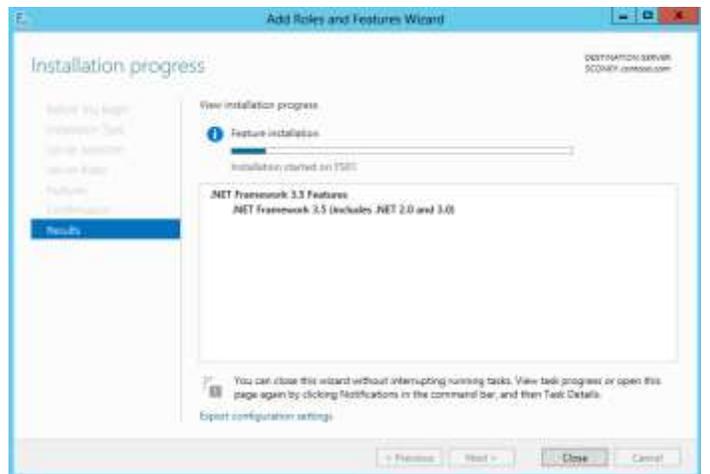
Note: The **Specify an alternate source path** is required if the VM is not connected to the internet to download this specific feature.



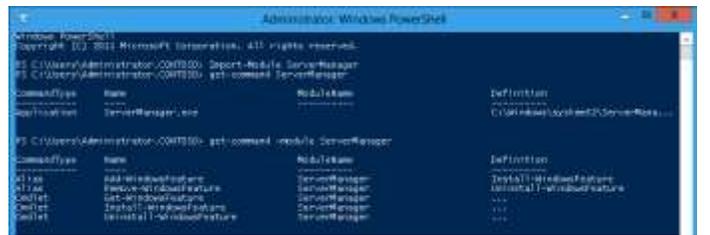
Optional: If you need to specify the source for a feature, enter the path to obtain the binaries for the feature to be installed. If the Windows installation media is mounted locally, the path would be something like **E:\Sources\sxs**. If it is available on a share, it would be something like **\\server\share\sources\sxs**.



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



Note: Although this installation was performed interactively, the installation of roles and features can be automated by using the Server Manager module for Windows PowerShell.



Install the SQL Server Reporting Services (Split Configuration) and Analysis Services

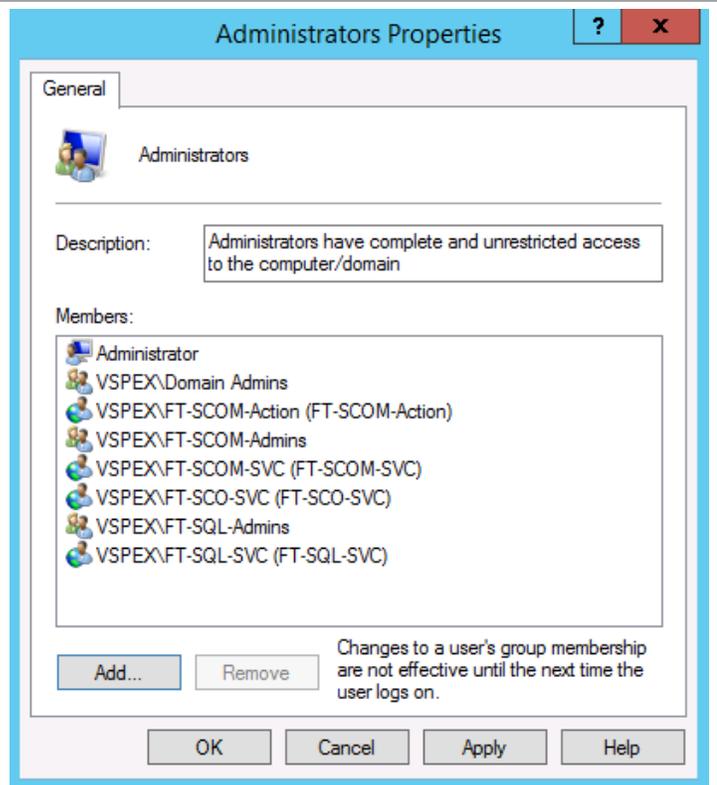
The Operations Manager installation requires SQL Server Reporting Services and SQL Server Analysis Services to be installed to support the Operations Manager reporting features and integration with Virtual Machine Manager. Perform the following procedure to install SQL Server Reporting Services and SQL Server Analysis Services to support the Operations Manager reporting features.

- ▶ Perform the following steps on only the Operations Manager reporting server virtual machine.

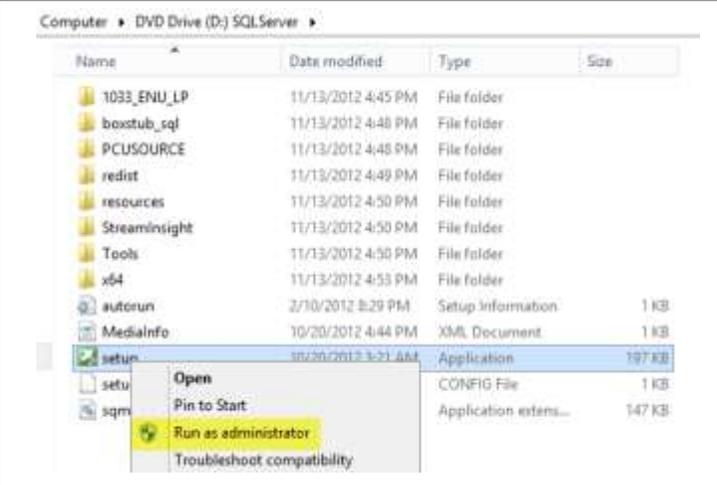
Log on to the Operations Manager reporting server virtual machine as a user with local Admin rights.

Verify that the following accounts or groups are members of the local Administrators group on the Operations Manager reporting server virtual machine:

- Orchestrator service account
- Operations Manager action account
- Operations Manager Admins group
- Operations configuration service and data access service account
- SQL Server service account
- SQL Server Admins group



From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



The **SQL Server Installation Center** will appear. Click **Installation** in the left pane.



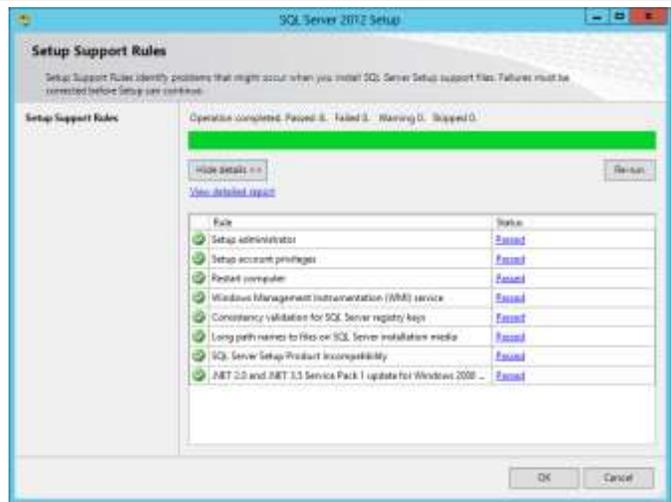
From the **SQL Server Installation Center**, click the **New SQL Server stand-alone installation or add features to an existing installation** link.



New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2012 in a non-clustered environment or to add features to an existing SQL Server 2012 instance.

The **SQL Server 2012 Setup Wizard** will appear. On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **OK** to continue.



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

Rule Name	Rule Description	Result	Message/Correction Action
Installation: SQL Server 2012 setup configuration checks for rules group 'Installation'			
InstallationPackageIsInstalled	This rule determines whether the computer has the required update package for .NET Framework 3.5 or .NET Framework 4.5 SP1 that is needed for a successful installation of most SQL Server components that are included in SQL Server.	Not applicable	This rule does not apply to your system configuration.
ServerInstanceIsLocal	Checks if the instance of SQL Server is local.	Not applicable	This rule does not apply to your system configuration.
ServerIsSupportedArch	Checks if the version of SQL is supported on the currently running Windows Server Core OS.	Not applicable	This rule does not apply to your system configuration.
SQLServerEditionIsLocal	Checks if the SQL Server edition keys are consistent.	Passed	SQL Server edition keys are consistent and can support SQL Server installation or upgrade.
MicrosoftStorageIsSupportedCheck	Checks whether the account that is running SQL Server setup has the right to back up files and directories, the right to manage auditing and the security log, and the right to delete programs.	Passed	The account that is running SQL Server setup has the right to back up files and directories, the right to manage auditing and security log, and the right to delete programs.
MinimumLanguage	Checks whether the SQL Server installation media is the lang.	Passed	The SQL Server installation media is not too long.
InstallationStorage	This rule determines whether the computer has the required update package for .NET Framework 3.5 or .NET Framework 4.5 SP1 that is needed for a successful installation of most SQL Server components that are included in SQL Server.	Passed	This computer has the required update package.
AntiSpamAgentCheck	Checks if a pending computer restart is required, a pending restart can cause setup to fail.	Passed	The computer does not require a restart.
ServerCompatibilityLevel	Checks whether the current version of SQL Server is compatible with a later installed version.	Passed	Setup has not detected any incompatibilities.
ServiceAccountIsLocalCheck	Checks whether the account running SQL Server setup has administrative rights on the computer.	Passed	The account running SQL Server setup has administrative rights on the computer.
WindowsEventLogCheck	Checks whether the WMI service is started and running on the computer.	Passed	The Windows Management Instrumentation (WMI) service is running.

On the **Product Key** page, select the **Enter the product key** option, and type the associated product key in the provided text box. Click **Next** to continue.

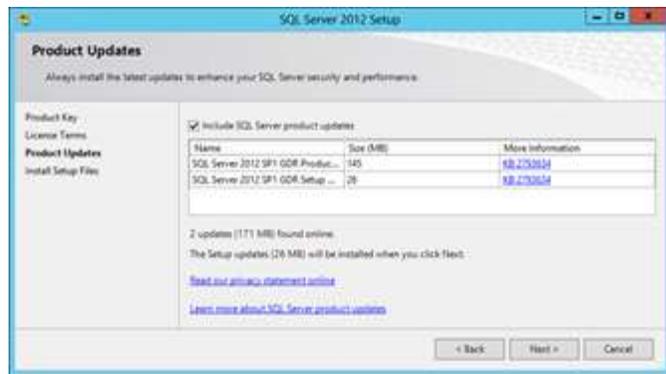
Note: If you do not have a product key, select the **Specify a free edition** option, and select **Evaluation** from the drop-down list for a 180-day evaluation period.



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



On the **Product Updates** page, select the **Include SQL Server product updates** check box, and click **Next** to continue.



On the **Install Setup Files** page, click **Install** and allow the support files to install.



On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. **Note:** Common issues include MSDTC, MSCS, and Windows Firewall warnings. The use of MSDTC is not required for the System Center 2012 R2 environment. Click **Next** to continue.



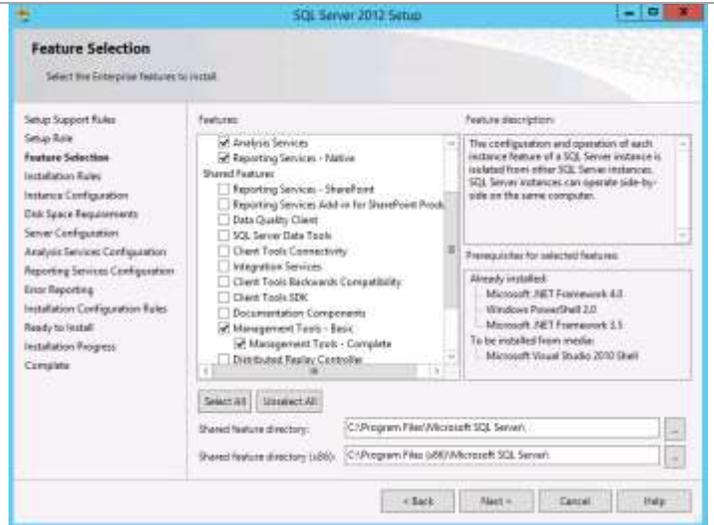
On the **Setup Role** page, select the **SQL Server Feature Installation** button, and click **Next** to continue.



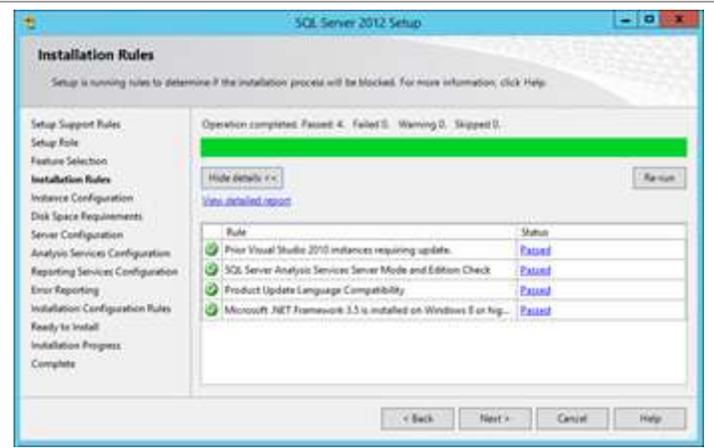
On the **Feature Selection** page, select the following check boxes:

- **Analysis Services**
- **Reporting Services - Native**
- **Management Tools – Basic**
- **Management Tools – Complete**

When all selections are made, click **Next** to continue.



On the **Installation Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.

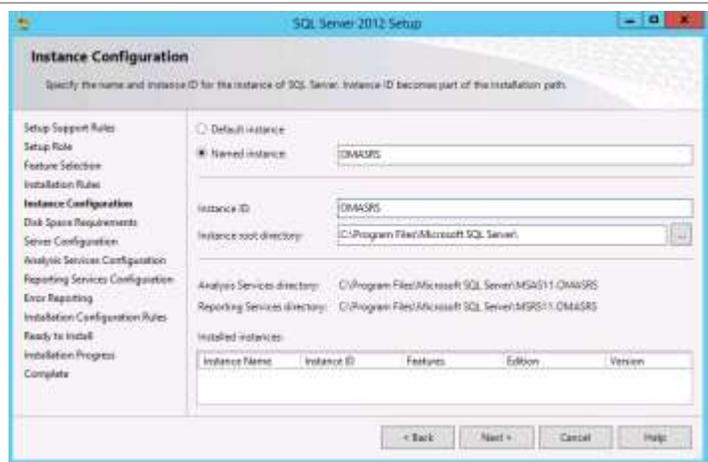


On the **Instance Configuration** page, select the **Named instance** option. In the provided text box, specify the name of the instance being installed.

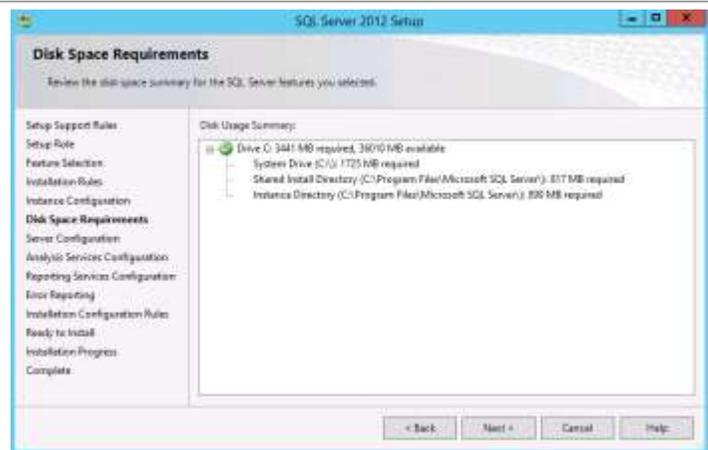
- **Instance ID** – Select the **Named instance** option and specify OMASRS in the provided text box. Verify that the Instance ID is listed as OMASRS in the associated text box. Keep the default Instance root directory value, and then click **Next** to continue.

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

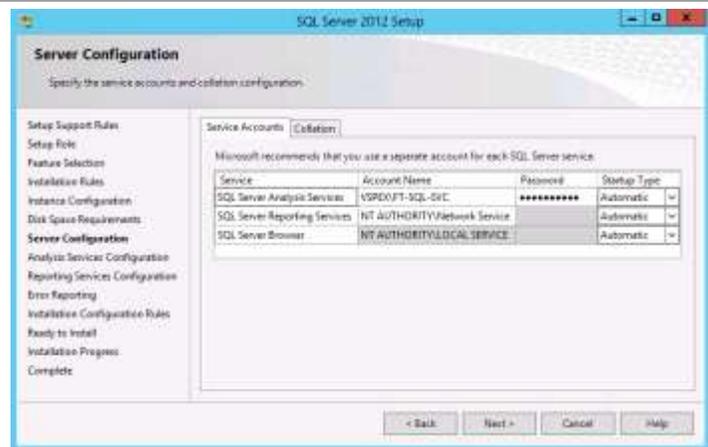
Note: A post-installation configuration process will occur to configure the reporting server database to leverage the Operations Manager data warehouse SQL Server instance database engine.



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



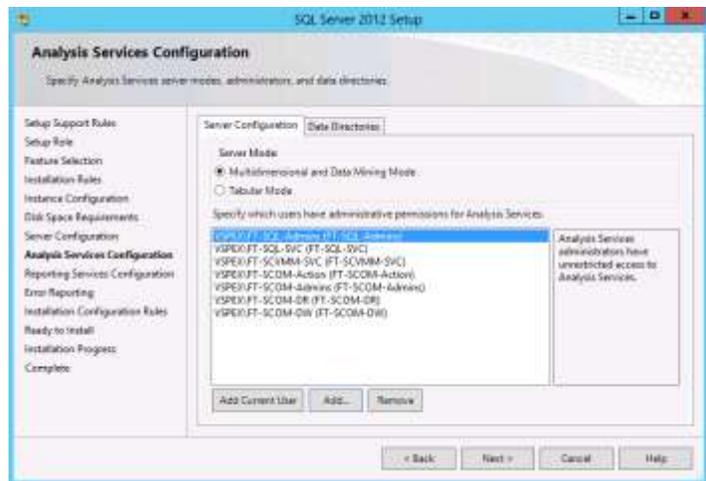
On the **Server Configuration** page, click the **Service Accounts** tab. For **SQL Server Reporting Services**, in the Account Name drop-down list, enter the **NT AUTHORITY\Network Service** account. For **SQL Server Analysis Service** account name and password values, provide the **domain SQL service account** used previously for the SQL Failover Cluster instances. For this example the account is VSPEX\FT-SQL-SVC. Click **Next**.



On the **Analysis Services Configuration** page, add the necessary accounts to the administrative users list. Click **Next**.

For the reference architecture deployment the accounts are:

- FT-SQL-Admins
- FT-SQL-SVC
- FT-SCVMM-SVC
- FT-SCOM-Action
- FT-SCOM-Admins
- FT-SCOM-DR
- FT-SCOM-DW



On the **Reporting Services Configuration** page, select the **Install only** option.

Note: Other options should not be available because the database engine was not selected as a feature for installation.

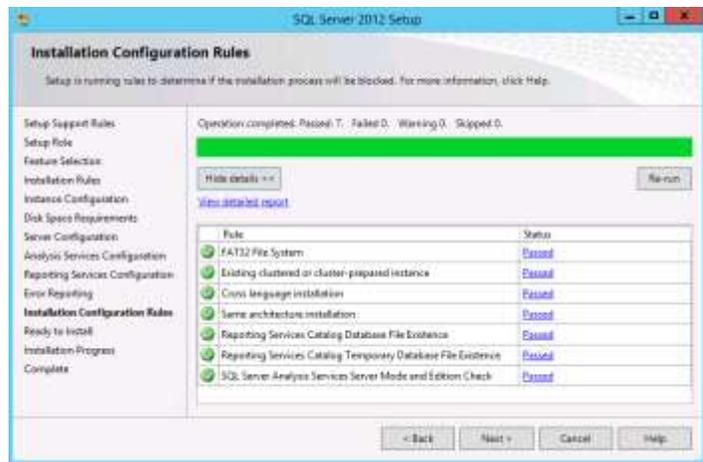
Click **Next** to continue.



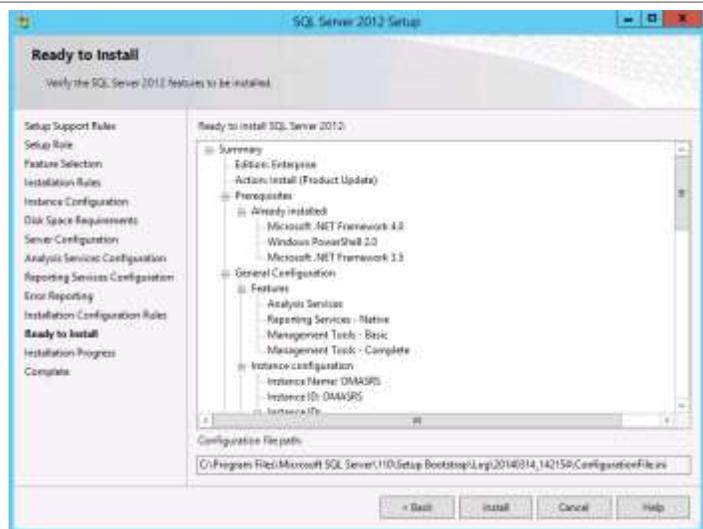
On the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies, and click **Next** to continue.



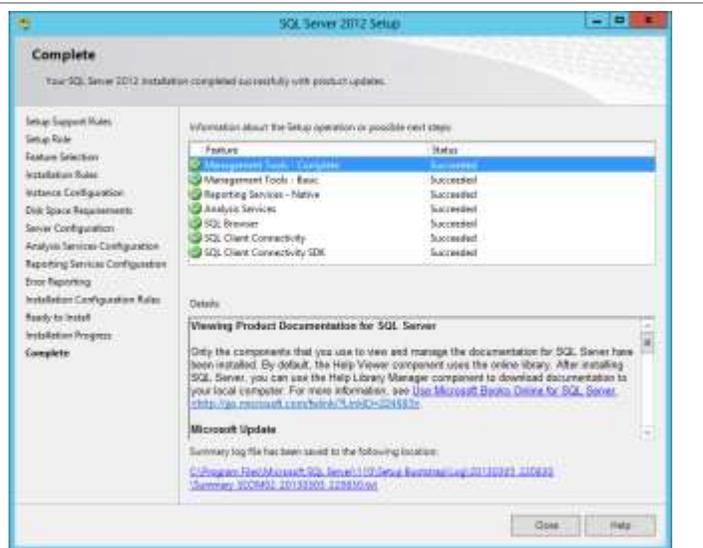
On the **Installation Configuration Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



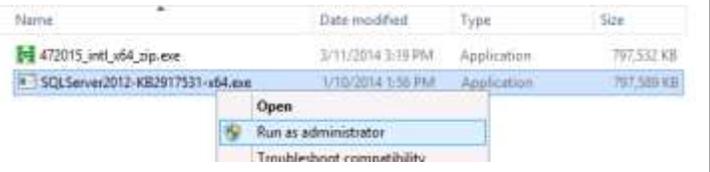
On the **Ready to Install** page, verify all of the settings that were entered during the setup process, and click **Install** to begin the installation of the SQL Server instance.



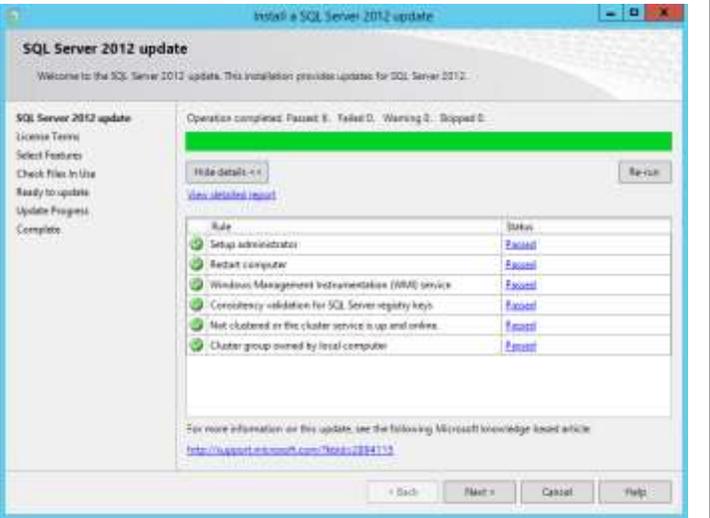
When complete, the **Complete** page will appear. Click **Close** to complete the installation of this SQL Server database instance.



Browse to the folder where the latest **Cumulative Update for SQL Server 2012 SP1**. Right-click the extracted executable and select **Run as administrator** from the menu.



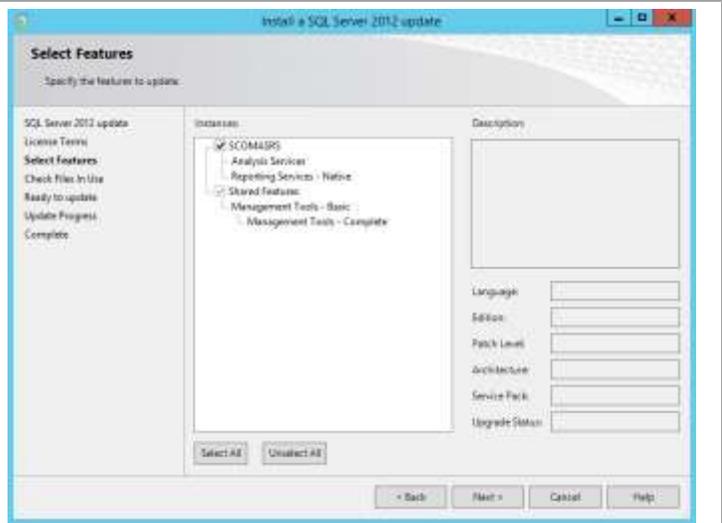
On the **SQL Server 2012 update** page, review the rules report and then click **Next**.



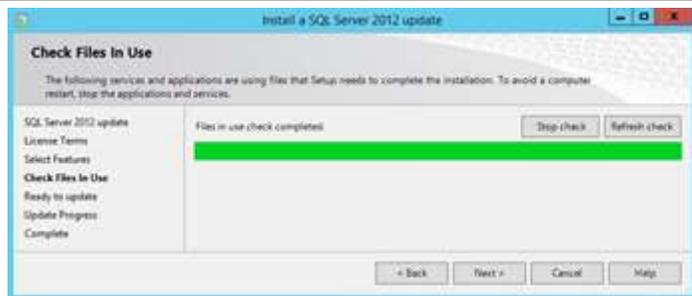
On the **License Terms** page, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box, based on your organization's policies, and click **Next** to continue.



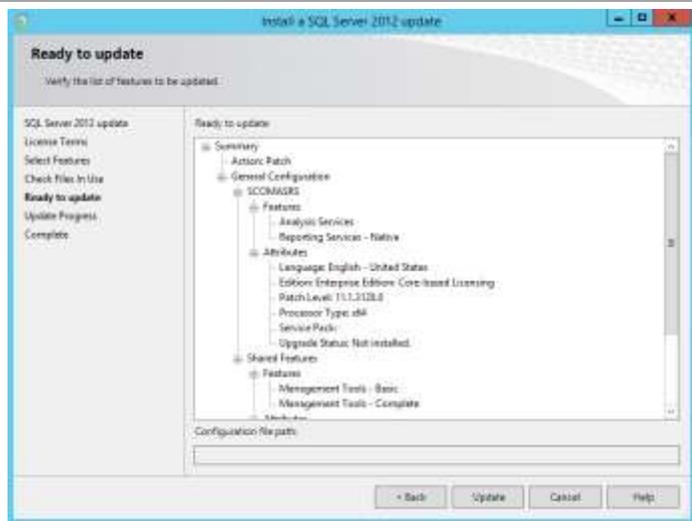
On the **Select Features** page, confirm that all features are selected and then click **Next**.



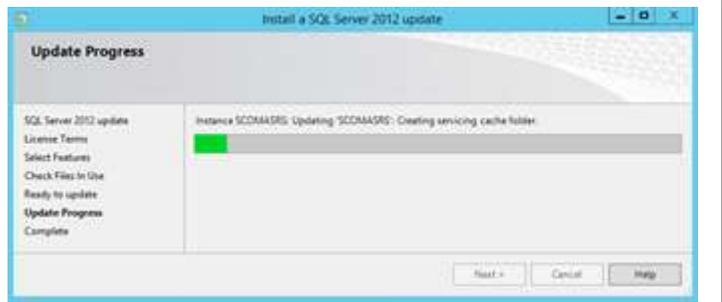
On the **Check Files In Use** page, click **Next**.



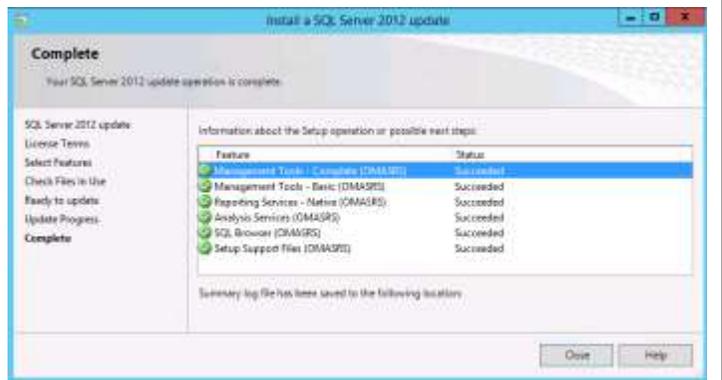
On the **Ready to update** page, click **Update**.



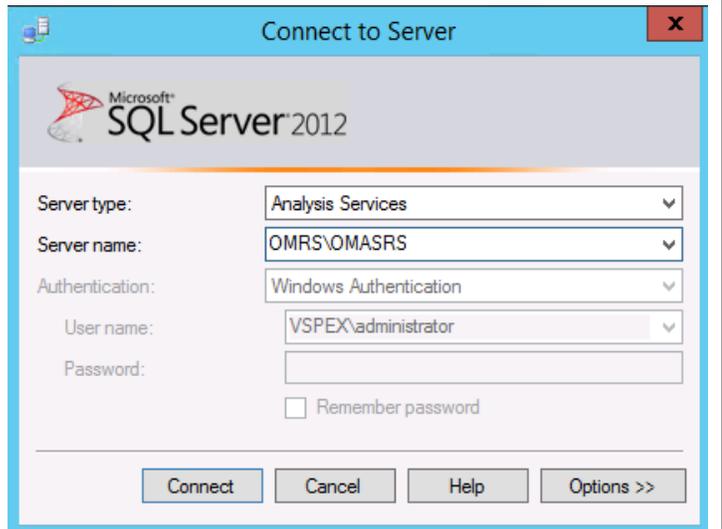
The **Update Progress** page will display until installation completes.



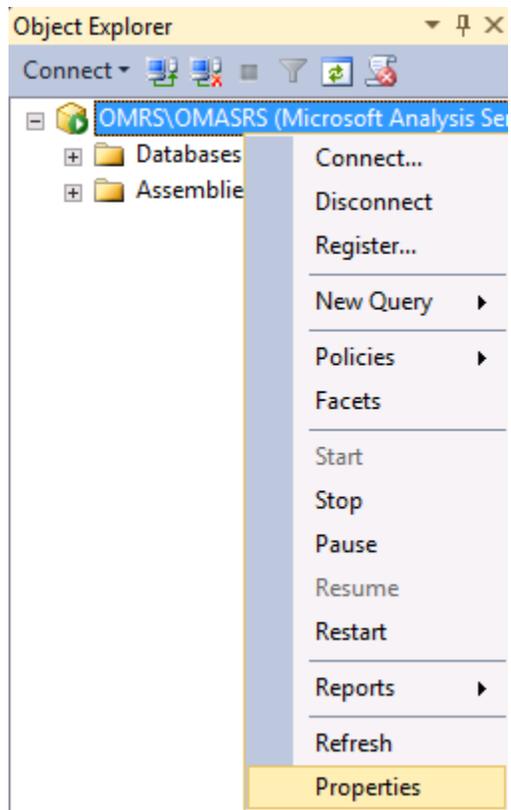
When the update is complete click **Close**.



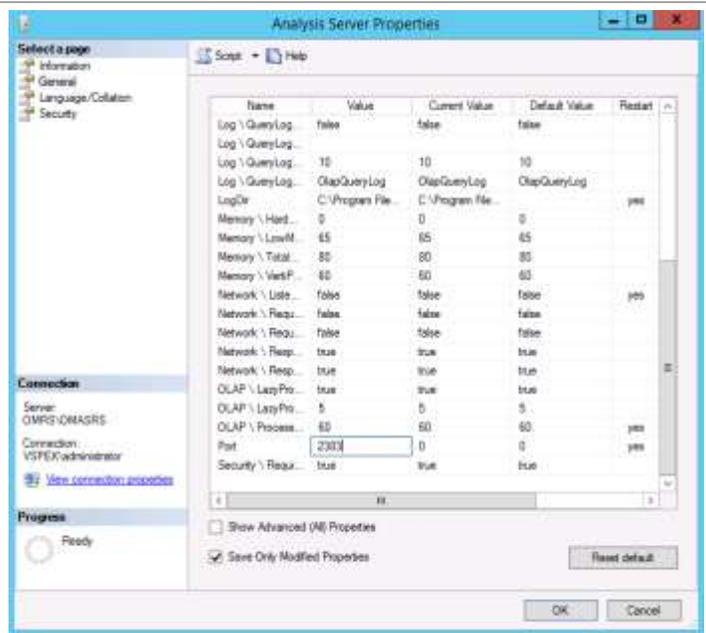
Open **SQL Server Management Studio** and connect to Analysis Services at *ServerName\InstanceName*.



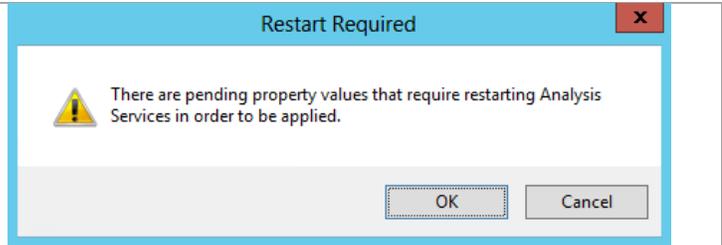
By default, named instances will use dynamic ports. For better compatibility with firewalls, the instance port should be set to static. To do so, right-click the SQL Server Analysis Services instance and click **Properties**.



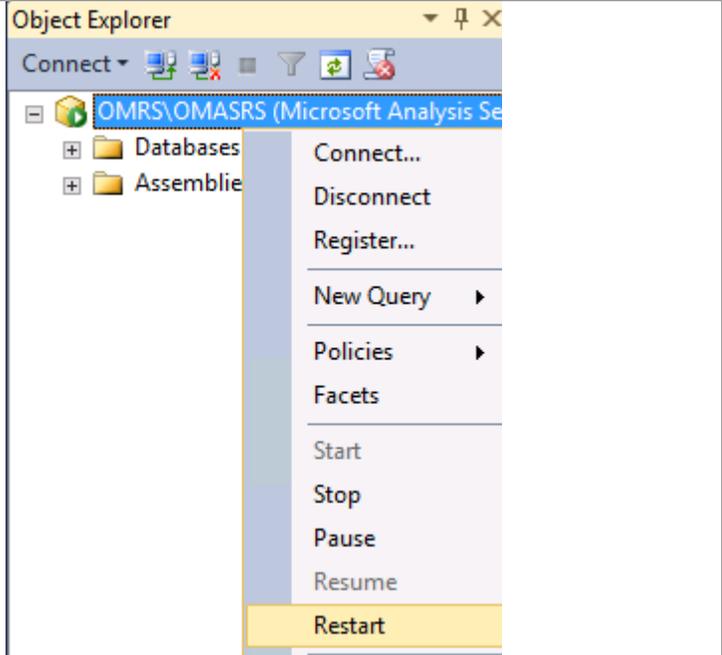
On the **Properties** page, click the **General** tab. Scroll down to the **Port** value in the **Name** column. Click the value and change the value of 0 (zero) to 2383 or a port value of your choice. Click **OK** to continue.



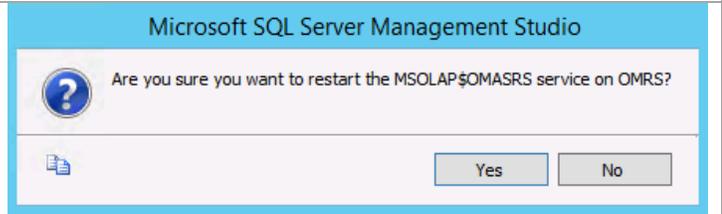
When prompted by the **Restart Required** message, click **OK**.



Within **SQL Server Management Studio**, in **Object Explorer**, right-click the SSAS instance, and click **Restart**.

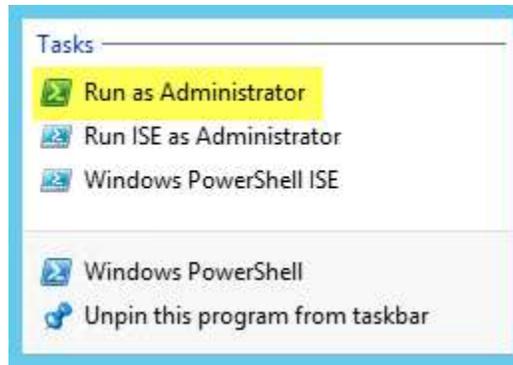


On the confirmation screen, click **Yes**. Close **SQL Server Management Studio**.



By default, the Windows Firewall will not allow traffic for SQL Server services or for the SSRS Web Service. You need to create firewall exceptions if the Windows Firewall is enabled.

To do so, open an administrative session of Windows PowerShell.



Run the following commands to create the needed firewall rules:

`New-NetFirewallRule -DisplayName "SQL Analysis Services Browser Service" -Protocol TCP -LocalPort 2382`

`New-NetFirewallRule -DisplayName "SQL Analysis Services OMASRS Instance" -Protocol TCP -LocalPort 2383`

`New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80`

Adjust the display names and ports based on organizational requirements.

```

Name : (f66026c1-8b3f-4e6d-b9d2-9d0186e6881f)
Displayname : MS Analysis Services Browser Service
Security :
LocalPolicy :
Created :
Group :
Enabled : True
Platform :
Platform :
Action : Allow
EdgeTraversePolicy : Block
LocalPortMapping :
LocalPortMapping :
LocalPortMapping :
Name :
Priority :
Status : The rule was parsed successfully from the store. (805382)
Inbound :
Inbound :
Inbound :
LocalPolicy :
LocalPolicy :
LocalPolicy :
Name : (c0723965-8788-429a-b07e-f426164f0463)
Displayname : MS Analysis Services OMASRS Instance
Security :
LocalPolicy :
Created :
Group :
Enabled : True
Platform :
Platform :
Action : Allow
EdgeTraversePolicy : Block
LocalPortMapping :
LocalPortMapping :
LocalPortMapping :
Name :
Priority :
Status : The rule was parsed successfully from the store. (805382)
Inbound :
Inbound :
Inbound :
LocalPolicy :
LocalPolicy :
LocalPolicy :
Name : (f66026c1-8b3f-4e6d-b9d2-9d0186e6881f)
Displayname : MS Reporting Service
Security :
LocalPolicy :
Created :
Group :
Enabled : True
Platform :
Platform :
Action : Allow
EdgeTraversePolicy : Block
LocalPortMapping :
LocalPortMapping :
LocalPortMapping :
Name :
Priority :
Status : The rule was parsed successfully from the store. (805382)
Inbound :
Inbound :
Inbound :
LocalPolicy :
LocalPolicy :
LocalPolicy :
  
```

Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.

Windows Firewall with Advanced Security - Inbound Rules			
Name	Local Port	Profile	
SQL Analysis Services Browser Service	2382	All	✓
SQL Analysis Services OMASRS Instance	2383	All	✓
SQL Reporting Services	80	All	✓

To verify that SQL Server Reporting Services installed properly, on the **Start** menu, click the **Reporting Services Configuration Manager** tile.



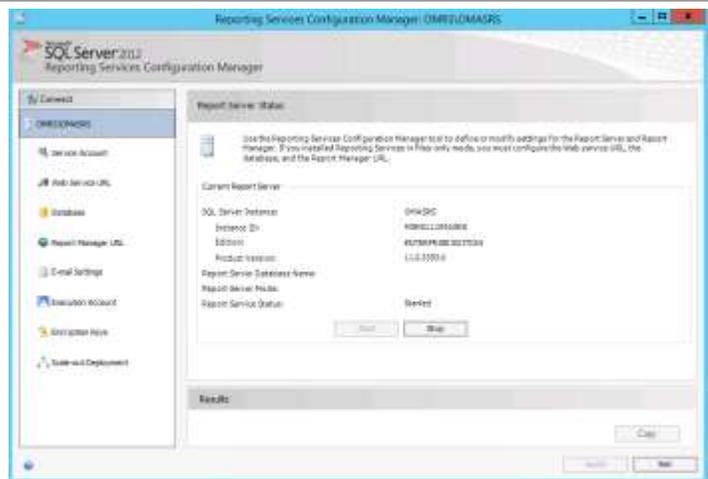
The **Reporting Services Configuration Connection** page will appear.

- In the **Server Name** text box, specify the name of the Operations Manager server.
- In the **Report Server Instance** text box, select the default value **SCOMASRS** from the drop-down list.

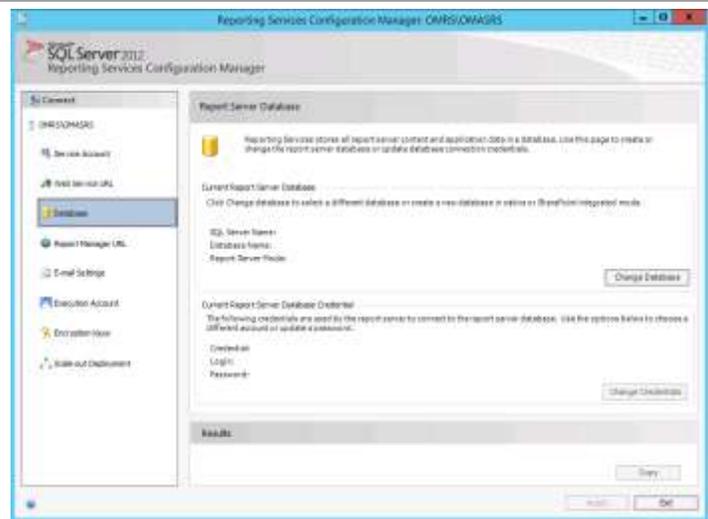
Click **Connect**.



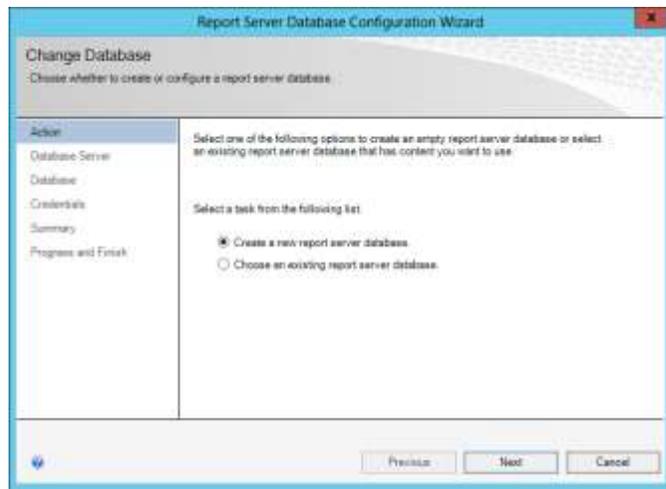
The **Reporting Services Configuration Manager** will appear.



Click **Database** in the left pane, and then in the **Current Report Server Database** section, click the **Change Database** button.



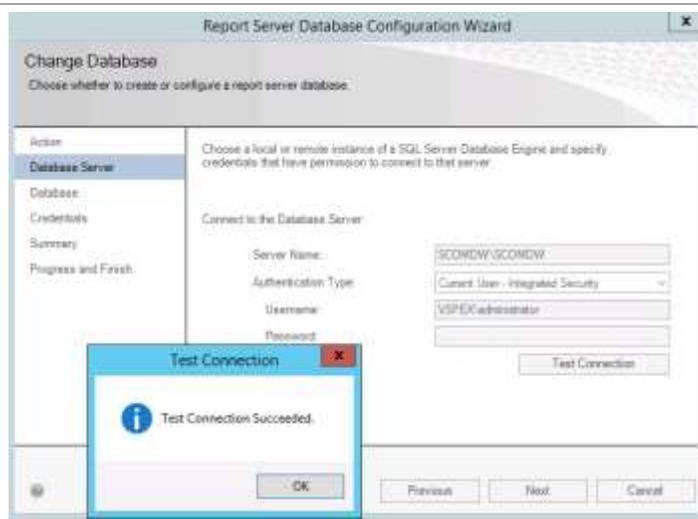
The Reporting Services Database Configuration Wizard will appear. In the **Action** section, select **Create a new report server database**. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – Specify the name of the remote **SQL Server failover cluster name and the database instance name created for the Operations Manager installation**. For the reference architecture deployment the name is **SCOMDW\SCOMDW**
- **Authentication Type** – Specify **Current User – Integrated Security** from the drop-down list.

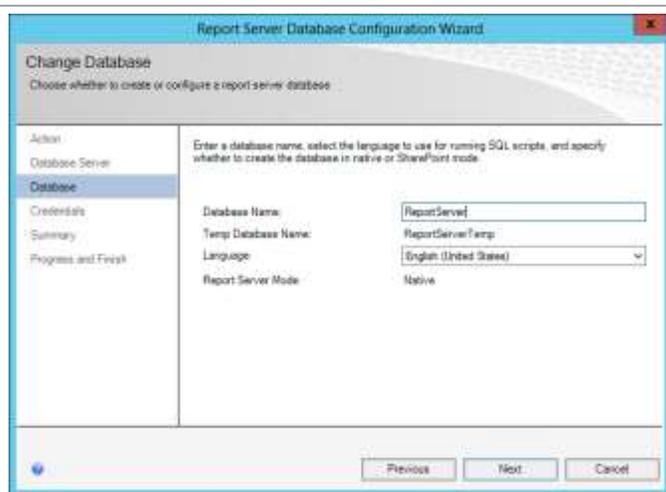
Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



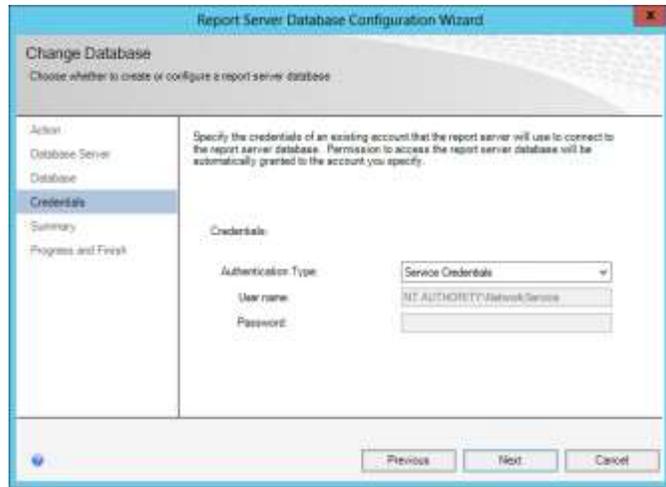
In the **Database** section, specify the following values:

- **Database Name** – Accept the default value of **ReportServer**.
- **Language** – Specify the desired language option from the drop-down list.

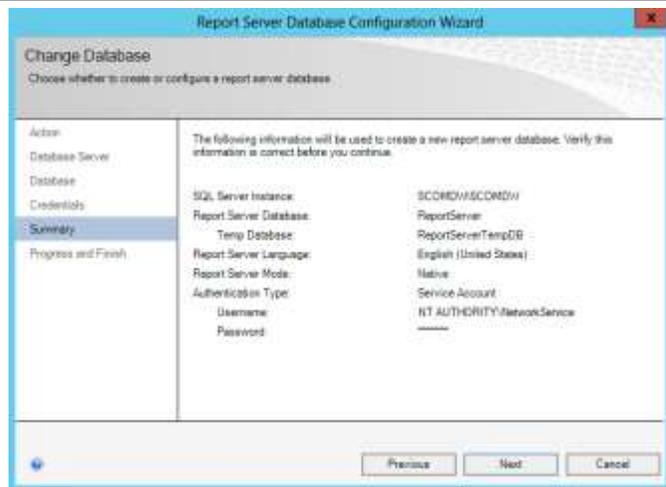
Click **Next** to continue.



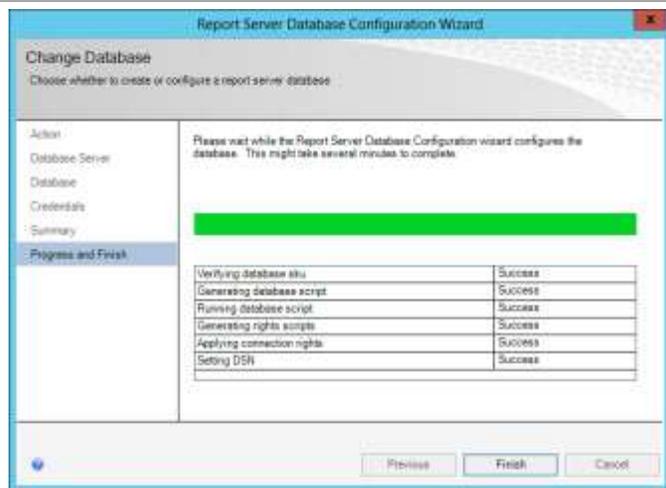
In the **Credentials** section, for **Authentication Type**, select **Service Credentials** from the drop-down list. The User name value should show **NT Authority\Network Service**. Click **Next** to continue.



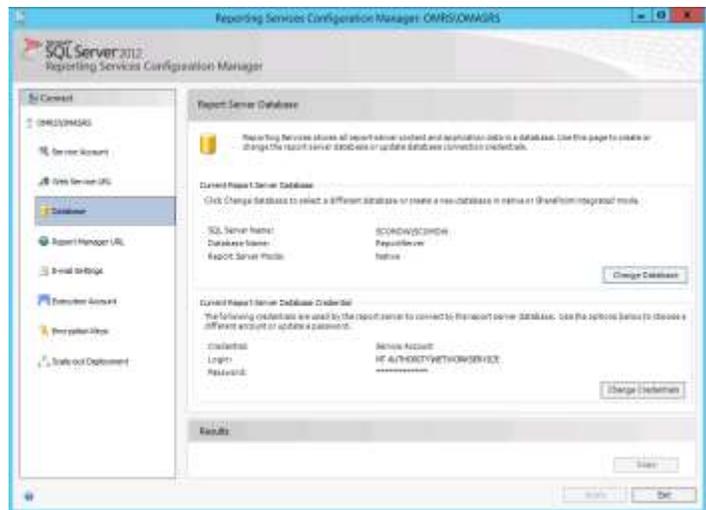
In the **Summary** section, review the selections that you made, and click **Next** to create the SQL Server Reporting Services database on the remote SQL Server cluster instance supporting the Operations Manager Data Warehouse.



The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation and click **Finish**.

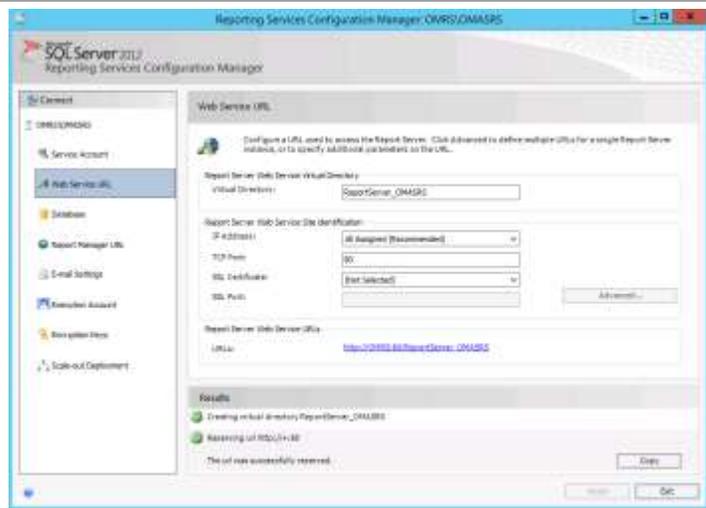


In **Reporting Services Configuration Manager**, the **Database** option will now display the database and report server database credentials that you specified in the wizard.



In **Reporting Services Configuration Manager**, click **Web Service URL** in the left pane. Specify the following values:

- In the **Report Server Web Service Virtual Directory** section, set the **Virtual Directory** value to **ReportServer_OMASRS** in the provided text box. **This default value must be used for VMM and SCOM integration to function properly.**
- In the **Report Server Web Service Site Identification** section, set the following values:
 - **IP Address** – Select **All Assigned** from the drop-down list.
 - **TCP Port** – Specify the desired TCP Port (the default is 80).
 - **SSL Certificate** – Select the available certificate or choose the default of (Not Selected).

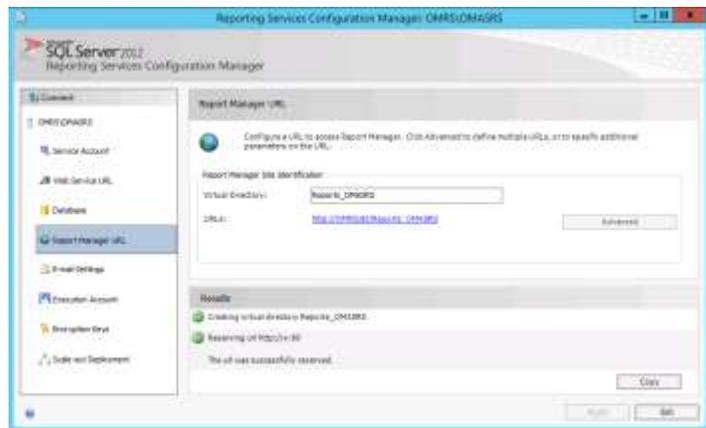


Click the **Apply** button to save the settings and create the Web Service URL.

In **Reporting Services Configuration Manager**, click **Report Manager URL** in the left pane. Specify the following value:

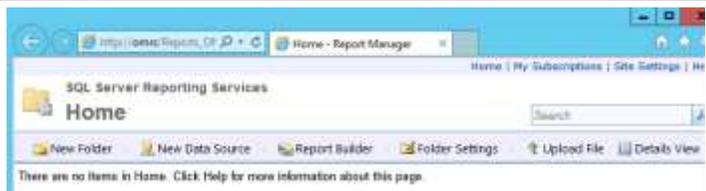
- In the **Report Manager Site Identification** section, set the **Virtual Directory** value to **Reports_OMASRS** in the provided text box. **This default value must be used for VMM and SCOM integration to function properly.**

Click the **Apply** button to save the settings and create the Report Manager URL.



Note: To test the URL directory from the Operations Manager server, Internet Explorer Enhanced Security Configuration (ESC) needs to be temporarily disabled.

Connect to the Report Manager URL within a web browser to verify the SQL Server Reporting Services portal is operating properly.



Connect to the Web Service URL within a web browser to verify the SQL Server Reporting Services web service is operating properly.



Close the Reporting Server Configuration Manager.

Install Microsoft Report Viewer 2012

The Operations Manager installation requires that Microsoft Report Viewer 2012 is installed prior to installing Operations Manager. Use the following procedure to install Microsoft Report Viewer 2012.

- ▶ Perform the following steps on the **Operations Manager management server** virtual machine.

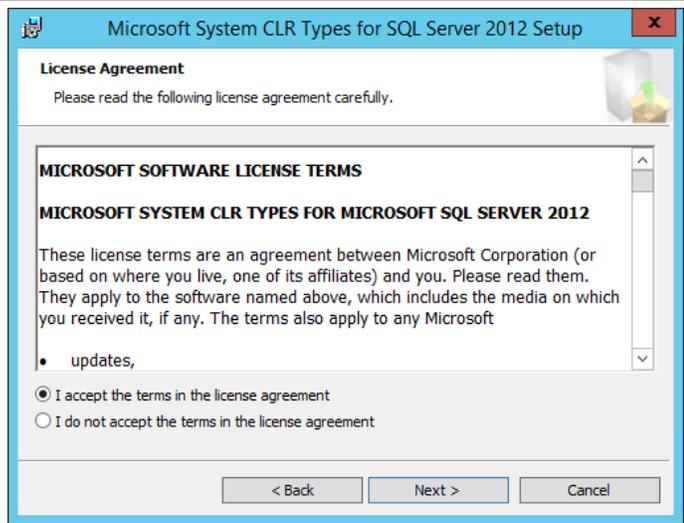
From the installation media source, double-click **SQLSysClrTypes.msi** to begin setup.

Name	Type	Size
SQLSysClrTypes	Windows Installer Package	2,460 KB

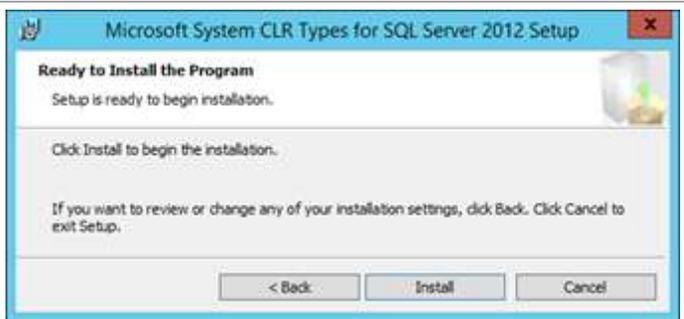
On the **Welcome to the Installation...** page click **Next**.



On the **License Agreement** page, select the **I accept the license terms** check box and click **Next** to continue.



On the **Ready to Install the Program** page click **Install**.



On the **Completing the Microsoft System...Installation** page click **Finish**.

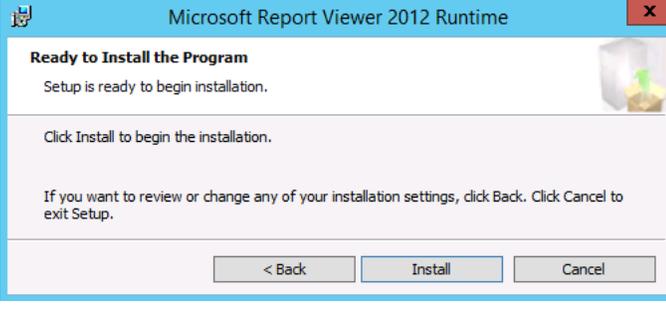


From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** to begin setup.

Name	Type	Size
 ReportViewer	Windows Installer Package	7,444 KB

On the Microsoft Report Viewer 2012 Runtime setup wizard **Welcome to the Installation...** page click **Next**.



<p>On the License Agreement page, select the I accept the license terms check box and click Next to continue.</p>	
<p>On the Ready to Install the Program page click Install.</p>	
<p>On the Completing the Microsoft Report Viewer 2012 Runtime Installation page click Finish.</p>	

Configure Operations Manager SQL Server Prerequisites

The following prerequisite steps must be completed prior to the installation of Operations Manager roles.

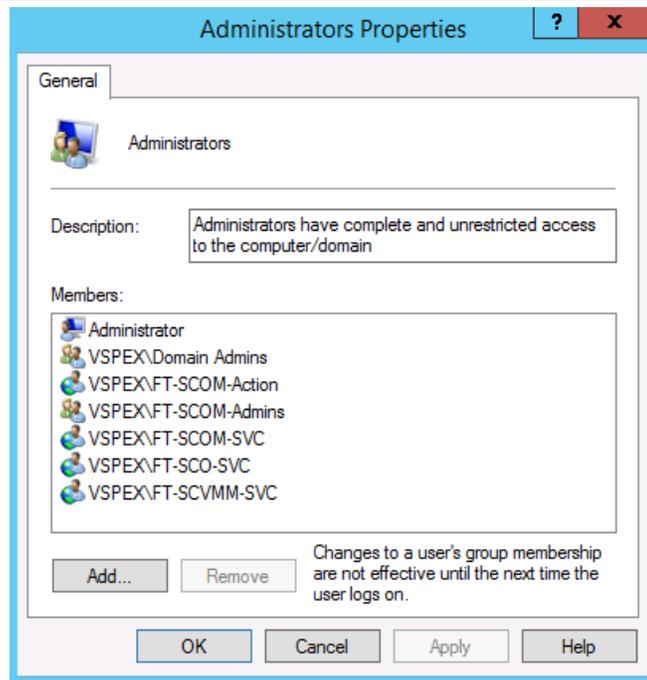
Note: Specific requirements for Operations Manager are outlined in the Before You Begin section of [Deploying System Center 2012 R2 - Operations Manager](#) in the TechNet Library.

- ▶ Perform the following steps on the Operations Manager management server virtual machines.

Log on to the Operations Manager virtual machine as a user with local Admin rights.

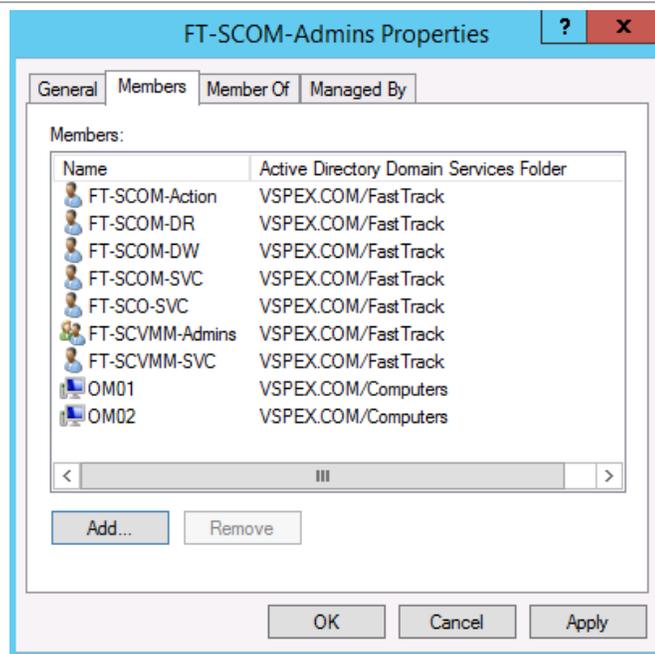
Verify that the following accounts or groups are members of the local Administrators group on the Operations Manager virtual machine:

- Orchestrator service account
- Operations Manager action account
- Operations Manager Admins group
- Operations configuration service and data access service account
- VMM service account



- ▶ Perform the following step on an Active Directory domain controller in the target environment.

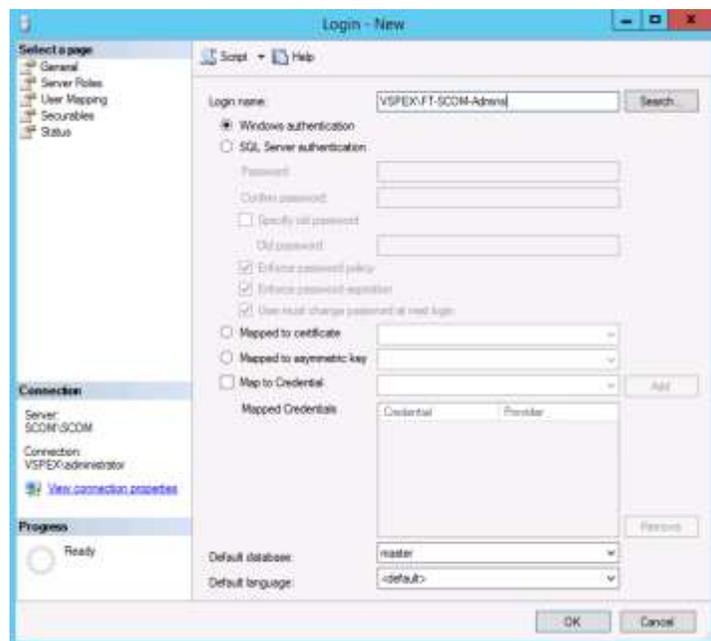
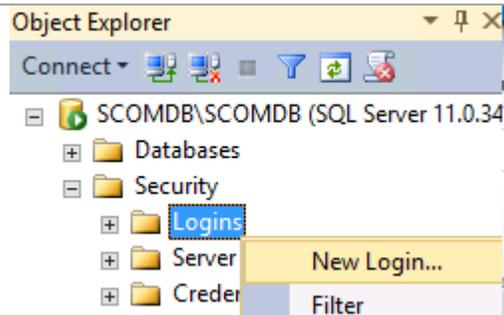
In the domain where Operations Manager will be installed, verify that the Operations Manager computer account and the groups outlined in the previous table are members of the SCOM Admins group that you created earlier.



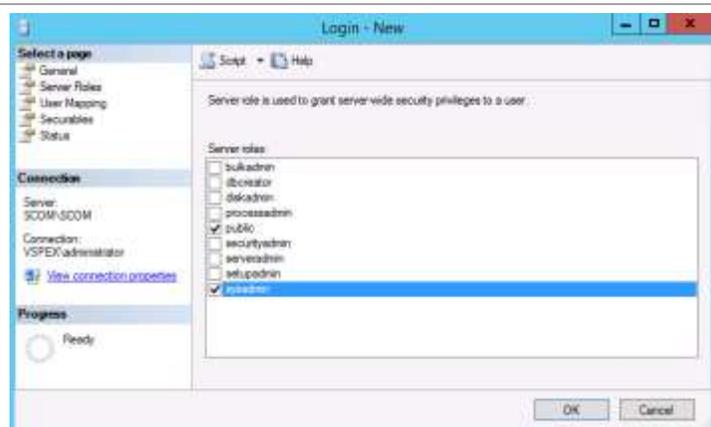
► Perform the following steps on the primary SQL Server cluster node.

Using Administrative credentials, log on to the first SQL Server and open SQL Server 2012 Management Studio. Connect to the Operations Manager SQL Server instance by using the values specified earlier. Expand **Security**, right-click **Logins**, and click **New Login...**

In the **Login – New** dialog box, select the Operations Manager Admins group created earlier as the new **Login name**.



While still in the **Login – New** dialog box, click the **Server Roles** page. Select the **sysadmin** role, and click **OK** to create and add this login to the sysadmin role of the instance.



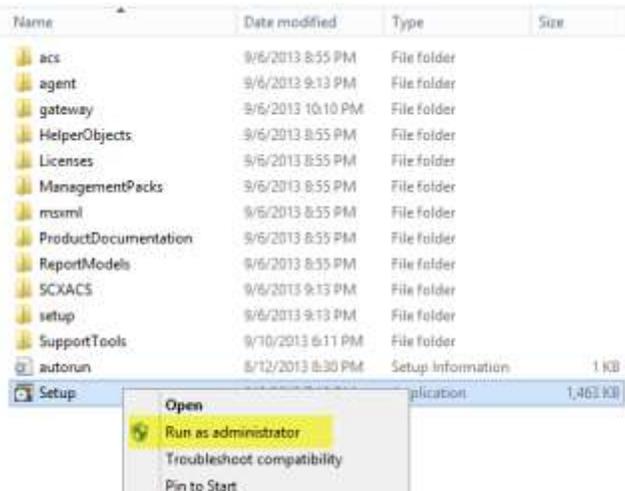
Installation

Install the Operations Manager Management Server

The following steps must be completed to install and configure the Operations Manager database and server roles.

- ▶ Perform the following steps on the **first** Operations Manager management server virtual machine.
- ▶ Note that this installation assumes connectivity to the Internet for certain automatic downloads.

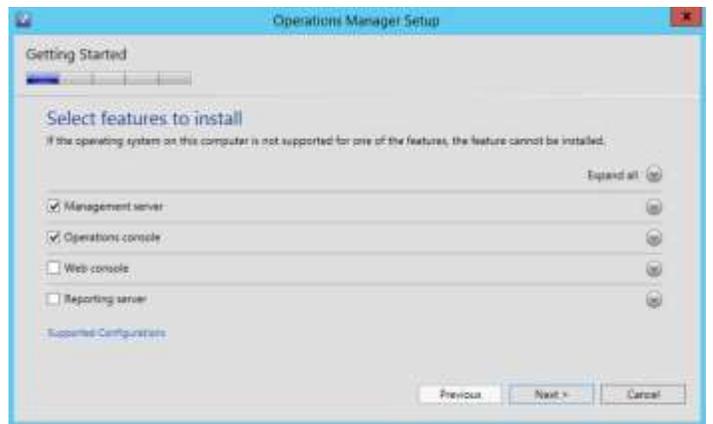
From the Operations Manager installation media source, right-click **setup.exe**, and select **Run as administrator** to begin setup.



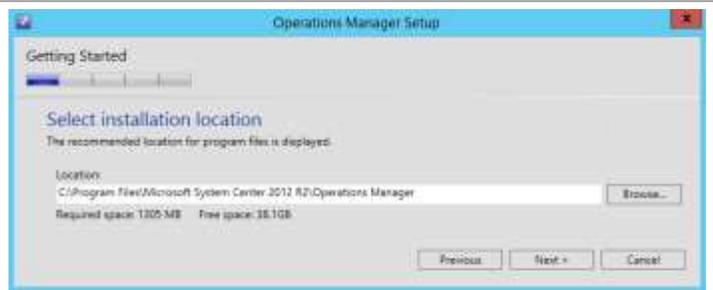
The Operations Manager Setup Wizard will appear. Select the **Download the latest updates...** option and then Click **Install** to begin the Operations Manager management server installation.



On the **Select features to install** page, verify that the **Management server** and **Operations console** check boxes are selected. Click **Next** to continue.



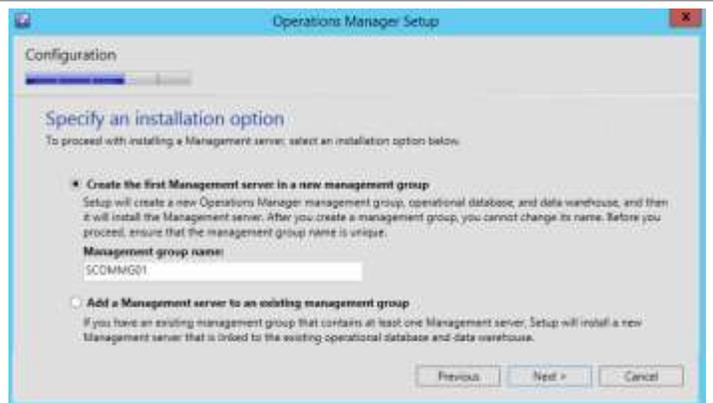
On the **Select installation location** page, specify a location or accept the default location of `%ProgramFiles%\System Center 2012\Operations Manager` for the installation. Click **Next** to continue.



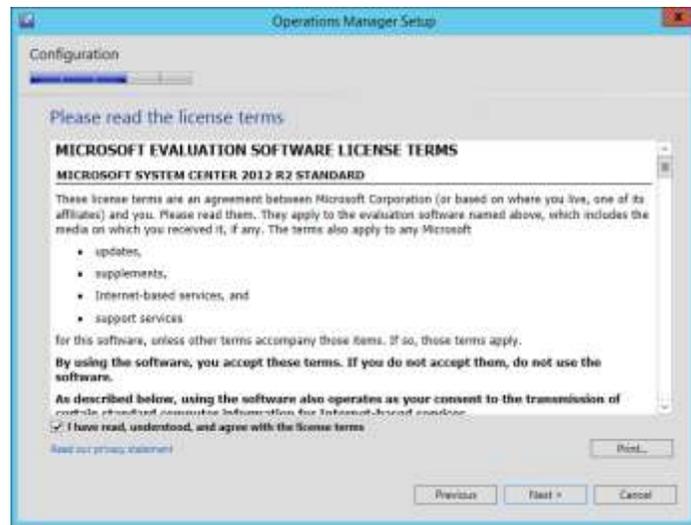
The wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the **Proceed with Setup** page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Specify an installation option** page, select the **Create the first Management server in a new management group** option, and type 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.

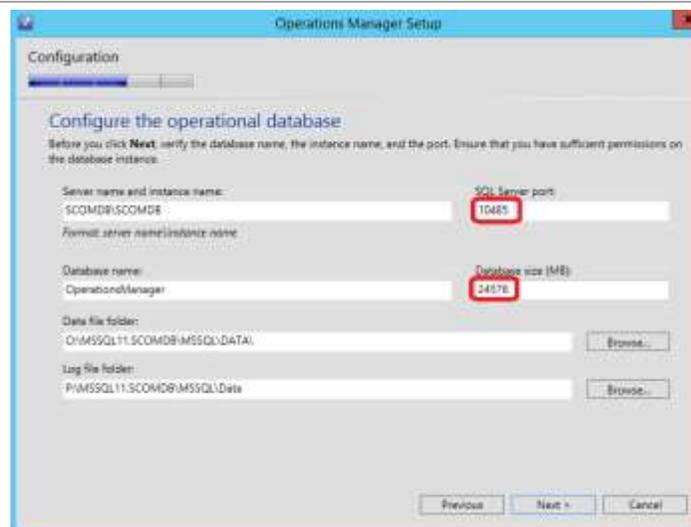


On the **Please read the license terms** page, verify that the **I have read, understood and agree with the terms of the license agreement** installation option check box is selected, and click **Next** to continue.



On the **Configure the operational database** page, specify the following information in the provided text boxes:

- **Server name and instance name** – Specify the name of the SQL Server cluster network name (cluster name object) and the database instance created for the Operations Manager installation.
- **SQL Server port** – Specify the TCP port used for SQL Server connectivity. Port 1433 is the default; however, this may be different based on instance requirements outlined earlier. As long as the browser service is enabled the correct port will be detected even if 1433 is selected as the port value for setup. Alternatively you may simply provide the correct port assignment. For the reference deployment the static port is 10485.
- **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.² The following values can be used as a general guideline:
 - Up to 500 agents: 12 GB



² For general guidance for database sizing, see [System Center 2012 - Operations Manager Component Add – On](#).

○ Up to 1000 agents: 24 GB

- **Data file folder** – Specify the drive letter associated in the SQL Server cluster data files for the Operations Manager database. This should be detected by the setup process, however it 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 detected by the setup process, however it should be cross-checked with the worksheet identified earlier.

Click **Next** to continue.

On the **Configure the Data warehouse database** page, specify the following information in the provided text boxes:

- **Server name and instance name** – Specify the name of the SQL Server cluster network name (cluster name object) and the database instance created for the Operations Manager installation.
- **SQL Server port** – Specify the TCP port used for SQL Server connectivity. Port 1433 is the default; however, this may be different based on instance requirements outlined earlier. As long as the browser service is enabled the correct port will be detected even if 1433 is selected as the port value for setup. Alternatively you may simply provide the correct port assignment. For the reference deployment the static port is 10486.
- **Database name** – Specify the name of the Operations Manager data warehouse database. In most cases the default value of OperationsManagerDW should be used.
- **Database size (MB)** – Specify the initial database size. The following values can be used as a general guideline:

Operations Manager Setup

Configuration

Configure the data warehouse database

Before you click **Next**, verify the database name, the instance name, and the port. Ensure that you have sufficient permissions on the database instance.

Server name and instance name: SCOMDW\SCOMDW SQL Server port: 10486

Format: server name\instance name

Create a new data warehouse database
 Use an existing data warehouse from a different management group

Database name: OperationsManagerDW Database size (MB): 50000

Data file folder: Q:\MSSQL11.SCOWM\MSSQL\DATA\ Browse...

Log file folder: R:\MSSQL11.SCOWM\MSSQL\Data Browse...

Previous Next > Cancel

- 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 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 log files for the Operations Manager data warehouse database. This should be cross-checked with the worksheet identified earlier.

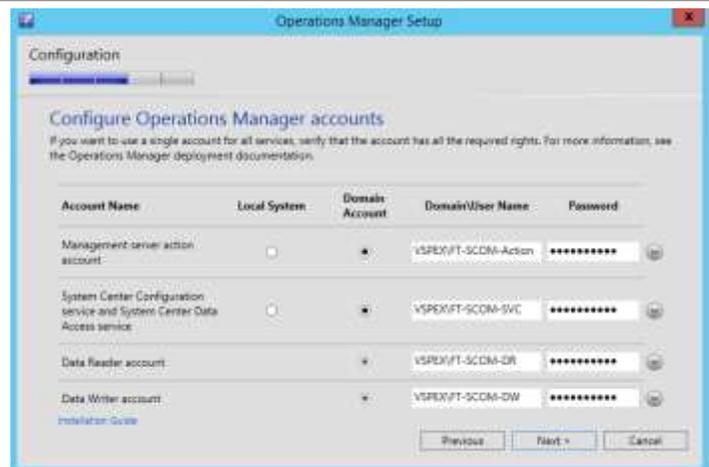
Click **Next** to continue.

On the **Configure Operations Manager accounts** page, for each of the following accounts, specify the appropriate **Domain Account** name and password:

- Management server action account (reference deployment: **FT-SCOM-Action**)
- System Center Configuration service and System Center Data Access service (reference deployment: **FT-SCOM-SVC**)
- Data reader account (reference deployment: **FT-SCOM-DR**)
- Data writer account (reference deployment: **FT-SCOM-DW**)

Domain Accounts are specified as **<DOMAIN>\<USERNAME>**.

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

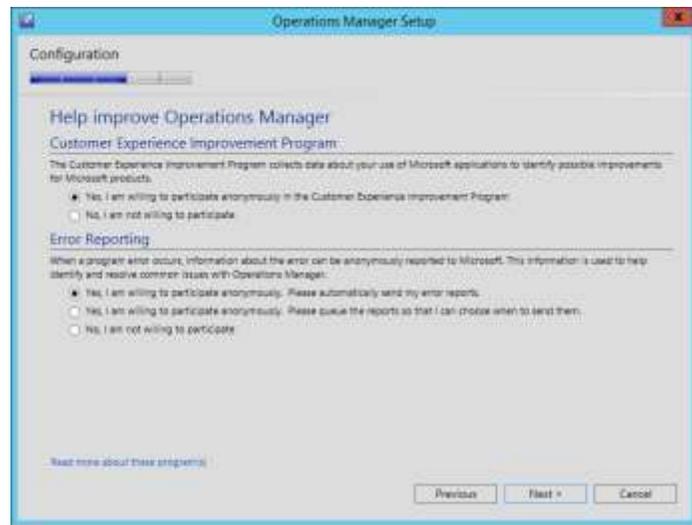


The **Help Improve System Center 2012 - Operations Manager** page provides options for participating in various product feedback mechanisms. These include:

Customer Experience Improvement Program

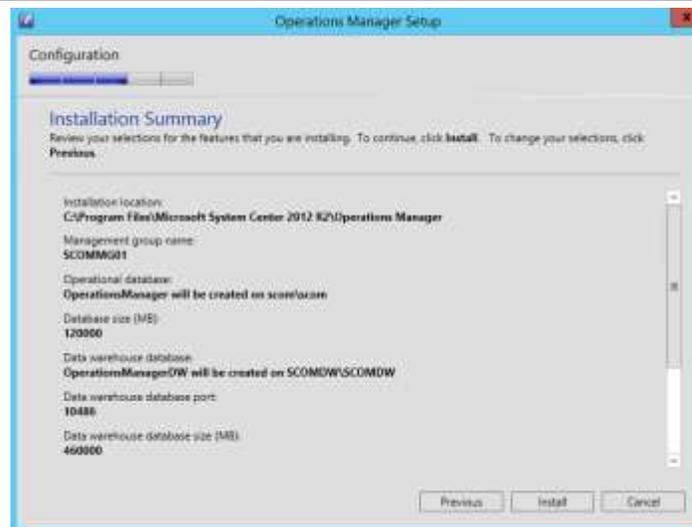
Error Reporting

Select the appropriate option based on your organization's policies, and click **Next** to continue.

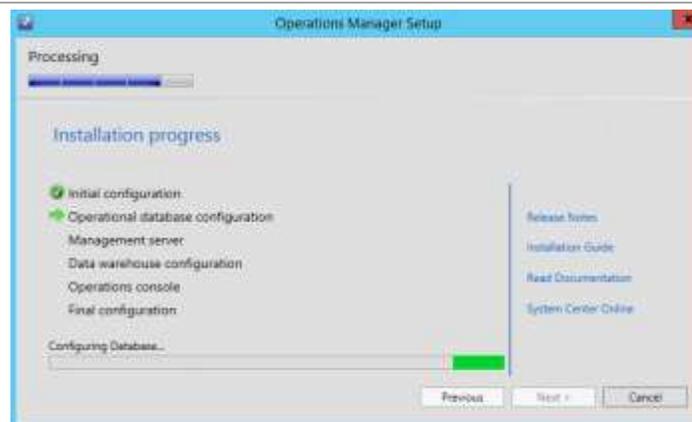


The **Installation Summary** page will appear and display the selections you made during the Setup Wizard. Review the options selected, and click **Install** to continue.

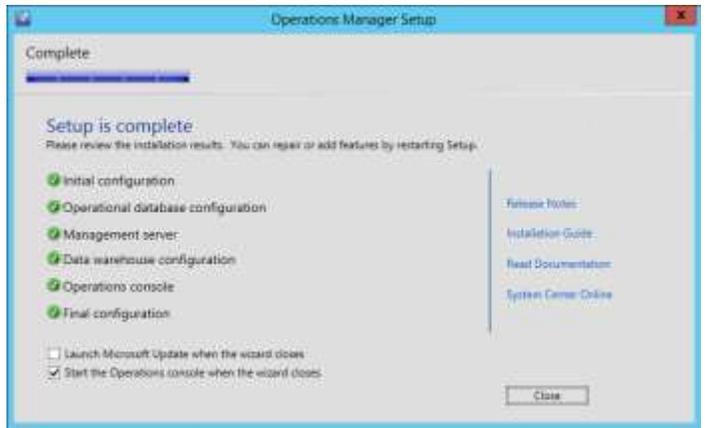
Note: Make sure that you set the database sizes appropriately for your particular deployment. Both databases will be fully allocated at deployment time as operations manager databases are not set to auto grow by default.



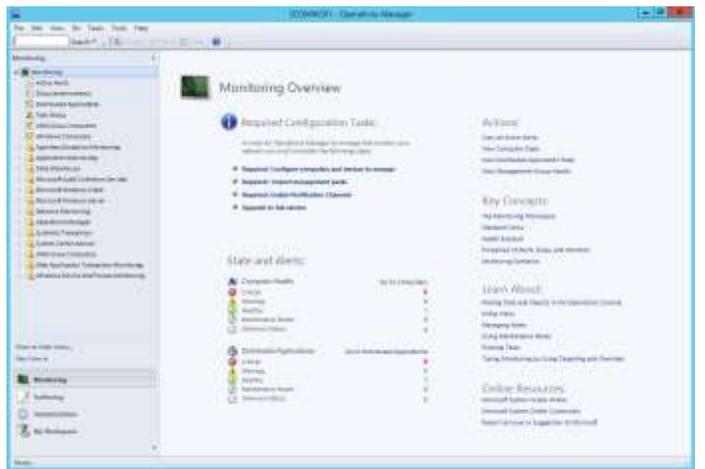
The wizard will display the progress while installing features. The time it takes for installation is dependent upon the size databases you requested.



When the installation completes, the wizard will display the **Setup is complete** page. Verify that the **Start the Operations console when the wizard closes** check box is selected, and click **Close** to complete the installation.



The **Operations Manager** console will open. Validate the installation by reviewing the configuration and Make sure that the console operates properly.



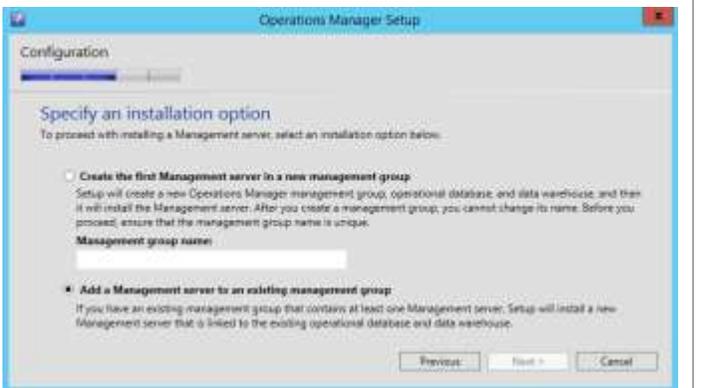
Install the Second Operations Manager Management Server

Installation of the second Operations Manager management server is almost identical to installing the first server. The following steps show which setup entries are different during installation.

► Perform the following altered steps on the **second Operations Manager management server** virtual machine.

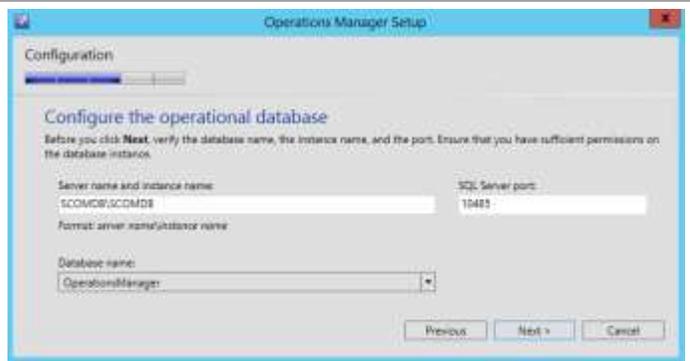
On the **Configuration/Specify and installation option** screen of setup, select the **Add a Management server to an existing management group** radio button.

Click **Next** to continue.



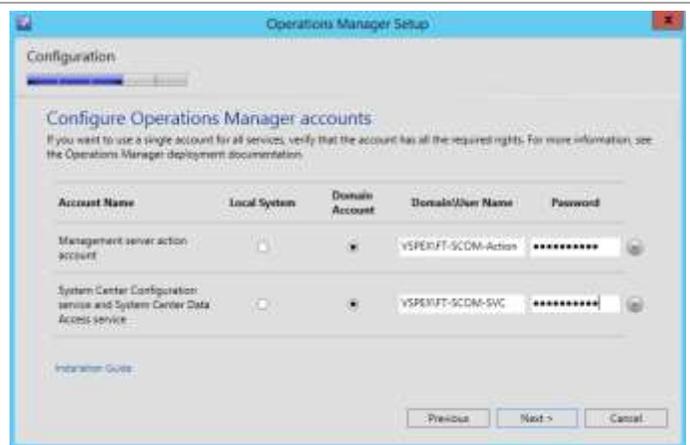
On the **Configuration/Configure the operational database** screen of setup, specify the CNO and database instance name of the Operations Manager database. Specify the port number that you assigned to this instance. From the dropdown list of the Database name field, select the OperationsManager database.

Click **Next** to continue.



On the **Configuration/Configure Operations Manager accounts** screen of setup, specify the Management server action account and Configuration service and data access accounts with the appropriate passwords.

Click **Next** to continue.

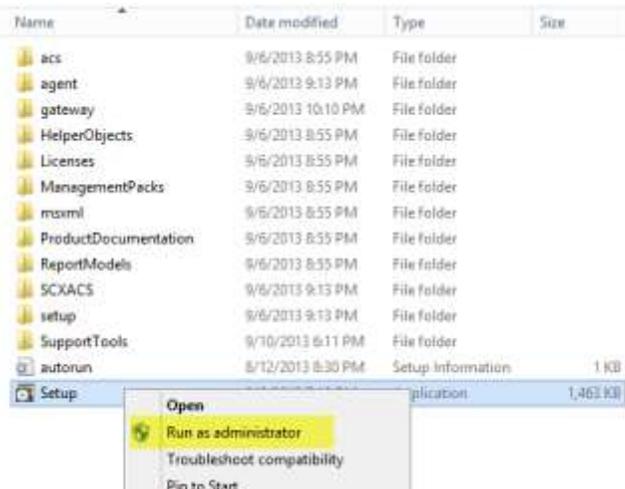


Install the Operations Manager Reporting Server

The following steps must be completed to install and configure the Operations Manager reporting server role.

▶ Perform the following steps on the Operations Manager reporting server virtual machine.

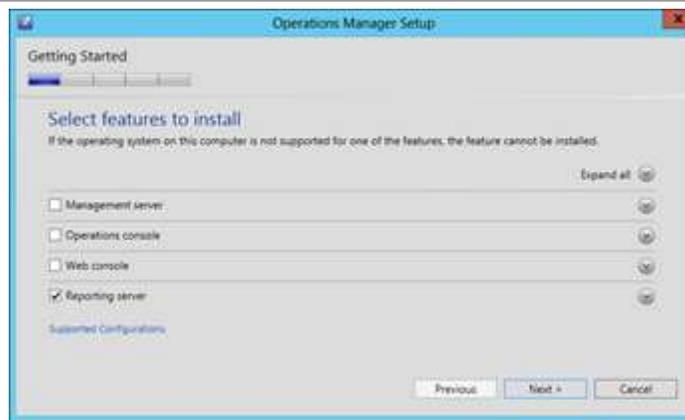
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



The Operations Manager installation wizard will begin. Click **Install** to begin the Operations Manager management server installation.



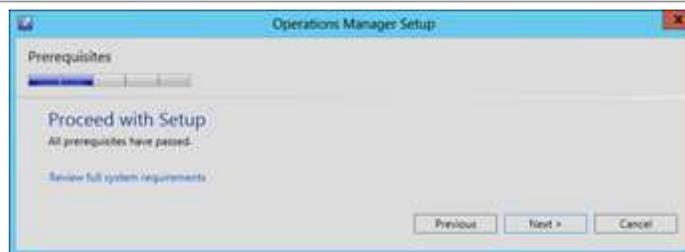
On the **Select features to install** page, verify that the **Reporting server** check box is selected. Click **Next** to continue.



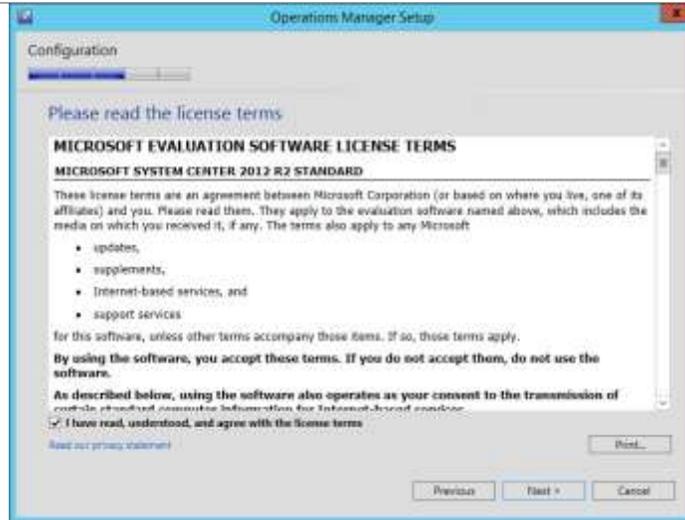
On the **Select installation location** page, specify a location or accept the default location of %ProgramFiles%\System Center 2012\Operations Manager for the installation. Click **Next** to continue.



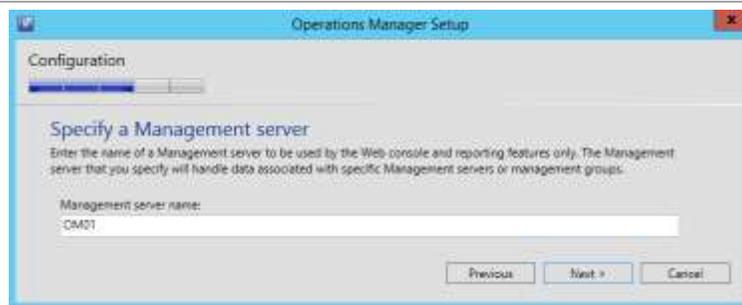
The wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the **Proceed with Setup** page. After you verify that the prerequisites are met, click **Next** to continue.



On the **Please read the license terms** page, select the **I have read, understood and agree with the license terms** check box, and click **Next** to continue.



On the **Specify a Management server** page, type the name of the previously installed management server in the **Management server name** text box. Click **Next** to continue.



On the **SQL Server instance for reporting services** page, select the SQL Server instance that hosts the local SQL Server Reporting Services and SQL Server Analysis Services from the drop-down list created earlier. Click **Next** to continue.

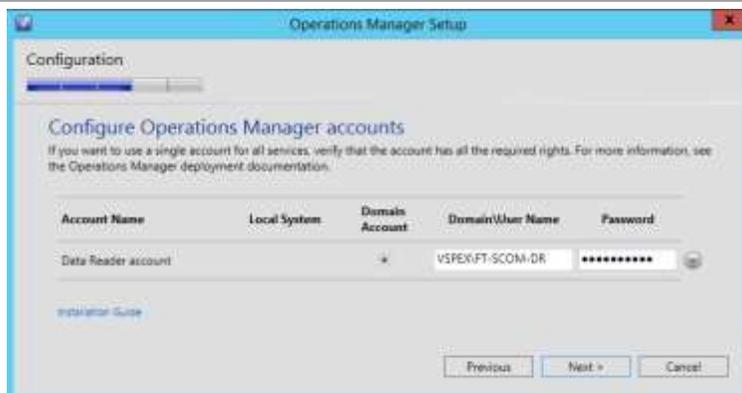


On the **Configure Operations Manager accounts** page, specify whether the following account is a **Local System** or **Domain Account** by using the available options:

- **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.

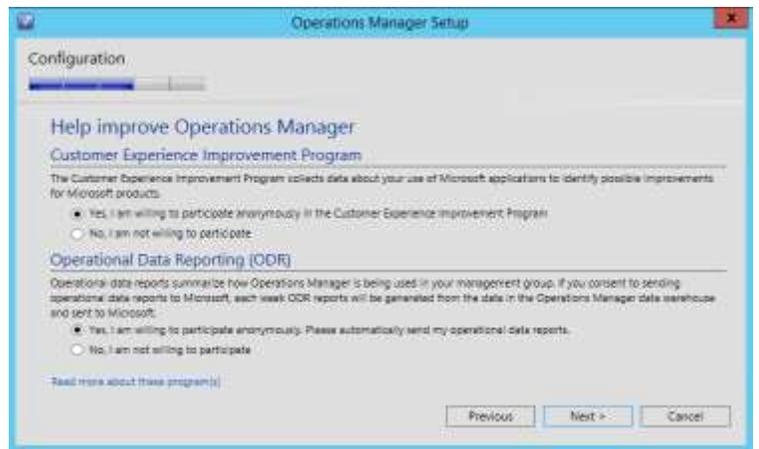
Click **Next** to continue.



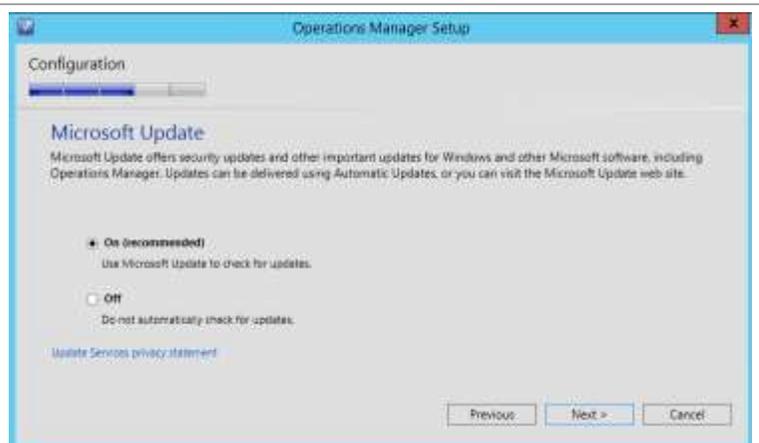
The **Help Improve Operations Manager 2012** page provides options for participating in various product feedback mechanisms. This includes:

- **Operational Data Reporting (ODR)**

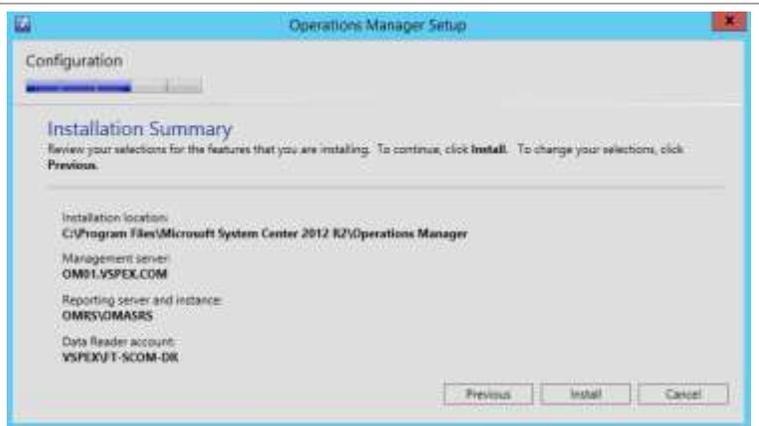
Select the appropriate option based on your organization's policies, and click **Next** to continue.



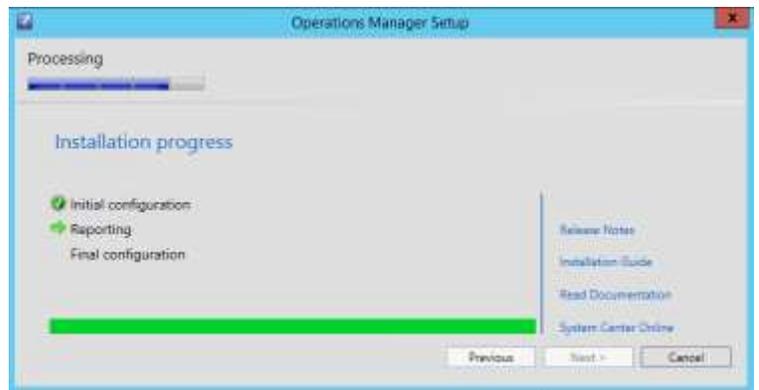
On the **Microsoft Update** page, select the appropriate update setting for your organization and click **Next**.



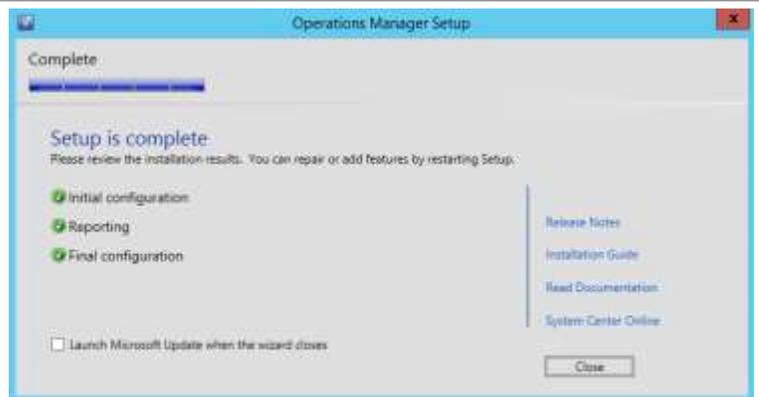
The **Installation Summary** page will appear and display the selections made during the installation wizard. Review the options selected, and click **Install** to continue.



The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup is complete** page. Verify that the **Launch Microsoft Update when the wizard closes** check box is selected, and click **Close** to complete the installation.



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

After the installation is complete, the following tasks must be performed to complete Operations Manager and Virtual Machine Manager integration.

Register the Required Service Principal Names for the Operations Manager Management Servers

The following steps must be performed on a domain controller or on one of the Operations Manager servers by using a domain admin account or an account with permissions to create service principal names.

- ▶ Perform the following steps on a domain controller in the domain where Operations Manager is installed.

The Operations Manager Health Service service principal names should be set automatically by the management server's computer account. To confirm that the service principal names are set correctly, open an administrative command prompt and run the following command:

```
SETSPN -L <DOMAIN>\<SERVERNAME>
```

Where <DOMAIN> is the Active Directory domain name where the Operations Manager management server is installed and <SERVERNAME> is the name of the Operations Manager management server.

```
PS C:\Users\Administrator.VSPEX> setspn -l vsplex/om01
Registered ServicePrincipalNames for CN=OM01,CN=Computers,DC=VSPEX,DC=COM:
MSOMSvc/OM01
MSOMSvc/OM01.VSPEX.COM
MSMAN/OM01
MSMAN/OM01.VSPEX.COM
TERMSRV/OM01.VSPEX.COM
TERMSRV/OM01
RestrictedKrbHost/OM01
HOST/OM01
RestrictedKrbHost/OM01.VSPEX.COM
PS C:\Users\Administrator.VSPEX> setspn -l vsplex/om02
Registered ServicePrincipalNames for CN=OM02,CN=Computers,DC=VSPEX,DC=COM:
MSOMSvc/OM02
MSOMSvc/OM02
MSMAN/OM02.VSPEX.COM
MSMAN/OM02
TERMSRV/OM02.VSPEX.COM
TERMSRV/OM02
RestrictedKrbHost/OM02
HOST/OM02
RestrictedKrbHost/OM02.VSPEX.COM
HOST/OM02.VSPEX.COM
PS C:\Users\Administrator.VSPEX>
```

The Data Access Service account runs under a domain user account context, and it is not able to create the appropriate service principal names in Active Directory. The following command must be run from a domain admin account or from an account with delegated permissions to user objects.

To set the service principal name, run the following commands from an administrative command prompt:

```
SETSPN.exe -A MSOMSdkSvc/<ManagementServerFQDN> <domain>\<SDKServiceAccount>
```

```
SETSPN.exe -A MSOMSdkSvc/<ManagementServerNetBIOS> <domain>\<SDKServiceAccount>
```

Where <ManagementServerFQDN> is the name of the Operations Manager management server and <SDKServiceAccount> is the name of the Operations Manager service account.

If there is more than one management server being deployed, these commands must be run for each management server.

```
C:\Users\Administrator.VSPEX>setspn -A MSOMSdkSvc/OM01.VSPEX.com VSPEX\FT-SCDM-SVC
Checking domain DC=VSPEX,DC=COM
Registering ServicePrincipalNames for CN=FT-SCDM-SVC,OU=FastTrack,DC=VSPEX,DC=COM
MSOMSdkSvc/OM01.VSPEX.com
Updated object
C:\Users\Administrator.VSPEX>setspn -A MSOMSdkSvc/OM01.VSPEX\FT-SCDM-SVC
Checking domain DC=VSPEX,DC=COM
Registering ServicePrincipalNames for CN=FT-SCDM-SVC,OU=FastTrack,DC=VSPEX,DC=COM
MSOMSdkSvc/OM01
Updated object
C:\Users\Administrator.VSPEX>setspn -A MSOMSdkSvc/OM02.VSPEX.com VSPEX\FT-SCDM-SVC
Checking domain DC=VSPEX,DC=COM
Registering ServicePrincipalNames for CN=FT-SCDM-SVC,OU=FastTrack,DC=VSPEX,DC=COM
MSOMSdkSvc/OM02.VSPEX.com
Updated object
C:\Users\Administrator.VSPEX>setspn -A MSOMSdkSvc/OM02.VSPEX\FT-SCDM-SVC
Checking domain DC=VSPEX,DC=COM
Registering ServicePrincipalNames for CN=FT-SCDM-SVC,OU=FastTrack,DC=VSPEX,DC=COM
MSOMSdkSvc/OM02
Updated object
C:\Users\Administrator.VSPEX>
```

When complete, the service principal name s can be confirmed with the following command:

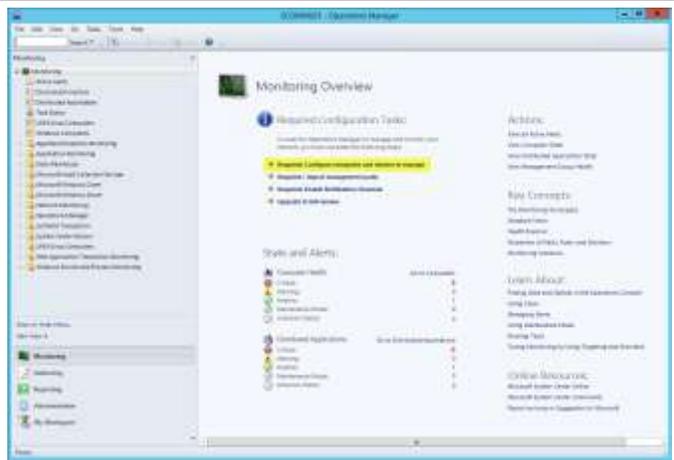
```
SETSPN -L <DOMAIN>\<SDKServiceAccount>
```

```
C:\Users\Administrator_VSPEX>
C:\Users\Administrator_VSPEX>SETSPN -L VSPEX\FT-SCOM-SVC
RegistLrad ServicePrincipalsNames For CN=FT-SCOM-SVC,OU=FastTrack,DC=VSPEX,DC=COM:
MSORDDKSvc/DM02.VSPEX.com
MSORDDKSvc/DM01.VSPEX.com
MSORDDKSvc/DM01.VSPEX.com
C:\Users\Administrator_VSPEX>
```

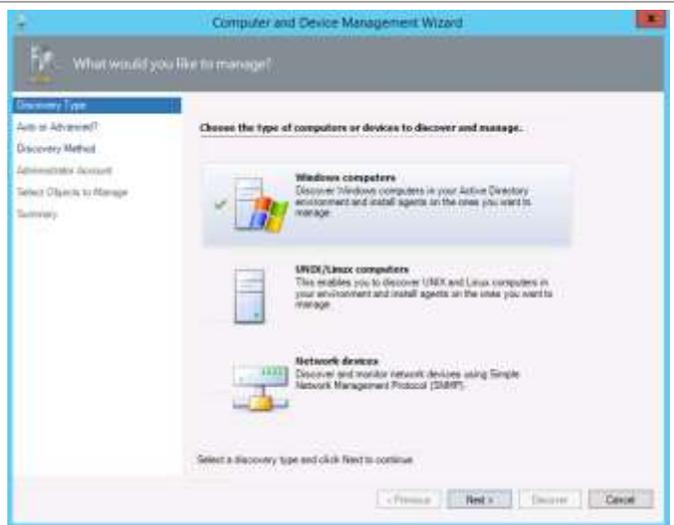
Deploy and Configure the Operations Manager Agent on the Virtual Machine Manager Management Server Nodes

► Perform the following steps on the Operations Manager management server virtual machine.

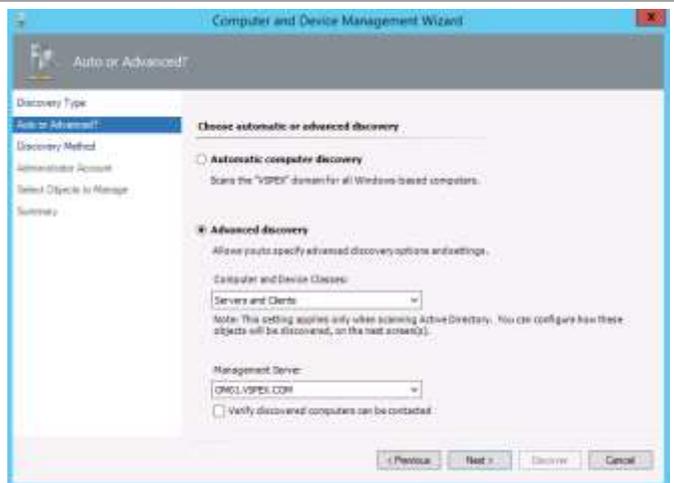
From the Operations Console **Monitoring** or **Administration** view, select the **Configure computers and devices to manage** task item link.



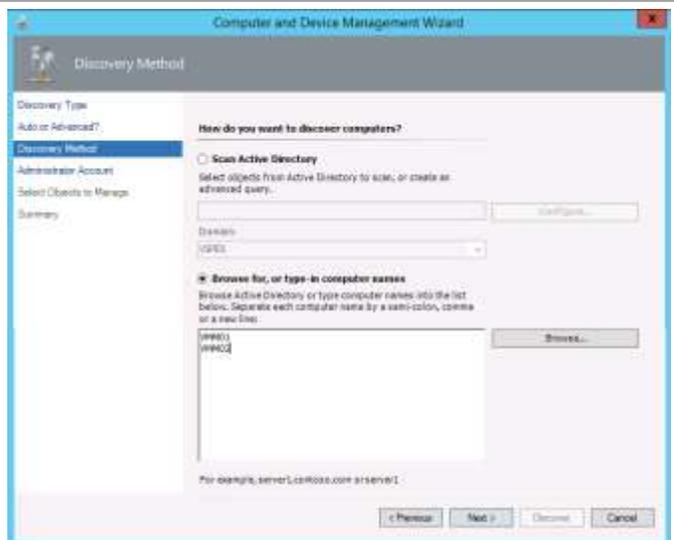
The Computer and Device Management Wizard will appear. On the **Discovery Type** page, select **Windows computers** from the available options, and click **Next** to continue.



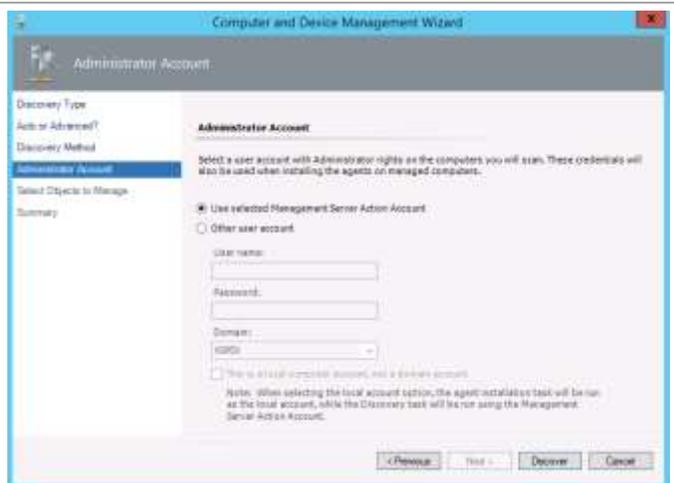
On the **Auto or Advanced?** page, select the **Advanced discovery** option, and click **Next** to continue.



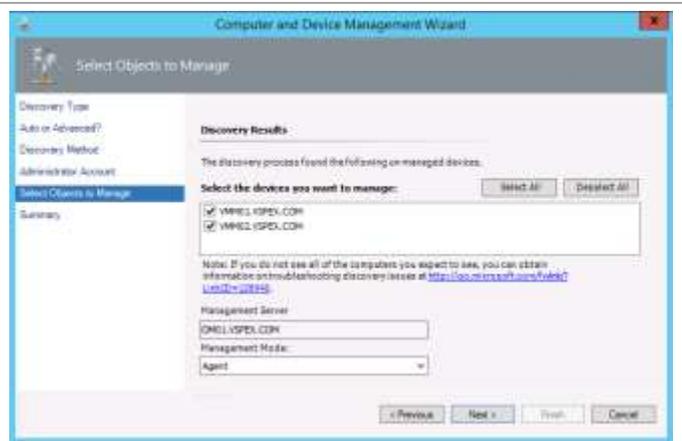
On the **Discovery Method** page, under **Browse for**, or **type-in computer names**, input the names of both Virtual Machine Manager servers. Click **Next** to continue.



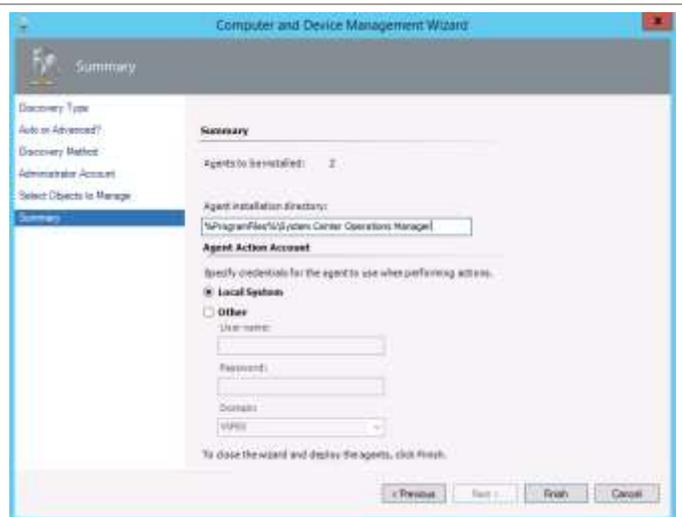
On the **Administrator Account** page, If the account you are logged in with is a local administrator on the VMM server then leave the default selection in place, if not then select the **Other user account** option, and provide the credentials that are required to access Active Directory and perform discovery in your environment. Verify that the **This is a local computer account, not a domain account** check box is clear, and click **Discover** to continue.



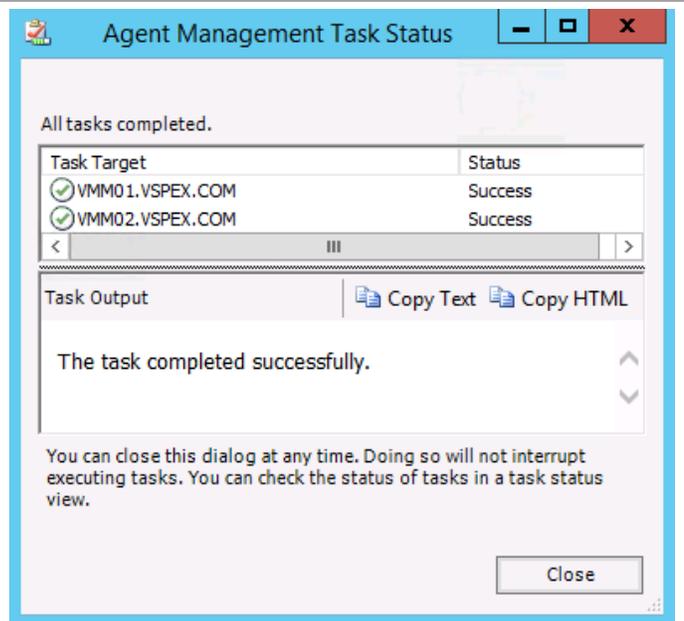
On the **Select Objects to Manage** page, review the **Discovery Results**. In the **Select the devices you want to manage** dialog box, select the Virtual Machine Manager server. From the **Management Mode** drop-down list, select **Agent**, and click **Next** to continue.



On the **Summary** page, accept the default **Agent installation directory** as %ProgramFiles%\System Center Operations Manager. In the **Agent Action Account** section, select the **Local System** option. Click **Finish** to perform the agent installation.



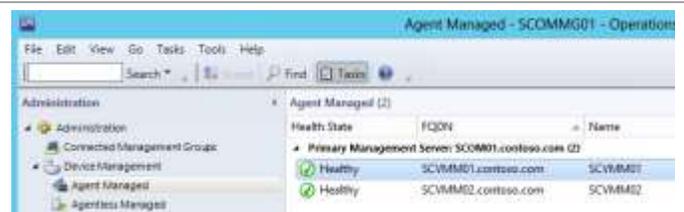
On the **Agent Management Task Status** page, verify that the agent installation completes successfully, and then click **Close** to complete the operation.



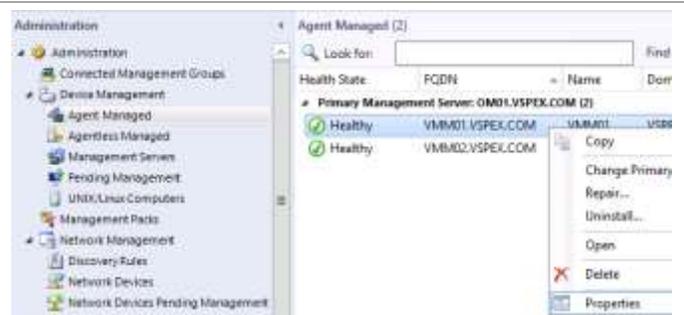
The next step is to enable the Operations Manager agent that is deployed on the Virtual Machine Manager management server to be a proxy agent.

In the **Operations Manager** console, navigate to the **Administration** workspace, expand the **Device Management** node, and select the **Agent Managed** view.

Note: It can take several minutes for the **Health State** to transition from **Not Monitored** to **Healthy**.



In the **Agent Managed** pane, select the agent that is associated with the Virtual Machine Manager management server, and click **Properties** in the task pane.



On the **Agent Properties** page, click the **Security** tab. Verify that the **Allow this agent to act as a proxy and discover managed objects on other computers** check box is selected, then click **OK** to save the changes. Repeat this process for each Virtual Machine Manager agent-managed system.

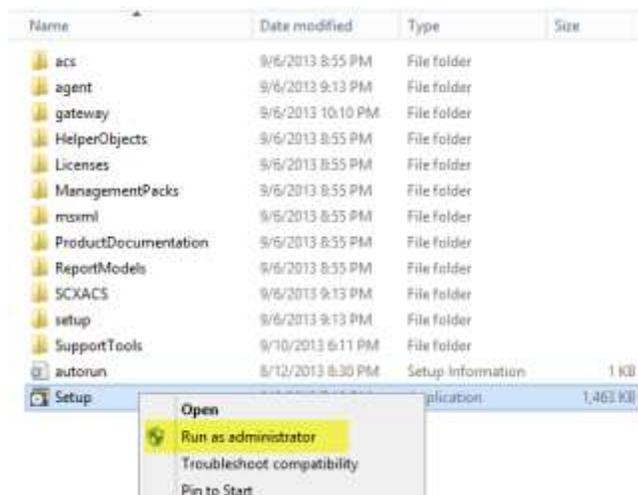
Note: When hosts are brought in VMM to be managed they must also have the SCOM agent installed for VMM to and SCOM integration to continue functioning properly.



Install Operations Manager Console on the Virtual Machine Manager Management Server

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

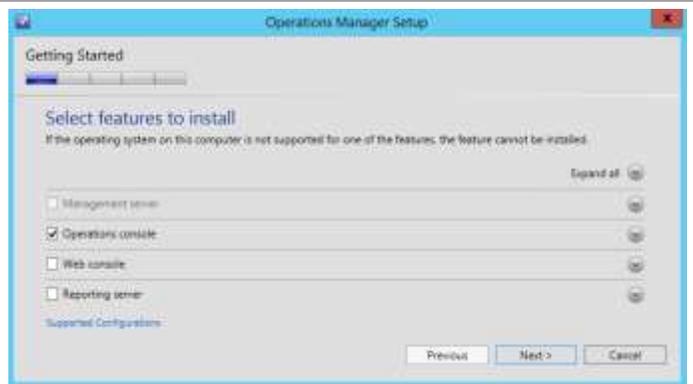
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



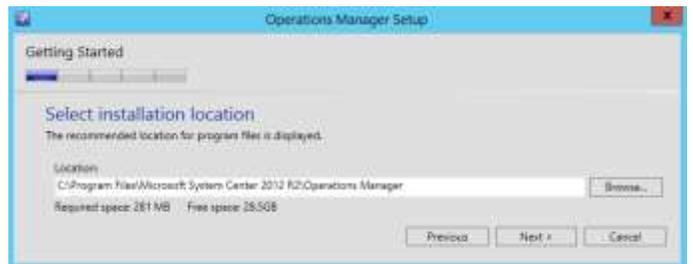
The Operations Manager installation wizard will begin. Click **Install** to begin the Operations Manager console installation.



On the **Select features to install** page, verify that the **Operations console** check box is selected. Click **Next** to continue.



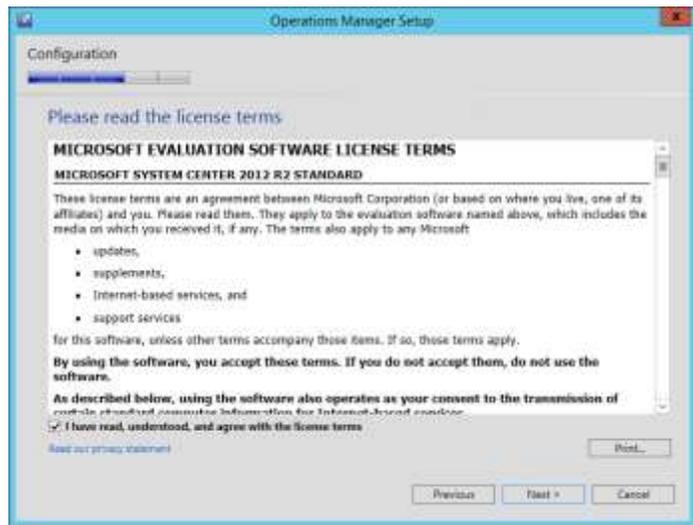
On the **Select installation location** page, specify a location or accept the default location of %ProgramFiles%\System Center 2012 R2\Operations Manager for the installation. Click **Next** to continue.



The wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the **Proceed with Setup** page. After you verify that the prerequisites are met, click **Next** to continue.



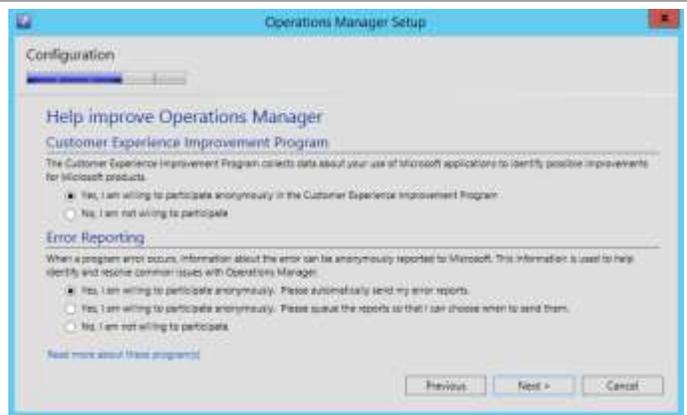
On the **Please read the license terms** page, verify that the **I have read, understood and agree with the license terms** check box is selected, and click **Next** to continue.



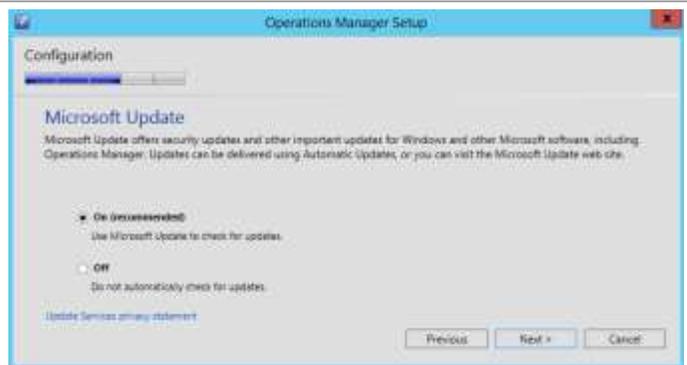
The **Help Improve Operations Manager** page provides options for participating in various product feedback mechanisms. These include:

- Customer Experience Improvement Program
- Error Reporting

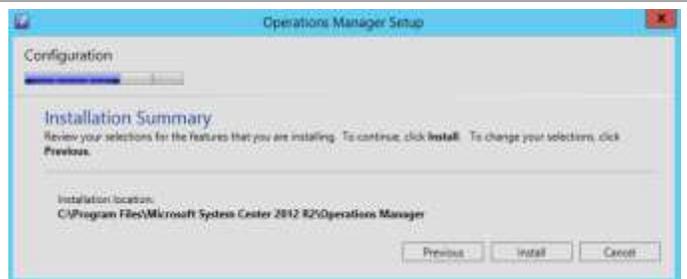
Select the appropriate option based on your organization's policies, and click **Next** to continue.



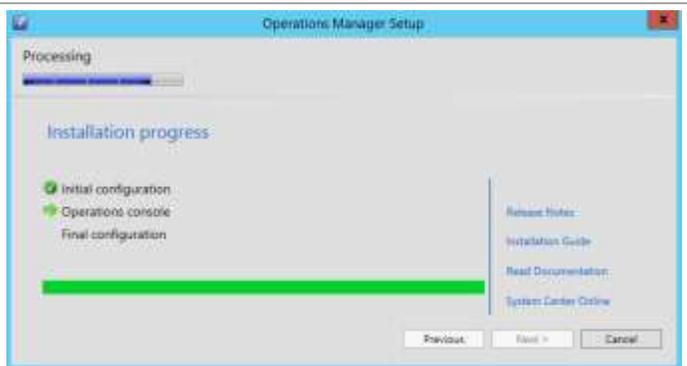
The **Microsoft Update** page provides the option to automatically check for updates. Make your selection and click **Next** to continue.



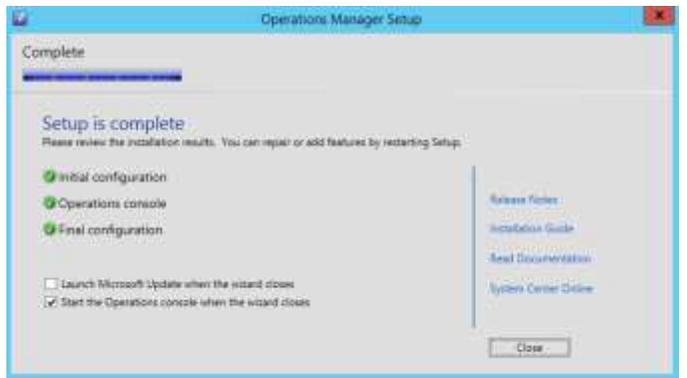
The **Installation Summary** page will appear and display the selections made during the installation wizard. Review the options selected, and click **Install** to continue.



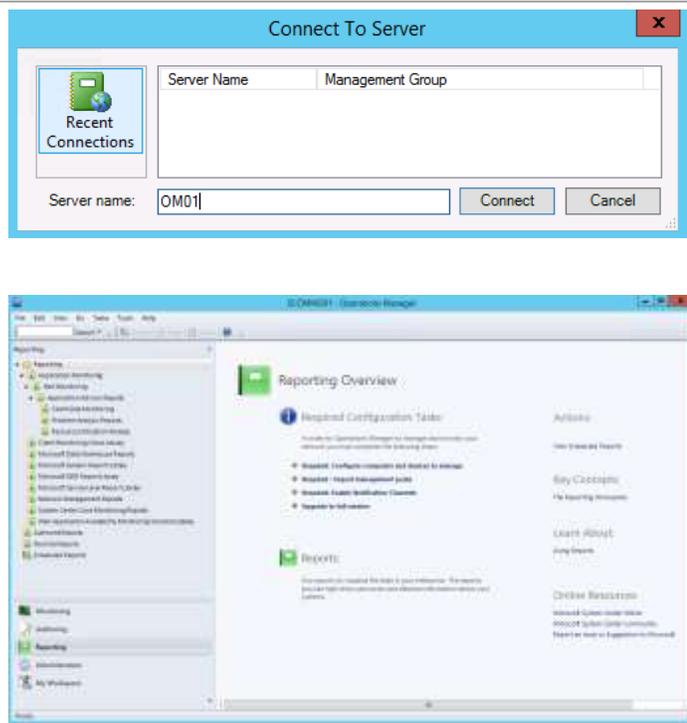
The wizard will display the progress while performing the installation.



After the installation completes, the wizard will display the **Setup is complete** page. Verify that the **start the Management console when the wizard closes** check box is selected, and click **Close** to complete the installation.



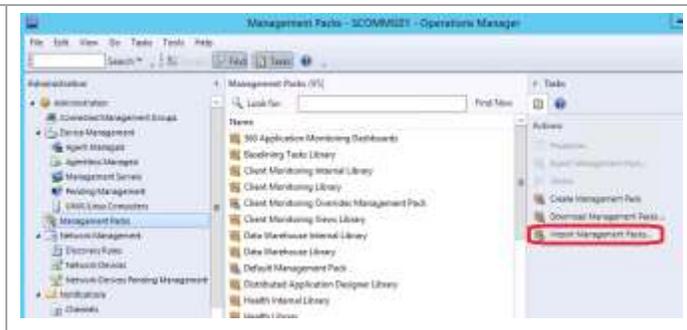
The **Operations Manager console** will open. Validate the installation by reviewing the configuration and Make sure that the console operates properly.



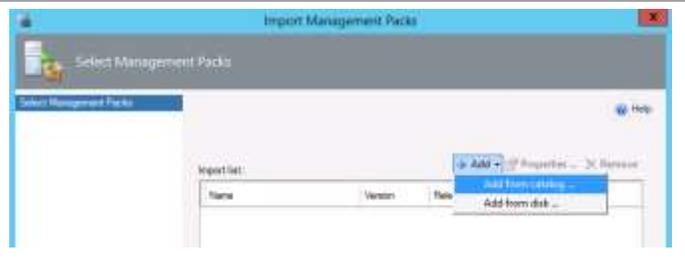
Download and Import the Required Prerequisite Management Packs in Operations Manager

▶ Perform the following steps on the Operations Manager virtual machine.

In the **Operations Manager** console, navigate to the **Administration** pane and click the **Management Packs** node. In the **Actions** pane, click **Import Management Packs...**



On the **Select Management Packs** page, click the **Add** button, and click **Add from catalog...** in the drop-down list.



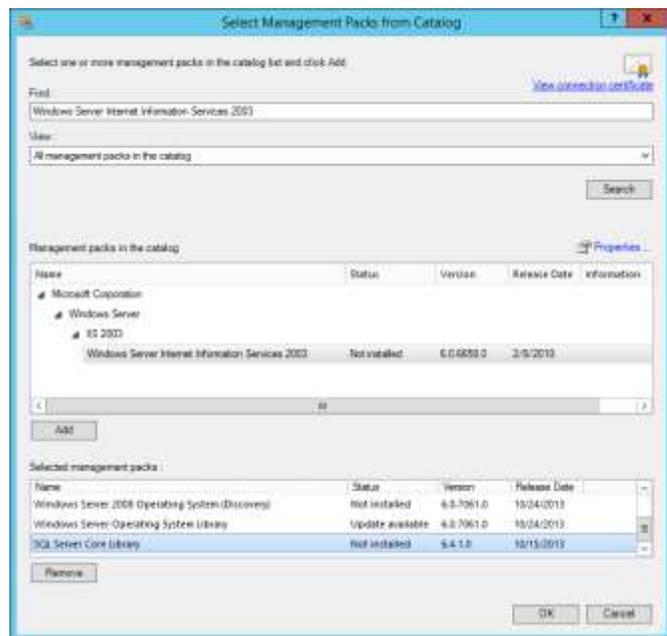
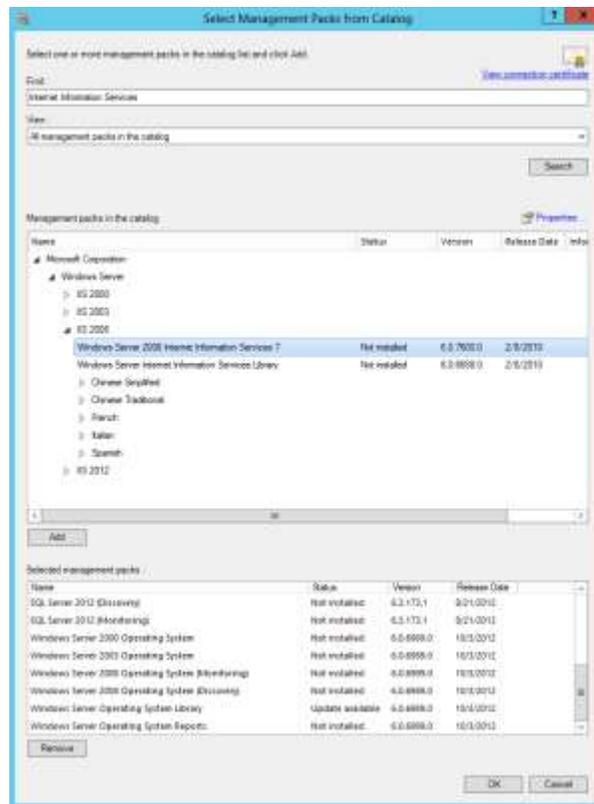
On the **Select Management Packs from Catalog** page, find and add the following management packs (in this order):

- Windows Server Internet Information Services Library
- Windows Server Internet Information Services 2003
- Windows Server 2008 Internet Information Services 7
- Windows Server 2008 Operating System (Discovery)
- Windows Server Operating System Library
- Windows Server 2012 R2 Operating System (Discovery)
- Windows Server 2012 R2 Cluster Management Library
- SQL Server Core Library

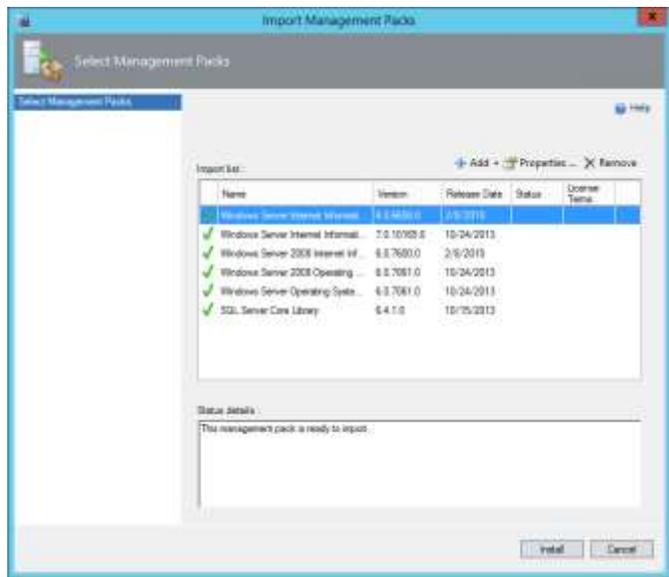
After they are added, click **OK** to continue.

Note that additional management packs may be required to satisfy dependencies or monitoring requirements for the target infrastructure.

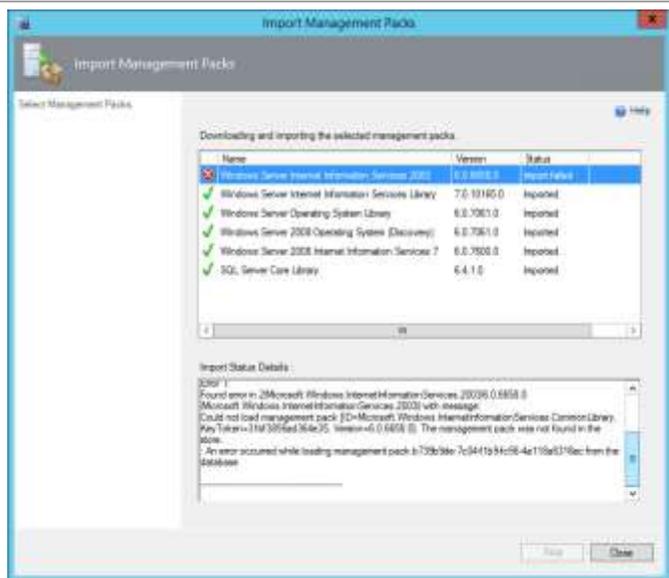
If you get an error on the import, you might have to try a second time to get it imported properly.



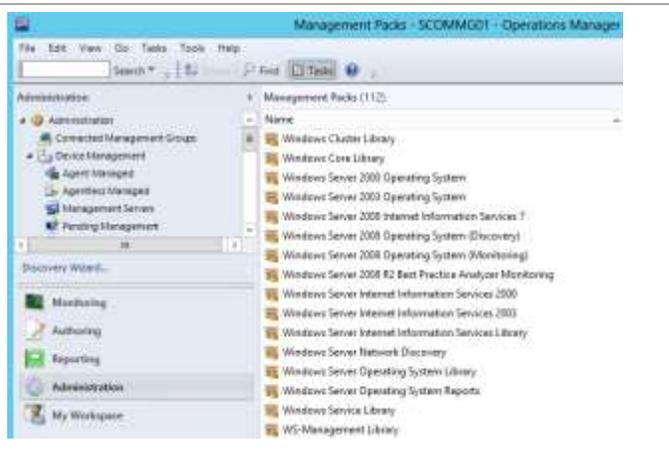
On the **Select Management Packs** page, click **Install** to import the selected management packs.



The management packs will download 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, navigate to the Administration workspace and verify that the previously selected management packs are installed.

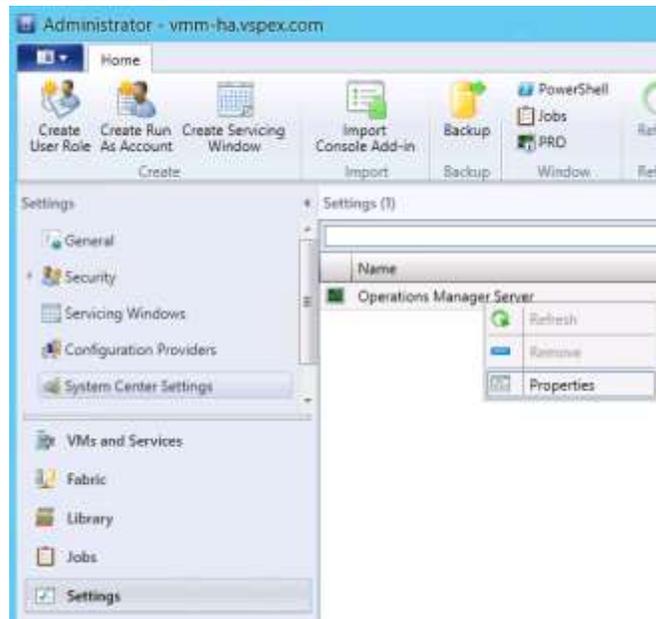


Perform Virtual Machine Manager and Operations Manager Integration

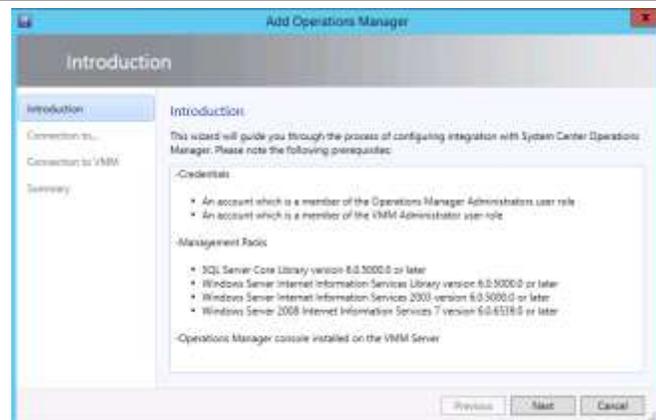
After all prerequisite configurations and installations are performed, the integration of Virtual Machine Manager and Operations Manager can be completed.

► Perform the following steps on the Virtual Machine Manager virtual machine.

In the **Virtual Machine Manager** console, navigate to **Settings** pane, and select **System Center Settings**. Right-click **Operations Manager Server**, and select **Properties**.



The **Add Operations Manager Wizard** will appear. On the **Introduction** page, verify that the prerequisites have been met, and click **Next** to continue.



On the **Connection to Operations Manager** page:

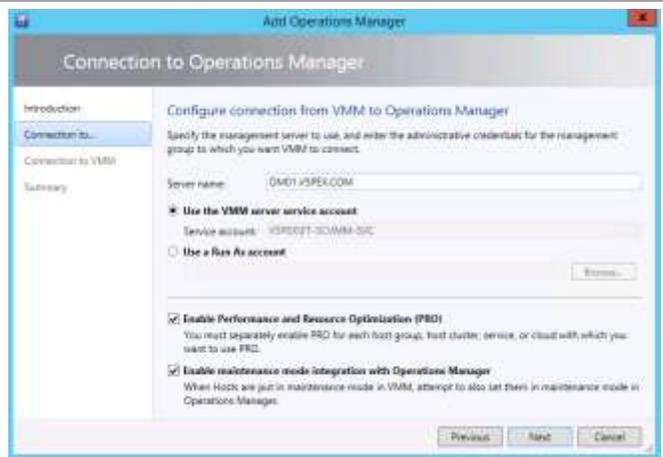
Type the FQDN of the Operations Manager server in the **Server name** text box.

Select **Use the VMM server service** account.

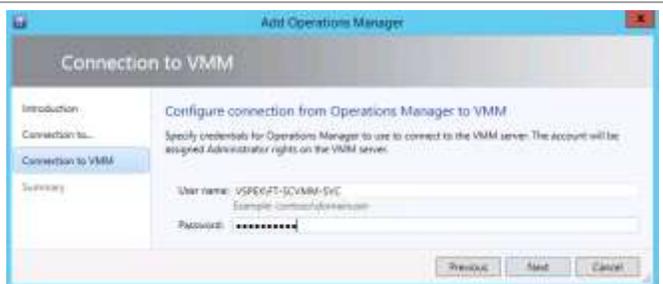
Select **Enable Performance and Resource Optimization (PRO)**.

Select **Enable maintenance mode integration with Operations Manager**.

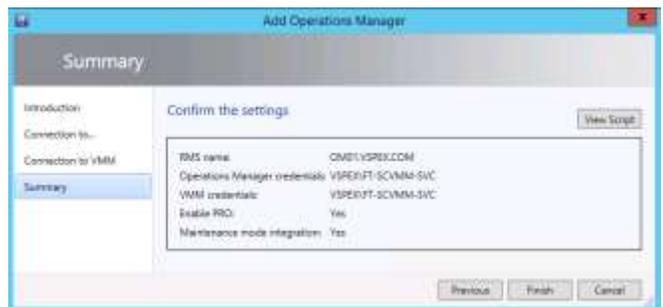
Click **Next** to continue.



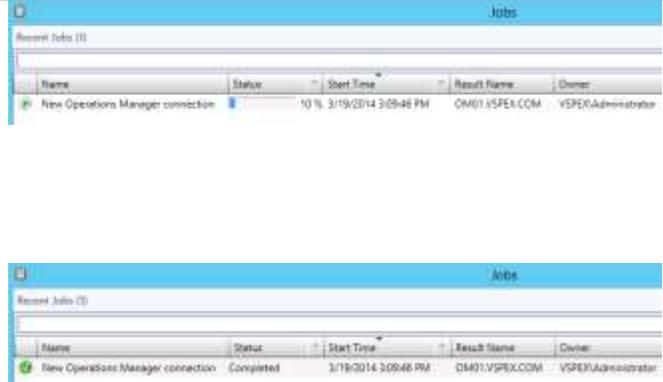
On the **Connection to VMM** page, specify the Virtual Machine Manager service account credentials in the **User name** and **Password** text boxes, and click **Next** to continue.



On the **Summary** page, verify the options selected, and click **Finish** to begin the Operations Manager integration process.



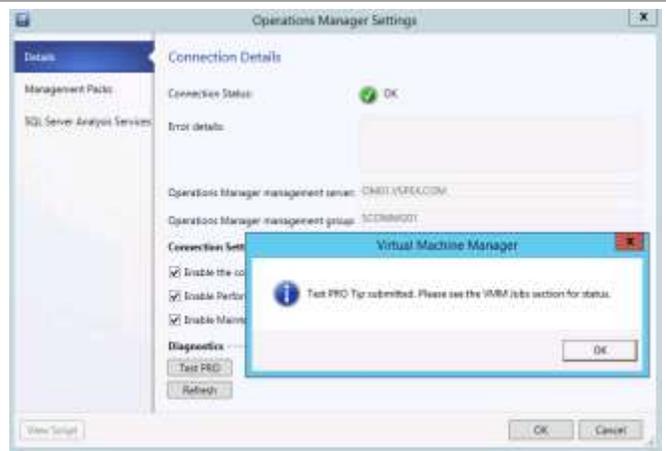
The **Jobs** pane will appear. Before moving forward, wait for the job to complete successfully.



In the Virtual Machine Manager console, navigate back to **Settings**. Click **System Center Settings**, and double-click **Operations Manager Server**. The Operations Manager Settings page will appear.

In the **Details** pane, click the **Test PRO** button.

Note: The PRO test will not succeed immediately. Some synchronization needs to complete from previous steps. This can take up to an hour or more. You will need to simply keep trying until it succeeds.



As part of the test, the **PRO** page appears and displays a diagnostics alert.

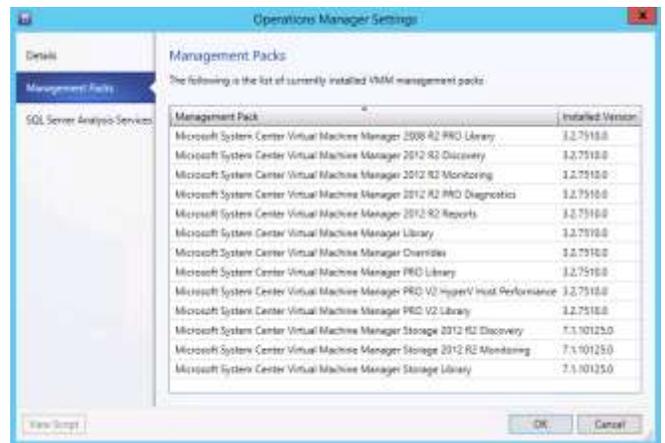


After a few minutes it will be possible to determine that the PRO test completed by navigating to the **Jobs** pane and verify that the PRO jobs completed successfully.



Step	Name	Status	Start Time	End Time
1	PRO diagnostics	Completed	3/20/2014 7:34:34 AM	3/20/2014 7:35:02 AM
1.1	Create new PRO tip	Completed	3/20/2014 7:34:34 AM	3/20/2014 7:34:54 AM
1.2	Implement the fix for a PRO tip	Completed	3/20/2014 7:34:54 AM	3/20/2014 7:35:02 AM
1.2.1	Invoke remediation	Completed	3/20/2014 7:34:55 AM	3/20/2014 7:34:55 AM
1.2.2	Wait for remediation	Completed	3/20/2014 7:34:55 AM	3/20/2014 7:35:02 AM

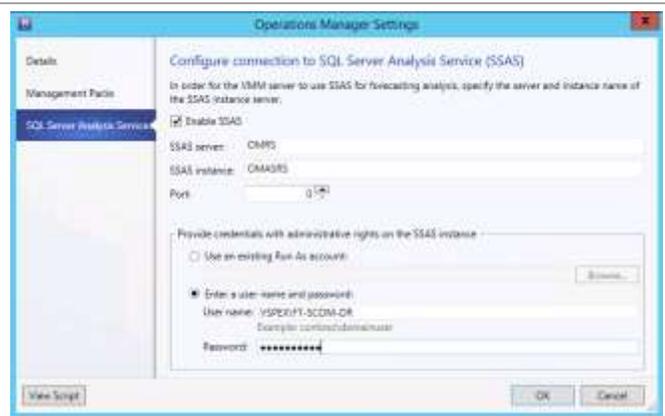
On the **Management Packs** page, verify that all Virtual Machine Manager Management Packs were successfully installed.



On the Configure connection to SQL Server Analysis Services (SSAS) page, provide the following information.

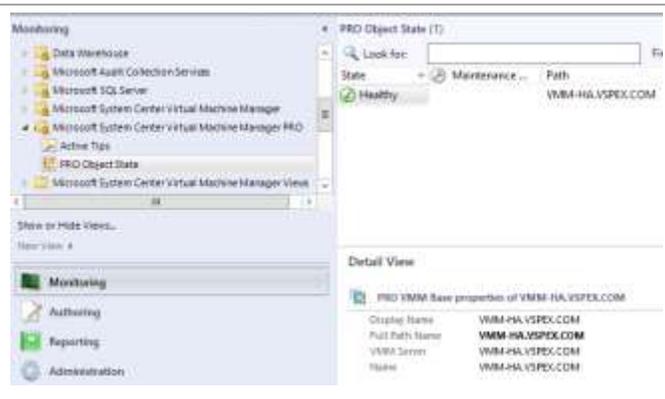
Select the Enable SSAS check box. Provide the following information in the text boxes provided:

- SSAS server – Specify the Operations Manager reporting server.
- SSAS Instance – Specify the SSAS instance name that you created earlier on the Operations Manager reporting server.
- Port – Leave the default value of 0.



In the Provide credentials with administrative rights on the SSAS instance section, 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.

In the **Operations Manager** console, navigate to the **Monitoring** workspace, select the **Microsoft System Center Virtual Machine Manager PRO** node and click **PRO Object State**. Verify that the Virtual Machine Manager is listed with a health state other than **Not Monitored**.



Service Manager

The Service Manager Management Server is installed on a pair of virtual machines. A third virtual machine hosts the Management Server for the Service Manager Data Warehouse and a fourth virtual machine hosts the Service Manager Self Service Portal.

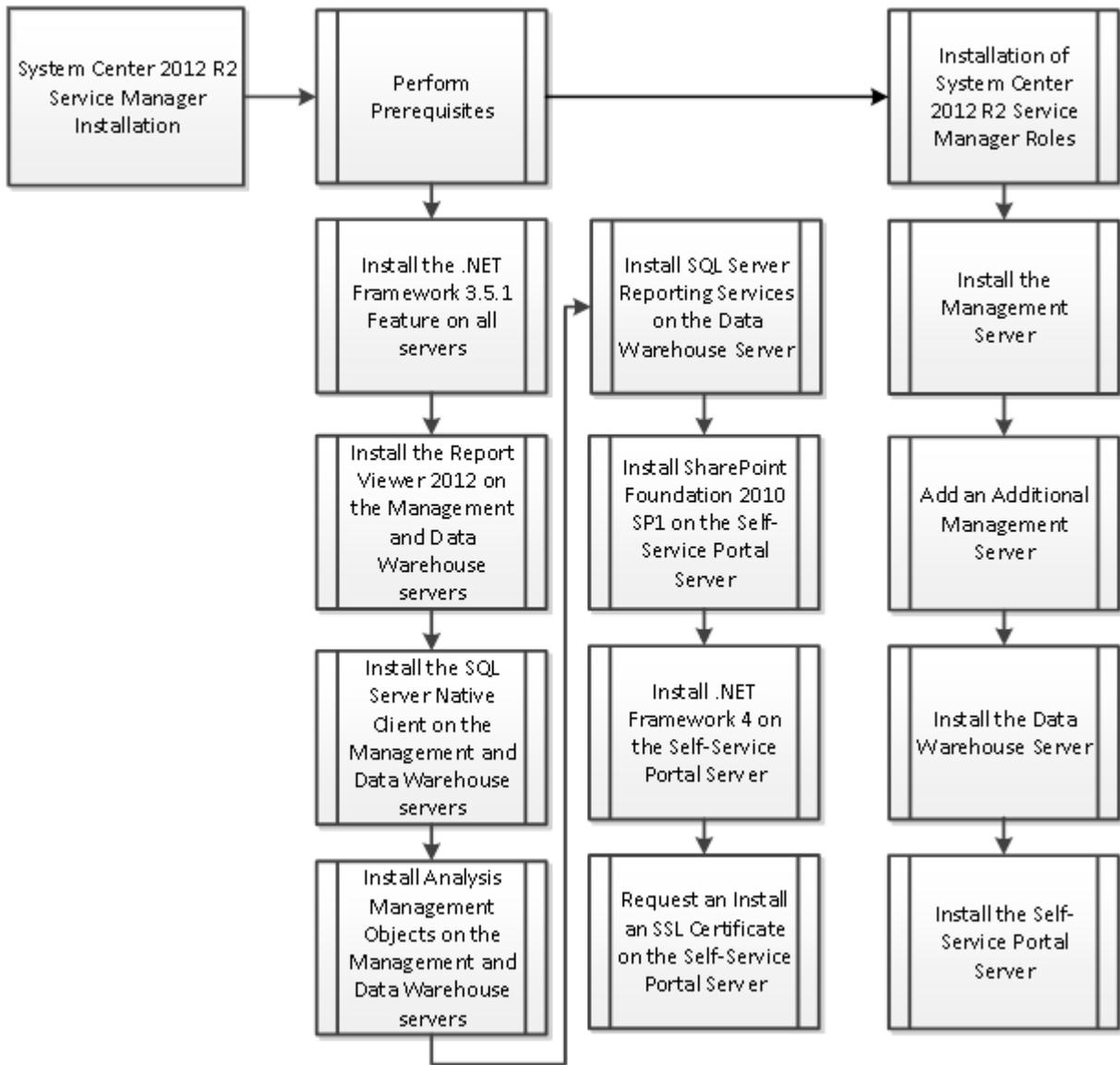
The Service Manager environment will be supported by four separate SQL instances on the virtual SQL Cluster:

- Service Manager Management Server database (CMDB);
- Service Manager Data Warehouse databases;
- Service Manager Data Warehouse Analysis database and
- SharePoint foundation database (used by the Service Manager portal).

For the IaaS PLA implementation, the Change request and Service requests are sized for 90-day retention instead of the default retention period of 365 days . The following virtual machine configurations are used.

The Service Manager installation process includes the high-level steps shown in the following figure.

Figure 9. Service Manager Installation Process



Overview

This section provides a high-level walkthrough for deploying Service Manager into the fabric management architecture. The following requirements are necessary to deploy the management, data warehouse, and self-service portal servers:

Management Server

- A base virtual machine running Windows Server 2012 R2 has been provisioned for the Service Manager management server role
- A multi-node, SQL Server 2012 SP1 cluster with dedicated Service Manager instances has been established in previous steps for Service Manager
 - SCSMDB - instance for Service Manager management database.

- .NET Framework 3.5 SP1 is installed
- Microsoft Report Viewer 2008 Service Pack 1 Redistributable is installed. To install, see article 971119 in the Microsoft Knowledge Base
- Microsoft SQL Server 2012 Native Client is installed. To install, see SQL Server 2012 Native Client
- The Microsoft SQL Server 2012 Analysis Management Objects are installed. To install, see SQL Server Analysis Management Objects

Data warehouse server

- A base virtual machine running Windows Server 2012 R2 has been provisioned for the Service Manager management server role
- A multi-node, SQL Server 2012 SP1 cluster with a dedicated instance has been established in previous steps for Service Manager, which includes:
 - SCSMAS – instance for SQL Server 2012 SP1 Analysis Services and SQL Server Reporting Services databases
 - SCSMDW – instance for Service Manager data warehouse databases
 - .NET Framework 3.5 SP1 is installed
- Microsoft Report Viewer 2008 Service Pack 1 Redistributable is installed. To install, see article 971119 in the Microsoft Knowledge Base
- Microsoft SQL Server 2012 Native Client is installed. To download, see SQL Server 2012 Native Client
- Microsoft SQL Server 2012 Analysis Management Objects are installed. To install, see SQL Server Analysis Management Objects.
- Microsoft SQL Server 2012 Reporting Services (split configuration) is installed. Microsoft SQL Server 2012 management tools are installed

Self-service Portal Server

- A base virtual machine running Windows Server 2008 R2 (x64) has been provisioned for the Service Manager management server role
- A multinode, SQL Server 2012 SP1 cluster with a dedicated instance has been established in previous steps for Service Manager
- .NET Framework 3.5 SP1 is installed
- Microsoft Report Viewer 2008 Service Pack 1 Redistributable is installed. To install, see article 971119 in the Microsoft Knowledge Base
- Microsoft SQL Server 2012 Native Client is installed. To download, see SQL Server 2012 Native Client
- Microsoft SQL Server 2012 Analysis Management Objects are installed. To install, see SQL Server Analysis Management Objects
- SharePoint Foundation 2010 Service Pack 2 is installed. To install, see Microsoft SharePoint Foundation 2010
- The .NET Framework 4 Redistributable

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following service accounts have been created:

Table 25. Service Manager Accounts

User name	Purpose	Permissions
<DOMAIN>\ SCSM-SVC	FT- 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>\ SCSM-WF	FT- SCSM workflow account	Must have permissions to send email and must have a mailbox on the SMTP server (required for the Email Incident feature) Must be member of local Users security group on all SCSM servers Must be a member of the Service Manager Administrators user role for email Must be a local Admin on all SQL Server nodes
<DOMAIN>\ SCSM-SSRS	FT- SCSM reporting account	Must be a local Admin on all SQL Server nodes
<DOMAIN>\ SCSM-OMCI	FT- SCSM Operations Manager CI connector account	Must be a member of the local Users security group on all SCSM servers. Must be an Operations Manager operator
<DOMAIN>\ SCSM-ADCI	FT- SCSM Active Directory CI connector account	Must be a member of the local Users 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 to the Service Manager database from Active Directory
<DOMAIN>\ SCSM-OMAlert	FT- SCSM Operations Manager alert connector account	Must be a member of the local Users security group on the Service Manager management server Must be a member of FT-SCSM-Admins
DOMAIN>\ SCSM-VMMCI	FT- Virtual Machine Manager CI connector account	Must be a member of the VMM Admin domain group and be in the Service Manager Advanced Operator role
DOMAIN>\ SCSM-OCI	FT- Orchestrator CI connector	Must be a member of SCO Operators (Users) domain group and be in the Service Manager Advanced Operator role
<DOMAIN>\ SCSM-OLAP	FT- 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:

Table 26. Service Manager Security Groups

Security group name	Group scope	Members	Member of
<DOMAIN>\ FT-SCSM-ADMINS	Global	DOMAIN\ FT-SCSM-SVC	Must be added to the Service Manager Administrators user role, added to the Operations Manager Administrators role in Operations Manager, and be a member of the Administrators group on each SQL Server

Add .NET Framework 3.5 on all Server Manager Servers

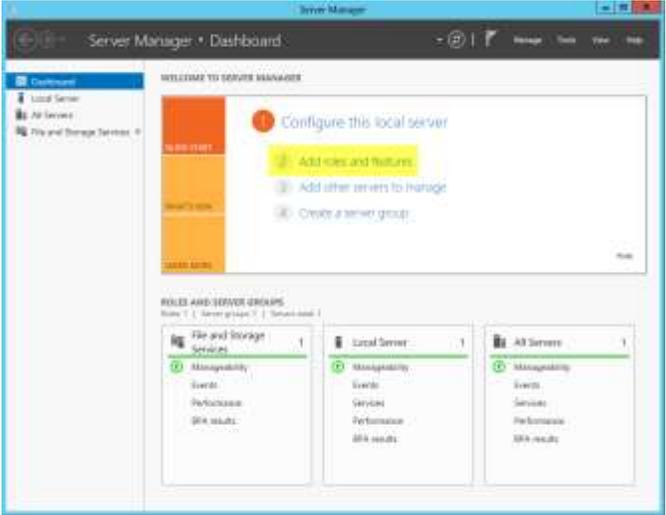
The Service Manager installation requires that .NET Framework 3.5 be enabled to support installation. Use the following procedure to enable .NET Framework 3.5.

► Perform the following steps on the Service Manager management server and the data warehouse virtual machines.

If you do not have access to the internet to contact Microsoft Update, you will need to have the Windows Installation files mounted locally or on an accessible file share.

The .NET Framework 3.5 feature can be installed with a PowerShell cmdlet, or the following instructions can be followed for using the GUI. If the VM has access to the internet, the `-Source` parameter should not be needed.

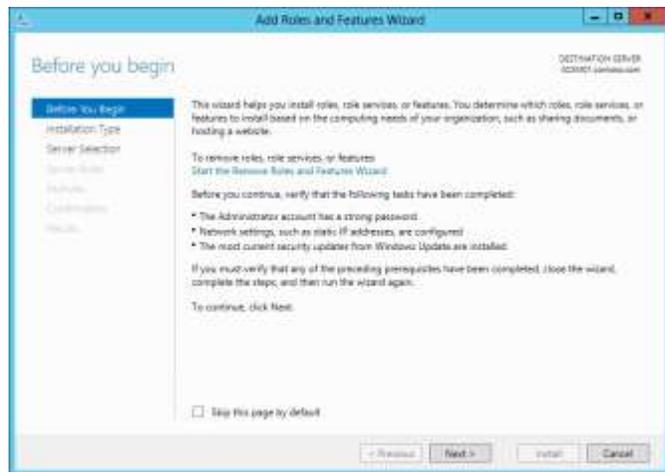
Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, click **Add roles and features**.



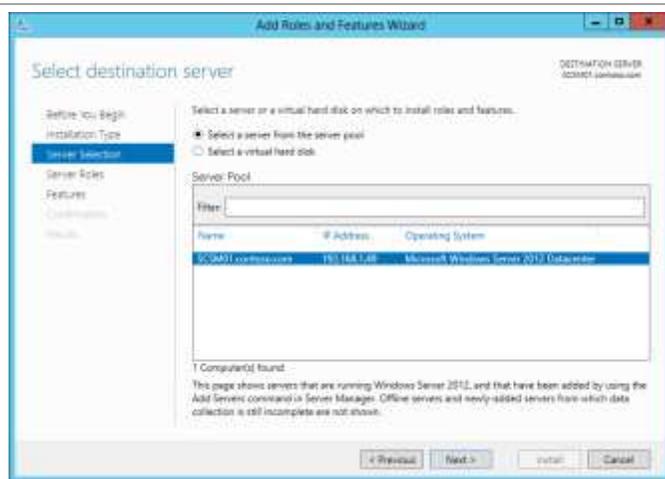
The screenshot shows the Server Manager Dashboard. The main area is titled 'WELCOME TO SERVER MANAGER' and 'Configure this local server'. Under 'Configure this local server', the 'Add roles and features' option is highlighted with a yellow box. Below this, there are three server groups: 'File and Storage Services', 'Local Server', and 'All Servers'. Each group has a 'Management' link and a 'Services' link. The 'Local Server' group also has 'Events', 'Performance', and 'SQL results' links.

```
Install-WindowsFeature -Name NET-  
Framework-Core -Source  
"E:\Sources\sxs"
```

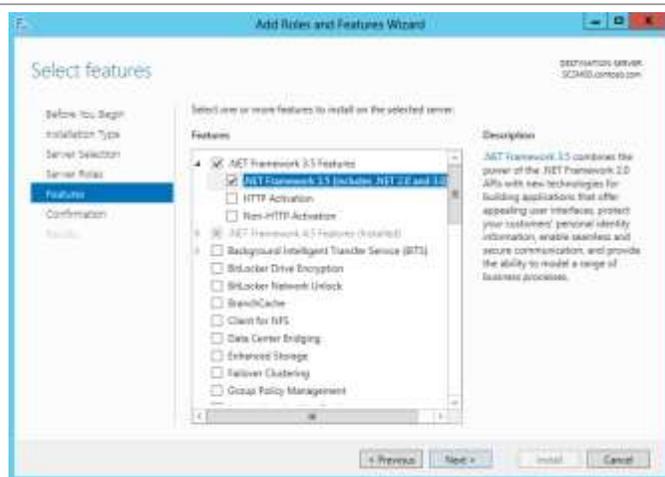
The Add Roles and Features Wizard will appear. On the **Before You Begin** page, click **Server Selection** in the left pane to continue.



On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server, and then, click **Features** in the left pane to continue.



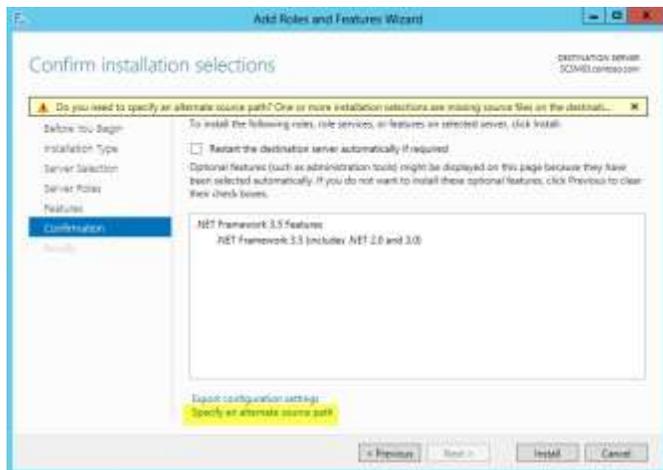
To add .NET Framework 3.5, On the **Select Features** page, in the **Features** pane, select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click **Next** to continue.



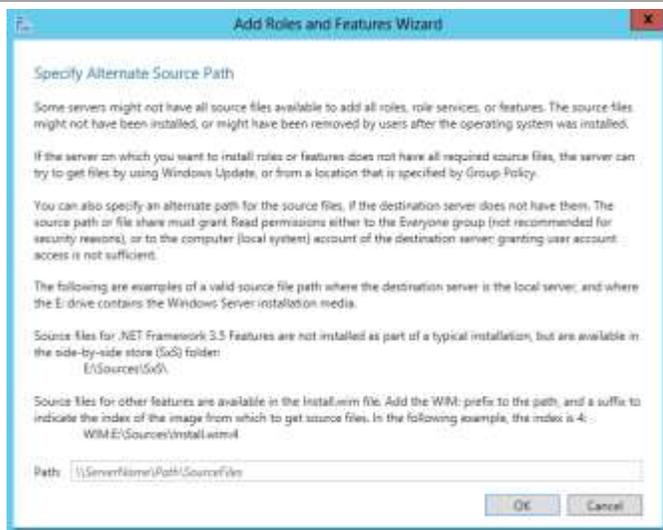
On the **Confirm installation selections** page, verify that **.NET Framework 3.5 Features** is listed. Make sure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

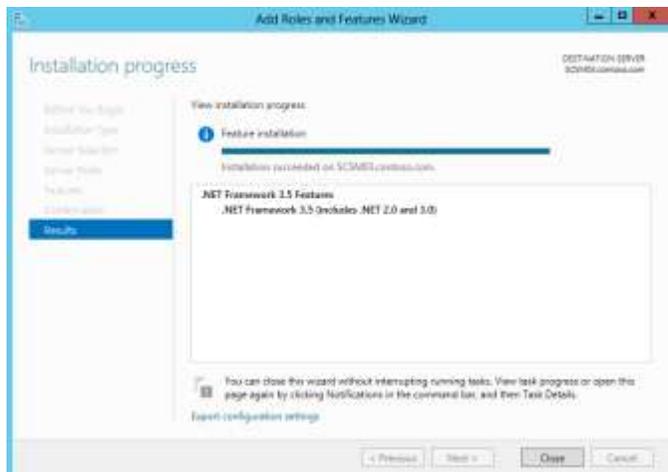
If the server does not have Internet access, an alternate source path can be specified by clicking the **Specify an alternate source path** link.



For servers without Internet access, or if the .NET Framework 3.5 source files already exist on the network, an alternate source location be specified here for the installation.

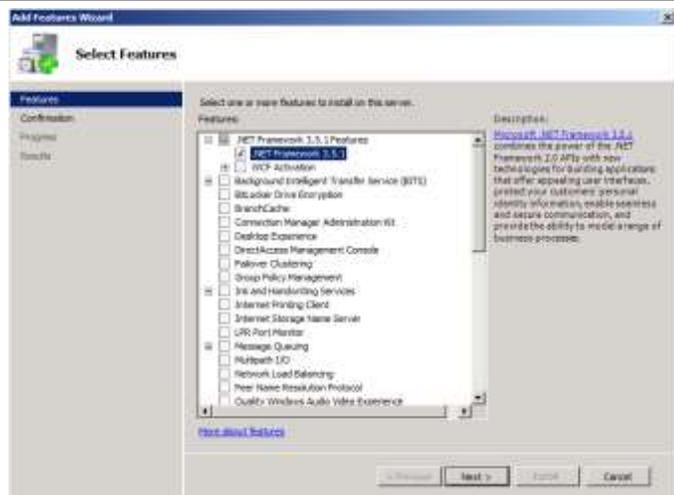


The **Installation Progress** page will show the progress of the feature installation. Click **Close** when the installation process completes.

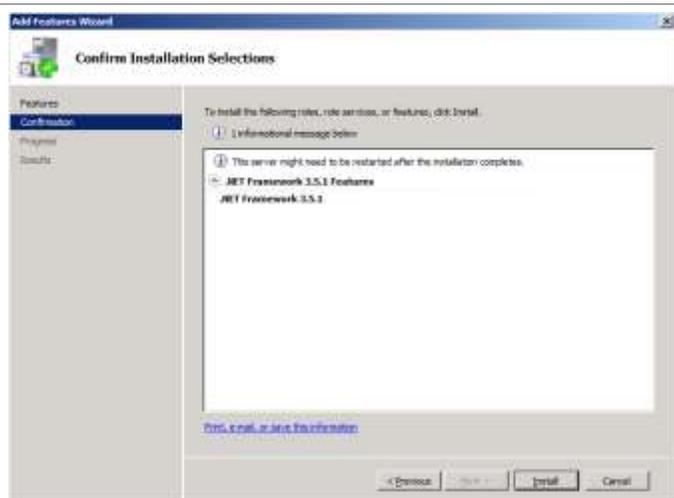


► Perform the following steps on the **Service Manager Self-Service Portal** virtual machine running **Windows Server 2008 R2**.

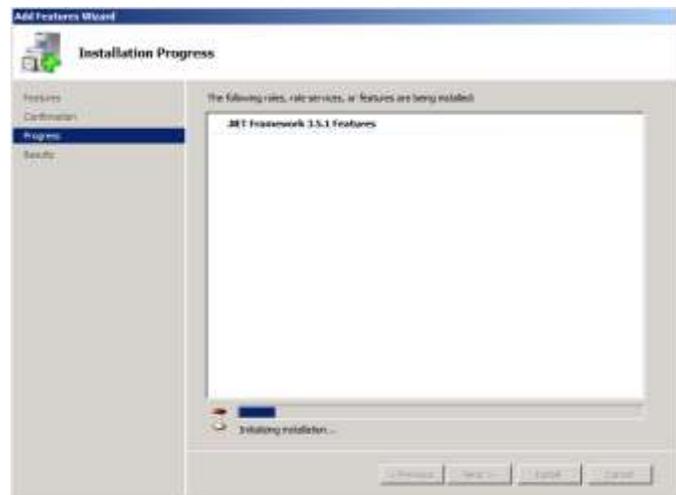
To add .NET Framework 3.5.1, from **Server Manager**, click the **Features** node, and then click **Add Features**. The Add Features Wizard will appear. On the **Select Features** page, select **.NET Framework 3.5.1 Features**, and then select the **.NET Framework 3.5.1** check box only. Leave **WCF Activation** check box clear.



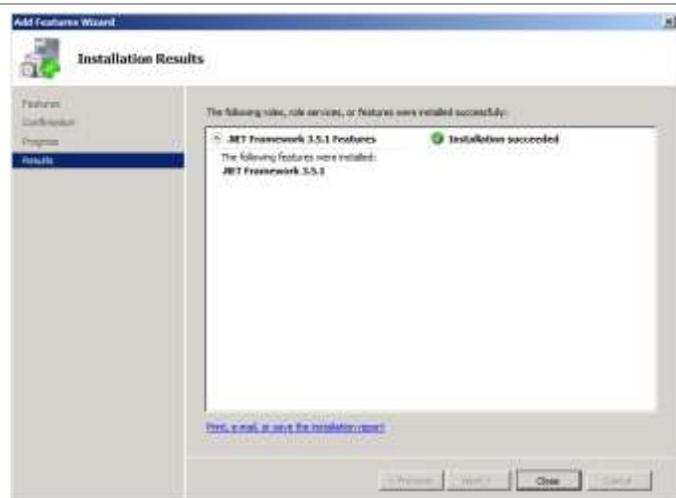
On the **Confirm Installation Selections** page, review the choices that you made during the wizard, and click **Install** to add the feature.



The **Installation Progress** page will show the progress of the feature installation.



When complete, the **Installation Results** page will appear. Verify that the .NET 3.5.1 Feature installed correctly. When verified, click **Close** to complete the installation of .NET Framework 3.5.1.



Install Microsoft Report Viewer 2008 SP1 Redistributable on the Management and Data Warehouse Servers

The Server Manager management server and the data warehouse server installations also require the Microsoft Report Viewer 2008 SP1 Redistributable. Use the following procedure to install the Microsoft Report Viewer 2008 SP1 Redistributable.

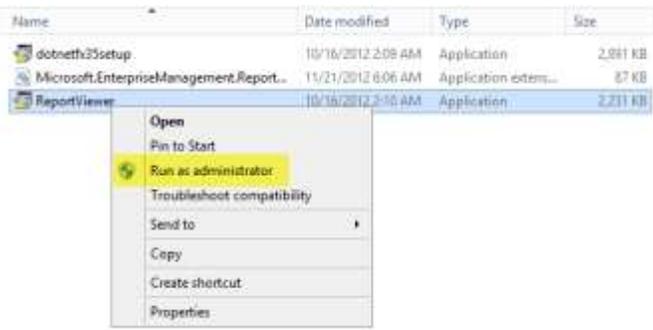
- ▶ Perform the following steps on the Server Manager management server and on data warehouse server virtual machines.

From the installation media, right-click **ReportViewer.exe** and click **Run as administrator** to begin setup.

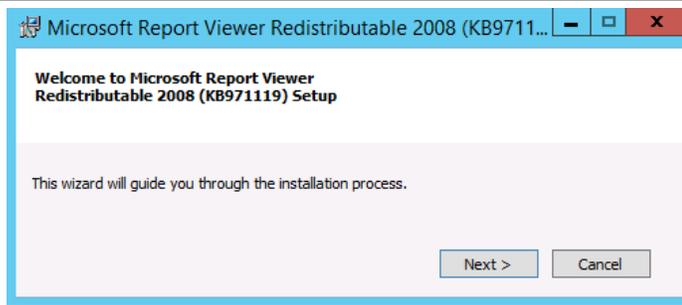
Note: You can find the Report Viewer 2008 SP1 Redistributable as follows:

In the **Prerequisites** folder of the Service Manager 2012 R2 installation media

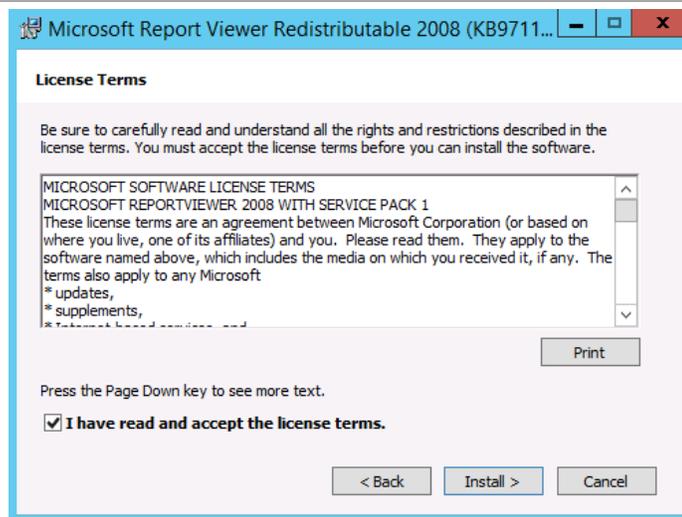
In the Microsoft Download Center:
[Report Viewer Redistributable 2008 Service Pack 1 GDIPLUS.DLL Security Update](#)



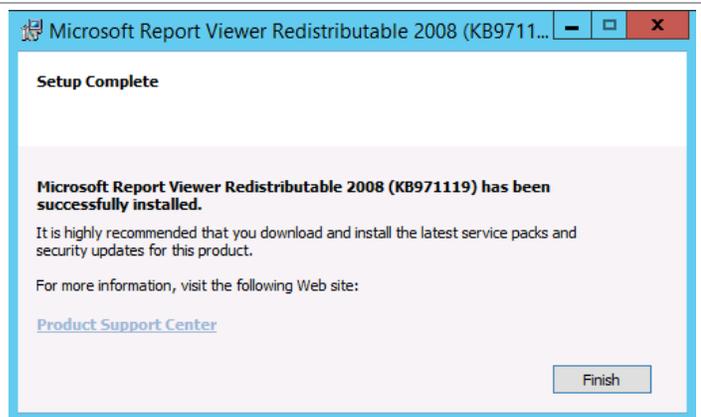
The Setup Wizard will appear. Click **Next** to continue.



On the **License Terms** page, select the **I have read and accept the license terms** check box. Click **Install** to begin the installation.



When the setup is complete, click **Finish**.



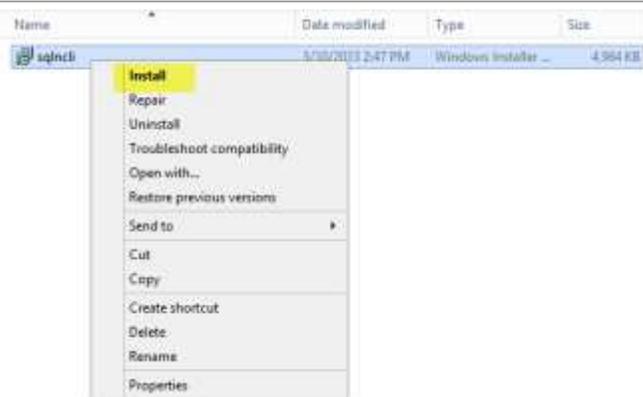
Install SQL Server 2012 Native Client on the Management and Data Warehouse Servers

The Server Manager management server and data warehouse server installations also require that SQL Server 2012 Native Client is installed prior to installation. Use the following procedure to install SQL Server 2012 Native Client.

- ▶ Perform the following steps on the Server Manager management server and on the data warehouse server virtual machines.

From the installation media source, right-click **SQLNCLI.MSI** and select **Install** to begin setup.

Note: Download SQL Server 2012 SP1 Native Client installer, 1033\x64\sqlncli.msi, from the Microsoft Download Center: [Microsoft SQL Server 2012 SP1 Feature Pack](#).



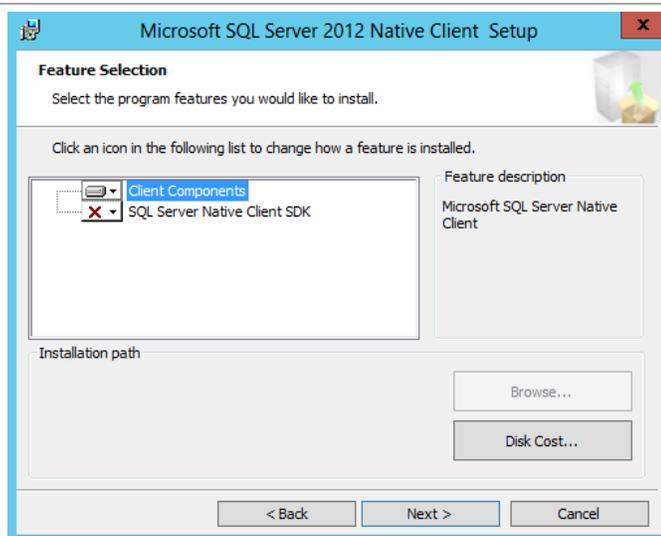
The setup wizard will appear. Click **Next** to continue.



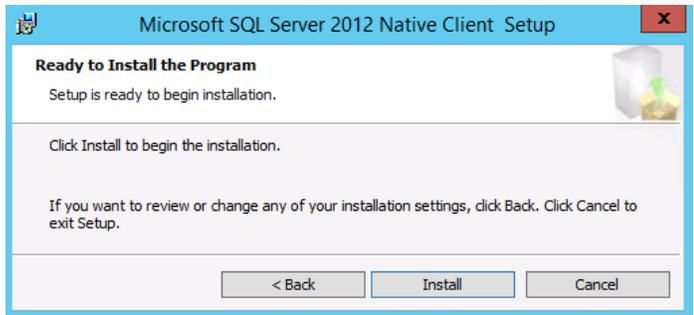
On the **License Terms** page, select the **I accept the terms in the license agreement** check box. Click **Next** to continue.



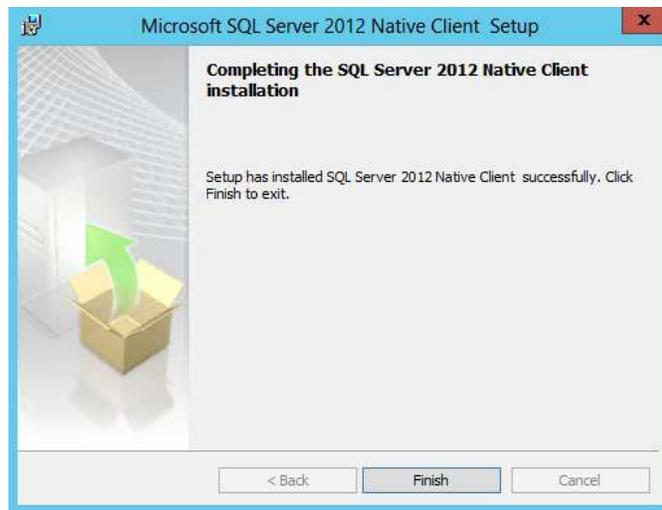
On the **Feature Selection** page, verify that **Client Components** is selected for installation. Click **Next** to continue.



On the **Ready to Install the Program** page, click **Install** to begin the installation.



When complete, click **Finish**.



Install SQL Server 2012 SP1 Analysis Management Objects

The Server Manager management server and data warehouse server installations also requires SQL Server 2012 SP1 Analysis Management Objects. Use the following procedure to install the SQL Server 2012 SP1 Analysis Management Objects.

- ▶ Perform the following steps on the Server Manager management server and on the data warehouse server virtual machines.

From the **SQL Server 2012 SP1 Analysis Management Objects** installation media source, double-click **SQL_AS_AMO.MSI** to begin setup.

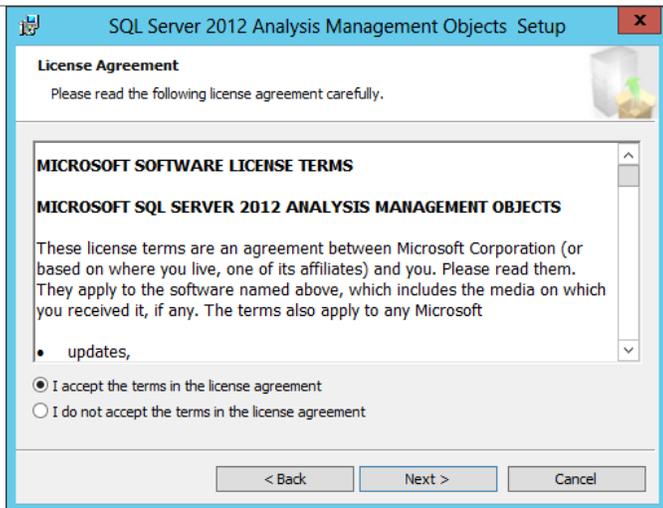
Note: Download the SQL Server 2012 SP1 Analysis Management Objects installer, **SQL_AS_AMO.MSI**, from the Microsoft Download Center: [Microsoft SQL Server 2012 SP1 Feature Pack](#).

Name	Date modified	Type	Size
SQL_AS_AMO	3/7/2013 11:04 AM	Windows Installer Package	3,604 KB

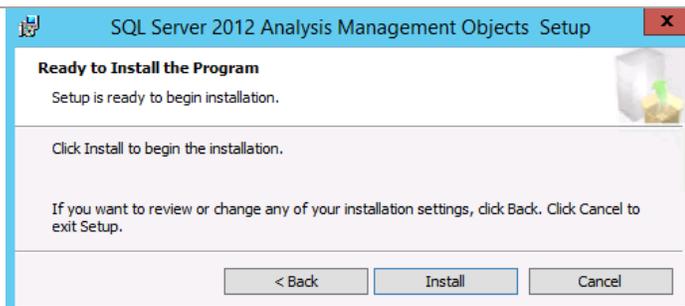
The Setup Wizard will appear. On the **Welcome** page, click **Next** to continue.



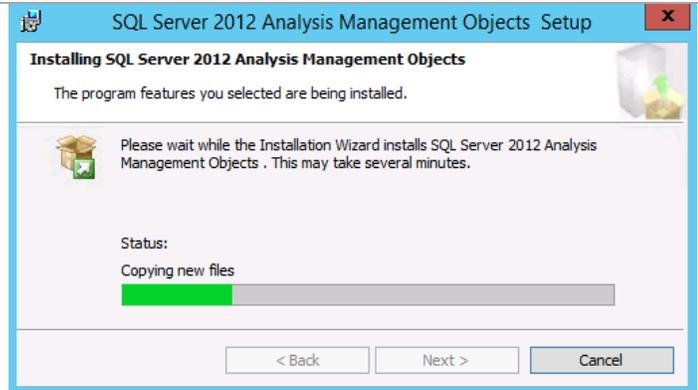
On the **License Agreement** page, review the license agreement, and select the **I accept the terms in the license agreement** button. Click **Next** to continue.



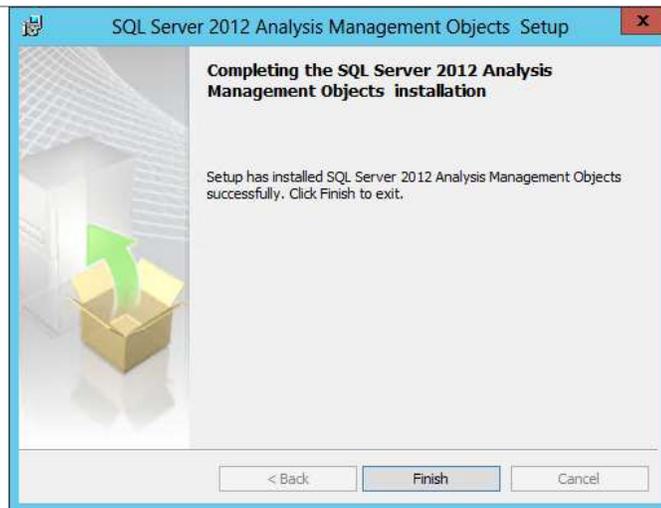
On the **Ready to Install the Program** page, click **Install** to begin the installation.



The installation process may take several minutes to complete. The progress is displayed in the status bar.



On the **Completing the SQL Server 2012 Analysis Management Objects** installation page, click **Finish**.

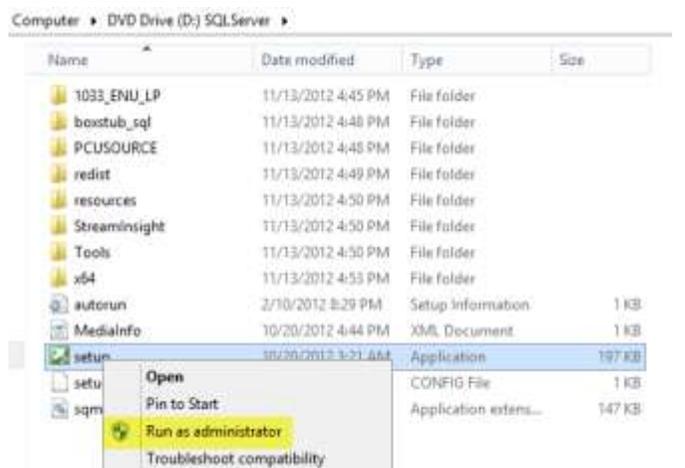


Install SQL Server Reporting Services (Split Configuration) on the Data Warehouse Server

The Service Manager data warehouse installation requires that SQL Server Reporting Services is installed to support the Service Manager reporting features. Use the following procedure to install SQL Server Reporting Services.

► Perform the following steps on the Service Manager data warehouse virtual machine.

From the SQL Server 2012 installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



The **SQL Server Installation Center** will appear. Select the **Installation** menu option.

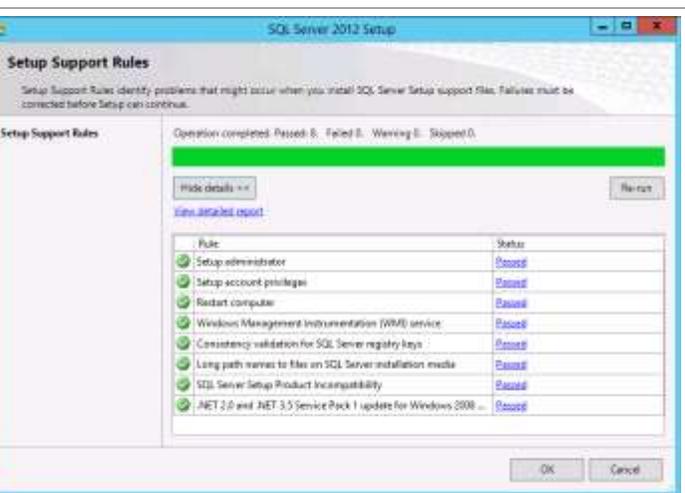


From the **SQL Server Installation Center**, click the **New SQL Server stand-alone installation or add features to an existing installation** link.

 [New SQL Server stand-alone installation or add features to an existing installation](#)

Launch a wizard to install SQL Server 2012 in a non-clustered environment or to add features to an existing SQL Server 2012 instance.

The **SQL Server 2012 Setup Wizard** will appear. On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **OK** to continue.



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

Rule Name	Rule Description	Result	Message/Correction Action
CheckDefaultSQLServer2012SetupConfigurationChecksForRulesGroupDefault	This rule determines whether the computer has the required system package for .NET Framework 4.5 or .NET Framework 4.5 SP1 that is needed for a successful installation of most Studio components that are included in SQL Server.	Not applicable	This rule does not apply to your system configuration.
ServerInstanceDefault	Checks if this version of SQL Server is valid.	Not applicable	This rule does not apply to your system configuration.
ServerInstanceDefaultCheck	Checks if this version of SQL is supported on the currently running Microsoft Windows Core OS.	Not applicable	This rule does not apply to your system configuration.
SQLServerInstanceCheck	Checks if the SQL Server registry keys are consistent.	Passed	SQL Server registry keys are consistent and are correct for SQL Server installation or upgrade.
MicrosoftSQLServerDefaultGroupCheck	Checks whether the account that is running SQL Server setup has the right to back up files and directories, the right to manage auditing and the security log and the right to delete programs.	Passed	The account that is running SQL Server setup has the right to back up files and directories, the right to manage auditing and security logs and the right to delete programs.
ProductLanguage	Checks whether the SQL Server installation media is not too long.	Passed	The SQL Server installation media is not too long.
InstallationStorage	This rule determines whether the computer has the required system package for .NET Framework 4.5 or .NET Framework 4.5 SP1 that is needed for a successful installation of most Studio components that are included in SQL Server.	Passed	This computer has the required update settings.
InstallationCheck	Checks if a pending computer update is required. A pending update can cause setup to fail.	Passed	The computer does not require a update.
SetupCompatibilityCheck	Checks whether the current version of SQL Server is compatible with a later installed version.	Passed	Setup has not detected any incompatibilities.
ServiceAccountDefaultGroupCheck	Checks whether the account running SQL Server Setup has administrator rights on the computer.	Passed	The account running SQL Server Setup has administrator rights on the computer.
InstanceAccountCheck	Checks whether the SQL Server instance is started and running on the computer.	Passed	The Instance Management Administration (IMC) service is running.

On the **Product Key** page, select the **Enter the product key** option and type the associated product key in the provided text box. Click **Next** to continue.

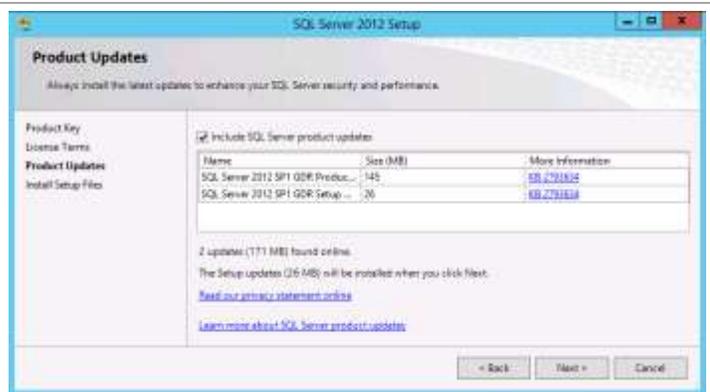
Note: If you do not have a product key, select the **Specify a free edition** option, and select **Evaluation** from the drop-down list for a 180-day evaluation period.



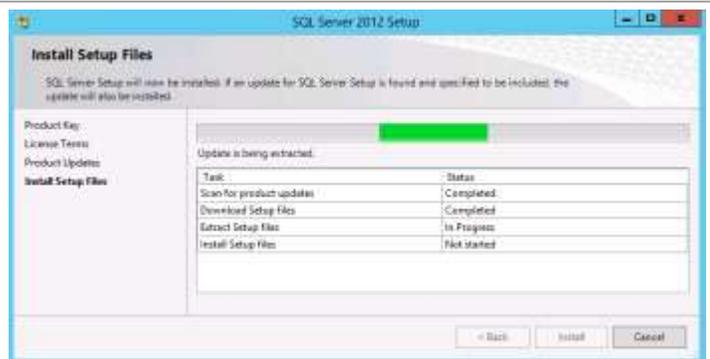
On the **License Terms** page, select the **I accept the license terms** check box. Select or clear the **Send feature usage data to Microsoft** check box, based on your organization's policies and click **Next** to continue.



On the **Product Updates** page, select the **Include SQL Server product updates** check box, and click **Next** to continue.



On the **Install Setup Files** page, click **Install** and allow the support files to install.



On the **Setup Support Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check.

Note: Common issues include MSDTC, MSCS, and Windows Firewall warnings. The use of MSDTC is not required for the System Center 2012 R2 environment. Click **Next** to continue.



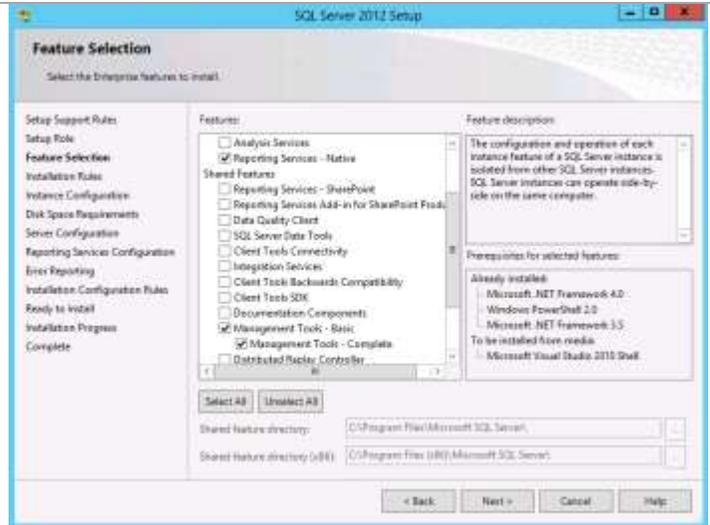
On the **Setup Role** page, select the **SQL Server Feature Installation** button, and click **Next** to continue.



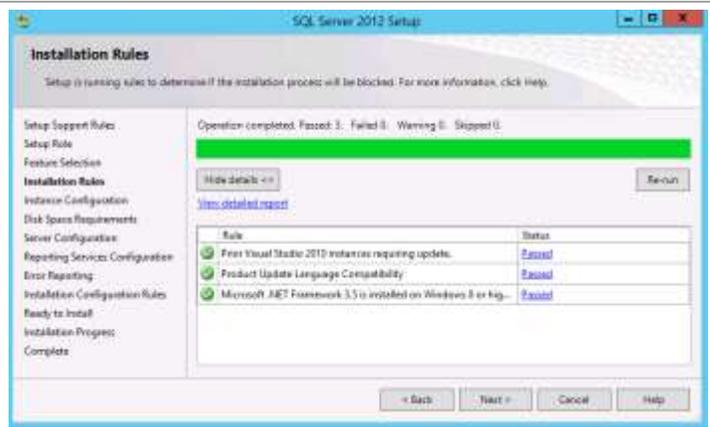
On the **Feature Selection** page, select the following check boxes:

- **Reporting Services - Native**
- **Management Tools – Basic**
- **Management Tools – Complete**

When all selections are made, click **Next** to continue.

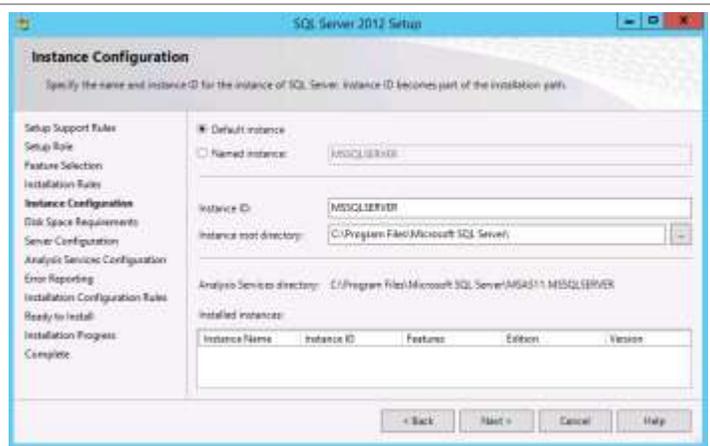


On the **Installation Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



On the **Instance Configuration** page, select the **Default instance** option, and accept the default options for **Instance ID** and **Instance root directory** values. Click **Next** to continue.

Note: A post-installation configuration process will occur to configure the reporting server database within the Service Manager data warehouse SQL Server instance.



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



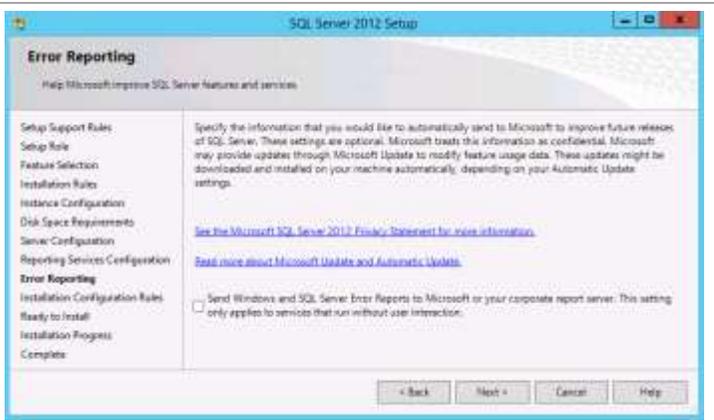
On the **Server Configuration** page, select the **Service Accounts** tab. In the **Account Name** drop-down list, enter the **NT AUTHORITY\NETWORK SERVICE** account for the SQL Server Reporting Services service. Click **Next** to continue.



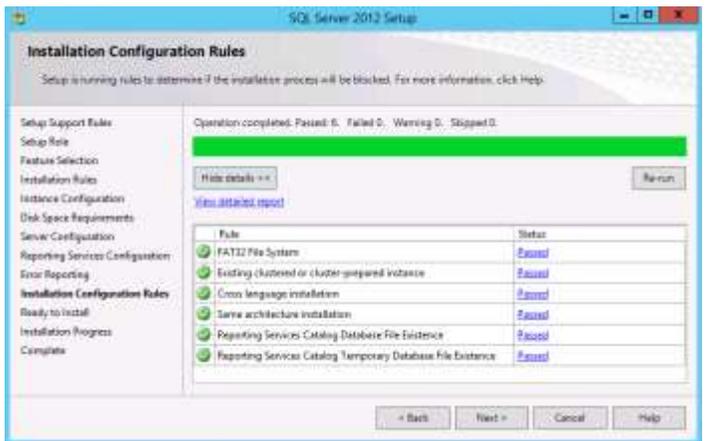
On the **Reporting Services Configuration** page, select the **Install only** option. Note that other options should not be available because the database engine was not selected as a feature for installation. Click **Next** to continue.



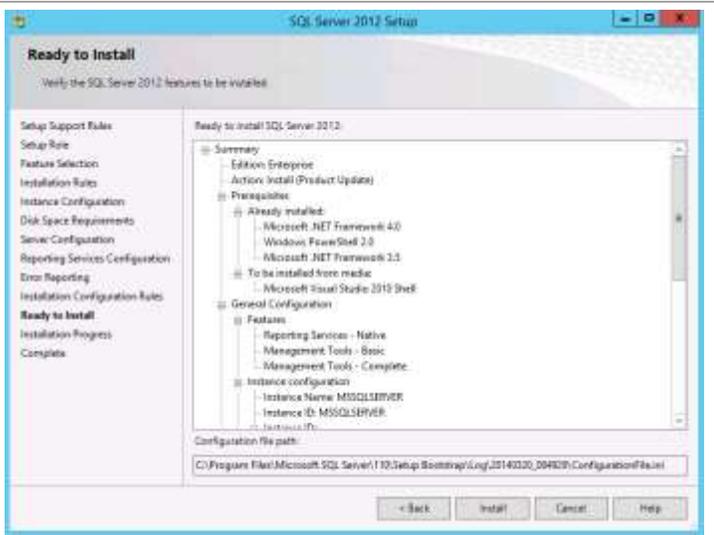
On the **Error Reporting** page, select or clear the **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** check box, based on your organization's policies and click **Next** to continue.



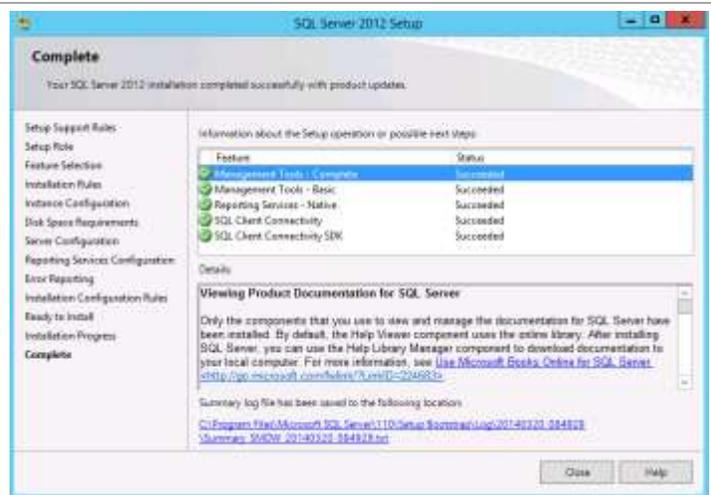
On the **Installation Configuration Rules** page, verify that each rule shows a **Passed** status. If any rule requires attention, remediate the issue and rerun the validation check. Click **Next** to continue.



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

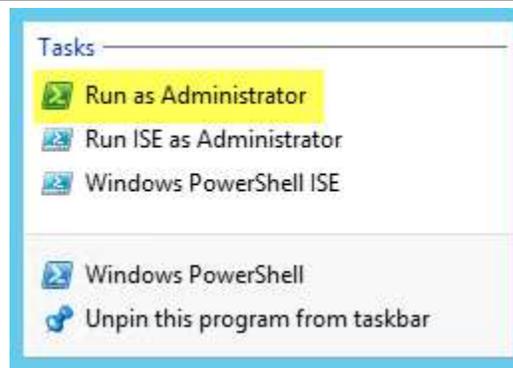


When the **Complete** page appears, click **Close** to complete the installation of this SQL Server database instance.



By default, Windows Firewall does not allow traffic for SQL Server services or for the SSRS Web Service. Firewall exceptions need to be created if the Windows Firewall is enabled.

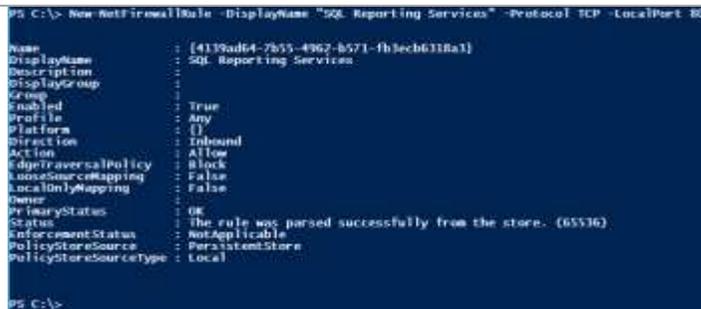
To create exceptions, open an administrative session of Windows PowerShell.



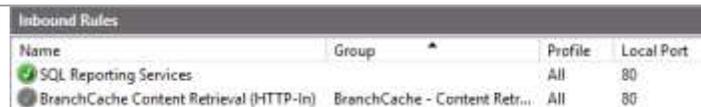
Run the following commands to create the needed firewall rules:

New-NetFirewallRule -DisplayName "SQL Reporting Services" -Protocol TCP -LocalPort 80

Adjust the display names and ports based on organizational requirements.



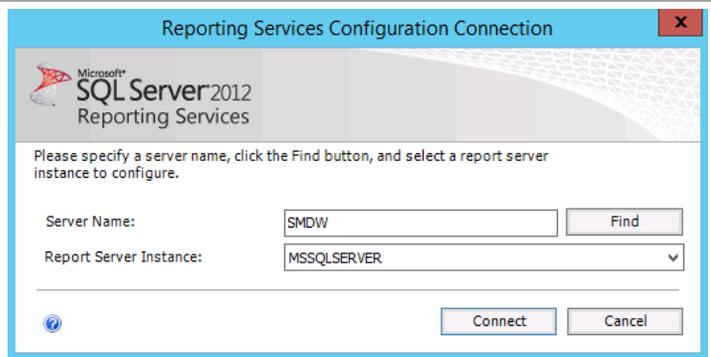
Open the **Windows Firewall with Advanced Security** MMC console to verify the results. When verified, close the MMC console.



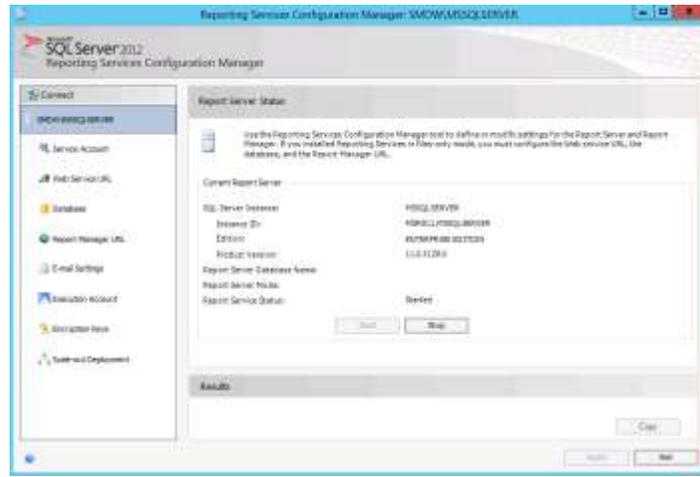
Verify that SQL Server Reporting Services installed properly by opening the console: on the **Start** screen, click the **Reporting Services Configuration Manager** tile.



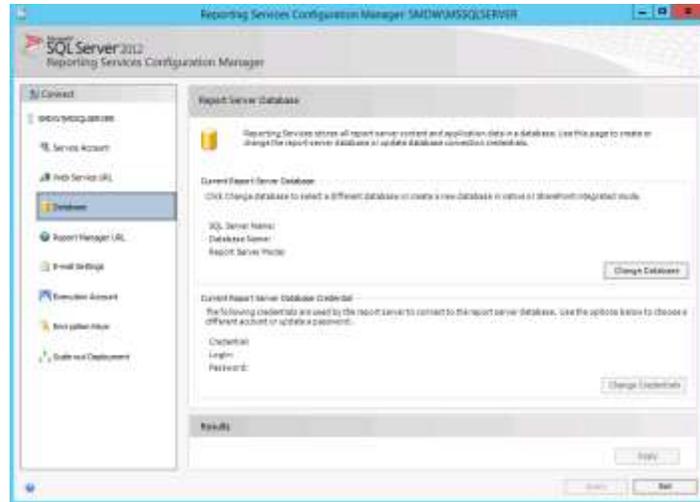
The **Reporting Services Configuration Connection** page will appear. In the **Server Name** text box, specify the name of the Service Manager server. In the **Report Server Instance** text box, use the default **MSSQLSERVER** value from the drop-down list. Click **Connect**.



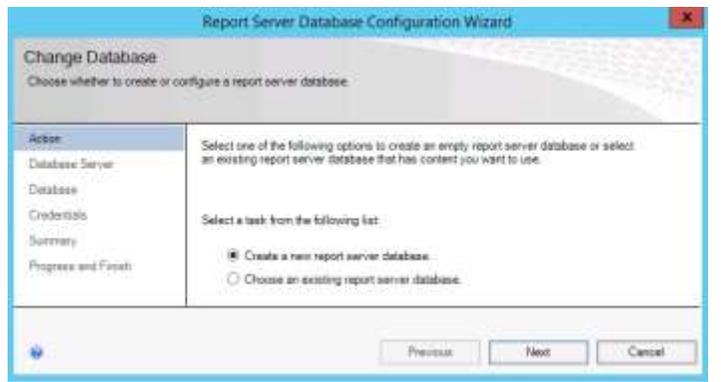
The **Reporting Services Configuration Manager** will appear.



In **Reporting Services Configuration Manager**, click the **Database** option in the left pane. In the **Current Report Server Database** section, click the **Change Database** button.



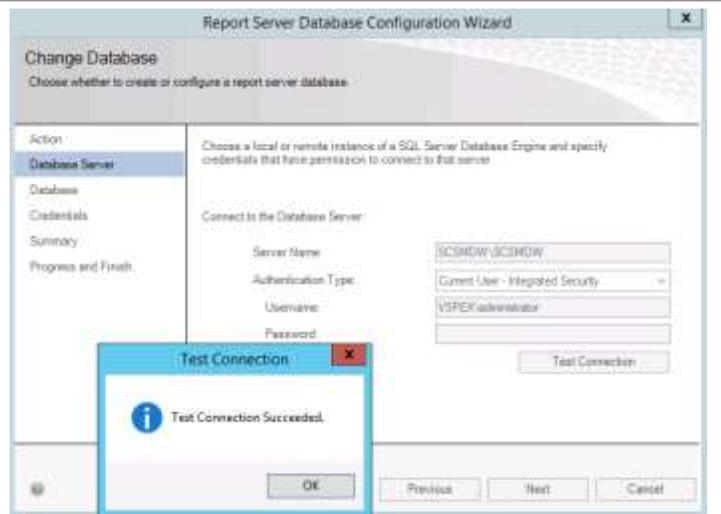
The Reporting Services Database Configuration Wizard will appear. In the **Action** section, select **Create a new report server database**. Click **Next** to continue.



In the **Database Server** section, specify the following values:

- **Server Name** – Specify the name of the SQL Server Cluster **SCSMDW** instance cluster name object and the database instance created for the Service Manager data warehouse installation.
- **Authentication Type** – Specify **Current User - Integrated Security** from the drop-down list.

Click the **Test Connection** button to verify the credentials and database connectivity. When verified, click **Next** to continue.



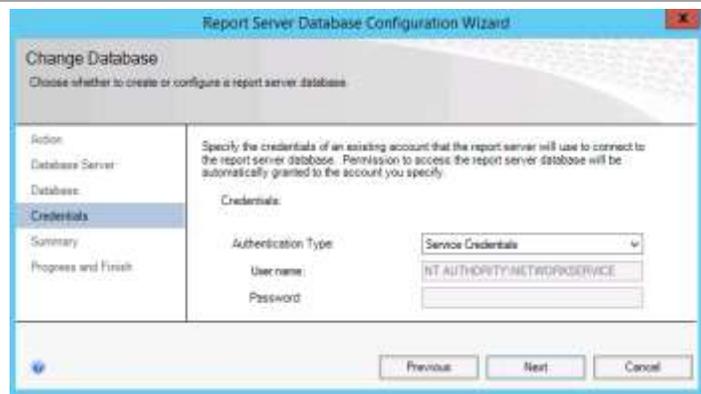
In the **Database** section, specify the following values:

- **Database Name** – Accept the default value of **ReportServer**.
- **Language** – Specify the desired language option from the drop-down list.

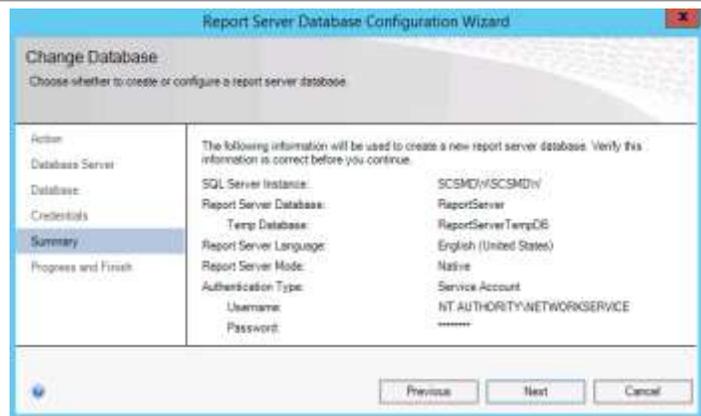
Click **Next** to continue.



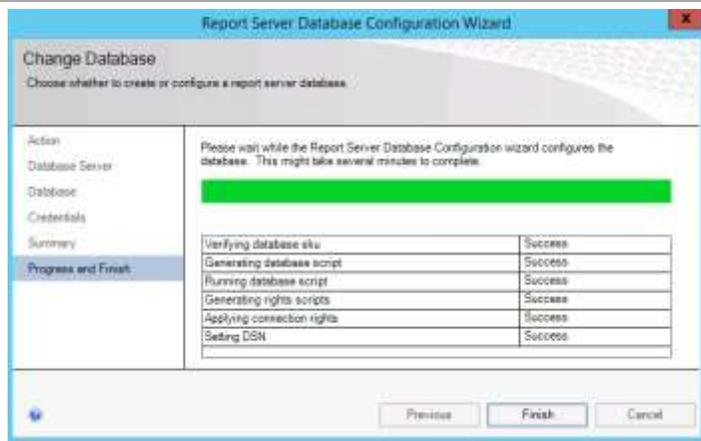
In the **Credentials** section, specify the **Authentication Type** as **Service Credentials** from the drop-down list, and click **Next** to continue.



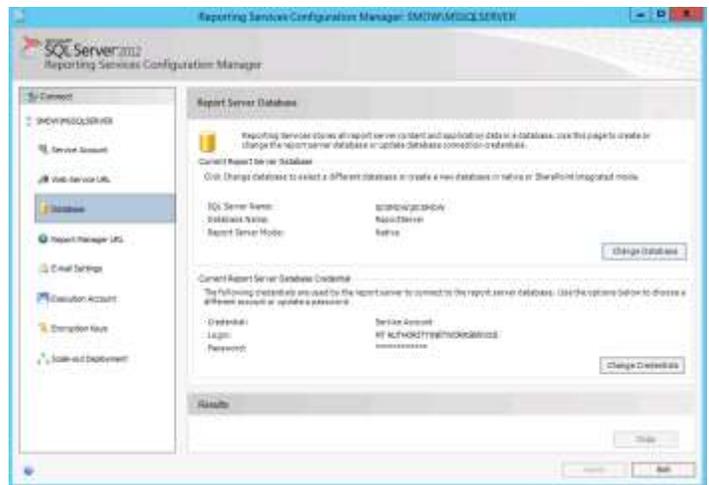
In the **Summary** section, review the selections made, and click **Next** to create the SQL Server Reporting Services database.



The **Progress and Finish** section will display the progress of the database creation. Review the report to verify successful creation, and then click **Finish**.

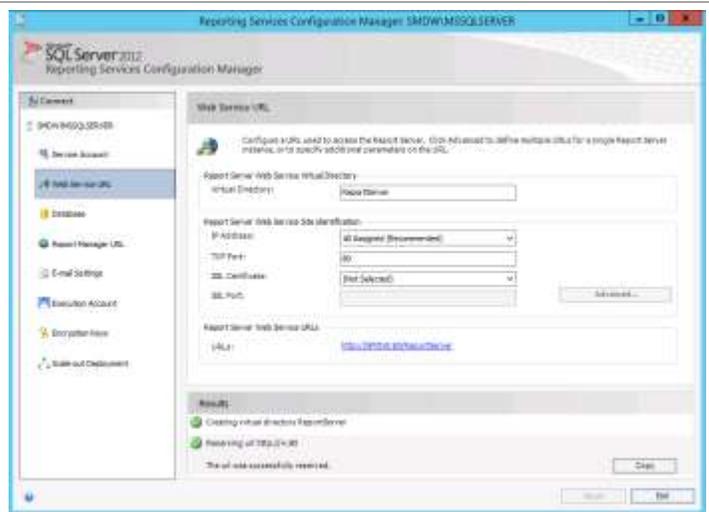


In **Reporting Services Configuration Manager**, the **Database** option will now display the database and report server database credentials specified in the wizard.



In **Reporting Services Configuration Manager**, 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** – Select **All Assigned** in the drop-down list.
 - **TCP Port** – Specify the desired TCP port (default is 80).
 - **SSL Certificate** – Select the available certificate or choose the default (**Not Selected**).

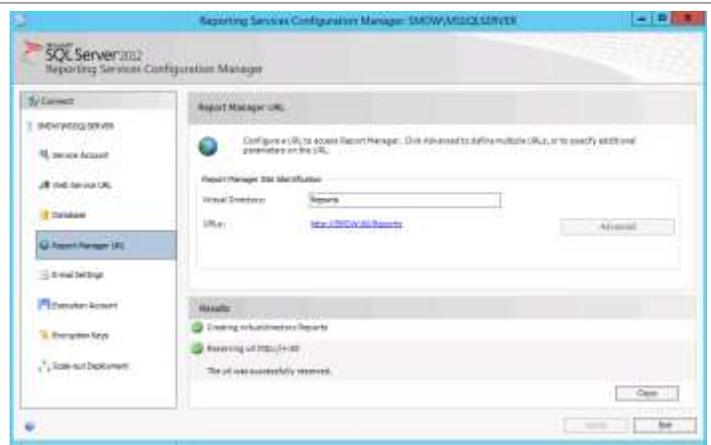


Click **Apply** to save the settings and create the Web Service URL.

In **Reporting Services Configuration Manager**, click the **Report Manager URL** option in the toolbar. Specify the following value:

In the **Report Manager Site Identification** section, keep the default **Virtual Directory** value, **Reports**, in the provided text box.

Click **Apply** to save the setting and create the Report Manager URL.



Connect to the Report Manager URL from a web browser to verify that the SQL Server Reporting Services portal is operating properly.



Connect to the Web Service URL from a web browser to verify that the SQL Server Reporting Services web service is operating properly.

Note: To test the URL directory from the Service Manager server, Internet Explorer Enhanced Security Configuration needs to be temporarily disabled.



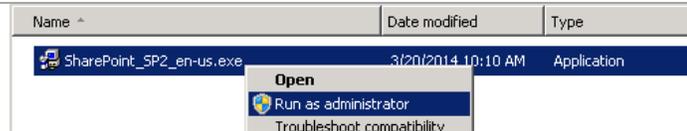
Close the Reporting Server Configuration Manager.

Install SharePoint Foundation 2010 SP2 on the Self-Service Portal Server

SharePoint Foundation 2010 Service Pack 2 (SP2) must be installed to configure SharePoint with the SQL Server 2012 SP1 installation. Use the following procedure to install SharePoint Foundation 2010 SP2 on the Service Manager self-service portal server only.

- ▶ Perform the following steps on the Service Manager self-service portal virtual machine.
- ▶ This installation requires connection to the Internet to download files.

Log on to the 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 **SharePoint_SP2_en-us.exe**, and click **Run as administrator** to begin setup.



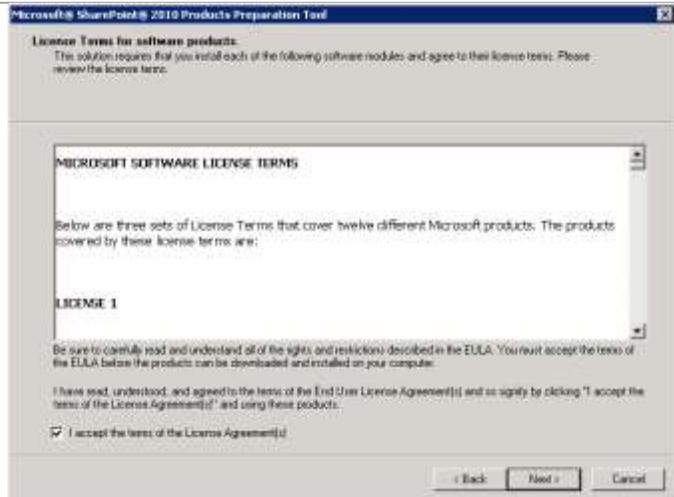
The **SharePoint Foundation 2010** setup page will appear. In the **Install** section, click **Install software prerequisites**.



The **Microsoft SharePoint 2010 Products Preparation Tool** will open. Click **Next** to continue.



On the **License Terms for software products** page, verify that the **I accept the terms of the License Agreement** installation option check box is selected, and click **Next** to continue.



After the prerequisites install, the **Installation Complete** page will appear. Click **Finish** to complete the installation, and then restart the system.



After the system restart, log on with an account with administrative privileges, and open the SharePoint Foundation 2010 setup page. In the **Install** section, click **Install SharePoint Foundation**.



On the **Read the Microsoft Software License Terms** page, verify that the **I accept the terms of this Agreement installation** option check box is selected, and click **Continue**.



On the **Choose the installation you want** page, click the **Server Farm** button.



On the **Server Type** page, select the **Complete** option, and click **Install Now**.



After installation, the Run Configuration Wizard will appear. Verify that 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.



A message will appear that states some services require a restart as part of the installation. Click **Yes** to restart the services.



On **Connect to a server farm** page, select **Create a new server farm**, and click **Next** to continue.



On the **Specify Configuration Database Settings** page, specify the following information in the provided text boxes:

- **Database server** – Specify the name of the SQL Server cluster name object and the database instance created for the Service Manager installation.
- **Database name** – Specify the name of the SharePoint database. In most cases, use the default value of SharePoint_Config.

In the **Specify Database Access Account** section, specify the Username in the form (<DOMAIN>\<USERNAME>) and an associated password for the Service Manager service account. Click **Next** to continue.



On the **Specify Farm Security Settings** page, enter a unique passphrase in the **Passphrase** text box. Retype the passphrase in the **Confirm passphrase** text box, and click **Next** to continue.



On the **Configure SharePoint Central Administration Web Application** page, click the **Specify port number** check box, and provide a port number in the provided text box. In the **Configure Security Settings** section, select the **NTLM** option. Click **Next** to continue.



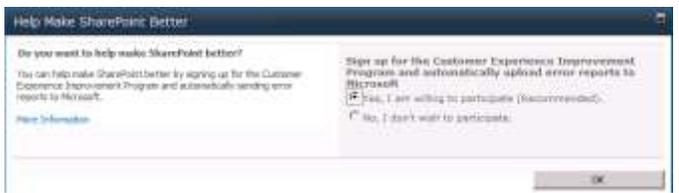
The wizard will display the progress while performing the SharePoint configuration.



When the **Configuration Successful** page appears, click **Finish** to complete the configuration of SharePoint Foundation 2010 Service Pack 2.



When prompted in the **Help Make SharePoint Better** page, select the appropriate option based on your organization's policies, and click **OK** to save this setting.



On the **Central Administration - Configure your SharePoint farm** page, click the **Start the Wizard** button to begin the SharePoint configuration.



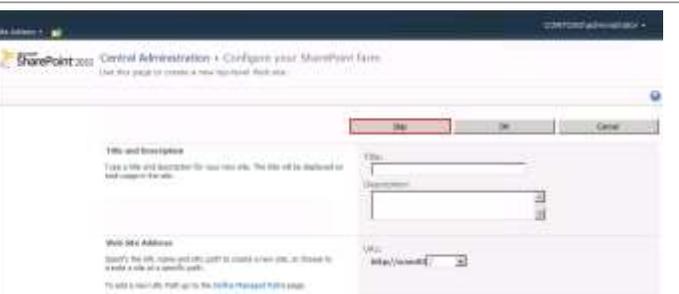
In the **Service Account** section, select **Use existing managed account**, and select the SQL Service account from the drop-down list.

In the **Services** section, select the **Business Data Connectivity Services** and **Usage and Health data collection** check boxes.

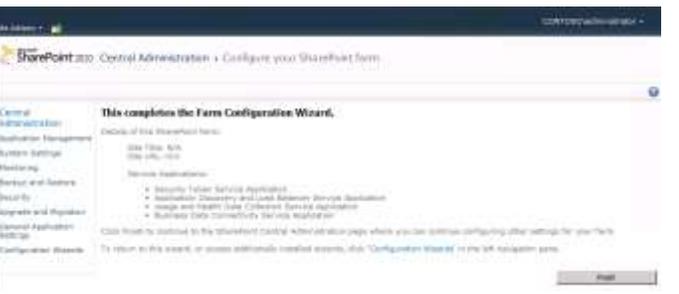


Click **Next** to continue.

On the website 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 wizard.



The **SharePoint Central Administration** portal will open. Verify that SharePoint is operating properly by opening the Central Administration portal prior to proceeding to the Service Manager self-service portal installation.

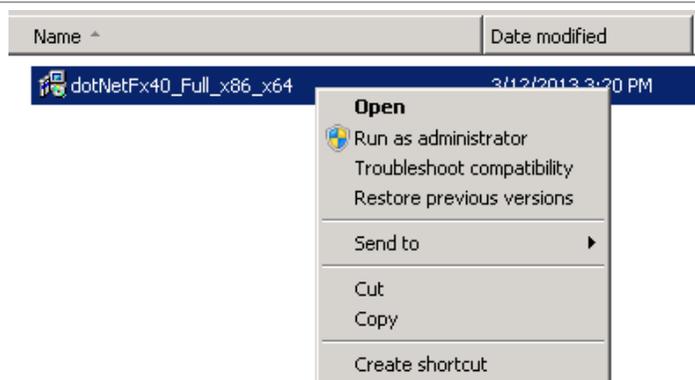


Install .NET Framework 4 on the Self-Service Portal Server

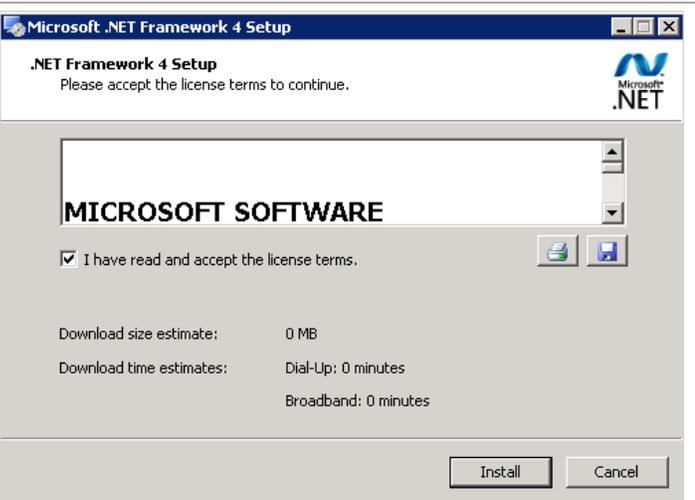
Additionally, the Service Manager self-service portal installation requires that the .NET Framework 4 package is installed. Use the following procedure to install .NET Framework 4 on the self-service portal.

▶ Perform the following steps on the Service Manager self-service portal virtual machine.

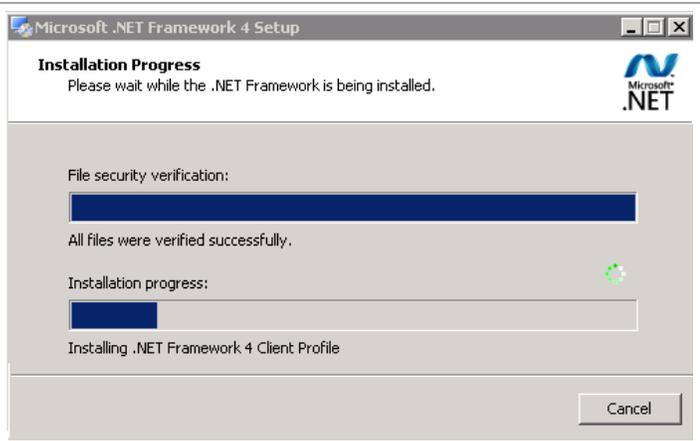
From the installation media source, right-click **dotNetFx40_Full_x86_x64.exe** and select **Run as administrator** to begin setup.



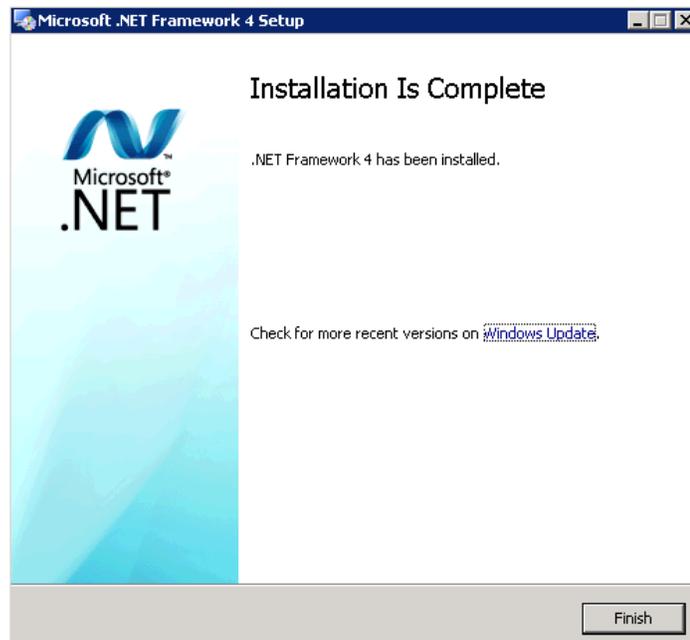
On the **Microsoft .NET Framework 4 Setup** page, select the **I have read and accept the license terms** check box, and click **Install** to begin the installation.



The wizard will display the installation progress.



When the installation is complete, click **Finish**.



Request and Install an SSL Certificate on the Self-Service Portal Server

Additionally, the Service Manager self-service portal installation requires a secure socket layer (SSL) certificate to enable SSL on the portal website. If you are installing the self-service portal without SSL, you can skip this section. There are several ways to request an SSL certificate. The following procedure describes how to request the certificate through the IIS Manager console. This procedure assumes that you are running a Certificate Authority within your environment. If you are using externally requested certificates, your procedure will be different.

► Perform the following steps on the Service Manager self-service portal virtual machine.

Log on to the Service Manager self-service virtual machine as a user with local Admin rights. From the Start menu, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.



In the **Internet Information Services (IIS) Manager** console, click the server node, and in the IIS section, double-click **Server Certificates**.



The **Server Certificates** pane will expand. In the **Actions** pane, click **Create Domain Certificate ...**



The **Create Certificate Wizard** will appear. On the **Distinguished Name Properties** page, complete the information as prompted.

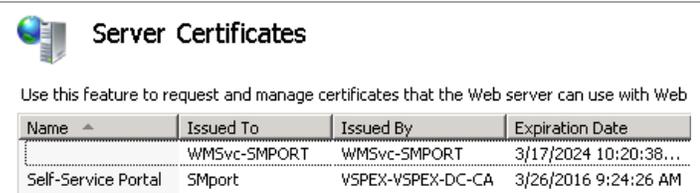
Note: The **Common Name** field must equal the exact name of the server as it will be accessed from the web browser. Click **Next** to continue.



On the **Online Certificate Authority** page, specify the name of your online certificate authority and a friendly name for the certificate. Click **Finish** to continue.



In the IIS Manager you will see the newly issued certificate.



Configure Service Manager Environmental Prerequisites

Complete the following procedures to install the Service Manager roles correctly.

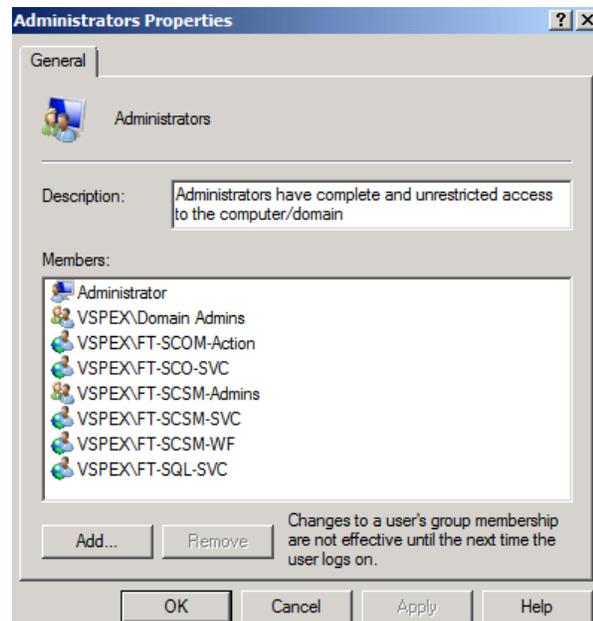
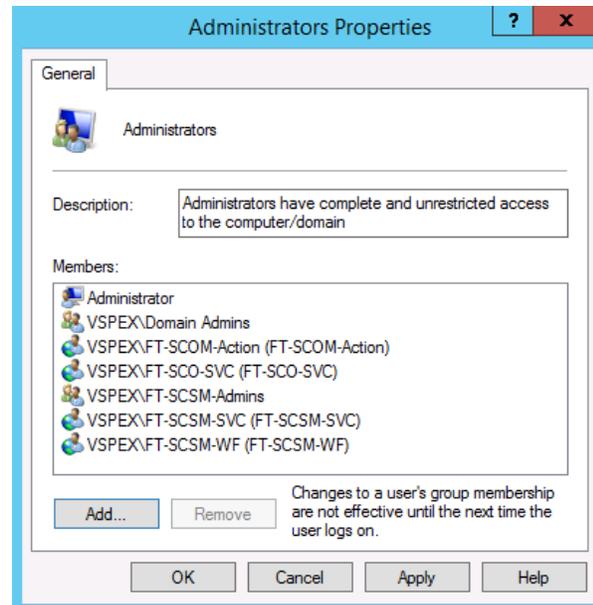
► Perform the following steps on **all** Service Manager Servers virtual machines.

Log on to each Service Manager virtual machine as a user with local Admin rights. Verify that the following accounts or groups are members of the local Administrators group on each Service Manager virtual machine:

- Operations Manager action account
- Service Manager workflow account
- Service Manager service account
- Service Manager Admins group
- Orchestrator service account

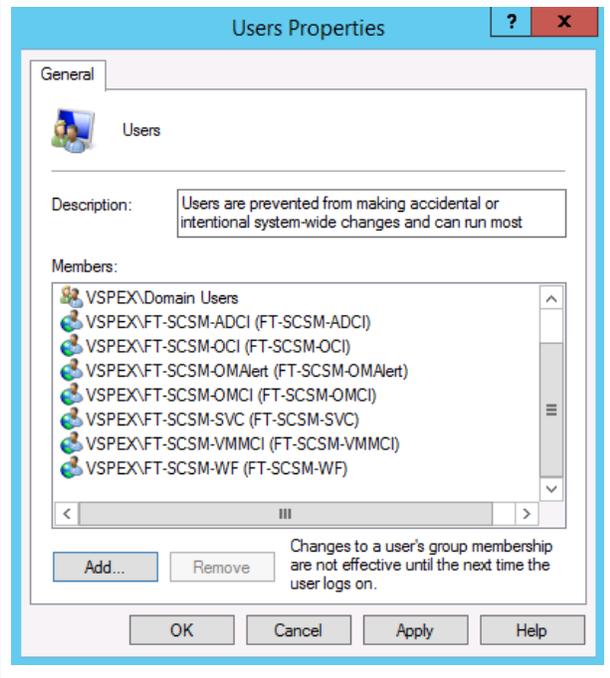
On the self-service portal server, also add the following account:

- SQL Server service account



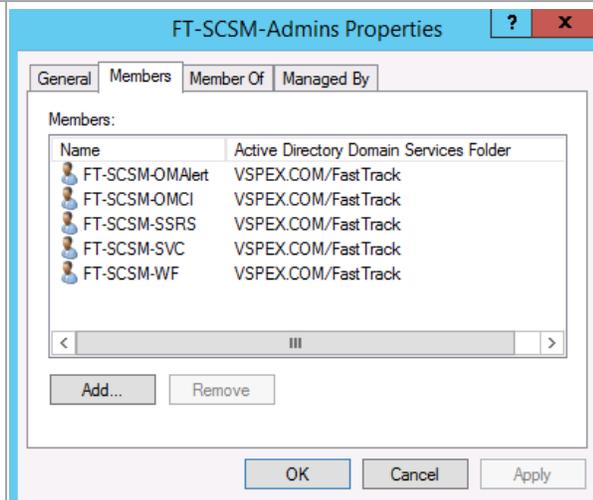
Verify that the following accounts or groups are members of the local Users group on each Service Manager virtual machine:

- 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

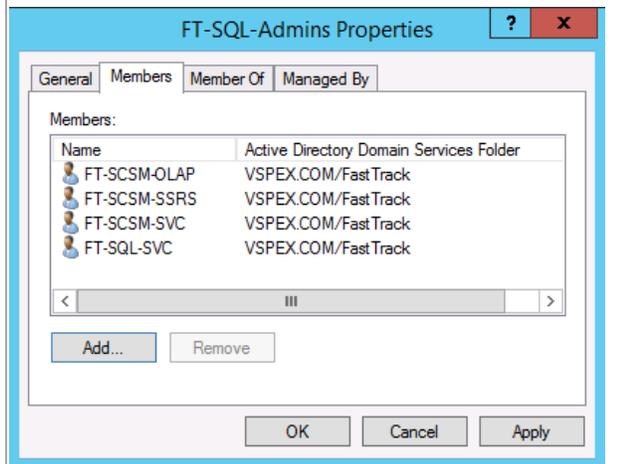


► Perform the following step on an Active Directory domain controller in the target environment.

In the domain where Service Manager will be installed, verify that the Service Manager Operations Manager alert connectors and the Service Manager service accounts are members of the Service Manager Admins group that you created earlier.

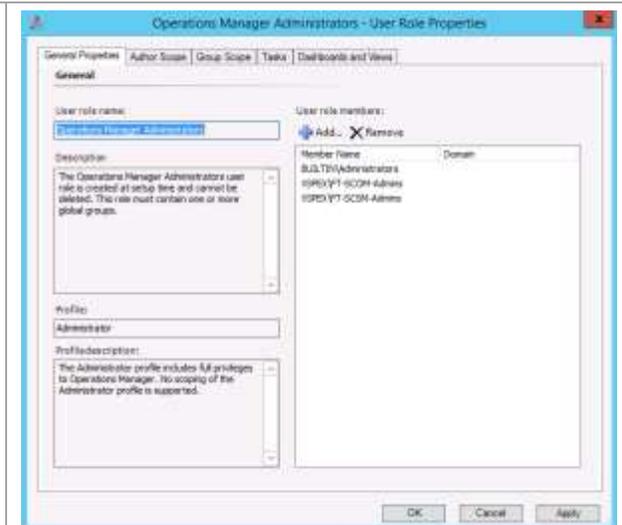


In the domain where Service Manager will be installed, verify that the FT-SCSM-OLAP and the Service Manager reporting accounts are members of the SQL Server Admins group that you created earlier.

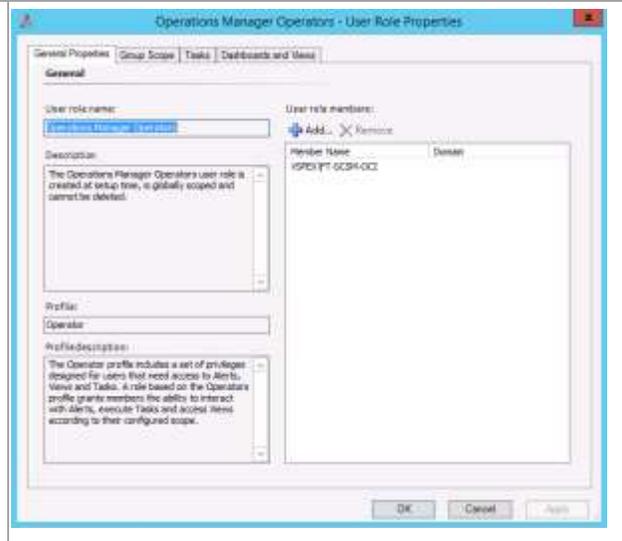


► Perform the following steps on the Operations Manager virtual machine.

Log on to the Operations Manager server as an Administrator. In the **Operations Manager console**, navigate to Administration pane, and click the **Security** node. Under **User Role name**, right-click **Operations Manager Administrators**, select Properties, and add **SCSM Admins**. Click **OK** to save the changes.



While still in the **Security** node under **User Roles**, right-click **Operations Manager Operators**, select **Properties**, and add **SCSM OMCI**. Click **OK** to save the changes.



Installation

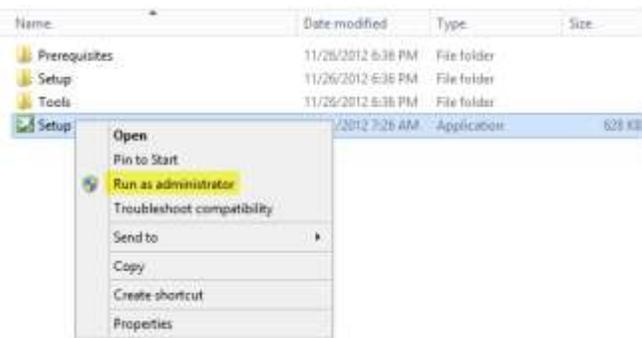
Install the Management Server

Complete the following procedure to install the Service Manager management server role.

- ▶ Perform the following steps on the **first** Service Manager management server virtual machine.

Log on to the 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** to begin setup.

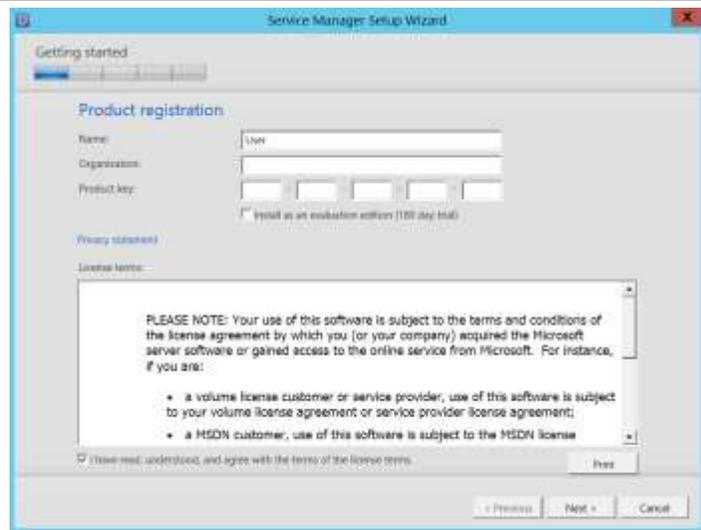


The Service Manager Setup Wizard will appear. In the **Install** section, click **Service Manager management server** to begin the installation.



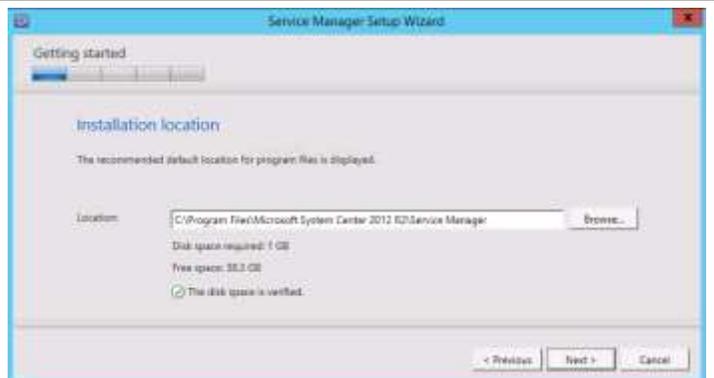
On the **Product registration** page, enter the following information in the provided text boxes:

- **Name** – Specify the name of the primary user or responsible party within your organization.
- **Organization** – Specify the name of the licensed organization.
- **Product key** – Provide a valid product key for installation of Service Manager. If no key is provided, select the **Install as an evaluation edition (180-day trial)** check box.



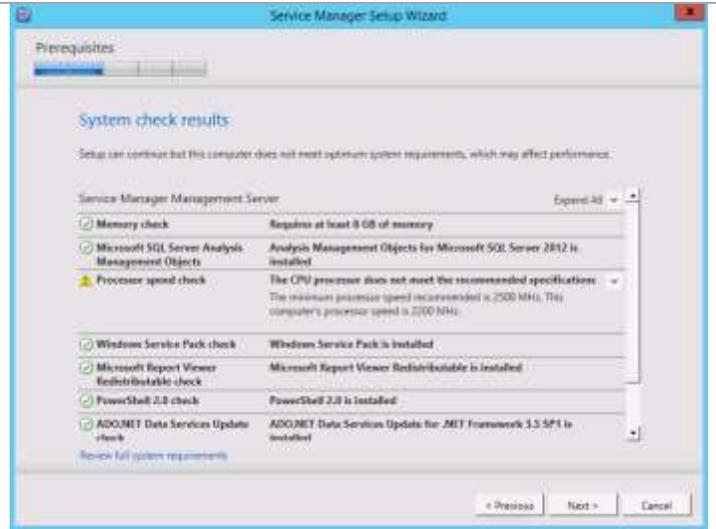
In the License terms section, select the **I have read, understood, and agree with the terms of the license terms** check box. When all selections are confirmed, click **Next** to continue.

On the **Installation location** page, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Service Manager for the installation. Click **Next** to continue.



On the **System check results** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on this page. When verified, click **Next** to continue.

Note: A warning will occur if your processor speed is less than 2500 MHz. With the latest Ivy Bridge processors, this should not be an issue except maybe for the largest of installations.



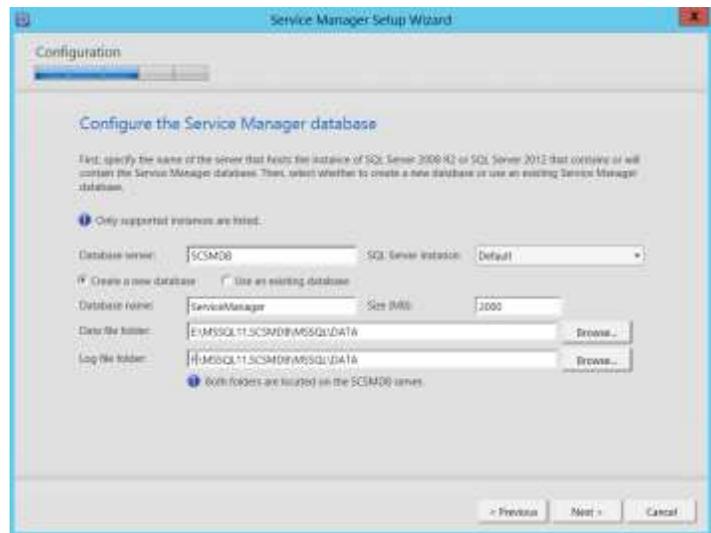
On the **Configure the Service Manager database** page, specify the following information in the provided text boxes:

- **Database server** – Specify the name of the SQL Server cluster name object 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, use the default value ServiceManager.
- **Size (MB)** – Specify the initial database size. The default value can be used. For more information, see [Planning for Performance and Scalability in System Center 2012 - Service Manager](#).
- **Data file folder** – Specify the drive letter associated in the SQL Server cluster data files for the Service Manager database. Cross-check this with the worksheet created earlier.
- **Log file folder** – Specify the drive letter associated in the SQL Server cluster for the log files for the Service Manager database. Cross-check this with the worksheet created earlier.

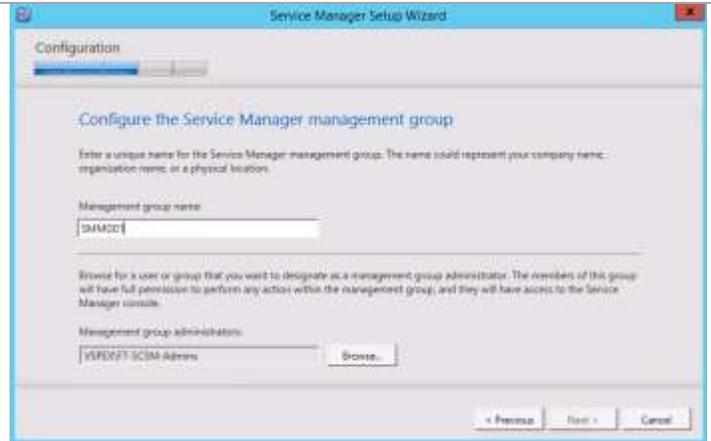
Click **Next** to continue.



On the **Configure the Service Manager management group** page, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 R2 products, such as the Service Manager data warehouse and Operations Manager installations.

In the **Management group administrators** text box, specify the Service Manager Administrators group.

Click **Next** to continue.

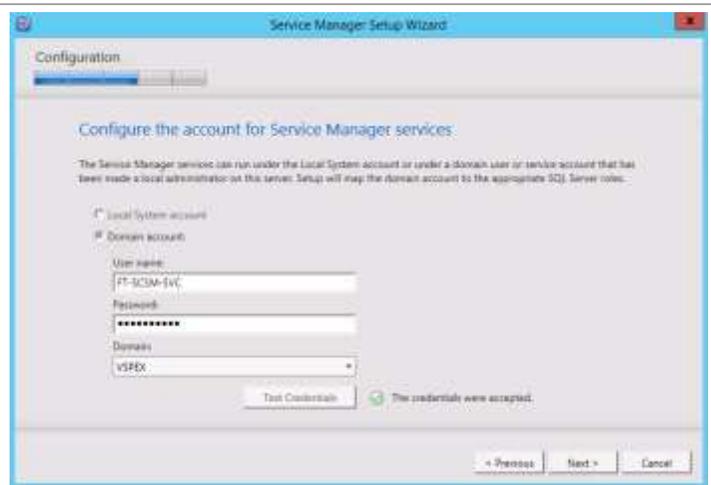


On the **Configure the account for Service Manager services** page:

- Verify that the **Domain account** option is selected.
- In the **User name** text box, specify the Service Manager service account.
- In the **Password** text box, type an appropriate password.
- In the **Domain** text box, select a domain from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



On the **Configure the account for Service Manager workflow account** page:

- Verify that the **Domain account** option is selected.
- In the **User name** text box, specify the Service Manager service account.
- In the **Password** text box, type an appropriate password.
- In the **Domain** text box, select a domain from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



On the **Help improve Microsoft System Center 2012 R2 Service Manager** page, select the option to participate or not participate in the CEIP by providing selected system information to Microsoft. Click **Next** to continue.



Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** page may appear.

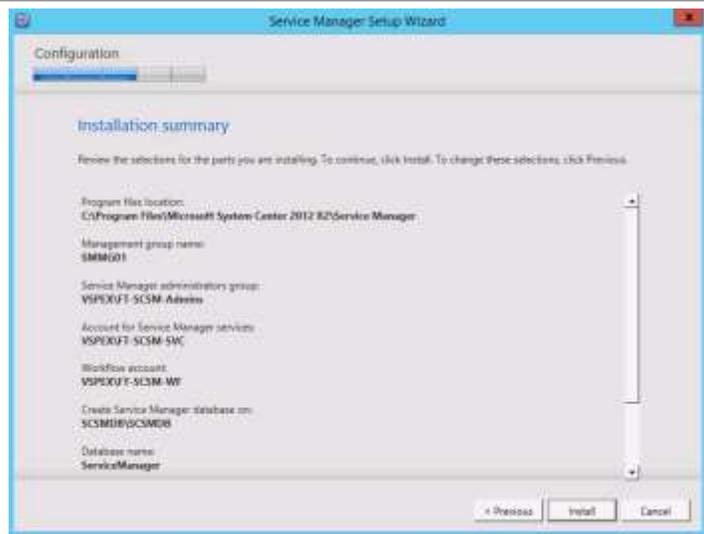
Select the appropriate option to participate or not participate in automatic updating.

Select the **Initiate machine wide Automatic Update** check box.

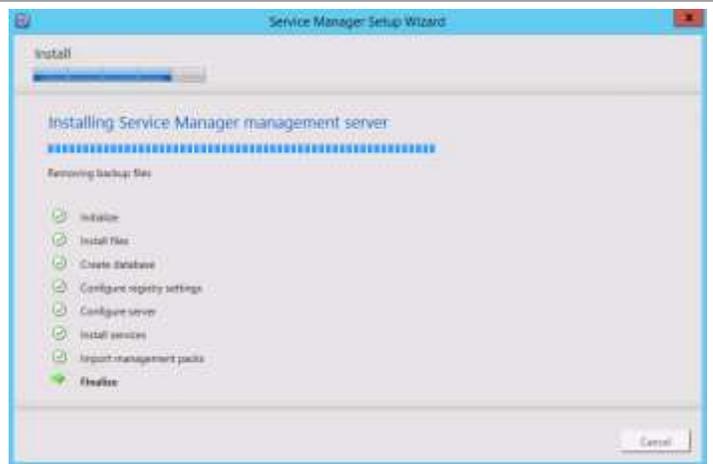
Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.



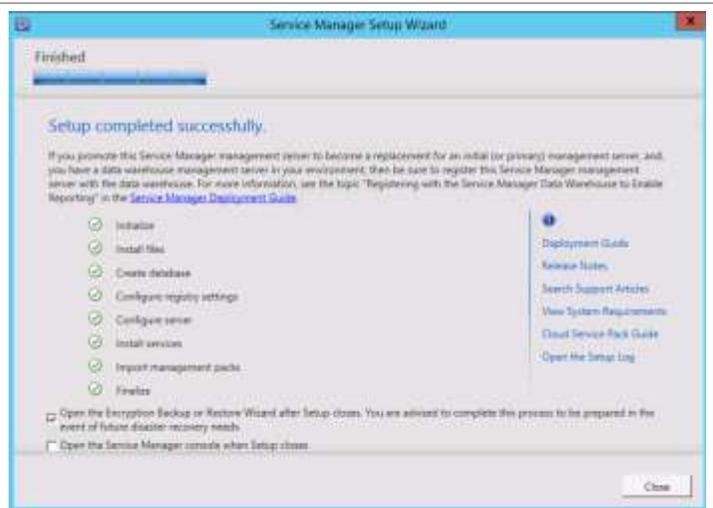
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** page.

When all steps show successful installation, Make sure that the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to open the wizard after setup.

Click **Close** to complete the installation.



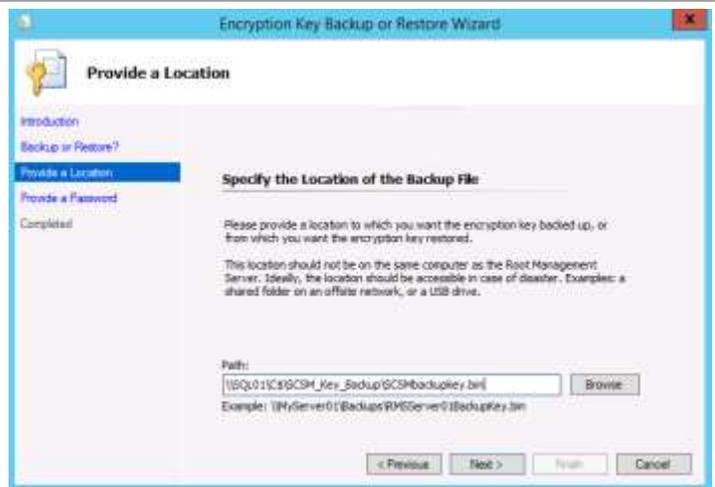
When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. On the **Introduction** page, click **Next** to continue.



On the **Select Action** page, select the **Backup the Encryption Key** option, and click **Next** to continue.



On the **Specify the Location of the Backup File** page, in the **Path** text box select the desired backup file name and path. Note the instructions about suggested location. The destination directory must exist. Click **Next** to continue.



On the **Provide a Password** page, type a desired password in the **Password** text box. Re-type the password in the **Confirm Password** text box, and click **Next** to begin the backup process.



Click **Finish** to exit the wizard.

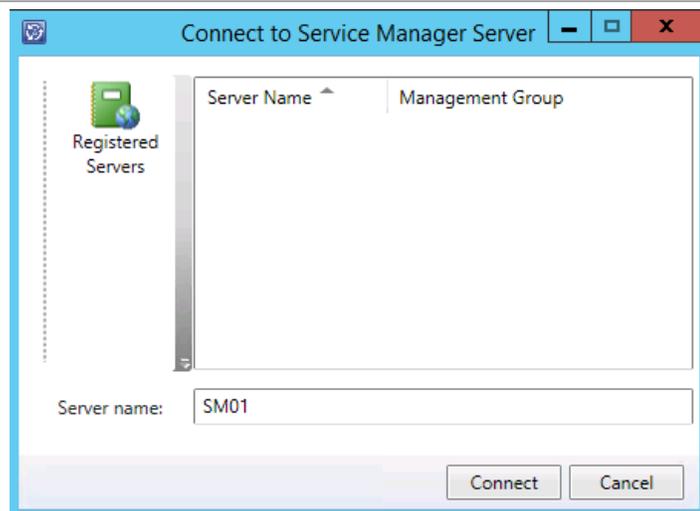
Note: If you receive an error and need to rerun the backup, the backup program is located on the Service Manager installation media at
\\amd64\Tools\SecureStorageBackup\SecureStorageBackup.exe.



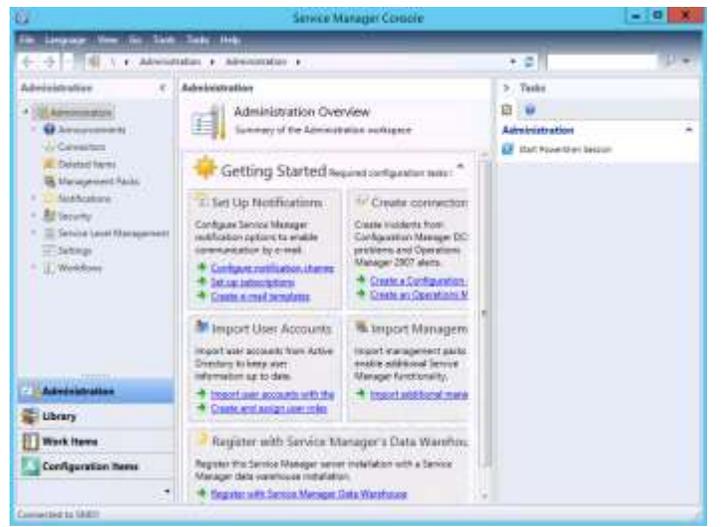
When installed, verify that the Service Manager management server installed properly by opening the console: on the **Start** screen, click the **Service Manager Console** tile.



On the **Connect to Service Manager Server** page, type the Service Manager management server name in the **Server name** text box, and click **Connect** to start the console.



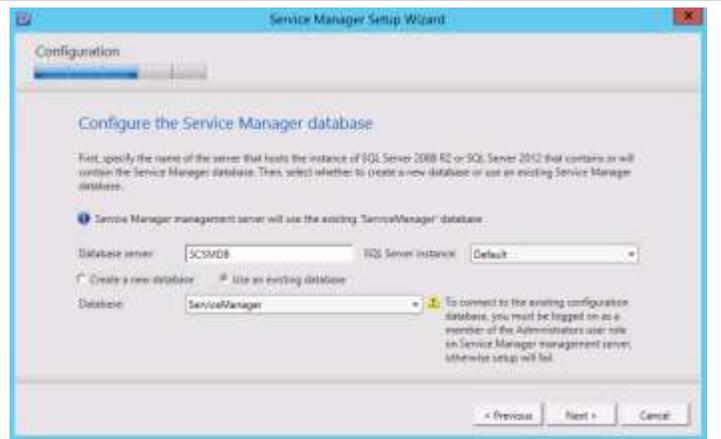
The **Service Manager Console** will open. Validate the installation by reviewing the configuration and make sure that the console operates properly.



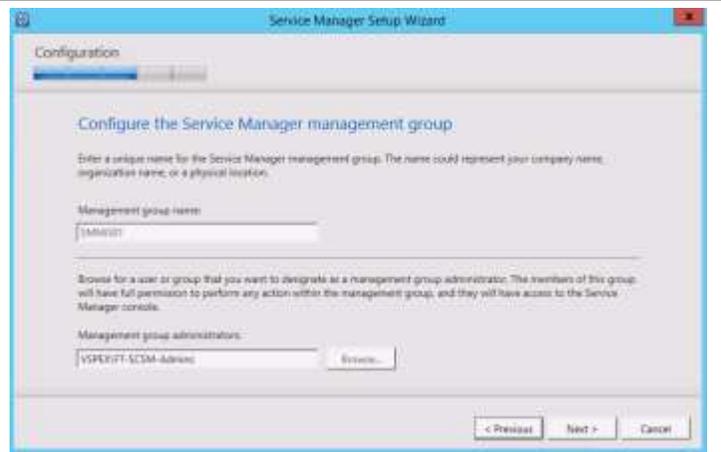
Install Subsequent Management Servers

Repeat the installation process for the second Service Manager Server. The installation is shorter in subsequent installations because the Service Manager database has already been created, so this installation will make use of that database.

When you reach the **Configure the Service Manager database** page, select the radio button for **Use and existing database**. In the Database dropdown list, select **ServiceManager**. Click **Next** to continue.



On the **Configure the Service Manager management group** page, accept the defaults. Click **Next** to continue.



On the **Configure the account for Service Manager services** page:

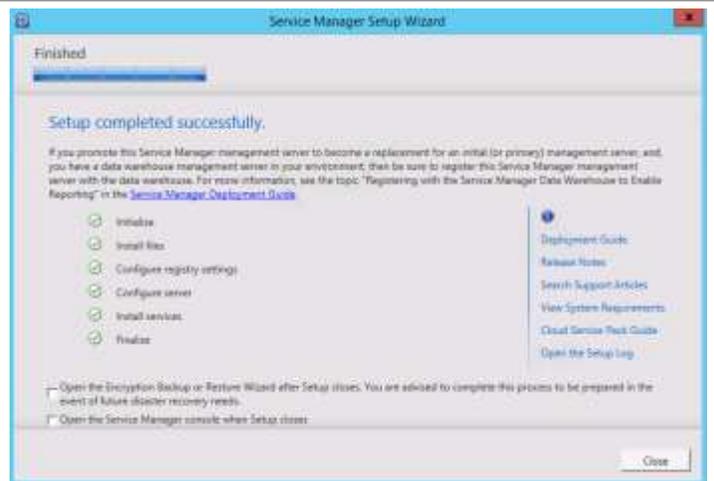
- Verify that the **Domain account** option is selected.
- In the **User name** text box, specify the Service Manager service account.
- In the **Password** text box, type an appropriate password.
- In the **Domain** text box, select a domain from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



Follow previous instructions for the next pages that appear. When the installation finishes, make sure the check box is cleared for starting the Encryption backup, as it was backed up earlier. Click **Finish** to complete the installation.



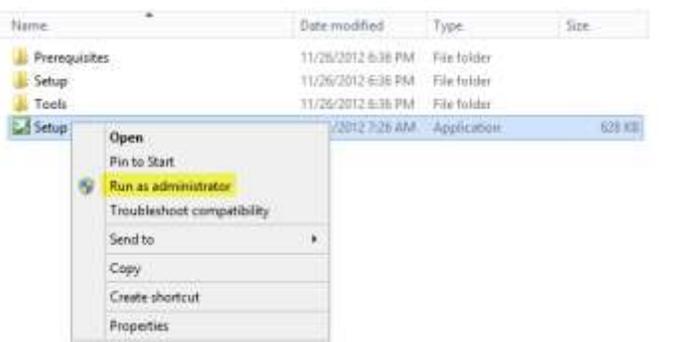
Install the Data Warehouse Server

The following steps must be completed to install the Service Manager data warehouse server role.

- ▶ Perform the following steps on the Service Manager data warehouse server virtual machine.

Log on to Service Manager data warehouse server (**not** the Service Manager management server or the self-service portal server).

From the Service Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



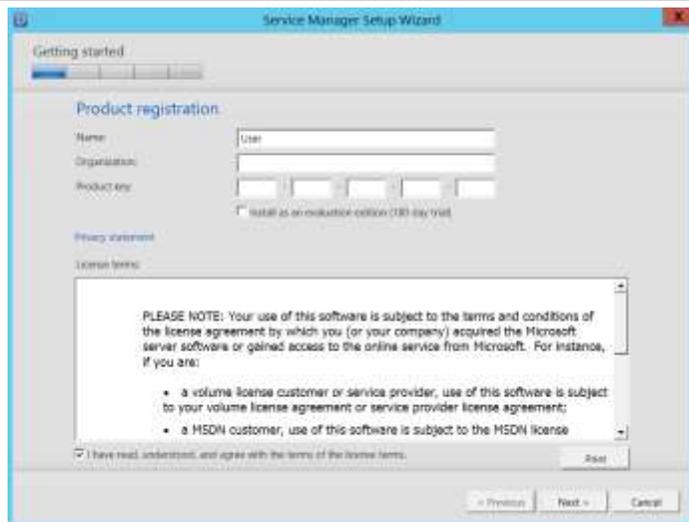
The Service Manager Setup Wizard will appear. In the **Install** section, click **Service Manager data warehouse management server** to begin the Service Manager server installation.



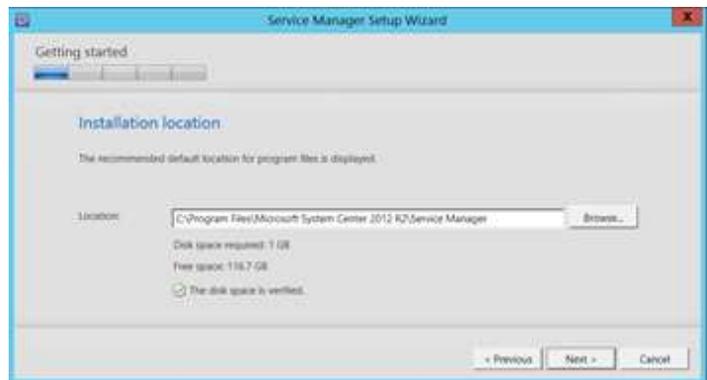
On the **Product registration** page, enter the following information in the provided text boxes:

- **Name** – Specify the name of the primary user or responsible party within your organization.
- **Organization** - Specify the name of the licensed organization.
- **Product key** – Provide a valid product key for installation of 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.

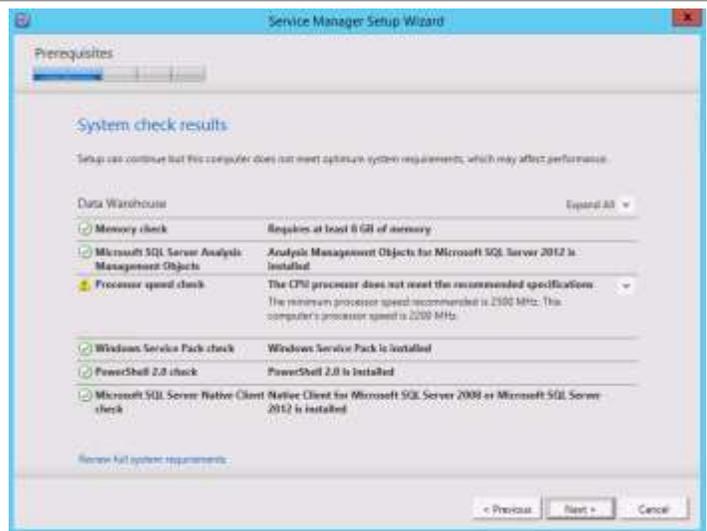


On the **Installation location** page, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Service Manager for the installation. Click **Next** to continue.



The wizard will verify that all system prerequisites are met on the **System check results** page. If any prerequisites are not met, they will be displayed on this page. When verified, click **Next** to continue.

Note: A warning will occur if your processor speed is less than 2500 MHz. With the latest Ivy Bridge processors, this should not be an issue except maybe for the largest of installations.



On the **Configure the data warehouse databases** page, each subcategory will appear with an error message until each of the following sections are configured:

- **Staging and Configuration**
- **Repository**
- **Data Mart**

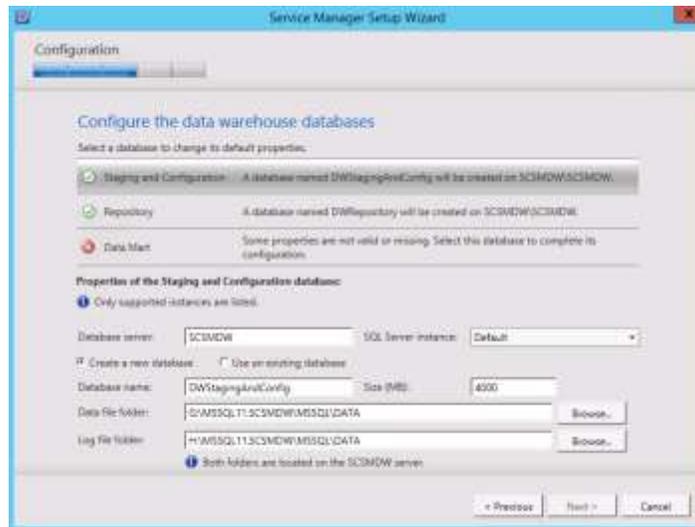


On the **Configure the data warehouse databases** page, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – Specify the name of the SQL Server cluster name object that was created for the Service Manager installation data warehouse.
- **SQL Server instance** – Specify **Default** as the name of the SQL Server database instance.

Select the **Create a new database** option and specify the following information in the provided text boxes:

- **Database name** – Specify the name of the Server Manager data warehouse database. In most cases, use the default value of DWStagingAndConfig for the **Staging and Configuration** section, and use DWRepository for the **Repository** section.
- **Size (MB)** – Specify the initial database size.
- **Data file folder** – Specify the drive letter associated in the SQL Server cluster for the database data files for the Service Manager data warehouse. Check your installation worksheet.
- **Log file folder** – As above. Check your installation worksheet.
- Click **Data Mart** to continue.



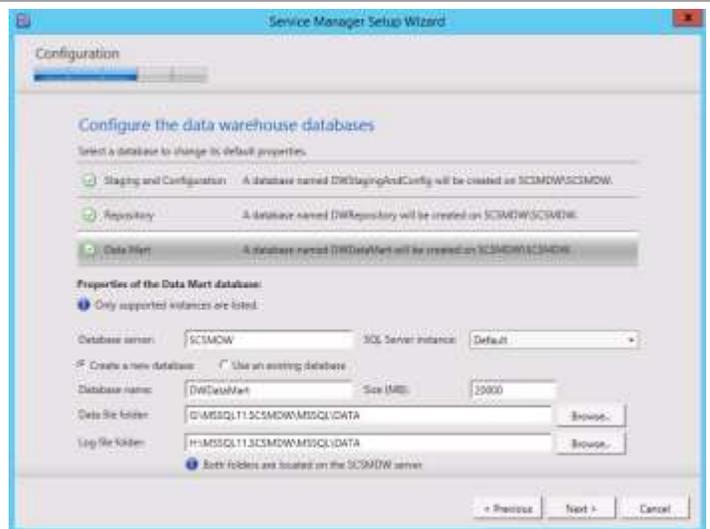
On the **Configure the data warehouse databases** page, supply the following information in the provided text boxes to configure the **Staging and Configuration** and **Repository** sections:

- **Database server** – Specify the name of the SQL Server cluster name object created for the Service Manager installation data warehouse. (This should be the same name that you used earlier for the **Staging and Configuration** and **Repository** sections).
- **SQL Server instance** – Specify Default as the name of the SQL Server database instance.

Select the **Create a new database** option and specify the following information in the provided text boxes:

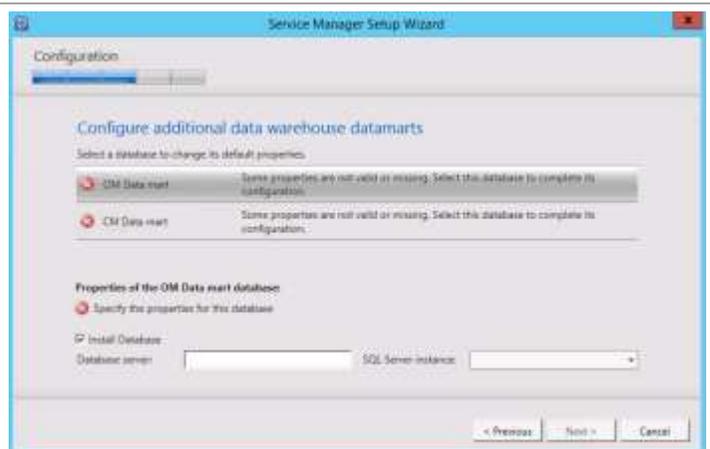
- **Database name** – Specify the name of the Service Manager data warehouse. In most cases, use the default value of DWDDataMart.
- **Size (MB)** – Specify the initial database size.
- **Data file folder** – As above. Check your installation worksheet.
- **Log file folder** – As above. Check your installation worksheet.

Click **Next** to continue.



On the **Configure additional data warehouse datamarts** page, each subcategory will appear with an error message until each of the following sections are configured:

- **OM Data mart**
- **CM Data mart**



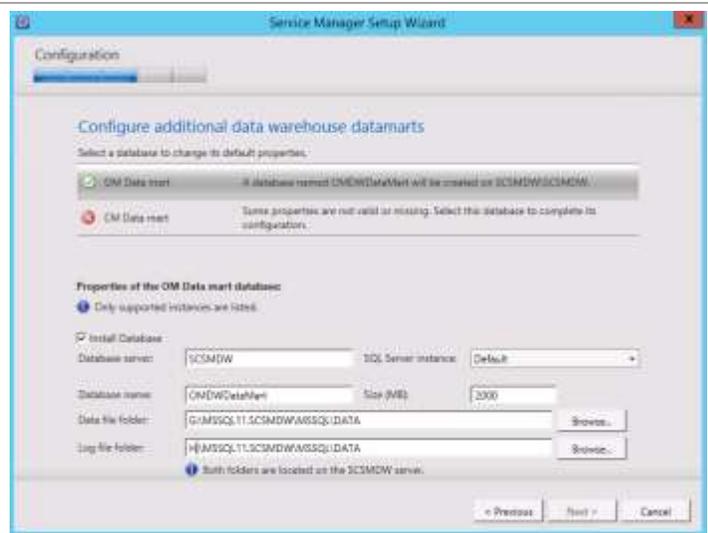
On the **Configure additional data warehouse datamarts** page, supply the following information in the provided text boxes to configure the **OM Data Mart** section:

- **Database server** – Specify the name of the SQL Server cluster name object created for the Service Manager installation data warehouse. (This should be the same name you used earlier for the **Staging and Configuration** and **Repository** sections.)
- **SQL Server instance** – Specify Default as the name of the SQL Server database instance.

Select the **Install 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, use the default value of OMDWDataMart.
- **Size (MB)** – Specify the initial database size.
- **Data file folder** – As above. Check your installation worksheet.
- **Log file folder** – As above. Check your installation worksheet.

Click **Next** to continue.



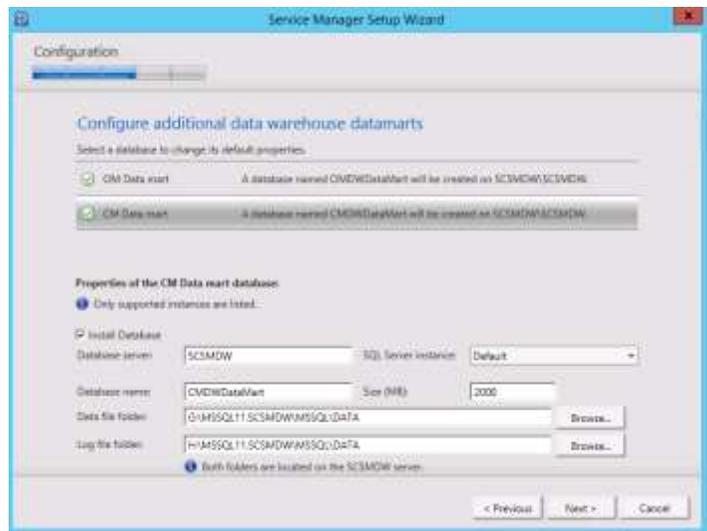
A CM Data mart is created for Configuration Manager integration. To complete this, on the **Configure additional data warehouse datamarts** page, supply the following information in the provided text boxes to configure the **CM Data Mart** section:

- **Database server** – Specify the name of the SQL Server cluster name object created for the Service Manager installation data warehouse. (This should be the same name you used earlier for the **Staging and Configuration** and **Repository** sections.)
- **SQL Server instance** – Specify Default as the name of the SQL Server database instance.

Select the **Install 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, use the default value of CMDWDataMart.
- **Size (MB)** – Specify the initial database size.
- **Data file folder** – As above. Check your installation worksheet.
- **Log file folder** – As above. Check your installation worksheet.

Click **Next** to continue.



On the **Configure the data warehouse management group** page, specify a unique name in the **Management group name** text box. This value must be unique across the System Center 2012 R2 products such as the Service Manager management server and Service Manager Operations Manager installations.

In the **Management group administrators** section, select the **SM Administrators** group from the Browse button.

Click **Next** to continue.



On the **Configure the reporting server for the data warehouse** page, specify the data warehouse server in the **Report server** text box.

In the **Report server instance** drop-down list, select **Default**.

In the **Web service URL** drop-down list, select the default reporting server URL.

Click **Next** to continue.



On the **Configure the account for Service Manager services** page:

- Verify that the **Domain account** option is selected.
- Specify the Server Manager service account in the **User name** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



On the **Configure the reporting account** page:

- Specify the SCSM SQL Server Reporting Services Account in the **User name** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

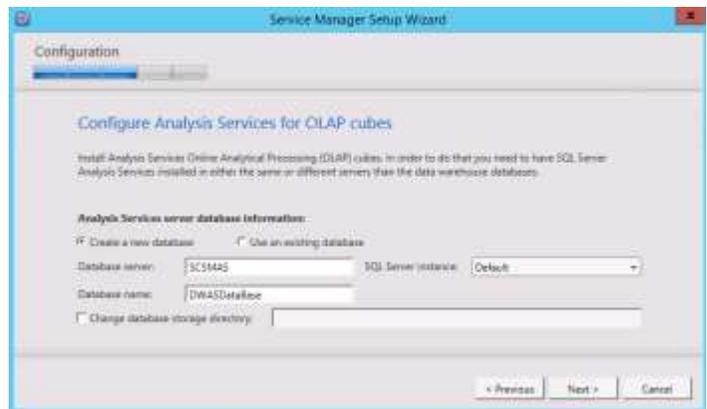
When successful, click **Next** to continue.



On the **Configure Analysis Services for OLAP cubes** page, 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 name object created for the Service Manager installation SQL Server Analysis Services.
- **SQL Server instance** – Specify Default as the name of the SQL Server database instance.
- **Database name** – Specify the name of the SQL Server Analysis Services database. In most cases, use the default value of DWASDataBase.

Confirm that the **Change database storage directory** check box is clear, and click **Next** to continue.

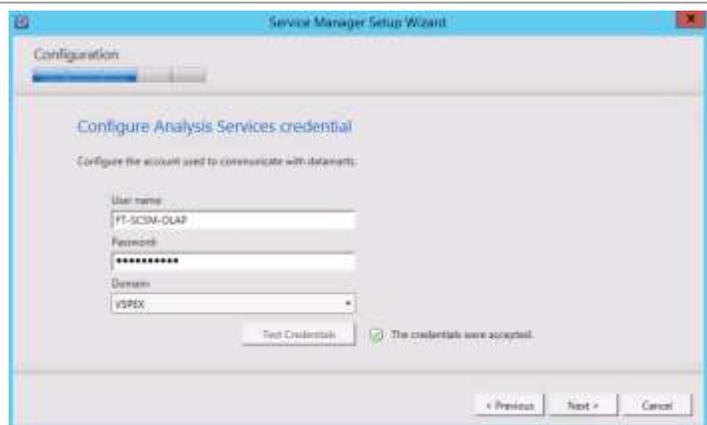


On the **Configure Analysis Services Credential** page:

- Specify the SM OLAP Account in the **User name** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



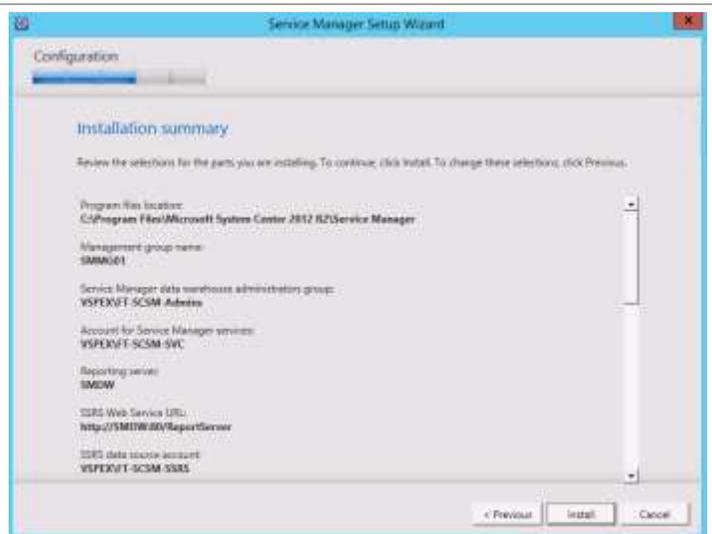
On the **Help improve Microsoft System Center 2012 R2 Service Manager** page, select the option to participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.



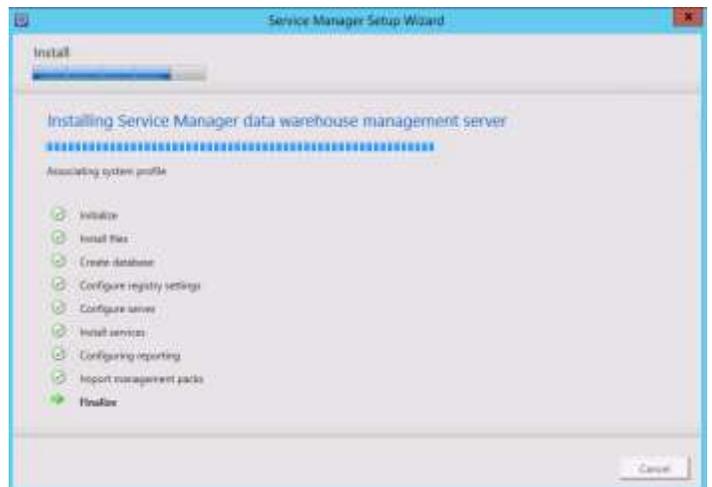
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** page may appear. Select the appropriate option to participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.



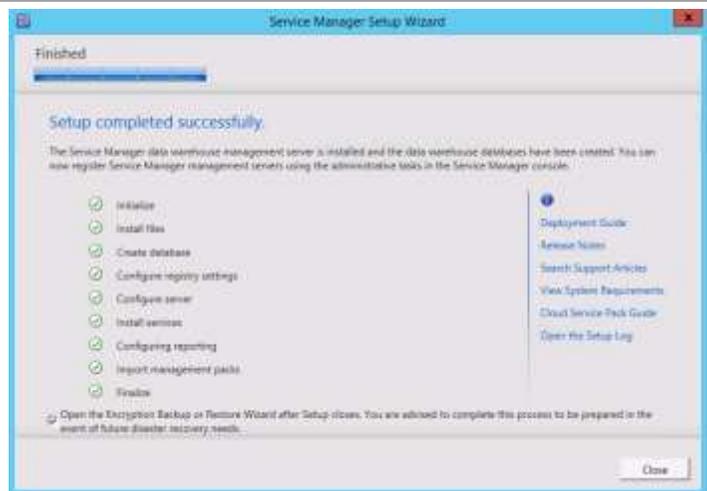
The wizard will display the progress while installing features.



When the installation completes, the wizard will display the **Setup completed successfully** page.

Make sure the **Open the Encryption Backup or Restore Wizard after Setup closes** check box is selected to open the wizard after setup.

Click **Close** to complete the installation.



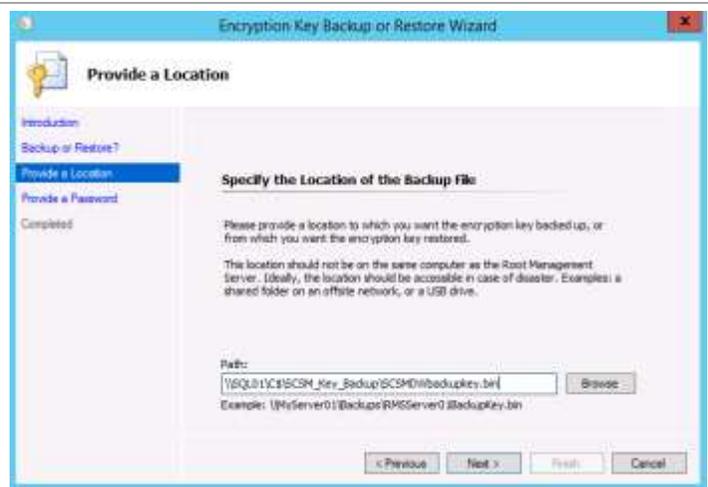
When the installation completes, the **Encryption Key Backup or Restore Wizard** will appear. On the **Introduction** page, click **Next** to continue.



On the **Select Action** page, select the **Backup the Encryption Key** option, and click **Next** to continue.



On the **Specify the Location of the Backup File** page, in the **Path** text box, select the desired backup file name and path from the drop-down list. Click **Next** to continue.



On the **Provide a Password** page, type a desired password in the **Password** text box. Retype the password in the **Confirm Password** text box, and click **Next** to begin the backup process.



Click **Finish** to exit the wizard.



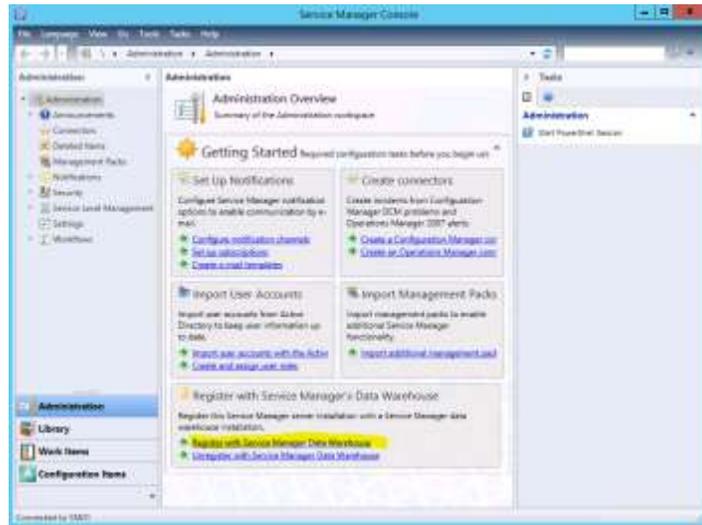
- ▶ Perform the following steps on the Service Manager management server virtual machine to register the Service Manager data warehouse and enable reporting in the Service Manager instance.

Log on to the Service Manager management server by using an account with Administrator permissions. From the Windows **Start** screen, click the **Service Manager Console** tile.



In the **Service Manager Console**, click the **Administration** node, and in the **Register with Service Manager's Data Warehouse** section, click **Register with Service manager data warehouse** to enable reporting.

Note: If the console was opened from the previous installation, close it and re-open the console.



The Data Warehouse Registration Wizard will appear. Click **Next** to begin registration.



On the **Specify the data warehouse management server name** page, select the Service Manager data warehouse server FQDN from the **Server name** drop-down list.

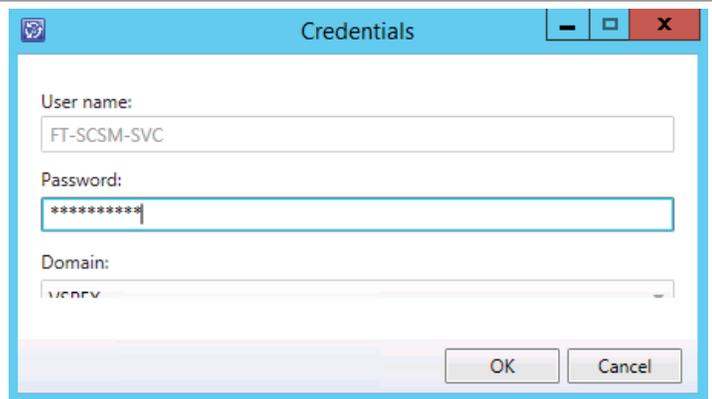
Click the **Test Connection** button to validate connectivity between the Service Manager management server and the data warehouse server. Click **Next** to continue.



On the **Provide credentials for the data warehouse** page, click **Next** to continue.



A **Credentials** page will appear and prompt you for the password for the SM service account. When provided, click **OK** to continue.



The **Summary** page will appear. Review the information that was provided earlier, and click **Create** to begin the registration process.



The **Completion** page will show the successful registration of the data warehouse. Click **Close** to exit the wizard.

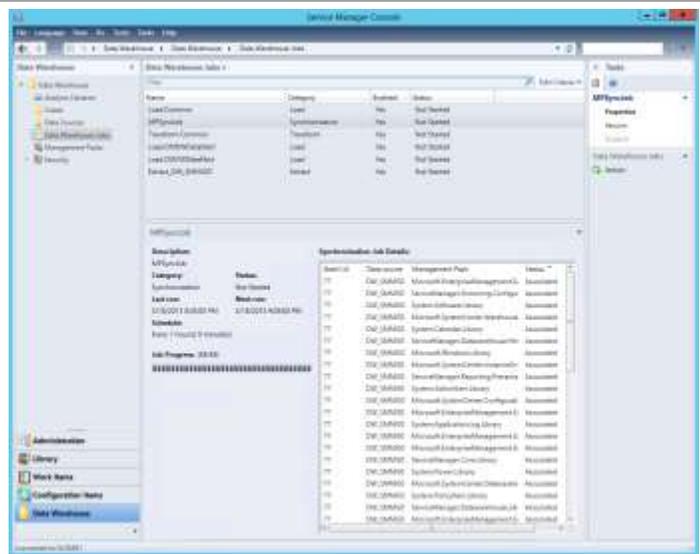


In the **Data Warehouse** pane, click **Data Warehouse Jobs**.

In the **Data Warehouse Jobs** pane, click **MPSyncJob**.

In the **MPSyncJob** section, 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 **Pending Association** or **Failed** in the status list. In the **Data Warehouse Jobs** pane, the status of the **MPSyncJob** will change from **Running** to **Not Started** when the registration process is complete.



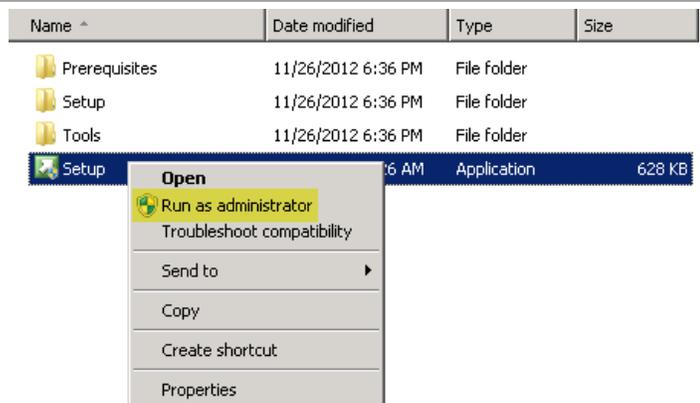
Install the Service Manager Self-Service Portal Server

The following steps must to be completed 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** to begin setup.



The Service Manager Setup Wizard will appear. In the **Install** section, click **Service Manager web portal** to begin the Service Manager self-service portal server installation.



On the **Portal Parts** page, 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.



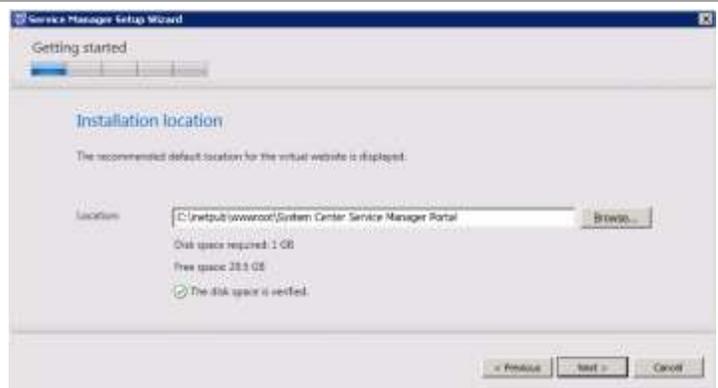
On the **Product registration** page, enter the following information in the provided text boxes:

- **Name** – Specify the name of the primary user or responsible party within your organization.
- **Organization** – Specify the name of the licensed organization.

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.

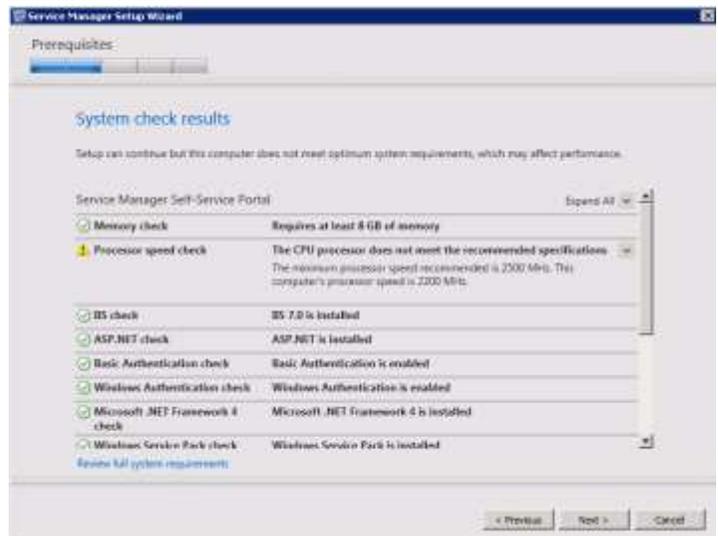


On the **Installation location** page, specify a location or accept the default location of C:\inetpub\wwwroot\System Center Service Manager Portal for the installation. Click **Next** to continue.



On the **System check results** page, the wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on this page. When verified, click **Next** to continue.

Note: The warning on processor speed can be safely ignored.

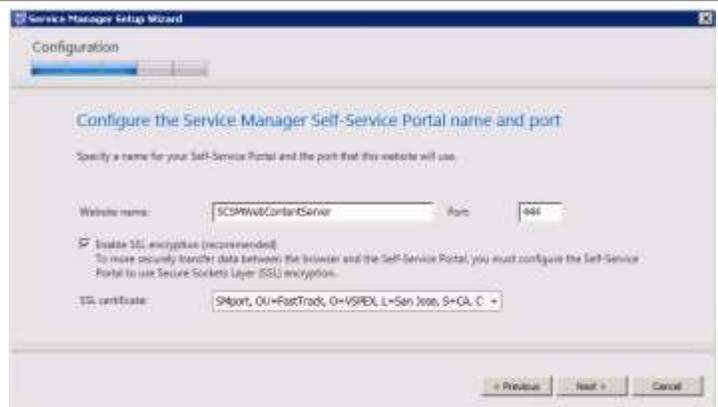


On the **Configure the Service Manager Self-Service Portal name and port** page, specify the following information in the provided text boxes:

- **Website name** – Specify the name of the website used for the self-service portal. In most cases, use the default name of SCSPWebContentServer.
- **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**.

Select the appropriate Server Authentication certificate from the **SSL certificate** drop-down list. The certificate CN field must match the name of the server.

Click **Next** to continue.



On the **Select the Service Manager database** page, specify the following information in the provided text boxes:

- **Database server** – Specify the name of the SQL Server cluster cluster name object created for the Service Manager management server.
- **SQL Server instance** – Specify **Default** as the SQL Server database instance.
- **Database** – Specify the name of the Service Manager database configured earlier. In most cases, use the default value of ServiceManager.

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window at the 'Configuration' step. The title is 'Select the Service Manager database'. Below the title, it says 'Specify the name of the server that hosts the instance of SQL Server 2008 R2 or SQL Server 2012 that contains the Service Manager database, and then select the Service Manager database.' There is a note: 'Service Manager Self-Service Portal will use the existing "ServiceManager" database.' Below this, there are three input fields: 'Database server' with the value 'SCSMDB', 'SQL Server instance' with the value 'Default', and 'Database' with the value 'ServiceManager'. A yellow warning icon is next to the 'Database' field with the text: 'To connect to the existing configuration database, you must be logged on as a member of the Administrators user role on Service Manager management server; otherwise setup will fail.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

On the **Configure the account for the Self-Service Portal** page:

- Verify that the **Domain account** option is selected, and
- Specify the SM Service Account in the **User name** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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

The screenshot shows the 'Service Manager Setup Wizard' window at the 'Configuration' step. The title is 'Configure the account for the Self-Service Portal'. Below the title, it says 'The Self-Service Portal can access the Service Manager database under the Local System account, if installed on the same computer, or under a domain user or service account. Setup will add the domain account to the Service Manager Administrators user role.' There are two radio buttons: 'Local System account' (unselected) and 'Domain account' (selected). Below the radio buttons, there are three input fields: 'User name' with the value 'FT-SCSM-SVC', 'Password' with masked characters '*****', and 'Domain' with the value 'VSPDM'. A 'Test Credentials' button is located below the input fields. A green checkmark icon is next to the text 'The credentials were accepted.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

On the **Configure the Service Manager SharePoint Web site** page, 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, use the default name of Service Manager Portal.
- **Port** – Specify the TCP port used for the Service Manager self-service portal server. The default value is 443. In most cases, keep the default value of **443**.
- Select the appropriate server authentication certificate from the **SSL certificate** drop-down list. 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 Default as the SQL Server database instance.
- **Database server** – Specify the database name for the portal. In most cases, use the default value of SharePoint_SMPortalContent.

Click **Next** to continue.

The screenshot shows the 'Service Manager Setup Wizard' window, specifically the 'Configuration' step for the 'SharePoint Web site'. The window title is 'Service Manager Setup Wizard' and the subtitle is 'Configuration'. The main heading is 'Configure the Service Manager SharePoint Web site'. Below this, there is a brief instruction: 'Specify the name and port number for the SharePoint Web site. Specify the server and database that will be used to store content for this SharePoint Web site, and then specify the URL for the web content server.'

The configuration fields are as follows:

- SharePoint site:**
 - Website name: Service Manager Portal
 - Port: 443
 - Enable SSL encryption (recommended)
 - SSL certificate: WMSvc-SMPORT
- SharePoint database:**
 - Database server: SCDB
 - SQL Server instance: Default
 - Database name: SharePoint_SMPortalContent
- Web content server:**
 - URL: http://SMRT07-443

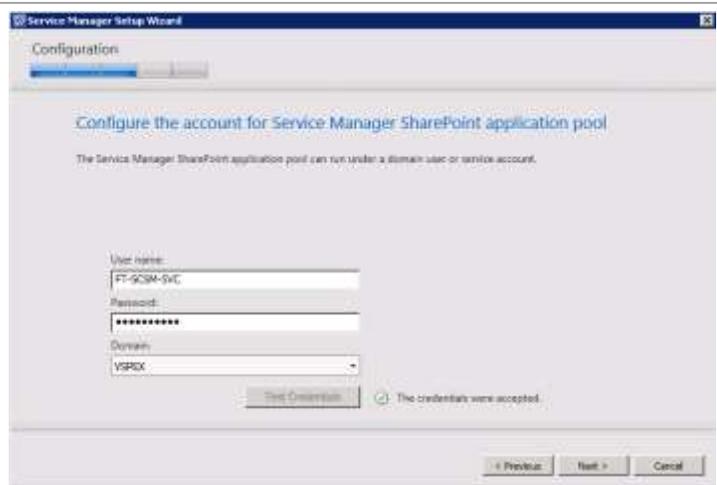
At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

On the **Configure the account for Service Manager SharePoint application pool** page:

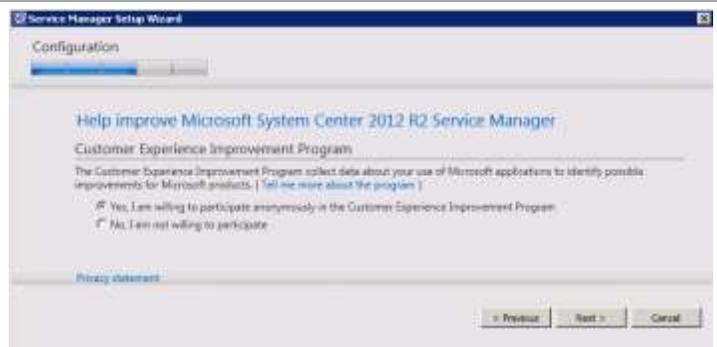
- Specify the SM service account in the **User name** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test Credentials** button to verify the credentials provided.

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



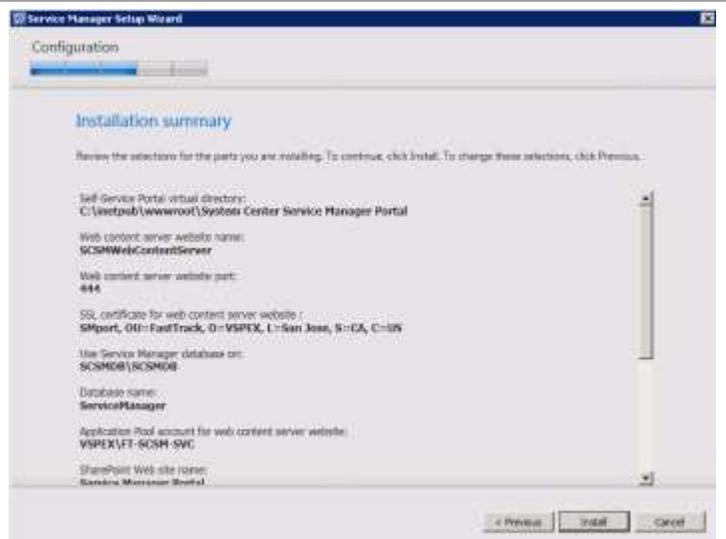
On the **Help improve Microsoft System Center 2012** page, select the option to participate or not participate in the CEIP and provide selected system information to Microsoft. Click **Next** to continue.



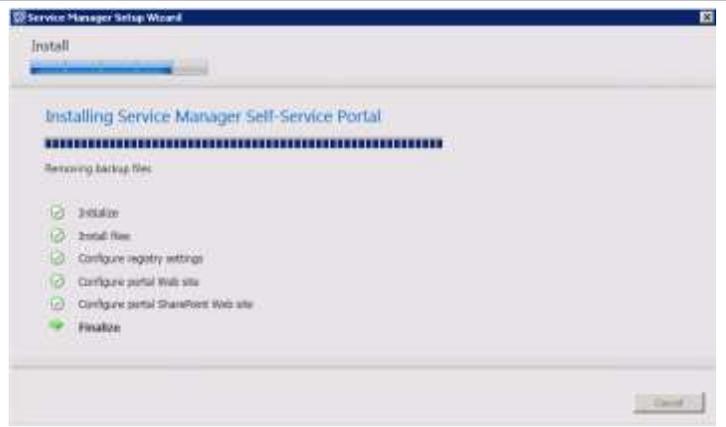
Depending on your system's configuration, the **Use Microsoft Update to help keep your computer secure and up-to-date** page may appear. Select the appropriate option to participate or not participate in automatic updating. Choose to invoke checking for updates by selecting the **Initiate machine wide Automatic Update** check box. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected and click **Install** to continue.

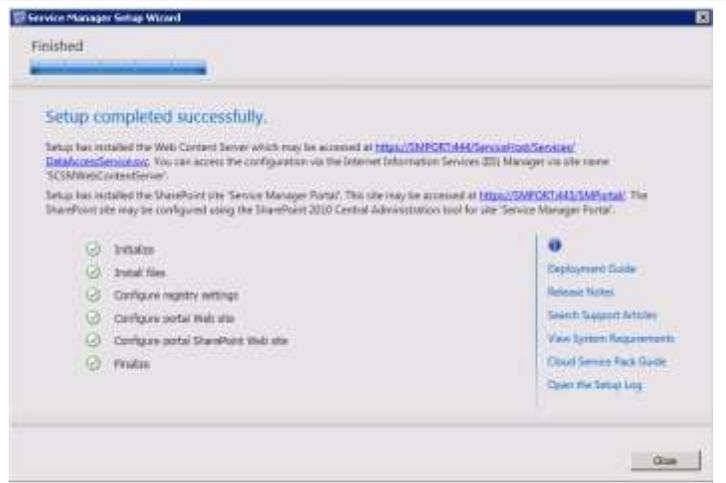


The wizard will display the progress while installing features.



When completed, the Service Manger Setup Wizard will display the **Setup completed successfully** page. Click **Close** to finish the installation.

Note the SMPortal link provided on the page.



From a system with Silverlight® installed, open the Service Manager self-service portal from Microsoft Internet Explorer at <https://<servername>/SMPortal>.

Verify that the page loads completely and that all sections display as expected.



Orchestrator

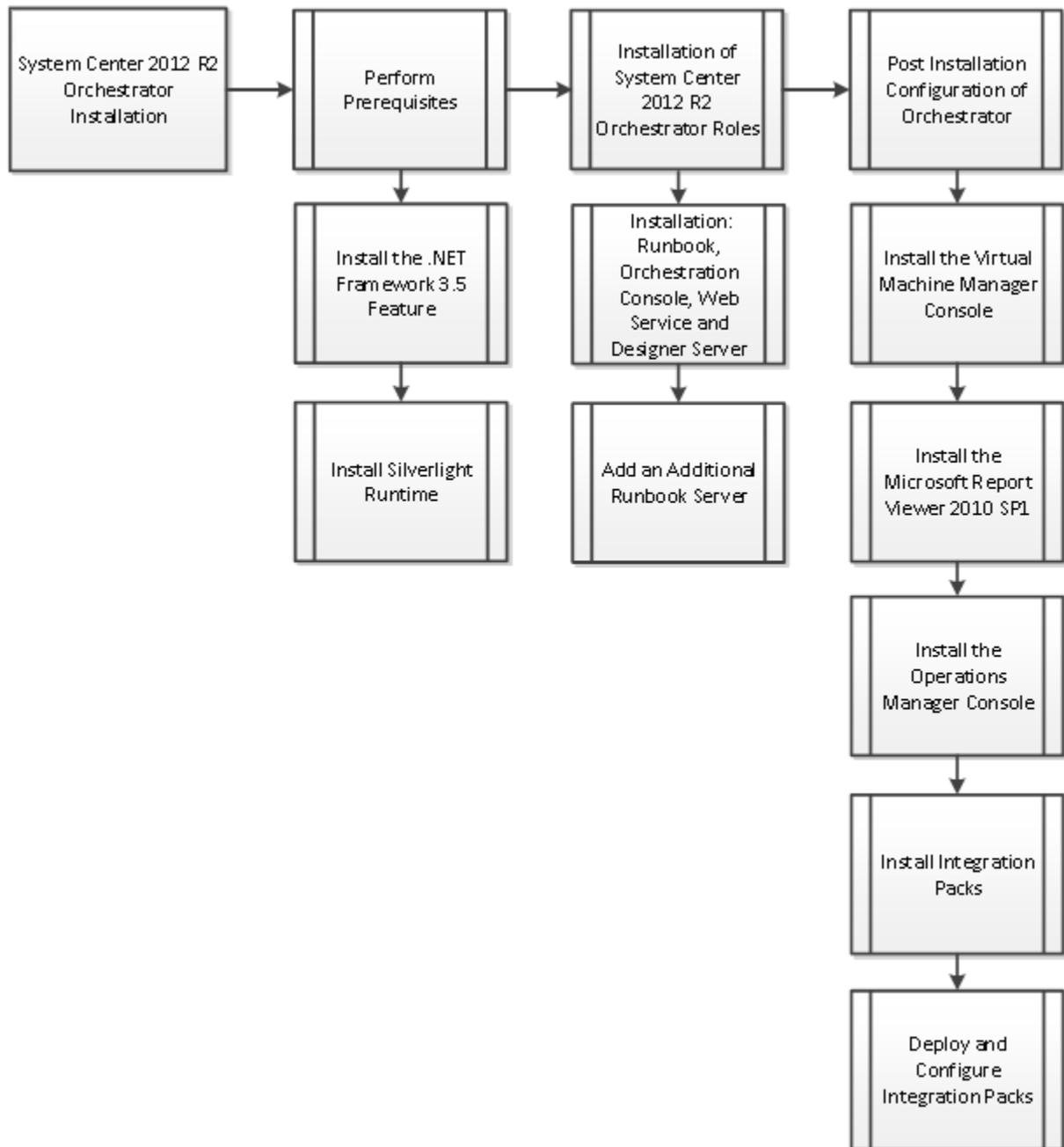
Two Orchestrator Runbook servers are deployed for high availability purposes. Orchestrator provides built-in failover capabilities. By default, if the primary Runbook server fails, any runbooks that were running on that server will be started from their beginning on the standby Runbook server. In addition, the use of multiple Runbook servers supports Orchestrator scalability. By default, each Runbook server can run a maximum of 50 simultaneous runbooks. To run larger number of simultaneous runbooks, additional Runbook servers are recommended to accommodate scale environments.

Orchestrator Web service is a REST-based service that enables Orchestration Console and various custom applications, e.g. System Center Service Manager, to connect to Orchestrator in order to start and stop runbooks and retrieve information about jobs. If the Web service is unavailable, it is not possible to stop and start new runbooks. For high availability and additional capacity there are two IIS servers with Orchestrator Web service role installed and configured for load balancing. For the PLA, those two servers are the same as Runbook servers.

Domain accounts are used for Orchestrator services and a domain group for the Orchestrator Users group.

The Orchestrator installation process includes the high-level steps shown in the following figure.

Figure 10. Orchestrator Installation Process



Overview

This section provides the procedure to set up Orchestrator in the fabric management architecture. The following requirements are necessary for the setup:

- Base virtual machines running Windows Server 2012 R2 have been provisioned.
- A multinode, SQL Server 2012 SP1 cluster with a dedicated instance has been established for Orchestrator in previous steps.
- .NET Framework 3.5 is required

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following service accounts have been created:

Table 27. Orchestrator Accounts

User name	Purpose	Permissions
<DOMAIN>FT-SCO-SVC	Orchestrator service account	This account needs: Full Administrator permissions on all target systems to be managed Log on As a Service rights (user rights) Sysadmin on the SQL Server, or dbo rights to the Orchestrator database after its created Member of FT-SCVMM-Admins

Groups

Verify that the following security groups have been created:

Table 28. Orchestrator Security Groups

Security group name	Group scope	Members	Member of
<DOMAIN>\FT-SCO-Operators	Global	Any user account added to this group is granted permission to use the Runbook Designer and Deployment Manager tools.	
<DOMAIN>\FT-SCO-Admins	Global	<DOMAIN>\FT-SCO-SVC	Local Administrators Target Active Directory domain BUILTIN\Distributed COM Users

Add .NET Framework 3.5 and .NET Framework 4.5 with HTTP Activation

The Orchestrator installation requires that .NET Framework 3.5 and HTTP Activation for .NET 4.5 are enabled. Use the following procedure to enable these features.

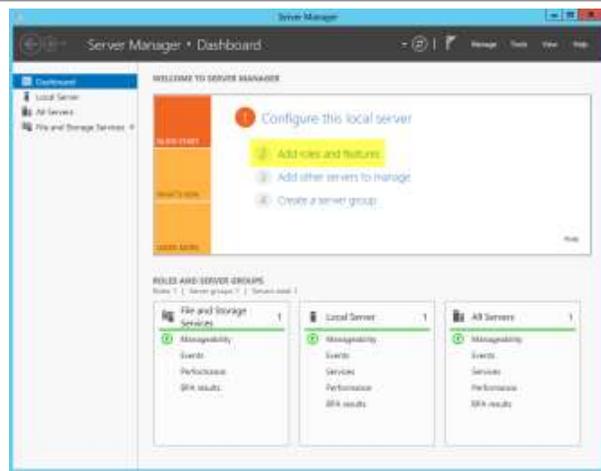
► Perform the following steps on the Orchestrator virtual machine.

If you do not have access to the internet to contact Microsoft Update, you will need to have the Windows Installation files mounted locally or on an accessible file share.

```
Install-windowsFeature -Name  
NET-Framework-Core -Source  
"E:\Sources\sxs"
```

The .NET Framework 3.5 feature can be installed with a PowerShell cmdlet, or the following instructions can be followed for using the GUI. If the VM has access to the internet, the `-Source` parameter should not be needed.

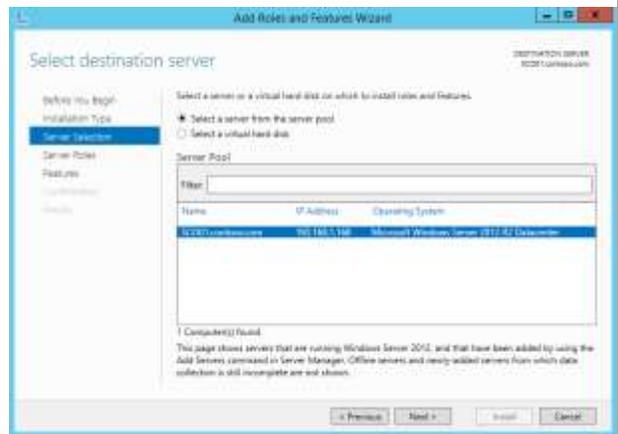
Open **Server Manager** and navigate to the **Dashboard** node. In the main pane, under **Configure this local server**, click **Add roles and features** from the available options.



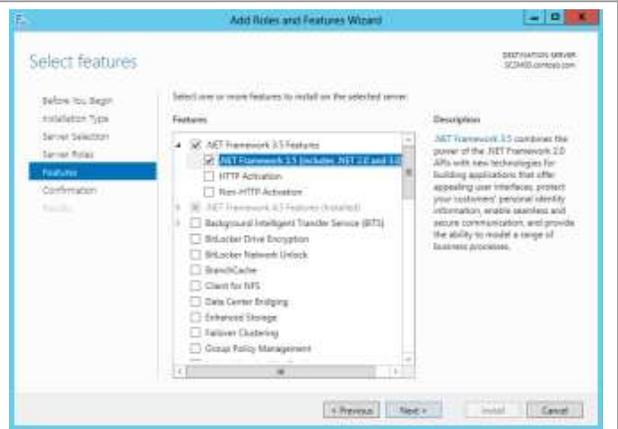
The Add Roles and Features Wizard will appear. On the **Before You Begin** page, click **Server Selection** in the left pane.



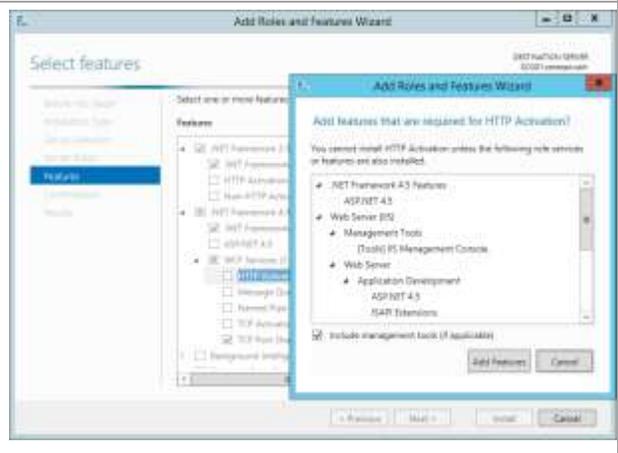
On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server, and then click **Features** in the left pane to continue.



To add .NET Framework 3.5, on the **Select Features** page in the **Features** pane, expand and select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear.



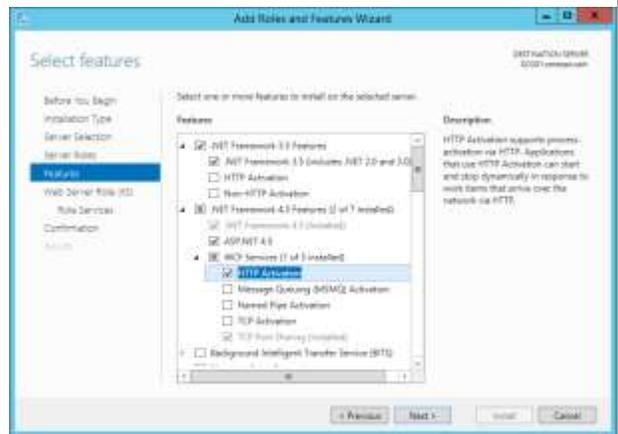
Expand **.NET Framework 4.5 Features** item and then expand the **WCF** item. Select **HTTP Activation** and then select **Add Features** on the **Add features that are required for HTTP activation** window.



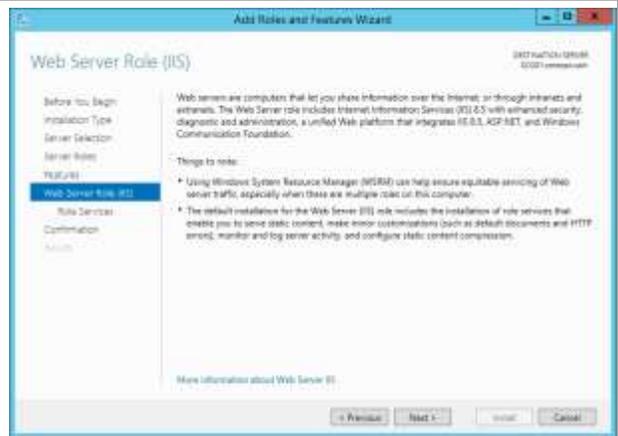
The following items should now show as enabled for the .NET Framework features:

- .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- .NET Framework 4.5 Features
 - .NET Framework 4.5
 - ASP.NET 4.5
 - WCF Services
 - HTTP Activation
 - TCP Port Sharing

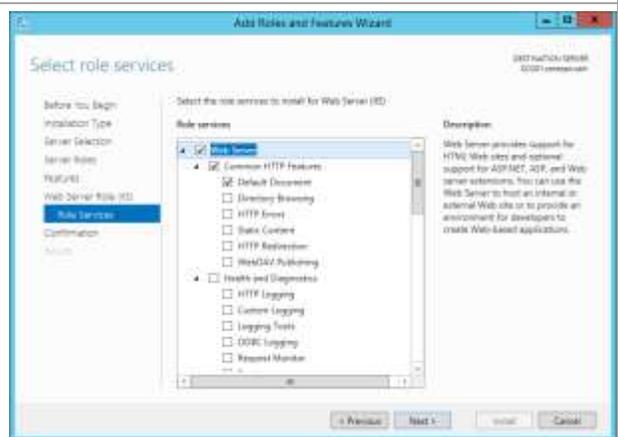
Click **Next** to continue.



On the **Web Server Role (IIS)** page click **Next** to continue.



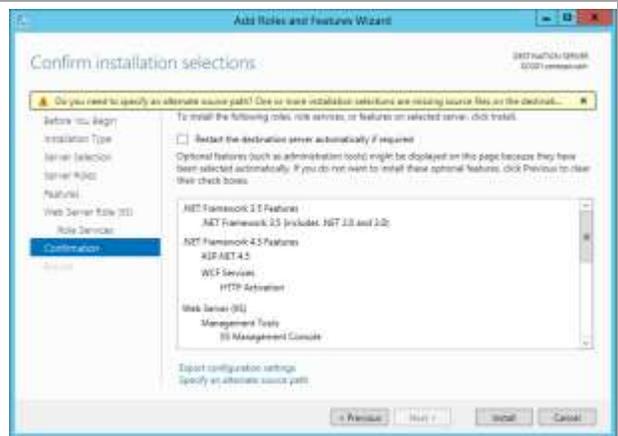
On the **Select role services** page, confirm that only **Web Server**, **Common HTTP Features** and **Default Document** are selected and then click **Next**.



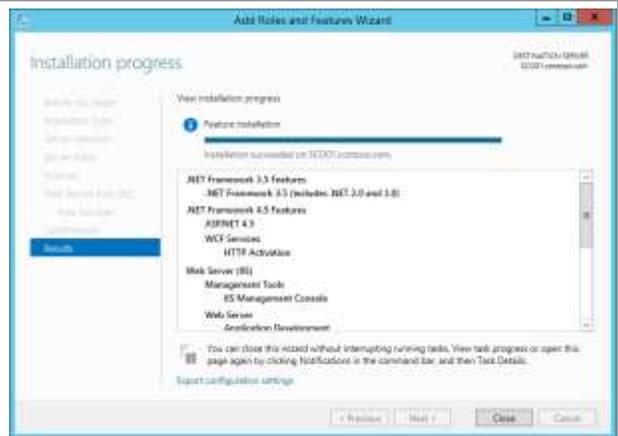
On the **Confirm installation selections** page, verify that **.NET Framework 3.5 Features** and **.NET Framework 4.5 Features** are listed. Make sure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

If the server does not have Internet access, an alternate source path can be specified by clicking the **Specify an alternate source path** link. For servers without Internet access or if the .NET Framework 3.5 source files already exist on the network, an alternate source location be specified here for the installation

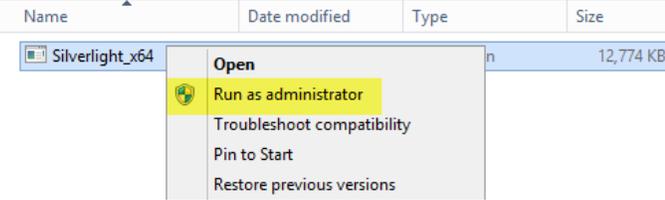


The **Installation Progress** page will show the progress of the feature installation. Click **Close** when the installation process completes.



Install Silverlight

► Perform the following steps on the Orchestrator virtual machine.

<p>From the installation media source, right-click Silverlight.exe and select Run as administrator to begin setup.</p>	
<p>On the Install Silverlight page, click Install now.</p>	
<p>On the Enable Microsoft Update page, select or clear the Enable Microsoft Update check box based on organizational preferences, and click Next to continue.</p>	
<p>On the Installation Successful page, click Close.</p>	

Installation

Install the Full Management Server

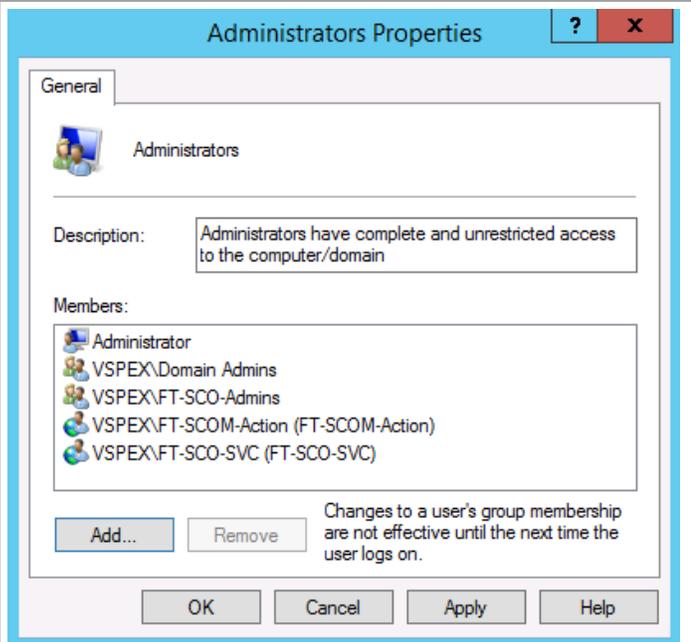
Complete the following steps to install all Orchestrator components.

- ▶ Perform the following steps on the Orchestrator virtual machine.

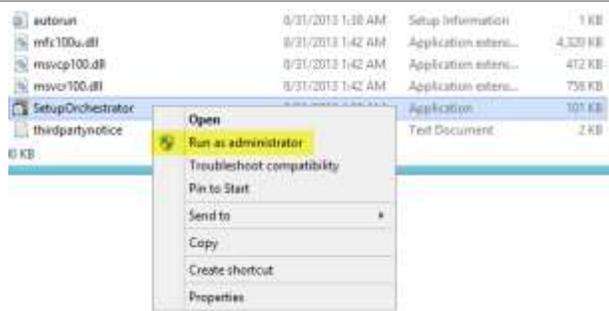
Log on to the Orchestrator virtual machine as a user with local Admin rights.

Verify that the following accounts 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** to begin setup.



The **Orchestrator Setup Wizard** will appear. Click **Install** to begin the Orchestrator server installation.



On the **Product registration information** page, enter the following information in the provided text boxes:

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

Click **Next** to continue.



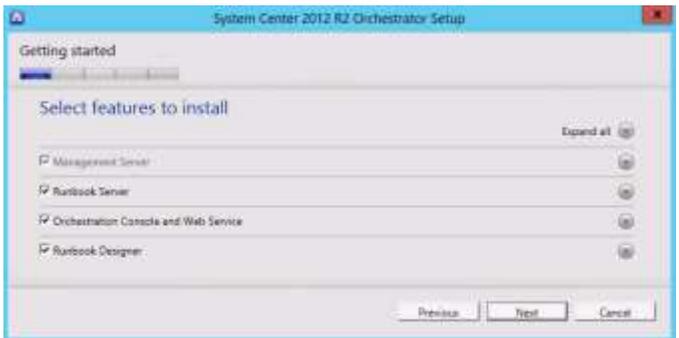
On the **Please read this License Terms** page, verify that the **I accept the license terms** installation option check box is selected, and click **Next** to continue.



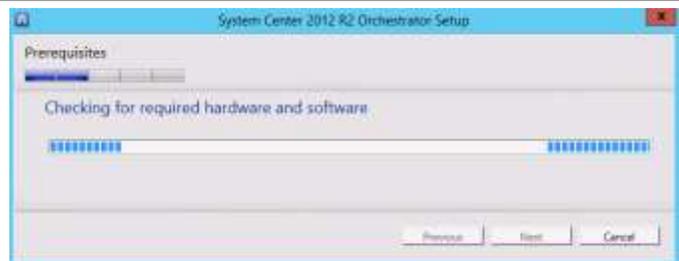
On the **Select Features to install** page, select the following check boxes:

- **Management Server** (default selected)
- **Runbook server**
- **Orchestration console and web service**
- **Runbook Designer**

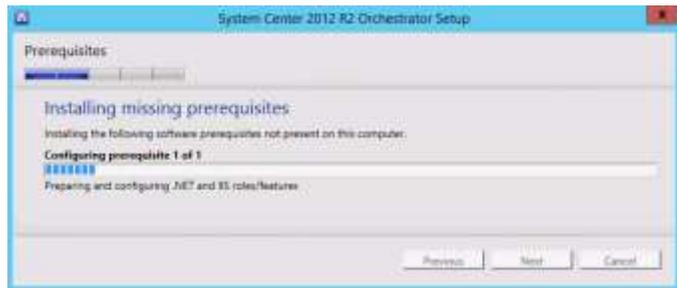
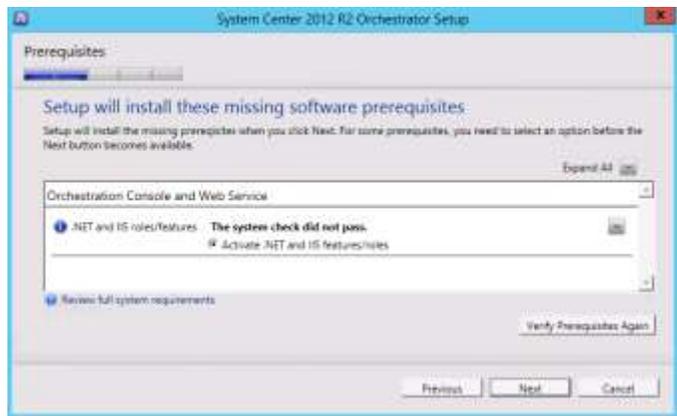
Click **Next** to continue.



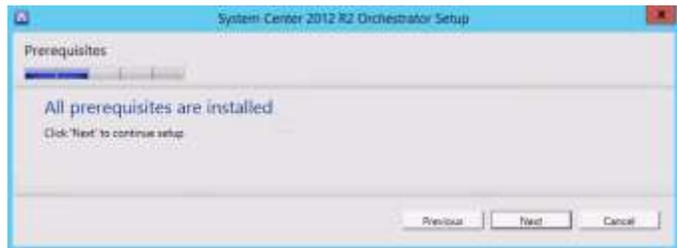
The **Checking for required hardware and software** page will appear to verify the installation prerequisites. When validation completes, click **Next** to continue.



The Orchestrator Setup Wizard will identify any prerequisite software required for the installation to complete. The **Setup will install these missing software prerequisites** page will attempt to perform the installation of missing prerequisites. Select the radio button by the missing components and click **Next** to continue.



When the installation of the missing prerequisites is completed, click **Next** to continue.



On the **Configure the service account** page:

- Specify the Orchestrator service account in the **Username** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test** button to verify the credentials provided.

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

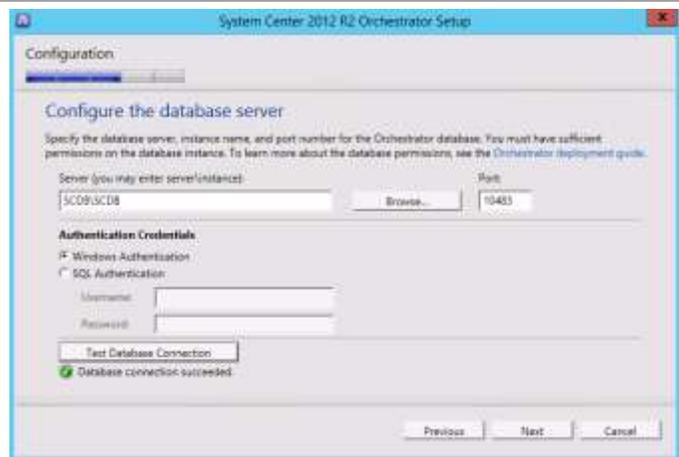


On the **Configure the database server** page, enter the following information in the provided text boxes:

- **Server** – Specify the SQL Server cluster name and instance name created earlier. For the reference deployment the server and instance value is **SCDB\SCDB**.
- **Port** – Specify the TCP port used for the SQL Server, if not the default. For the reference deployment the SCDB instance port is 10433.

In the **Authentication Credentials** section, select the **Windows Authentication** option, and click the **Test Database Connection** button.

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



On the **Configure the database** page in the **Database** section, select the **New Database** option. Type the default database name of *Orchestrator*.

Click **Next** to continue.



On the **Configure Orchestrator users group** page, select the Orchestrator users group created earlier from the **Browse...** button and select to search the domain.. For this installation, this is the domain Orchestrator operators group outlined at the beginning of this section.

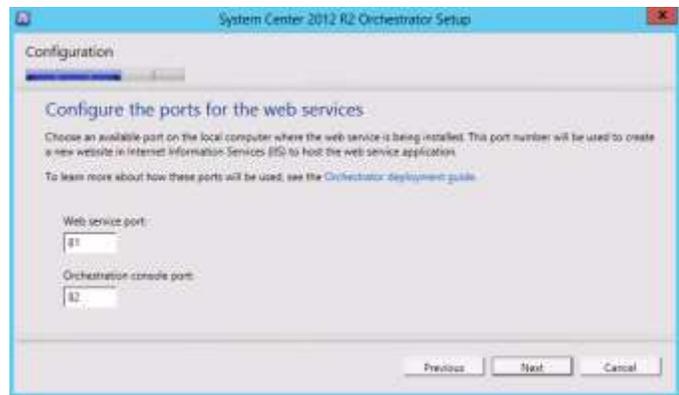
Verify that the **Grant remote access to the Runbook Designer** check box is selected, and click **Next** to continue.



On the **Configure the ports for the web services** page, enter 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.



On the **Select the installation location** page, specify a location or accept the default location of %ProgramFiles(x86)%\Microsoft System Center 2012 R2\Orchestrator for the installation. Click **Next** to continue.



On the **Microsoft Update** page, select the appropriate radio button for your environment.



The **Help Improve Microsoft System Center Orchestrator** page provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Error Reporting**

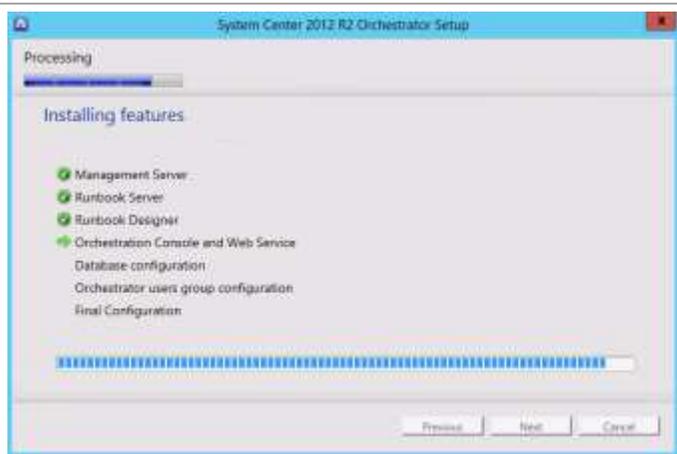
Select the appropriate option based on your organization's policies, and click **Next** to continue.



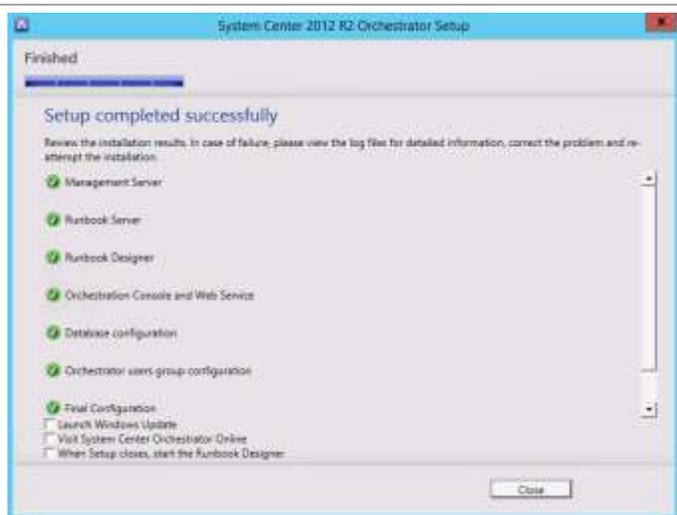
The **Installation summary** page will display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.



The **Installing features** page will show the installation progress.



The **Setup completed successfully** page will appear when all portions of the setup complete successfully. Verify that all check boxes are cleared, and click **Close** to finish the installation.

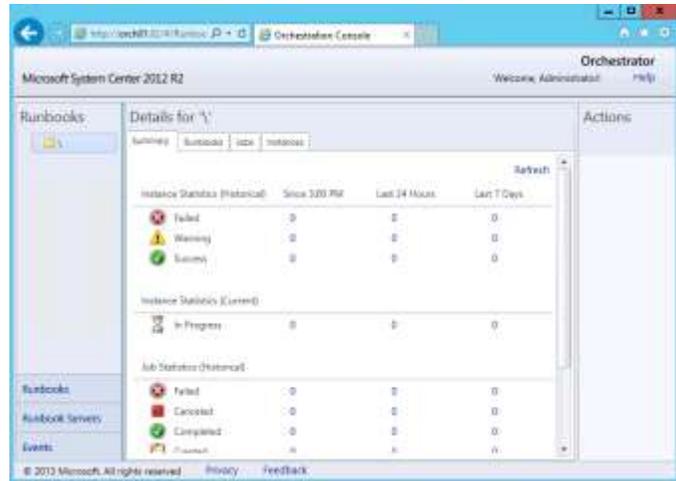


Verify that the Orchestrator roles installed properly by opening the consoles: on the **Start** screen, click the **Orchestration Console** tile.

Note: To run the Orchestration Console on the Orchestrator server, Internet Explorer Enhanced Security must be disabled or configured to function with the console.



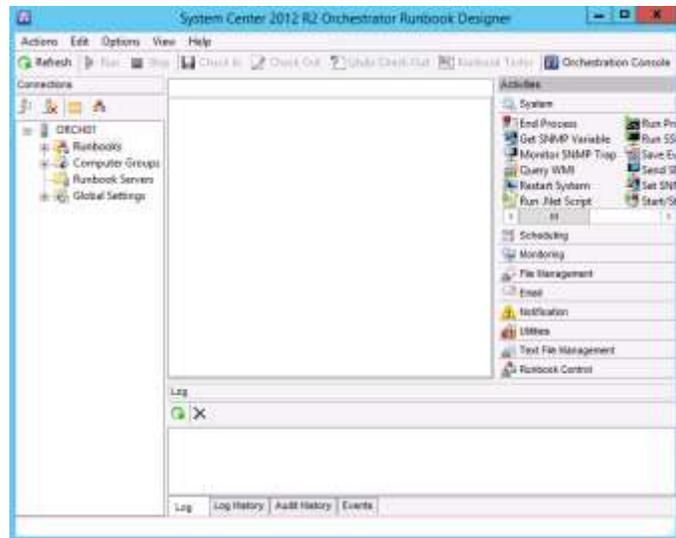
Validate that the **Orchestration console** performs properly in Internet Explorer.



On the **Start Menu**, click the **Runbook Designer** tile.



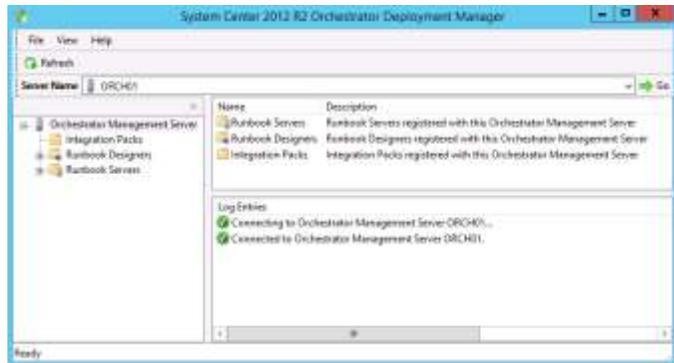
Open the **Runbook Designer** console, and verify that it performs properly.



On the **Start Menu**, click the **Deployment Manager** tile.



Open the **Deployment Manager** console, and verify that it performs properly.



On the Start Screen, click the **Windows Firewall** tile. Configure Windows Firewall for the first Orchestrator runbook server.³



If you want to leave 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 click **Enable Rule**.

Alternatively, the following Windows PowerShell commands can be run to allow the firewall rules:

```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (WMI-In)"
```

```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (DCOM-In)"
```

```
Enable-NetFirewallRule -DisplayName "Windows Management Instrumentation (ASync-In)"
```



³ Orchestrator guidance is provided by the following TechNet resources: [Using Windows Firewall with Orchestrator](#) and [TCP Port Requirements](#).

Since the first server runs the Orchestration console and web service, two additional ports (TCP 81 and 82) must be opened in Windows Firewall. Follow the preceding step to create and enable two additional firewall Program rules and name them as follows:

- **SCO – Orchestration Console (TCP 81)**
- **SCO – Web Service (TCP 82)**

Alternatively, run the following Windows PowerShell commands:

`New-NetFirewallRule -DisplayName "SCO - Orchestration Console (TCP-In 81)"`

`New-NetFirewallRule -DisplayName "SCO - Web Service (TCP-In 82)"`

The screenshot shows the Windows Firewall 'Inbound Rules' window with four rules enabled: 'SCO - Web Service (TCP-In 82)', 'SCO - Orchestrator Remoting Service (86)', 'SCO - Orchestrator Management Service (84)', and 'SCO - Orchestration Console (TCP-In 81)'. Below, a PowerShell terminal window shows the execution of the command to create the 'SCO - Web Service (TCP-In 82)' rule, displaying its properties such as Name, Description, Group, and Action.

Restart the Orchestrator server.

Install Second Server as Runbook Server

Complete the following steps to install the Orchestrator Runbook components on a second server.

► Perform the following steps on the second Orchestrator virtual machine.

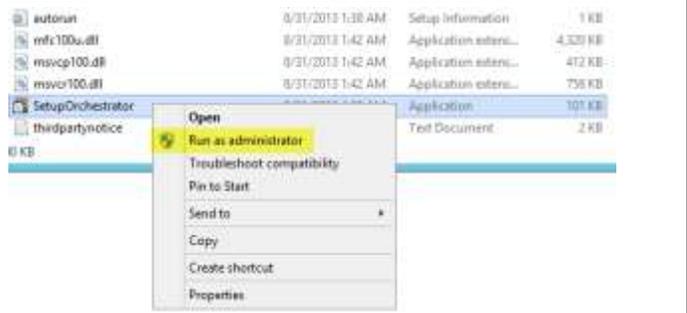
Log on to the Orchestrator virtual machine as a user with local Admin rights.

Verify that the following accounts or groups are members of the Local Administrators group on the Orchestrator virtual machine:

- Orchestrator service account
- Orchestrator Admins group
- Operations Manager action account

The screenshot shows the 'Administrators Properties' dialog box. The 'General' tab is selected, showing the 'Administrators' group. The description reads: 'Administrators have complete and unrestricted access to the computer/domain'. The 'Members' list includes: Administrator, VSPEX\Domain Admins, VSPEX\FT-SCO-Admins, VSPEX\FT-SCOM-Action (FT-SCOM-Action), and VSPEX\FT-SCO-SVC (FT-SCO-SVC). Buttons for 'Add...', 'Remove', 'OK', 'Cancel', 'Apply', and 'Help' are visible at the bottom.

Log on to System Center Orchestrator server. From the **System Center Orchestrator** installation media source, right-click **setuporchestrator.exe** and select **Run as administrator** to begin setup.



The **Orchestrator Setup Wizard** will appear. Click **Install** to begin the Orchestrator Runbook server installation.



On the **Product registration information** page, enter the following information in the provided text boxes:

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

Click **Next** to continue.



On the **Please read this License Terms** page, verify that the **I accept the license terms** installation option check box is selected, and click **Next** to continue.



On the **Select features to install** page, make sure only the **Runbook Server** is checked. Management Server is selected by default. Click **Next** to continue.



The **Checking for required hardware and software** page will appear to verify the installation prerequisites. When validation completes, click **Next** to continue.



On the **Configure the service account** page:

- Specify the Orchestrator service account in the **Username** text box.
- Type the appropriate **Password** in the provided text box.
- Select the appropriate **Domain** from the drop-down list.

Before proceeding, click the **Test** button to verify the credentials provided.

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



On the **Configure the database server** page, enter the following information in the provided text boxes:

- **Server** – Specify the SQL Server cluster name and instance name created earlier. For the reference deployment the server and instance value is **SCDB\SCDB**.
- **Port** – Specify the TCP port used for the SQL Server, if not the default. For the reference deployment the SCDB instance port is 10433.

In the Authentication Credentials section, select the Windows Authentication option, and click the Test Database Connection button.

When successful, click Next to continue.



On the **Configure the database** page, make sure you have selected **Existing database** and that the appropriate database is selected. The default is Orchestrator. Click **Next** to continue.

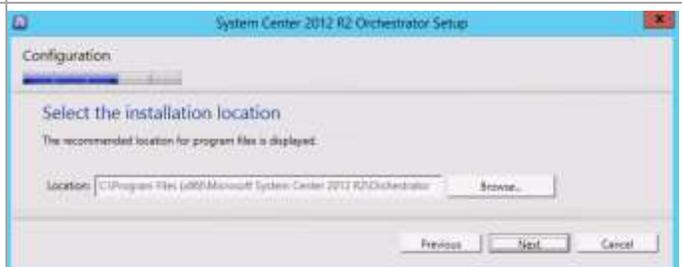


On the **Configure Orchestrator users group** page, select the Orchestrator users group created earlier from the **Browse...** button and select to search the domain. For this installation, this is the domain Orchestrator operators group outlined at the beginning of this section.

Verify that the **Grant remote access to the Runbook Designer** check box is not selected since that option is not being installed, and click **Next** to continue.



On the **Select the installation location** page, specify a location or accept the default location of %ProgramFiles(x86)%\Microsoft System Center 2012 R2\Orchestrator for the installation. Click **Next** to continue.



On the **Microsoft Update** page, select the appropriate radio button for your environment.



The **Help Improve Microsoft System Center Orchestrator** page provides options for participating in the error reporting feedback mechanisms. Select the appropriate option based on your organization's policies, and click **Next** to continue.



The **Installation summary** page will display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.



The **Installing features** page will show the installation progress.



The **Setup completed successfully** page will appear when all portions of the setup complete successfully. Verify that all check boxes are cleared, and click **Close** to finish the installation.



Some additional firewall rules are required. Enter the PowerShell cmdlets at the right to enable and add the required rules.

```
Enable-NetFirewallRule -  
DisplayName "Windows Management  
Instrumentation (WMI-In)"
```

```
Enable-NetFirewallRule -  
DisplayName "Windows Management  
Instrumentation (DCOM-In)"
```

```
Enable-NetFirewallRule -  
DisplayName "Windows Management  
Instrumentation (ASync-In)"
```

```
New-NetFirewallRule -DisplayName  
"SCO - Orchestrator Management  
Service (x64)" -Program  
"C:\Program Files (x86)\Microsoft  
System Center 2012  
R2\Orchestrator\Management  
Server\ManagementService.exe"
```

Post-Installation Tasks

After the installation is complete, install and configure Orchestrator Integration Packs on the target runbook servers.

Install Microsoft Report Viewer 2012

Additionally, Orchestrator requires the Operations Manager console, but prior to installing it, you must install the Microsoft Report Viewer 2012 package.

Use the following procedure to install the Microsoft Report Viewer 2012 package.

► Perform the following steps on all Orchestrator virtual machines.

From the installation media source, double-click **SQLSysClrTypes.msi** to begin setup.

Name	Type	Size
SQLSysClrTypes	Windows Installer Package	2,460 KB

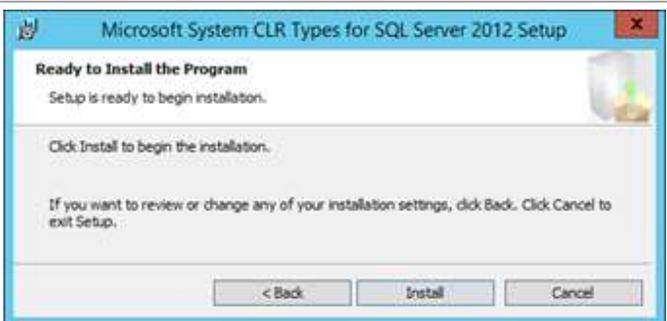
On the **Welcome to the Installation...** page click **Next**.



On the **License Agreement** page, select the **I accept the license terms** check box and click **Next** to continue.



On the **Ready to Install the Program** page click **Install**.



On the **Completing the Microsoft System...Installation** page click **Finish**.



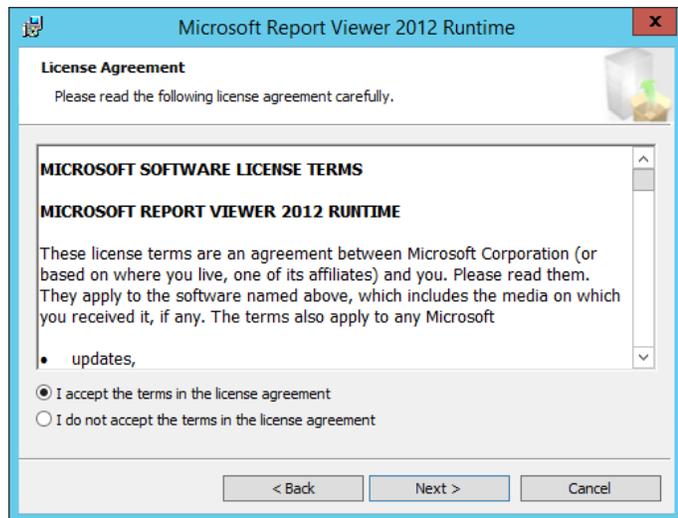
From the installation media source, right-click **ReportViewer.exe** and select **Run as administrator** to begin setup.



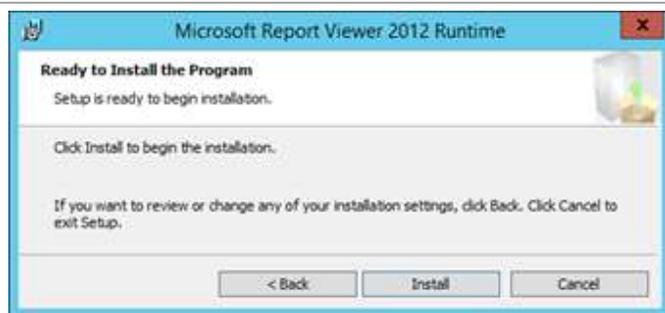
On the Microsoft Report Viewer 2012 Runtime setup wizard **Welcome to the Installation...** page click **Next**.



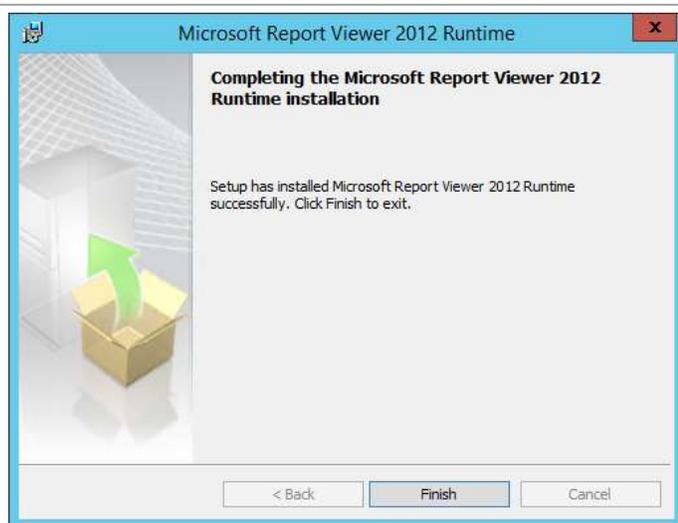
On the **License Agreement** page, select the **I accept the license terms** check box and click **Next** to continue.



On the **Ready to Install the Program** page click **Install**.



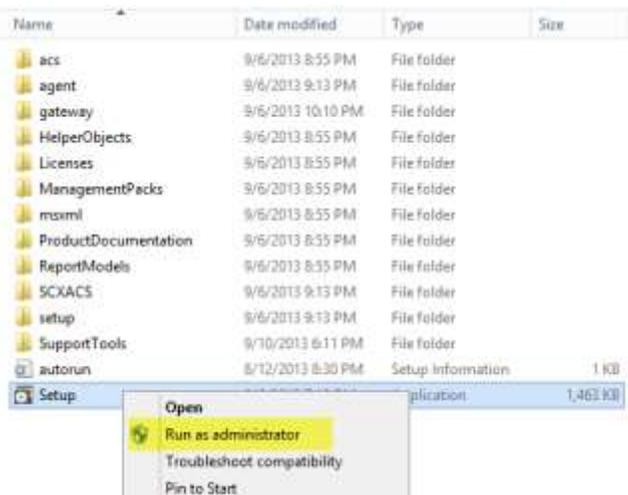
On the **Completing the Microsoft Report Viewer 2012 Runtime Installation** page click **Finish**.



Install the Operations Manager Console

► Perform the following steps on all Orchestrator virtual machines.

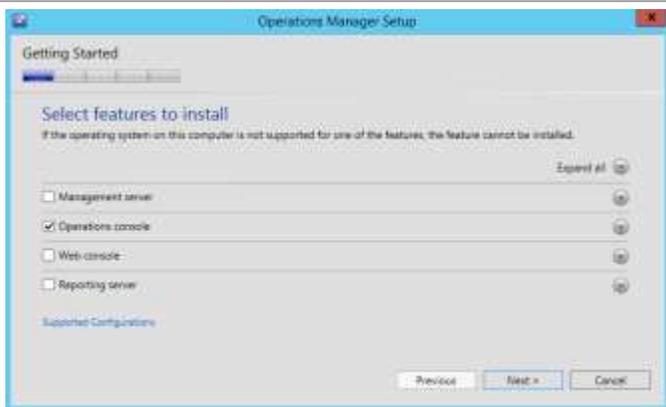
From the Operations Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



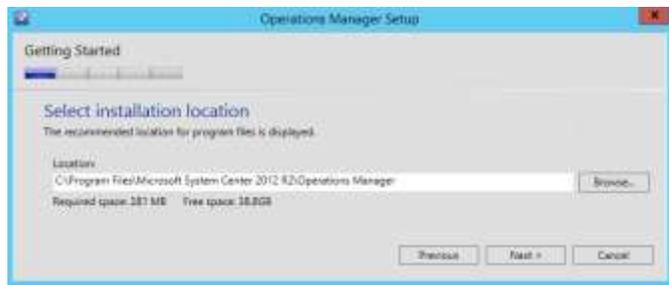
The Operations Manager installation wizard will begin. Click **Install** to begin the Operations Manager console installation.



On the **Select features to install** page, verify that the **Operations console** check box is selected. Click **Next** to continue.



On the **Select installation location** page, specify a location or accept the default location of C:\ProgramFiles\System Center 2012 R2\Operations Manager for the installation. Click **Next** to continue.



The wizard will verify that all system prerequisites are met. If any prerequisites are not met, they will be displayed on the **Proceed with Setup** page. After you verify that the prerequisites are met, click **Next** to continue.



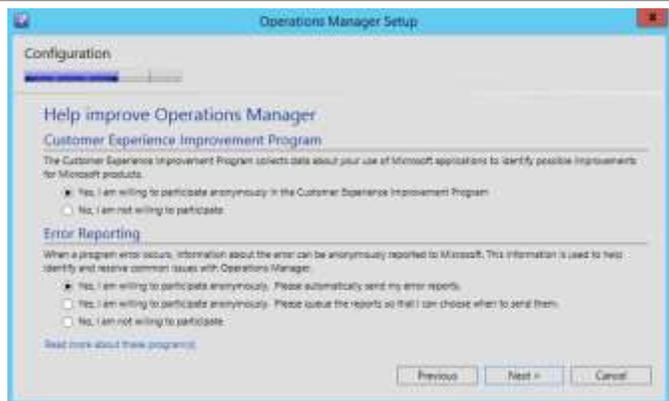
On the **Please read the license terms** page, verify that the **I have read, understood and agree with the license terms** check box is selected, and click **Next** to continue.



The **Help Improve Operations Manager** page 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.

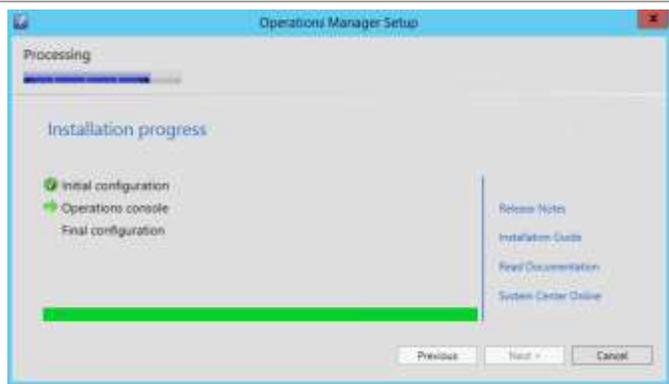


On the **Microsoft Update** page, select the update options for your environment. Click **Next** to continue.

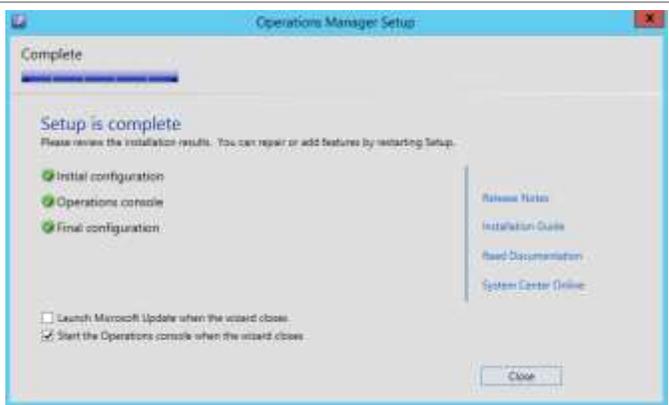
The **Installation Summary** page will appear and display the selections made during the installation wizard. Review the options selected, and click **Install** to continue.



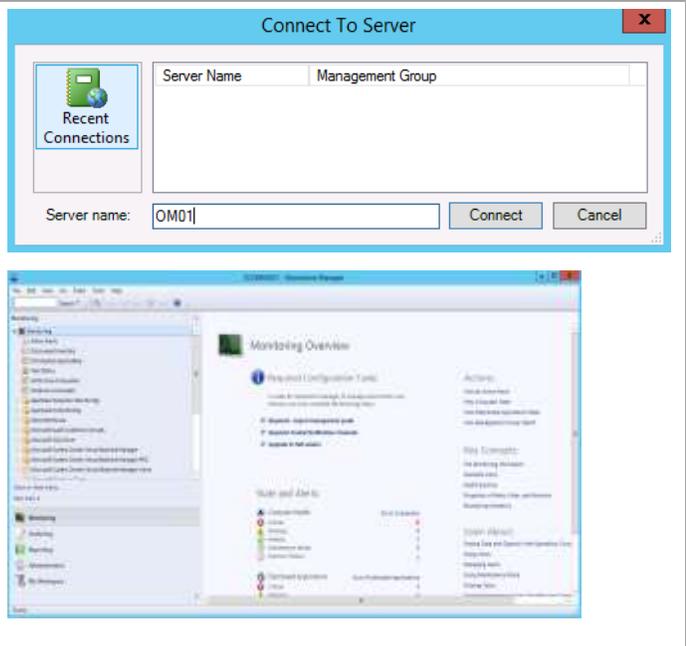
The wizard will display the progress while performing the installation.



After the installation completes, the wizard will display the **Setup is complete** page. Verify that the **start the Management console when the wizard closes** check box is selected, and click **Close** to complete the installation.



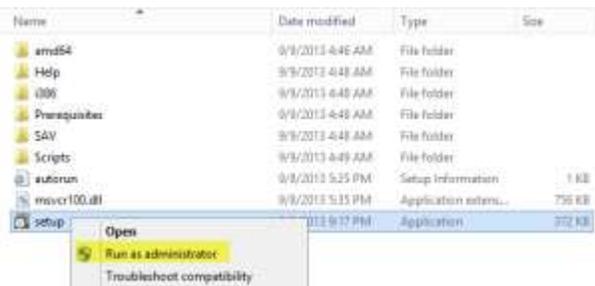
The **Operations Manager console** will open. Validate the installation by reviewing the configuration and make sure that the console operates properly.



Install the Virtual Machine Manager Console

► Perform the following steps on the Orchestrator virtual machines.

Log on to the Orchestrator server as a user with Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



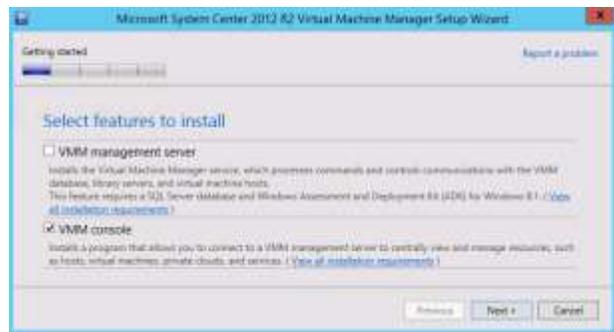
The Virtual Machine Manager Setup Wizard will appear. Click **Install** to begin the Virtual Machine Manager server installation.



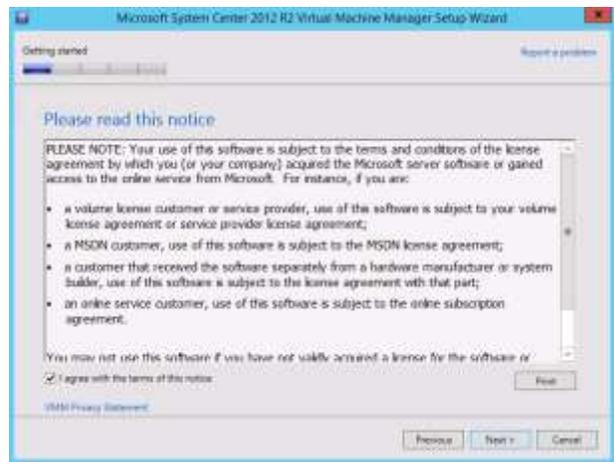
You will receive a message stating the prerequisite software was installed and the system will need to be restarted. Reboot the system, then restart the installation.



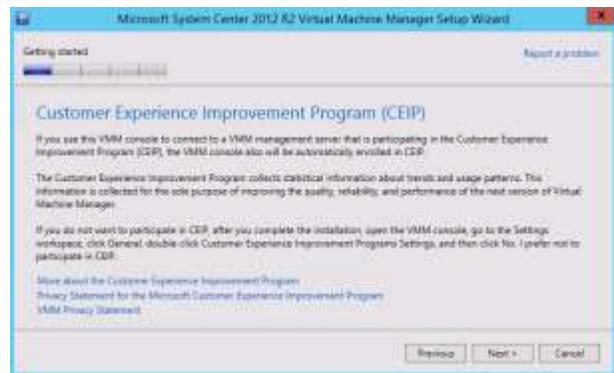
On the **Select features to install** page, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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



On the **Customer Experience Improvement Program** page, click **Next** to continue.



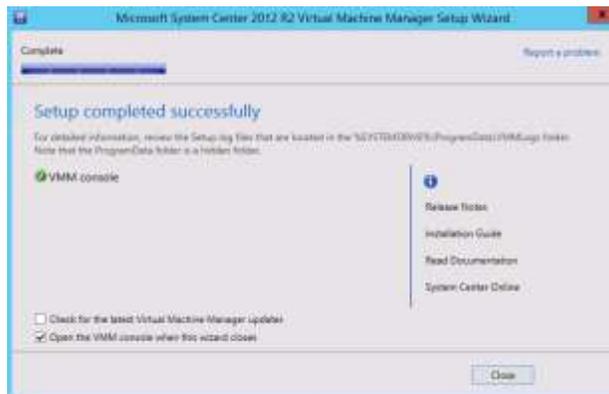
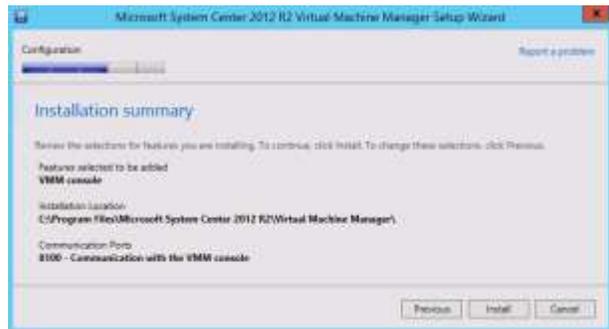
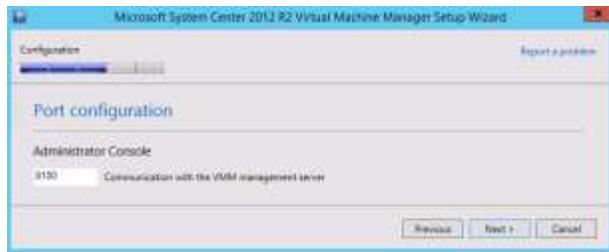
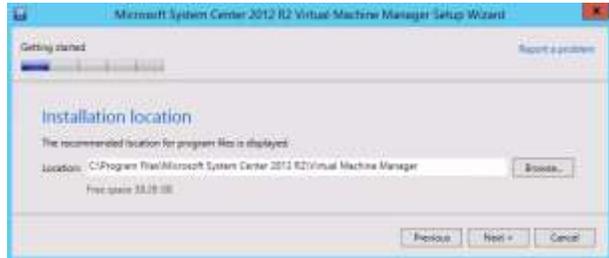
Depending on the current configuration of the server, the Microsoft Update page may appear. Select the option to allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates, based on your organization's policies. Click **Next** to continue.

On the **Select installation location** page, specify a location or accept the default location of **C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager** for the installation. Click **Next** to continue.

On the **Port Configuration** page, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be **8100**. Click **Next** to continue.

The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.

When the installation completes, the wizard will display the **Setup completed successfully** page. Clear the box to check for VMM updates. Make sure the box is checked to open the VMM console to make sure it is properly working. Click **Close** to complete the installation.



Download and Register the Orchestrator Integration Packs

Complete the following steps to register the Orchestrator Integration Packs.

► Perform the following steps on all Orchestrator runbook server virtual machines.

Download the [System Center 2012 R2 – Orchestrator Component Add-ons and Extensions](#) from the Microsoft Download Center.

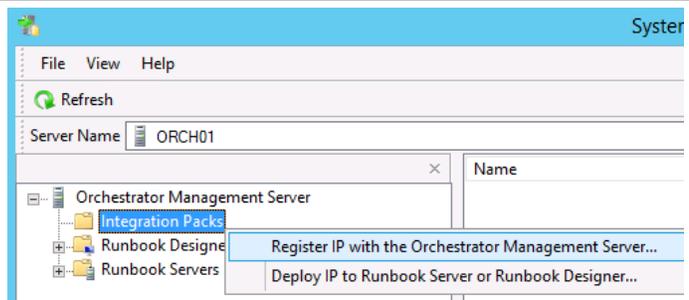
Expand the Orchestrator Integration Pack files.

Name	Date modified
attributions	3/14/2012 4:23 PM
Configuration_Manager_2007_Integration_Pack.oip	3/14/2012 5:11 PM
Data_Protection_Manager_2010_Integration_Pack.oip	3/14/2012 5:11 PM
Operations_Manager_2007_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Configuration_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Data_Protection_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Operations_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Service_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
SC2012_Virtual_Machine_Manager_Integration_Pack.oip	3/14/2012 5:11 PM
Service_Manager_2010_Integration_Pack.oip	3/14/2012 5:11 PM
Virtual_Machine_Manager_2008_Integration_Pack.oip	3/14/2012 5:11 PM

On the **Start** screen, click the **Deployment Manager** tile.



In the **Runbook Designer** console on the selected runbook server, right-click the **Integration Packs** node, and click **Register IP with the Orchestrator Management Server...**

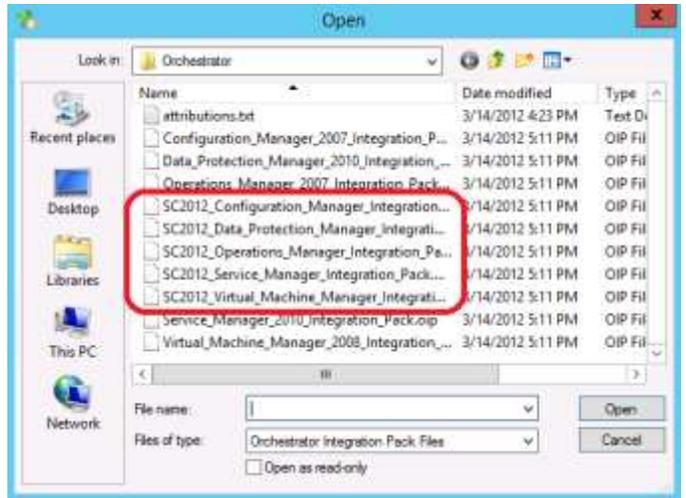
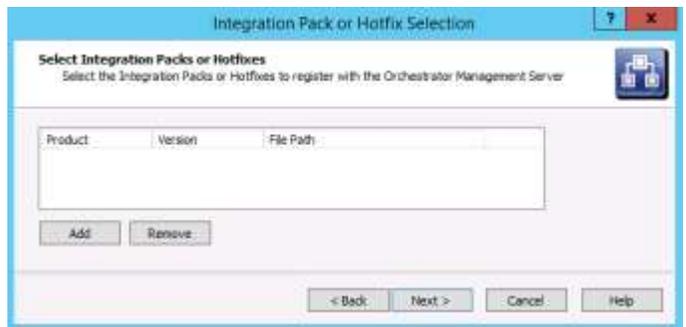


The **Integration Pack Registration Wizard** will appear. Click **Next** to continue.

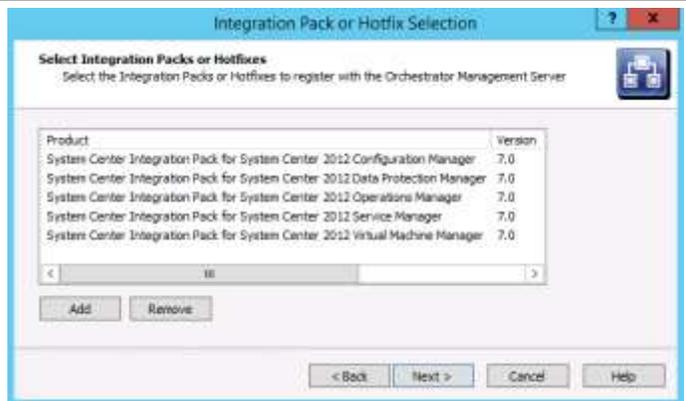


On the **Select Integration Packs or Hotfixes** page, click **Add**. Navigate to the expanded integration packs folder created earlier. Select the following integration packs from the **File name** drop-down list, and click **Open**:

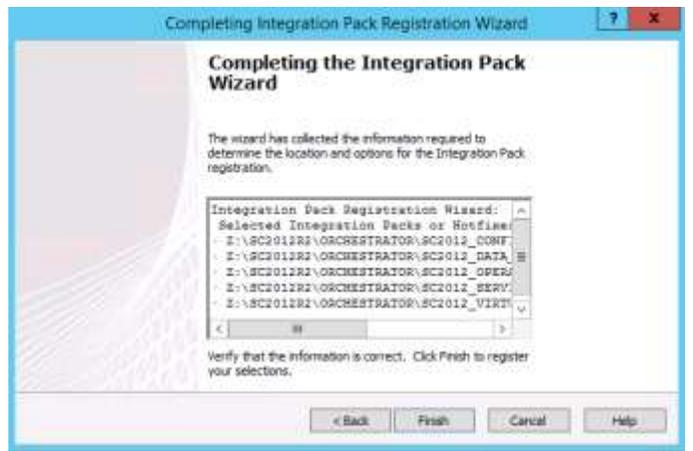
- System Center 2012 Configuration Manager
- System Center 2012 Data Protection Manager
- System Center 2012 Operations Manager
- System Center 2012 Service Manager
- System Center 2012 Virtual Machine Manager



When all the integration packs are open, click **Next** to continue.



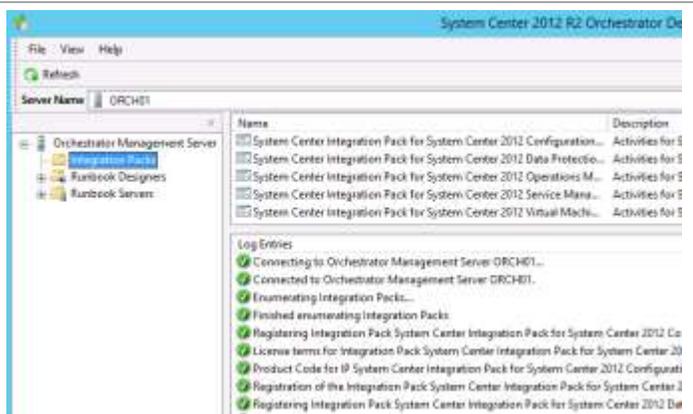
The **Completing the Integration Pack Wizard** page will appear with a summary of selections. Verify the selections, and click **Finish** to begin the integration pack installation.



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 Orchestrator Deployment Manager interface.



Deploy the Orchestrator Integration Packs

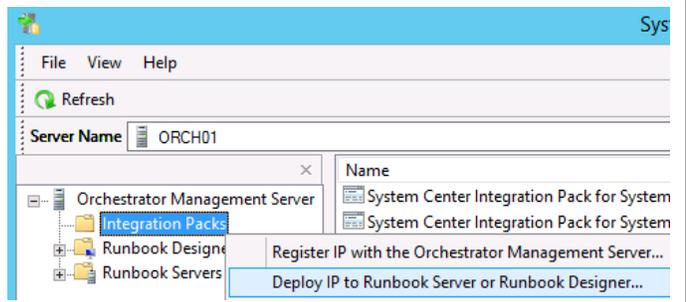
Complete the following steps to deploy the Orchestrator Integration Packs.

- ▶ Perform the following steps on Orchestrator virtual machine with the Runbook Designer role.

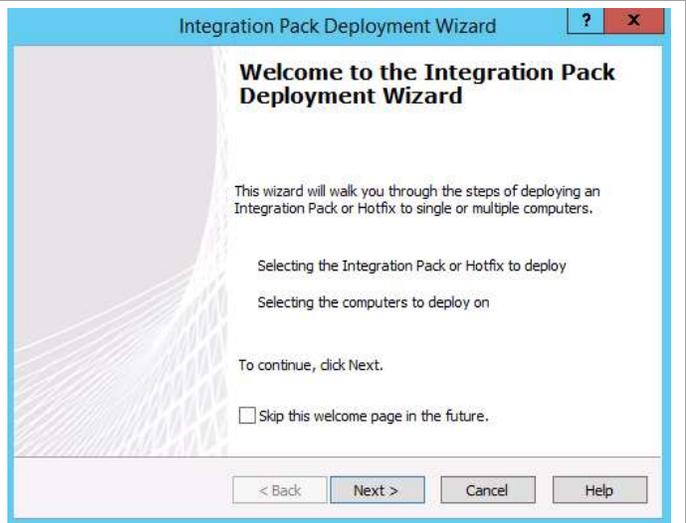
On the **Start** screen, click the **Deployment Manager** tile.



In the **Runbook Designer** console on the selected runbook server, right-click the **Integration Packs** node and select **Deploy IP to Runbook Server or Runbook Designer...**



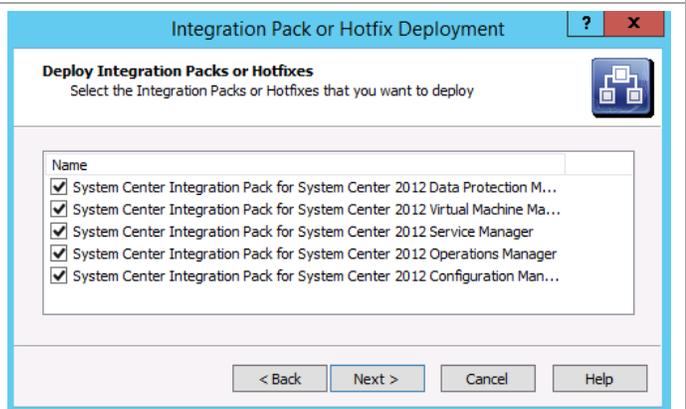
The **Integration Pack Deployment Wizard** will appear. Click **Next** to continue.



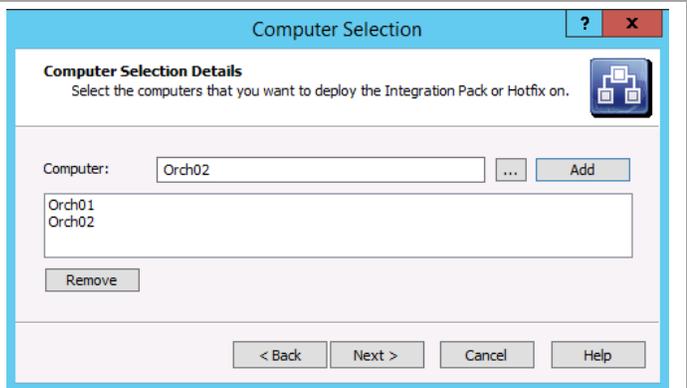
On the **Deploy Integration Packs or Hotfixes** page, select the check boxes for the following integration packs:

- System Center 2012 Configuration Manager
- System Center 2012 Data Protection Manager
- System Center 2012 Operations Manager
- System Center 2012 Service Manager
- System Center 2012 Virtual Machine Manager

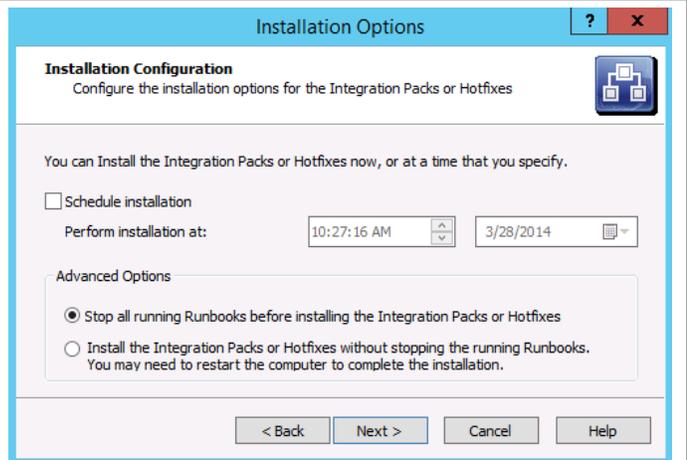
Click **Next** to continue.



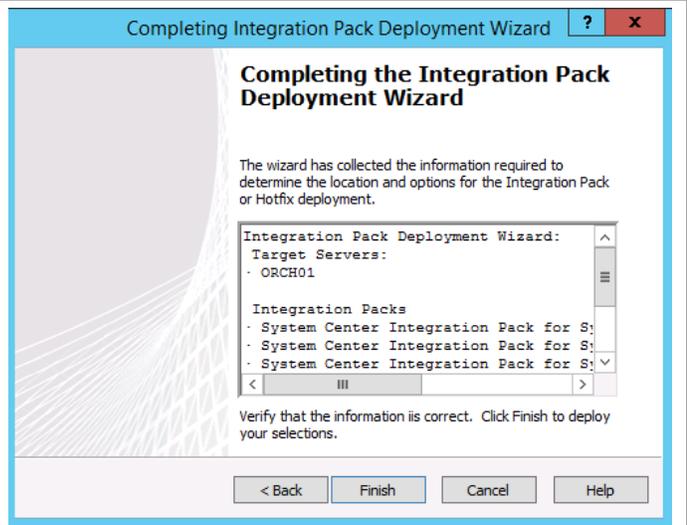
On the **Computer Selection Details** page, type the names of the Orchestrator management servers and click **Add**. When all servers are added, click **Next** to continue.



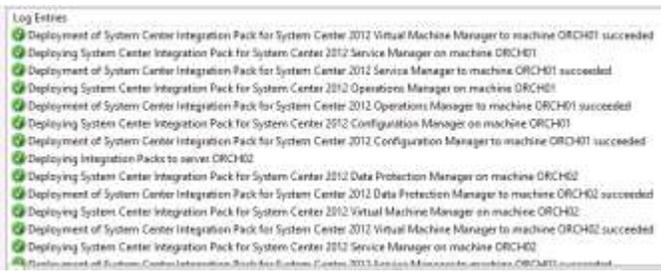
On the **Installation Configuration** page, in the **Advanced Options** section, select **Stop all running Runbooks before installing the Integration Packs or Hotfixes**. Click **Next** to continue.



The **Completing the Integration Pack Deployment Wizard** will appear with a summary of selections. Click **Finish** to begin the integration pack installation.



When complete, you will be able to see in the log file the success of the deployment.



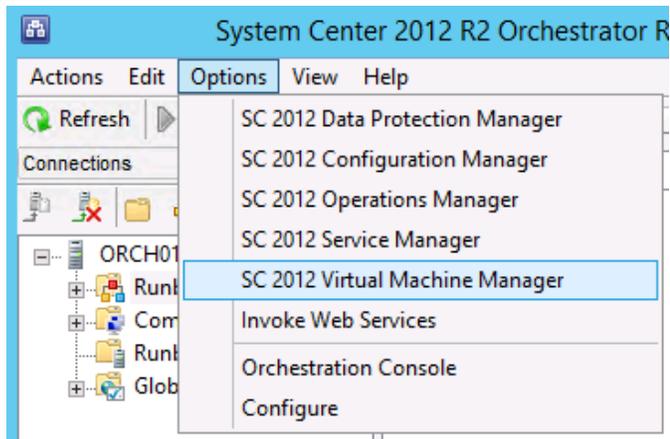
On the **Start** screen, click the **Runbook Designer** tile.



Verify that each integration pack is displayed in the **Runbook Designer** interface.



To complete the configuration of the integration packs, open the **Orchestrator Runbook Designer Console**, click the **Options** menu, and click **SC 2012 Virtual Machine Manager**.

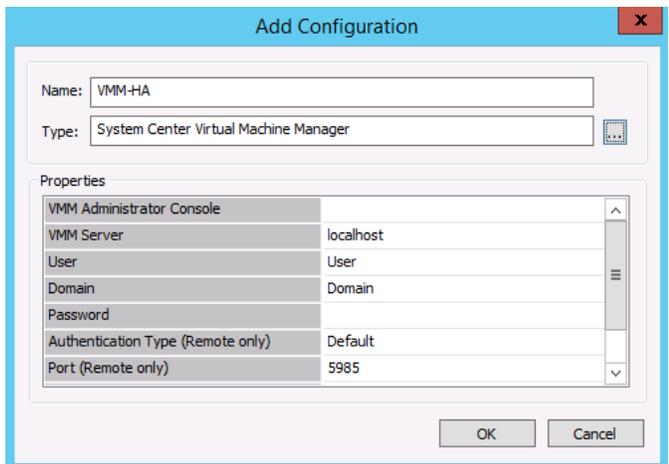


On the **Prerequisite Configuration** page, click **Add**.

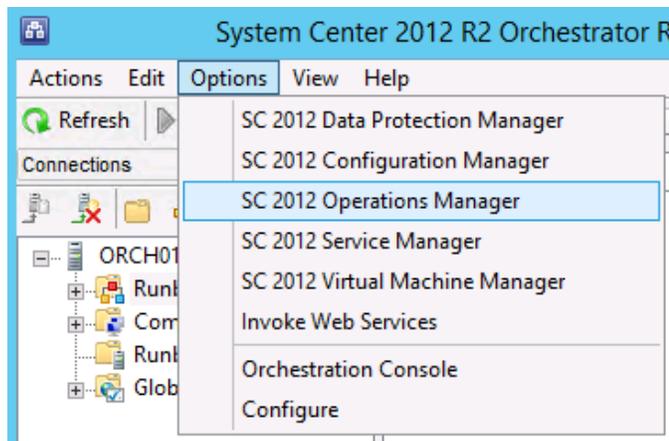


On the **Add Configuration** page, fill in the required information for the Virtual Machine Manager server and click **OK**.

On the **Prerequisite Configuration** page, click **Finish** to save the changes.



While still in the **Orchestrator Runbook Designer Console**, click the **Options** menu, and click **SC 2012 Operations Manager**.



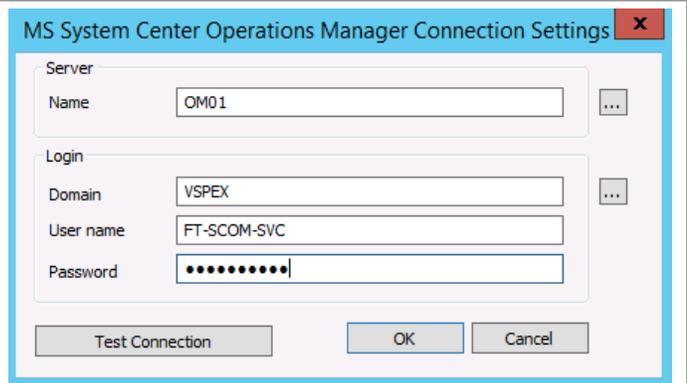
On the **Microsoft System Center Operations Manager Connections** page, click **Add**.



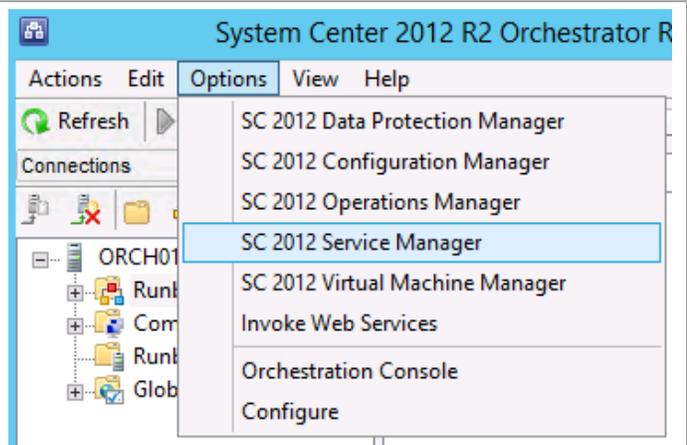
On the **MS System Center Operations Manager Connection Settings** page, fill in the required information for the Operations Manager management server, and click **Test Connection**⁴.

When connectivity is verified, click **OK**.

On the **Prerequisite Configuration** page, click **Finish** to save the changes.



In the **Orchestrator Runbook Designer** console, click the **Options** menu, and click **SC 2012 Service Manager**.



⁴ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

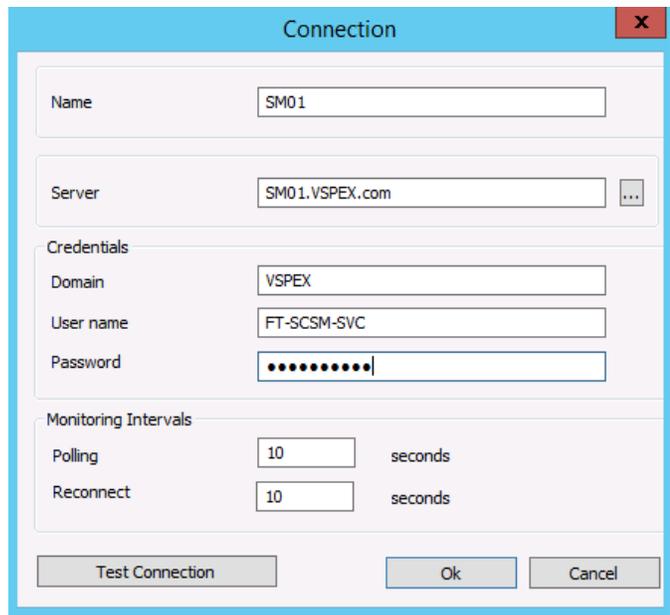
On the **Connections** page, click **Add**.



On the **Connection** page, fill in the required information for the Service Manager management server,⁵ and click **Test Connection**.

When connectivity is verified, click **OK**.

On the **Prerequisite Configuration** page, click **Finish** to save the changes.

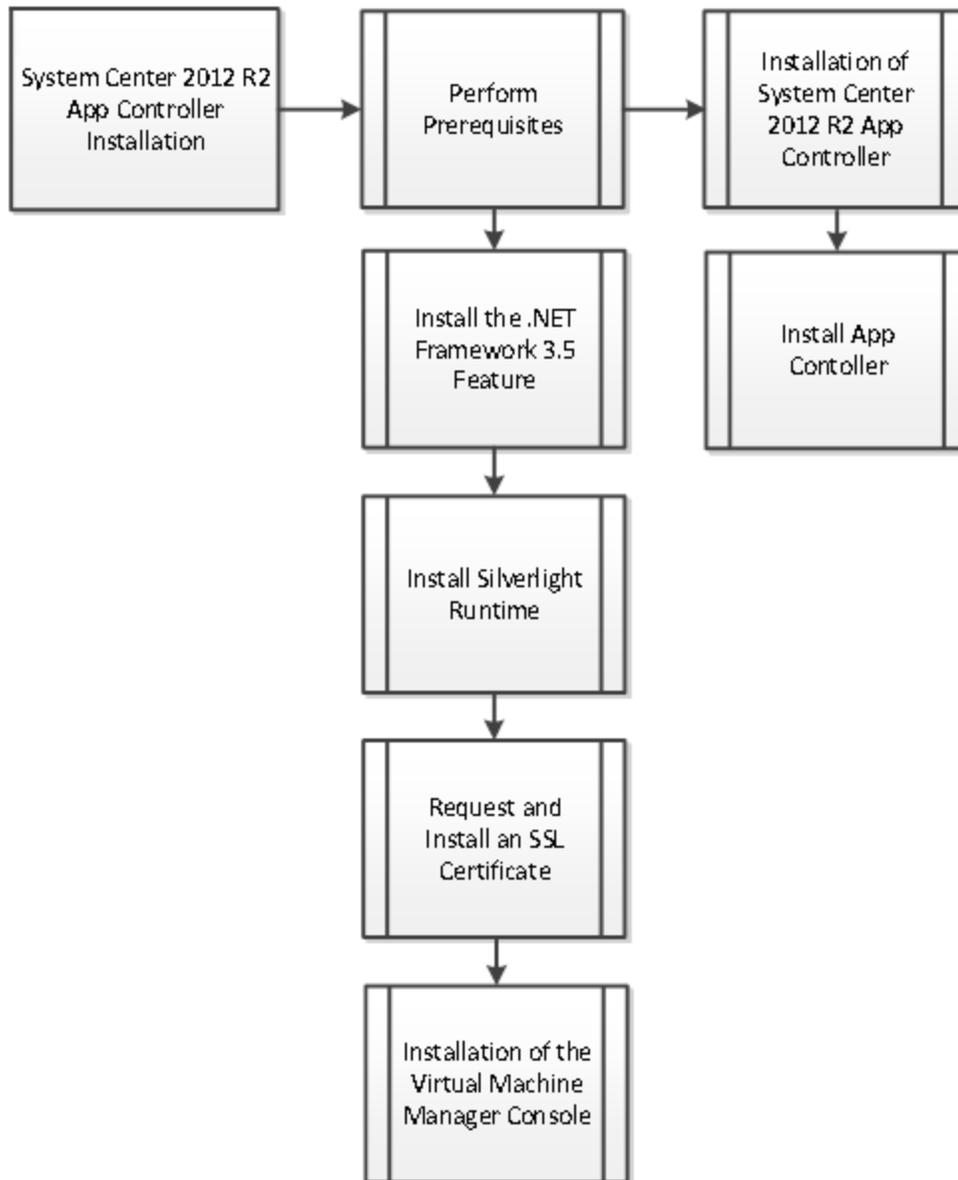


⁵ The use of the Administrator account is used as an example. Use account information that is applicable to your installation.

App Controller

The App Controller installation process includes the high-level steps shown in the following figure.

Figure 11. App Controller Installation Process



Overview

This section provides a high-level walkthrough for how to set up App Controller. The following requirements are necessary for the setup:

- A base virtual machine running Windows Server 2012 R2 has been provisioned for App Controller.
- A SQL Server 2012 SP1 cluster with dedicated instance has been established in previous steps for App Controller.

- The System Center Virtual Machine Manager console is installed.
- .NET Framework 3.5 is installed.
- Microsoft Silverlight Runtime is installed.
- A Trusted Server Authentication (SSL) Certificate (the CN field of the certificate must match the server name) is installed.

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following service accounts have been created:

Table 29. App Controller Accounts

User name	Purpose	Permissions
<DOMAIN>\ FT-SCAC-SVC	App controller service account	This account needs to be a member in the following groups: <ul style="list-style-type: none"> • FT-SCAC-Admins • FT-SCVMM-Admins

Groups

Verify that the following security groups have been created:

Table 30. App Controller Security Groups

Group name	Purpose	Members
<DOMAIN>\ FT-SCAC-Admins	App Controller Admin group	<DOMAIN>\ FT-SCAC-SVC <DOMAIN>\ FT-SCVMM-Admins

Add .NET Framework 3.5

The App Controller installation requires that .NET Framework 3.5 is enabled to support installation. Use the following procedure to enable .NET Framework 3.5.

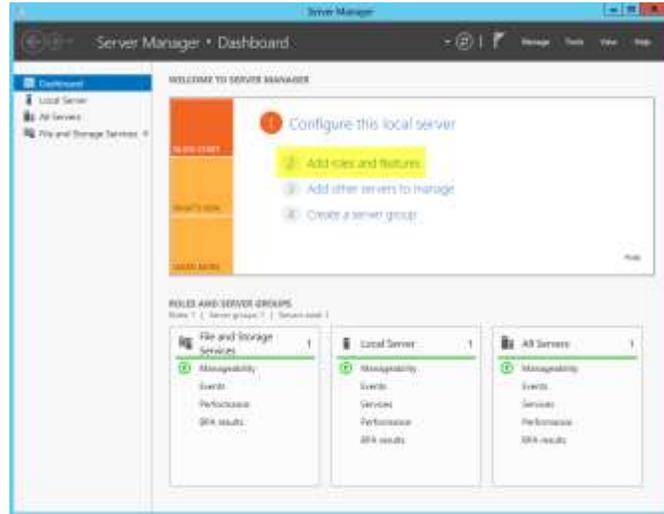
► Perform the following steps on the App Controller virtual machine.

If you do not have access to the internet to contact Microsoft Update, you will need to have the Windows Installation files mounted locally or on an accessible file share.

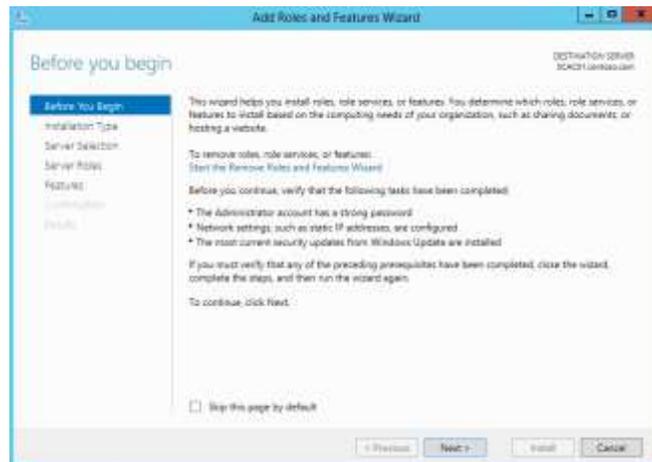
The .NET Framework 3.5 feature can be installed with a PowerShell cmdlet, or the following instructions can be followed for using the GUI. If the VM has access to the internet, the `-Source` parameter should not be needed.

```
Install-windowsFeature -Name NET-  
Framework-Core -Source  
"E:\Sources\sxs"
```

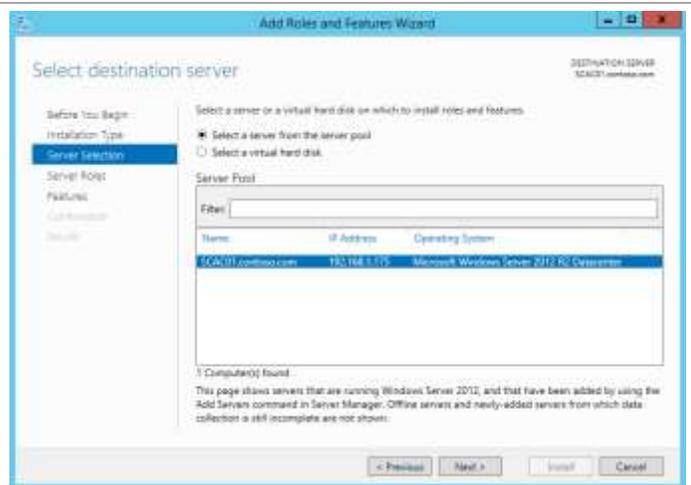
Open **Server Manager** and navigate to the **Dashboard**. In the main pane, under **Configure this local server**, click **Add roles and features**.



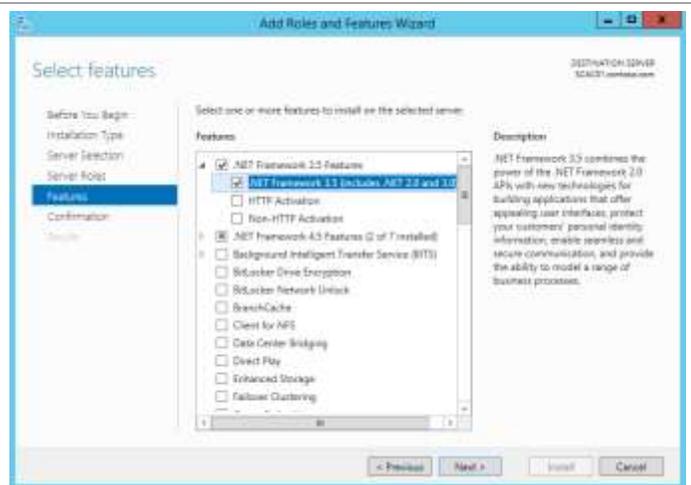
The Add Roles and Features Wizard will appear. On the **Before You Begin** page, click **Server Selection** in the left pane to continue.



On the **Select destination server** page, select the **Select a server from the server pool** button, select the local server, and then click **Features** in the left pane to continue.



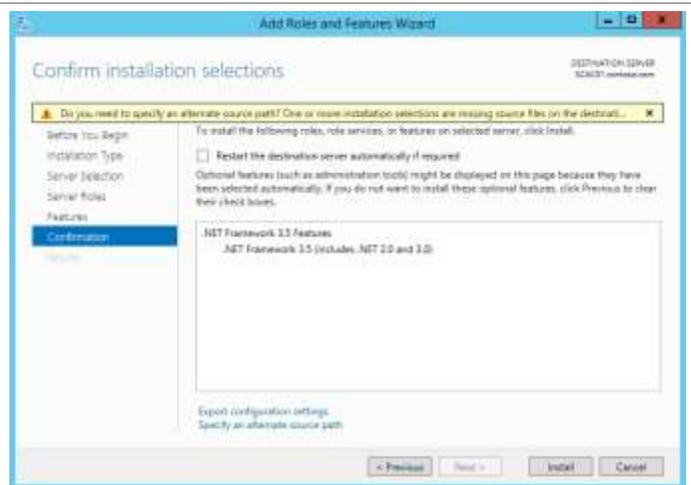
To add .NET Framework 3.5, on the **Select Features** page, in the **Features** pane select the **.NET Framework 3.5 Features** and **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** check boxes only. Leave all other check boxes clear. Click Next to continue.



On the **Confirm installation selections** page, verify that **.NET Framework 3.5 Features** is listed. Make sure that the **Restart each destination server automatically if required** is not selected. Click **Install** to begin installation.

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

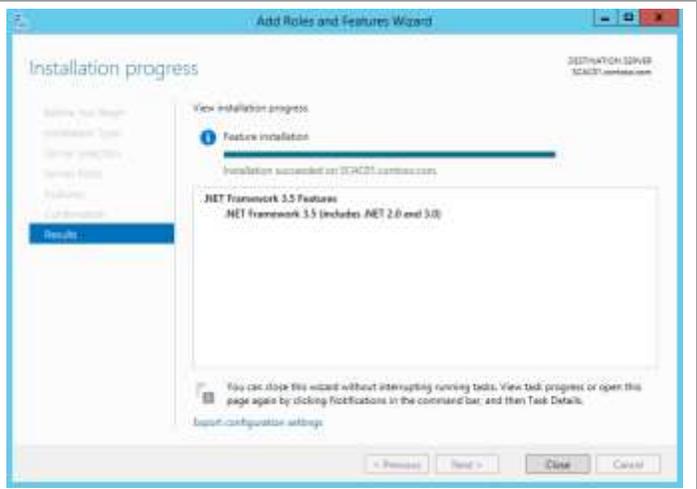
If the server does not have Internet access, an alternate source path can be specified by clicking the **Specify an alternate source path** link.



For servers without Internet access or if the .NET Framework 3.5 source files already exist on the network, an alternate source location be specified here for the installation.



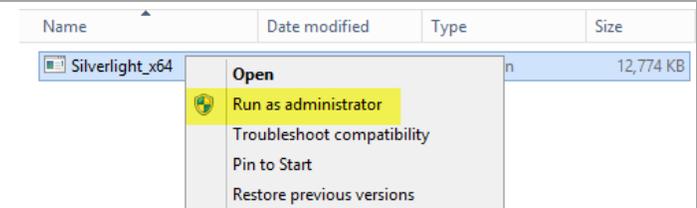
The **Installation Progress** page will show the progress of the feature installation. Click **Close** when the installation process completes.



Install Silverlight

► Perform the following steps on the App Controller virtual machine.

From the installation media source, right-click **Silverlight.exe** and select **Run as administrator** to begin setup.



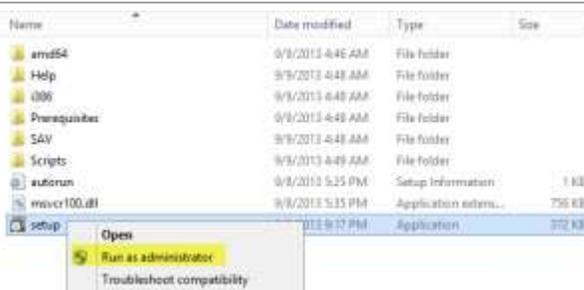
<p>On the Install Silverlight page, click Install now.</p>	
<p>On the Enable Microsoft Update page, select or clear the Enable Microsoft Update check box, based on organizational preferences, and click Next to continue.</p>	
<p>On the Installation Successful page, click Close.</p>	

Install the Virtual Machine Manager Console

Complete the following steps install the Virtual Machine Manager console on the target App Controller virtual machines.

► Perform the following steps on the App Controller virtual machines.

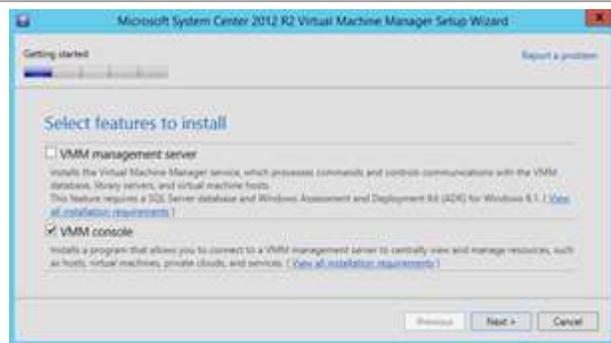
Log on to the App Controller server as a user with Administrator privileges. From the Virtual Machine Manager installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



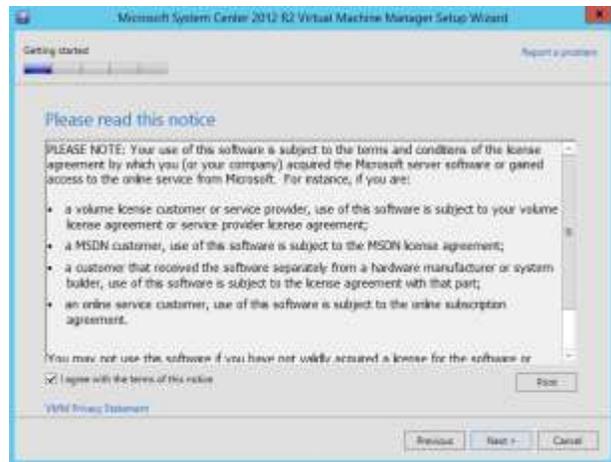
The Virtual Machine Manager Setup Wizard will appear. Click **Install** to begin the Virtual Machine Manager server installation.



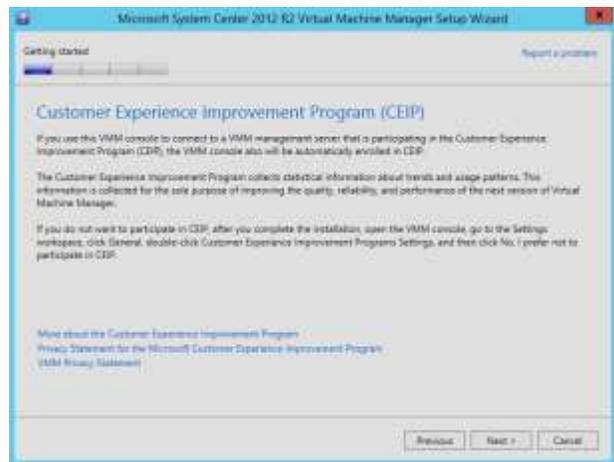
On the **Select features to install** page, verify that the **VMM console** installation option check box is selected. Click **Next** to continue.



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

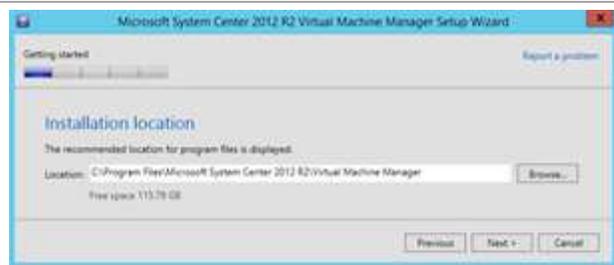


On the **Customer Experience Improvement Program** page, click **Next** to continue.

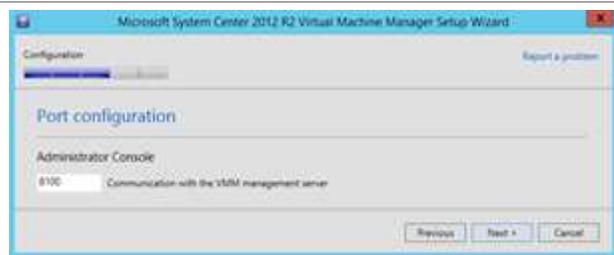


Depending on the current configuration of the server, the Microsoft Update page may appear. Select the option to allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates, based on your organization's policies. Click **Next** to continue.

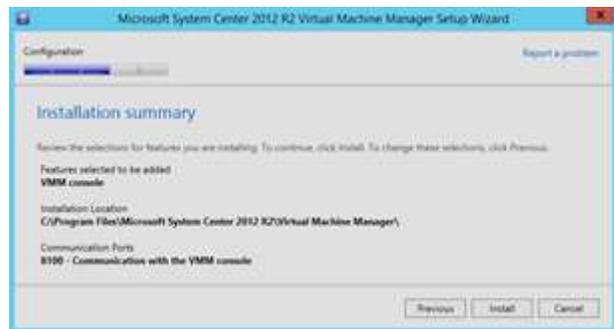
On the **Select installation location** page, specify a location or accept the default location of **C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager** for the installation. Click **Next** to continue.



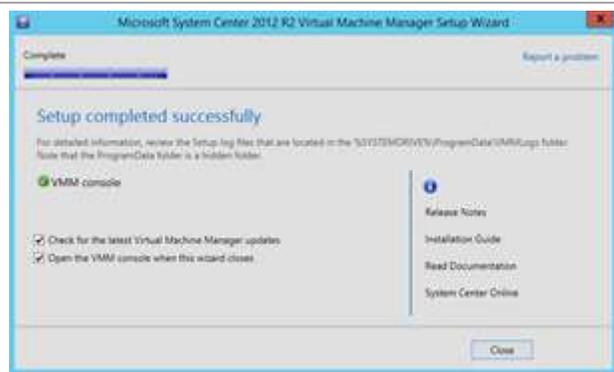
On the **Port Configuration** page, specify the port used for communication with the VMM management server in the provided text box. If no modifications were made during Virtual Machine Management installation, the default port would be 8100. Click **Next** to continue.



The **Installation summary** page will appear and display the selections made during the Setup Wizard. Review the options selected, and click **Install** to continue.



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



Installation

Install the App Controller Portal Server

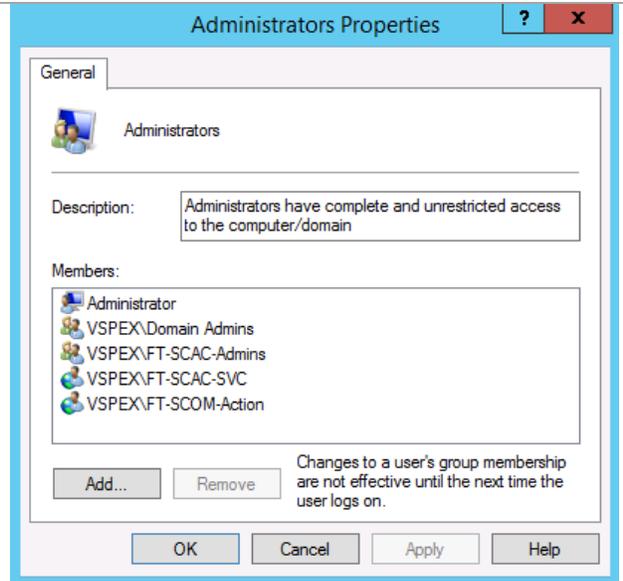
Complete the following steps to install the App Controller portal server.

- ▶ Perform the following steps on the App Controller virtual machine.

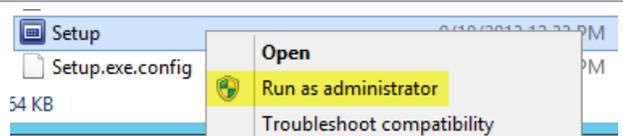
Log on to the App Controller virtual machine as a user with local Admin rights.

Verify the following accounts or groups are members of the local Administrators group on the App Controller portal virtual machine:

- Operations Manager action account
- App Controller service account
- App Controller Admins group



Log on to the System Center App Controller server. From the **System Center App Controller** installation media source, right-click **setup.exe** and select **Run as administrator** to begin setup.



The App Controller Setup Wizard will appear. Click **Install** to begin the App Controller server installation.



On the **Enter your product registration information** page, provide a valid product key for the Orchestrator installation. If no key is provided, App Controller will be installed in evaluation mode. Click **Next** to continue.



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



On the **Install missing software** page, 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 display the progress while installing features.



On the **Select the installation path** page, accept the default installation location of %ProgramFiles%\Microsoft System Center 2012\App Controller, or click the **Browse** button to specify a different location. After making a selection, click **Next** to continue.



Before proceeding with the following steps, install a certificate on this system. Earlier, steps had been provided to request and install a certificate from a third party. Active Directory also has a Certificate Services component. If your organization has its own Certificate Authority and it is set up for auto-enrollment, these following steps can be followed. It happens at this point in time because IIS has now been installed on this system.

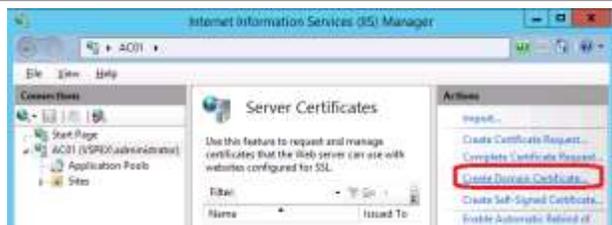
From the Start menu, launch the **Internet Information Services Manager**.



Click the Application Controller home page in the Connections pane. From the IIS section in the middle, double-click **Server Certificates**.

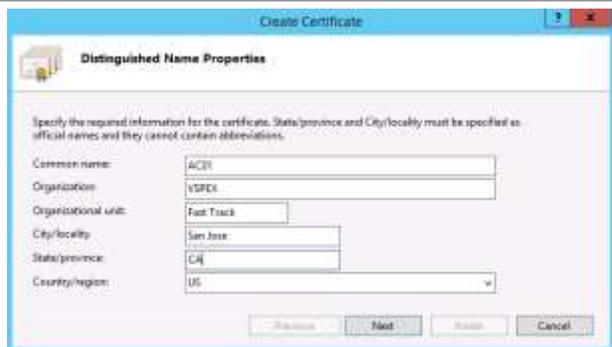


From the Actions pane, click **Create Domain Certificate ...**



Fill in the contents of the Create Certificate window. Make sure that Common Name is the same as the name of the Applications Controller server.

Click **Next** to continue.



Click the **Select...** button to obtain a drop-down list of available certificate servers. Select the one appropriate to your environment.

Enter the name of the Application Controller server as the Friendly name.

Click **Finish** to install the certificate.

When the certificate has been installed, return to the installation of the Application Controller server software.



On the **Configure the services** page, 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, keep the default port selection.

Click **Next** to continue.



On the **Configure the website** page, provide the following information:

In the **Type: HTTPS**, in the **IP address** text box, select **All unassigned** from the drop-down list. 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 list.

Click **Next** to continue.

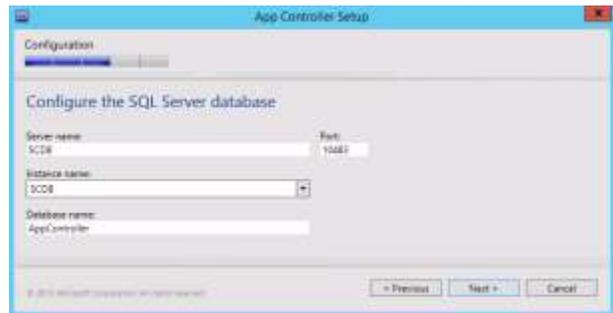
Note: Although not recommended, if a Server Authentication certificate cannot be obtained and installed on the App Controller server, you may choose the **Generate self-signed certificate** option to satisfy installation requirements.



On the **Configure the SQL Server database** page, make the following selections to 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. For the reference installation the server name is **SCDB**.
- **Port** – Specify the TCP port used for SQL Server connectivity. For the reference installation the port value is **10483**.
- **Instance name** - Specify the instance name where the AppController database will be installed (the SCDB instance). For the reference installation the instance name is **SCDB**.
- **Database name** – Specify the name of the App Controller database. In most cases, use the default value of AppController.

Click **Next** to continue.



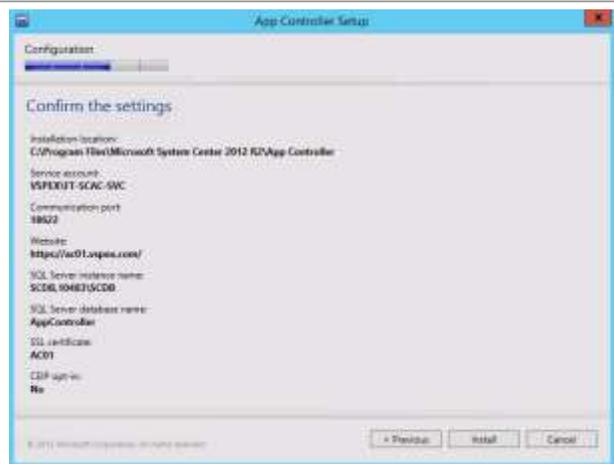
The **Help Improve App Controller for System Center 2012** page provides options for participating in various product feedback mechanisms. These include:

- **Customer Experience Improvement Program (CEIP)**
- **Microsoft Update**

Select the appropriate options, based on your organization's policies, and click **Next** to continue.



On the **Confirm the settings** page, verify the settings provided during the Setup Wizard, and click **Install** to begin the installation.

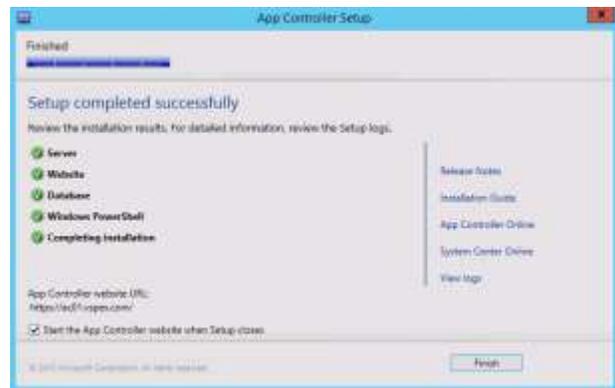


The wizard will display the progress while installing features



When complete, the **Setup completed successfully** page will appear with progress of each component. Verify that each component installed successfully. Note the App Controller website in the provided text box.

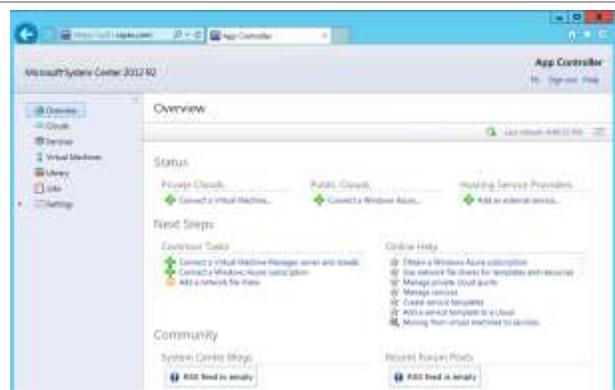
Verify that the **Start the App Controller website when Setup closes** check box is selected, and click **Finish**.



The **System Center 2012 App Controller** website will appear. Because no users have been created in SCVMM, enter in the administrative account used to install Virtual Machine Manager (which has been assigned an admin role in SCVMM). Click **Sign in**.



The App Controller portal will appear. After validating functionality, the App Controller installation is considered complete.



Cisco Integration Components

Cisco has created several integration components to assist organizations in running the Microsoft Private Cloud on Cisco UCS environments.

- PowerTool
- Operations Manager Management Pack
- Orchestrator Integration Pack

- Virtual Machine Manager User Interface Extension
- Cisco Nexus 1000V

Check the Software Revision table for the location from which these components can be downloaded.

Cisco UCS PowerTool and Cisco Nexus 1000V PowerShell Module

The Cisco UCS PowerTool need to be installed on several different systems:

- Configuration Workstation – a Microsoft Windows 8.1 or Microsoft Windows Server 2012 R2 system configured as a workstation from which the environment can be remotely configured and managed
- System Center Virtual Machine Manager – the Cisco Add-In for SCVMM relies on PowerTool
- System Center Operations Manager – the Cisco Management Pack utilizes PowerTool to provide information to SCOM
- System Center Orchestrator – the Cisco Integration Pack makes use of PowerTool and allows for call-out to PowerTool within runbooks

In addition to the Cisco UCS PowerTool module, the Cisco Nexus 1000V module needs to be installed in different systems:

- Configuration Workstation – The Cisco Nexus 1000V installation procedure has PowerShell scripts using the 1000V PowerShell module. Therefore, the 1000V module should be installed on the configuration workstation
- Hyper-V Hosts – For Hyper-V hosts that are running the Virtual Ethernet Module (VEM), the 1000V PowerShell module needs to be installed
- System Center Orchestrator – if you plan on creating runbooks to automate configuration of the Cisco Nexus 1000V, the 1000V PowerShell module should be installed on the runbook servers

Before You Begin

Before beginning the installation of Cisco PowerTool and the Cisco Nexus 1000V PowerShell module, make sure the following:

- There are no open windows running Windows PowerShell
- Uninstall all versions of Cisco UCS PowerTool that are older than Cisco UCS PowerTool, Release 0.9.1.0.
- You have downloaded the latest versions of software
 - Cisco PowerTool version 1.1.1
 - Cisco Nexus 1000V version 1.5(2a) contains PowerShell module

Install Cisco UCS PowerTool

<p>.Navigate to the location you have copied the CiscoUcs-PowerTool-1.1.1.0.exe file. Execute it from an elevated command prompt.</p>	
--	--

A splash screen shows as the compacted file is expanded for installation.



The routine checks to make sure no other instances of PowerShell are running. If so, it is necessary to stop those running instances before proceeding. Click **Next** to continue.



Click the radio button by **I accept the terms in the license agreement**. Click **Next** to continue.



Accept the default installation directory. Click **Next** to continue.



Click the checkbox by **Create Desktop Shortcut** if you want to have a desktop shortcut. Click **Install** to start the installation process.



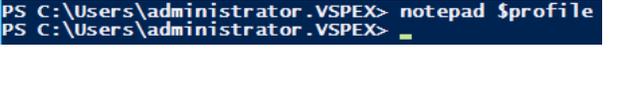
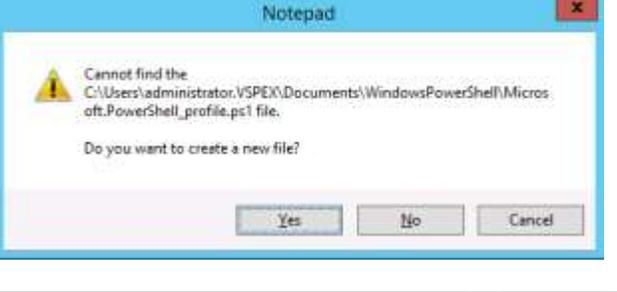
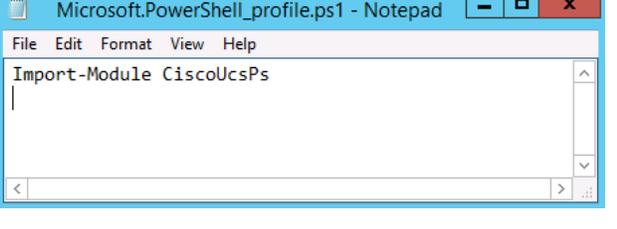
Click **Finish** when the installation process completes.



It is a good practice to include the loading of the PowerTool module in the default PowerShell profile. This helps ensure that PowerTool is available any time you launch PowerShell. Open a PowerShell window and execute the command **\$profile** to determine the location of the default profile location for the account you will be running under.



The information provided by the \$profile command shows the location PowerShell will look for the profile information, but on a fresh installation of an operating system, the directory and file do not exist. You will need to create a new directory. Enter a command to create a new directory as indicated by the previous command.

<p>When the WindowsPowerShell directory is created in the proper location, enter the command notepad \$profile to open the profile to edit it.</p>	
<p>AS the file does not exist, Notepad will report that it does not exist. Click Yes to indicate that you want the file created.</p>	
<p>Enter the string Import-Module CiscoUcsPs into Notepad, ensuring you terminate the line with a carriage return. Exit and save the file. Now whenever this user starts a PowerShell window, the CiscoUcsPs module will be automatically loaded and be ready for use.</p>	

Install Cisco Nexus 1000V PowerShell Module

The installation instructions for the Cisco Nexus 1000V PowerShell module is described in the section of this document detailing the installation of the Cisco Nexus 1000V.

System Center 2012 R2 Virtual Machine Manager Add-In

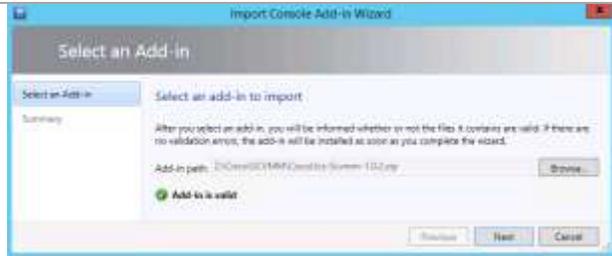
The UCS Add-in for Microsoft System Center 2012 R2 Virtual Machine Manager enables management of Cisco UCS from within SCVMM.

Installation of this add-in requires that Cisco UCS PowerTool is already installed on the servers to which the UI extensions add-in will be added. The add-in needs to be installed on any VMM console from which you want to use the extensions.

Install the SCVMM Add-In

<p>Launch the SCVMM console and navigate to Settings. Click Import Console Add-in.</p>	
--	--

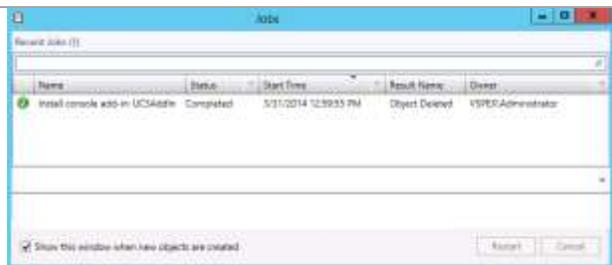
On the **Select an Add-in** page, browse to the location where you have downloaded the add-in installation zip file and select the zip file. Click **Next** to continue.



On the **Summary** page, verify you are installing the proper version. Click **Next** to continue.



The **Jobs** page will display showing a successful completion of the installation.



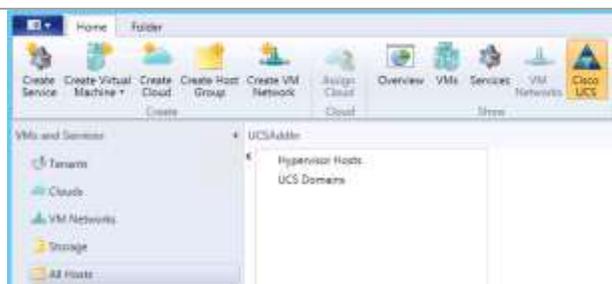
Navigate to **VMs and Settings** and you will see the **Cisco UCS Add-in** on the tool bar ribbon.



Configure the SCVMM Add-In

From the **VMs and Settings** panel, click the **Cisco UCS** icon in the tool bar ribbon. It will process for a short time and return with **UCSAddIn** in the working pane.

Note: The **All Hosts** option must be selected within **VMs and Settings** to enable configuration of Cisco UCS.

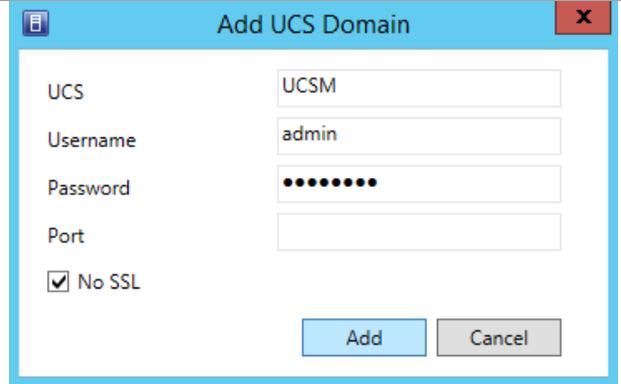


Click **UCS Domains** and select **Add UCS Domain** from the drop down menu.



On the **Add UCS Domain** page, enter the DNS name or the IP address of your UCS Manager in the **UCS** field. Enter the appropriate username and password in the **Username** and **Password** fields. If you are communicating on other than port 80, enter that in the **Port** field. If you are not using SSL, check the **No SSL** box. Click **Add** to add the connection to the UCS Manager.

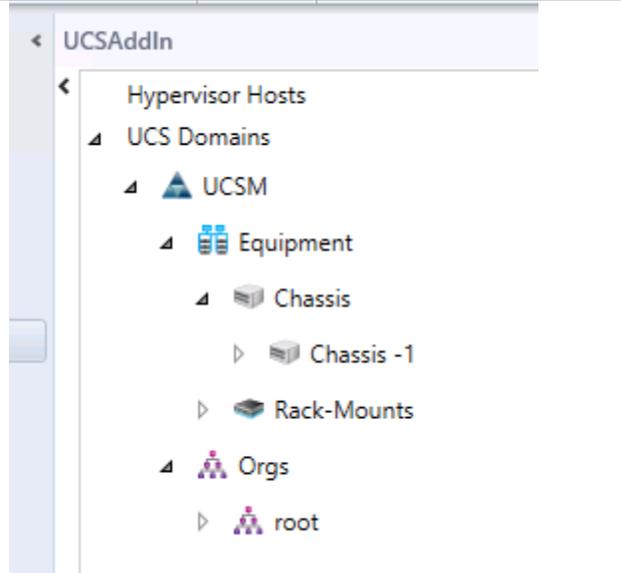
Note: If you have integrated UCSM credentials into Active Directory, these can be Active Directory credentials.



When the connection is made, you should be able to manage several components of Cisco UCS Manager.

Repeat this installation and configuration for each server running the SCVMM console if you plan on managing Cisco UCS from that console.

Note: If you plan on using the KVM Console feature available in this add-in, you need to install the Java runtime onto the server.



System Center 2012 R2 Operations Manager Management Pack

The Cisco UCS SCOM (System Center Operations Manager) Management Pack is a plug-in for System Center Operations Manager. It is used to monitor the health of the Cisco UCS system in the data center. With this plug-in, you can monitor chassis, blades, and service profiles across multiple Cisco UCS systems. Additionally, the Cisco UCS SCOM management pack enables correlation of faults and events between the Cisco UCS infrastructure and both bare-metal and virtualized operating systems already managed by SCOM.

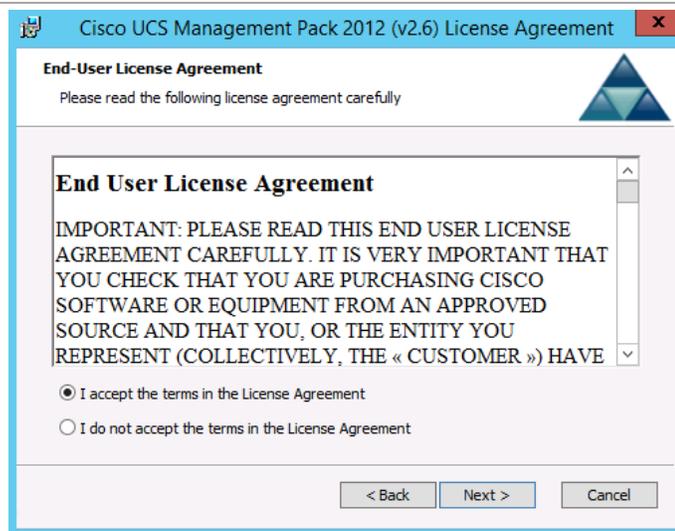
Install the Cisco UCS Management Pack

- ▶ Perform the following steps on the **first Operations Manager management server** virtual machine.

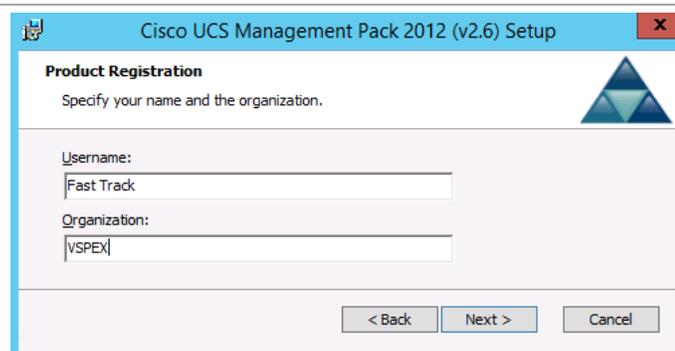
Make sure the Operations Manager management console is not running. Launch the management pack installer **Cisco.UCS.MP.2012.v2.6.2-x64.msi**. Click **Next** on the splash screen.



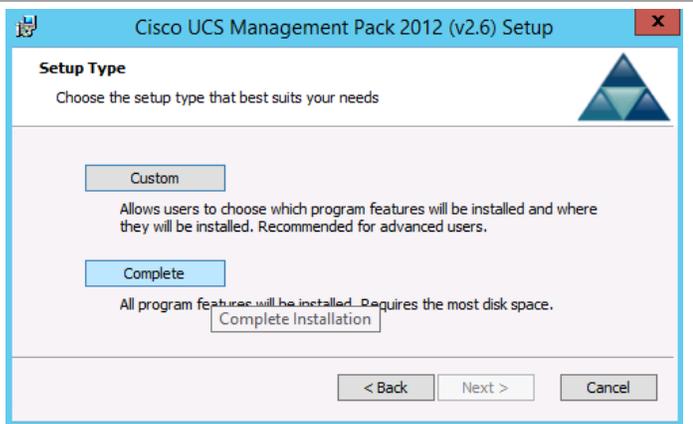
On the **End User License Agreement** page, select the **I accept the terms of the License Agreement** radio button. Click **Next** to continue.



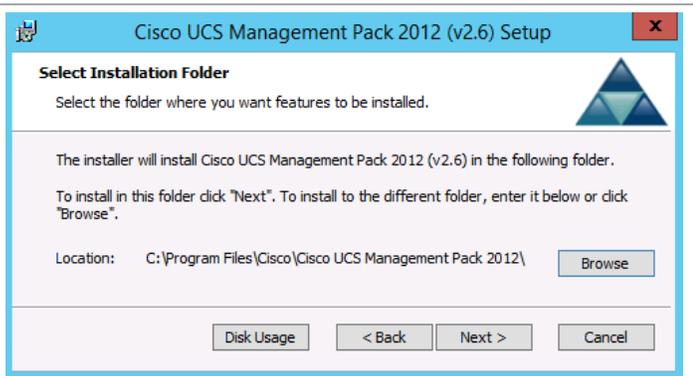
On the **Product Registration** page, enter an optional Username and Organization. Click **Next** to continue.



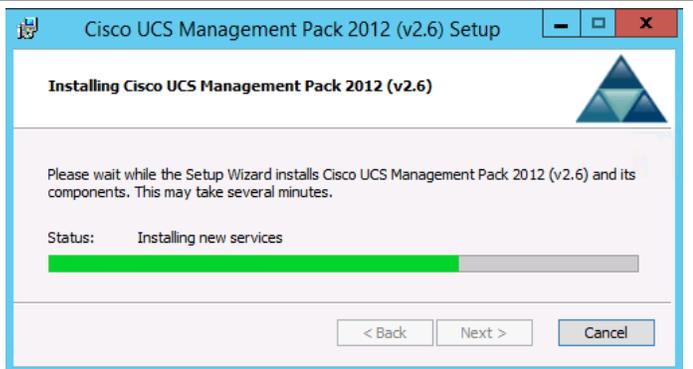
On the **Setup Type** page, click the **Complete** box.



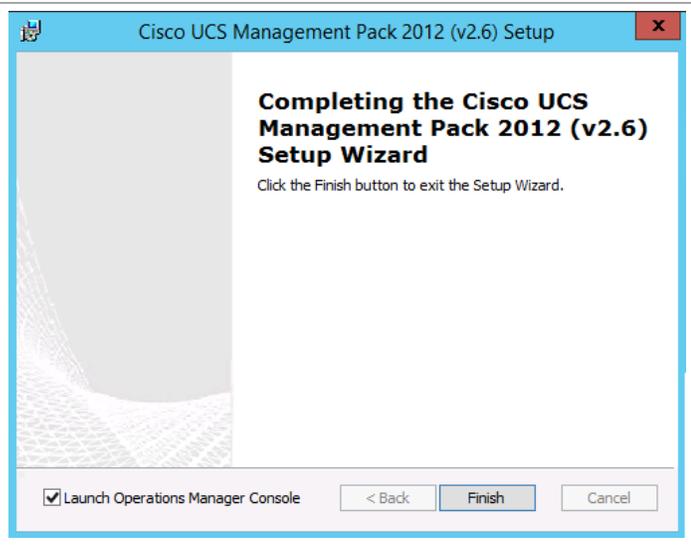
On the **Select Installation Folder** page it is recommended to accept the default location. Click **Next** to continue. Then click **Install** on the following screen to start the installation process.



The **Installing Cisco UCS Management Pack 2012 (v2.6)** page will track the progress of the installation.



After successful installation, you will receive the **Completing the Cisco UCS Management Pack 2012 (v2.6) Setup Wizard** page. Make sure the checkbox for **Launch Operations Manager Console** is selected and click **Finish** to continue.



Add Firewall Exceptions for the Cisco UCS Management Service

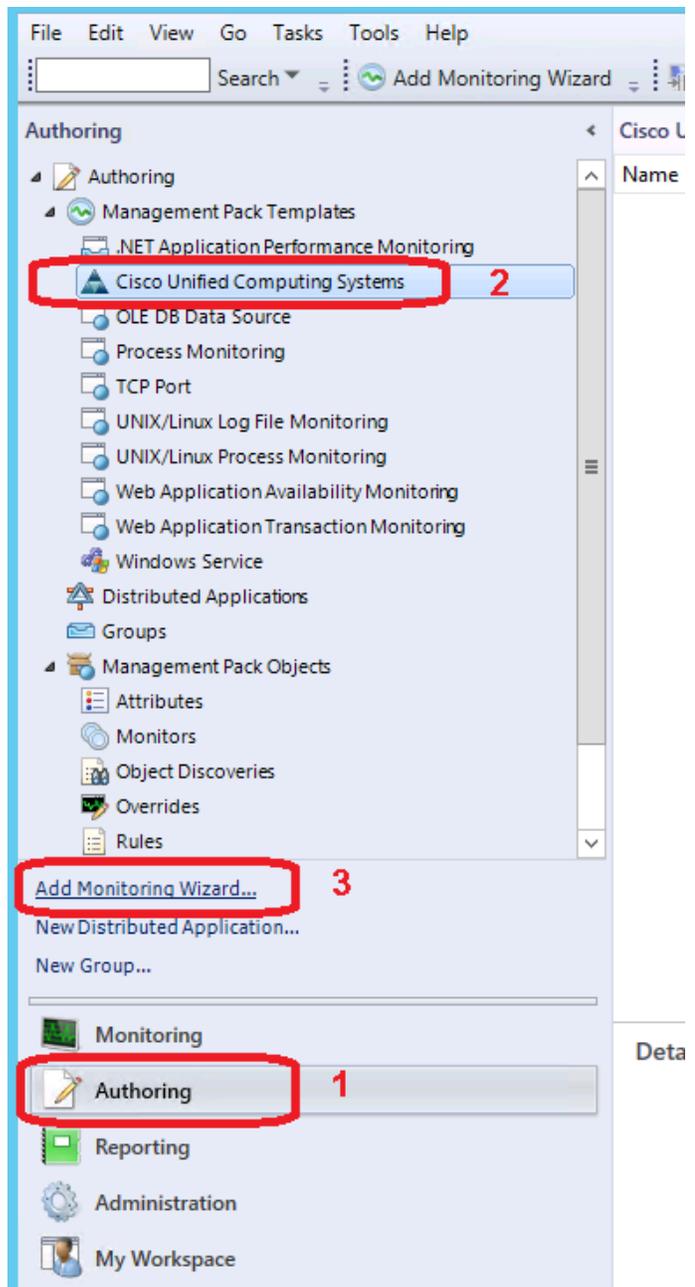
After you have installed the Cisco UCS management pack, you must add firewall exceptions for port 8732 on every management server hosting the Cisco UCS Management Service. Issue the following PowerShell commands to create the inbound and outbound rules.

```
New-NetFirewallRule -Name Cisco-UCS -DisplayName "Operations Manager Cisco UCS Management Service" -Action Allow -Direction Inbound -Protocol TCP -LocalPort 8732
New-NetFirewallRule -Name Cisco-UCS -DisplayName "Operations Manager Cisco UCS Management Service" -Action Allow -Direction Outbound -Protocol TCP -LocalPort 8732
```

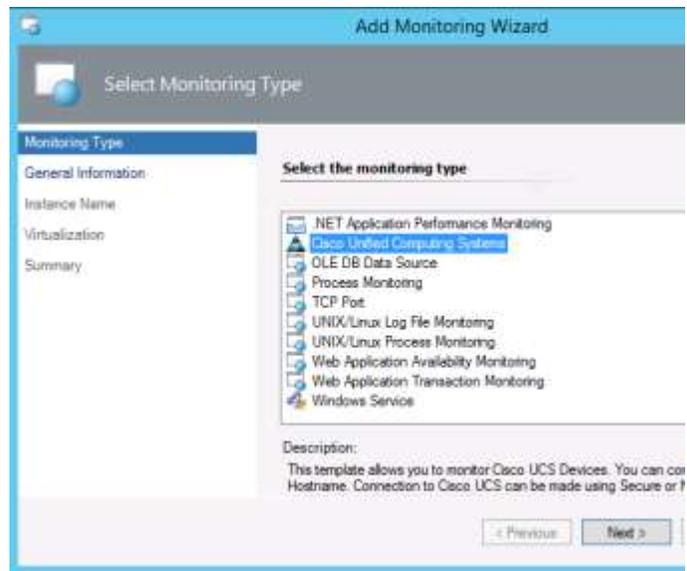
Add Cisco UCS Domains to Operations Manager

There are multiple combinations of how you may want to deploy the Cisco UCS management pack when deploying within an environment with multiple Operations Manager management servers. You can just deploy on the first management server, or you can deploy on both. These instructions provide the steps to deploy to the first management server.

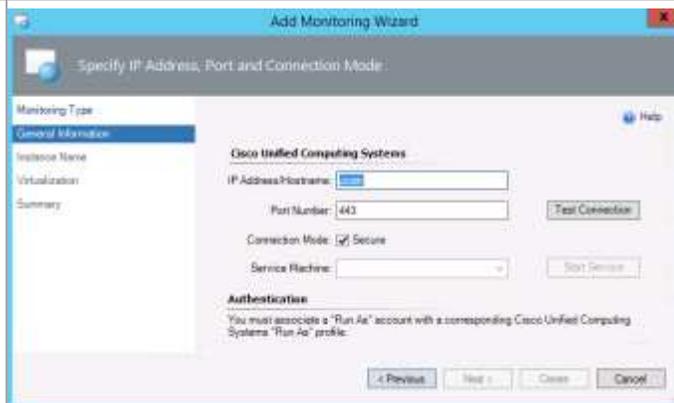
In the Operations Manager management console, select **Authoring**. Expand **Management Pack Templates** and select **Cisco Unified Computing Systems**. Then select **Add Monitoring Wizard...**



On the **Select Monitoring Type** page of the Add Monitoring Wizard, select **Cisco Unified Computing Systems**. Click **Next** to continue.



On the **Specify IP Address, Port and Connection Mode** page, enter the IP address or DNS name of the UCS management console. Specify **443** for the **Port Number** and check the box for **Secure** on the **Connection Mode**. Click **Test Connection** to test the connection to UCS Manager.



Depending upon how you have configured UCS in your environment, you may get a **Security Alert** window warning of a problem with the security certificate. If you have not configured certificates for UCS, this is expected. Click **Yes** to proceed.

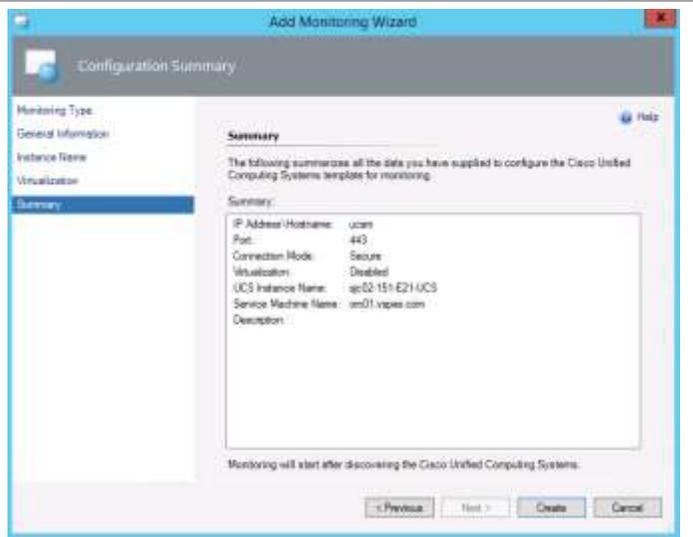


An **Authentication** page will appear from clicking on the Test Connection. Enter the **Username** and **Password** to access your UCS Manager console. Click **OK** to continue. If the username and password entered are correct, you will receive an information window informing of a successful connection. Click **OK** to continue. Click **Next** on the Add Monitoring Wizard page to continue.

On the **Cisco UCS Instance Name** page, the instance name is set by default to the name of the UCS Manager. It is recommended that the default instance name is not modified. Optionally enter a description. Check the box by **Use existing management pack or create new**. Select the **Default Management Pack** from the drop-down list. Click **Next** to continue.

Click **Next** on the **Enable to Detect Virtual Machines** page as this release does not support this capability.

Review the contents of the **Summary** page. Click **Create** to complete this step.



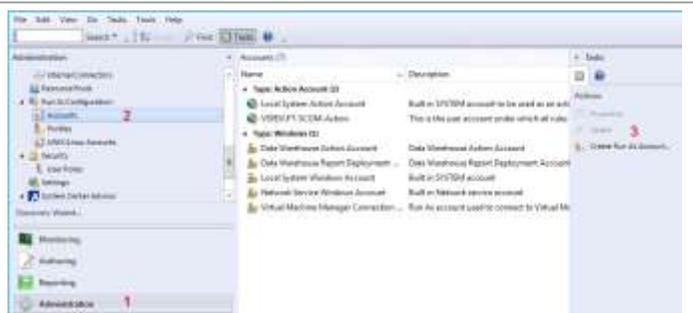
Upon completion, the newly created management pack will show in the Operations Manager console.



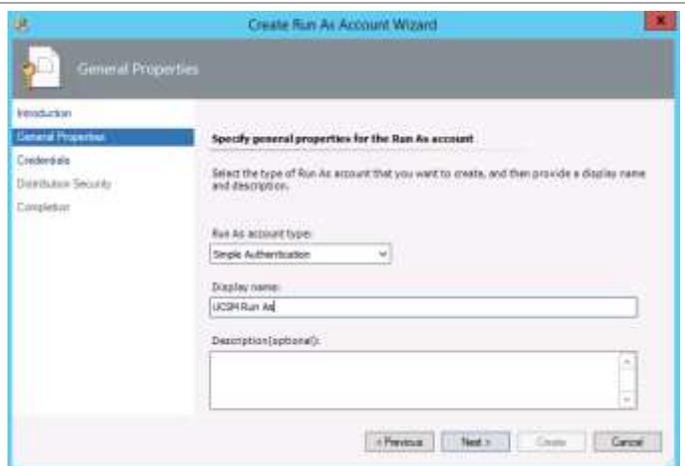
Configure Administrator Account

Operations Manager uses Run As accounts to establish a connection to a Cisco UCS domain. The Run As account must be an administrator account.

In the Operations Manager console, select the **Administration** section. Scroll down and expand **Run as Configuration** and select **Accounts**. From the Tasks pane on the right-hand side, click **Create Run As Account...** Click **Next** on the **Introduction** page to continue.



On the **General Properties** page, select **Simple Authentication** from the **Run As account type** drop-down list. Enter a descriptive name for this account in the **Display Name** field. Click **Next** to continue.



On the **Credentials** page, enter the UCS Manager credentials for accessing the UCS domain. Click **Next** to continue.

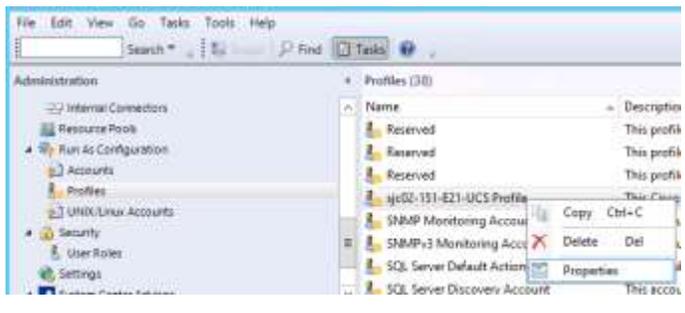


On the **Distribution Security** page, select the radio button by **Less secure**. Click **Create** to create the UCS run as account.

Note: Cisco UCS does not run on a Windows operating system. The More secure option is intended for management packs that target systems running a Windows operating system.



Click **Close** on the successful completion page. In the Operations Manager console, select **Profiles** (right below the previous Accounts selection). Scroll through the profiles to find the profile you just created. Right-click the profile and select **Properties**. Click **Next** on both the Introduction and the General Properties pages.



On the **Run As Accounts** page, click the **Add...** icon.



On the **Add a Run As Account** page, select the run as account you just created for communicating with UCS. Select the radio button by **All targeted devices**. Click **OK** to continue.

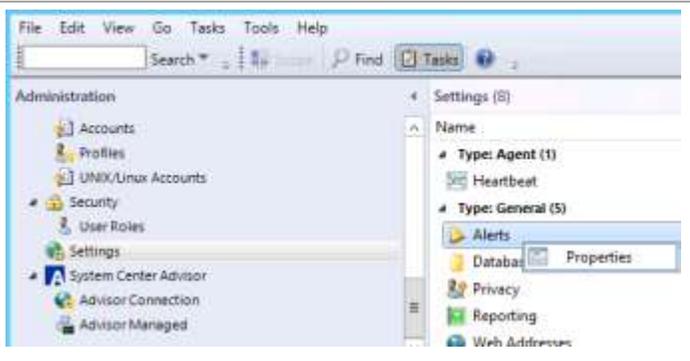


Back on the **Run As Accounts** page, click **Save** to continue. On the successful completion page, click **Close**.

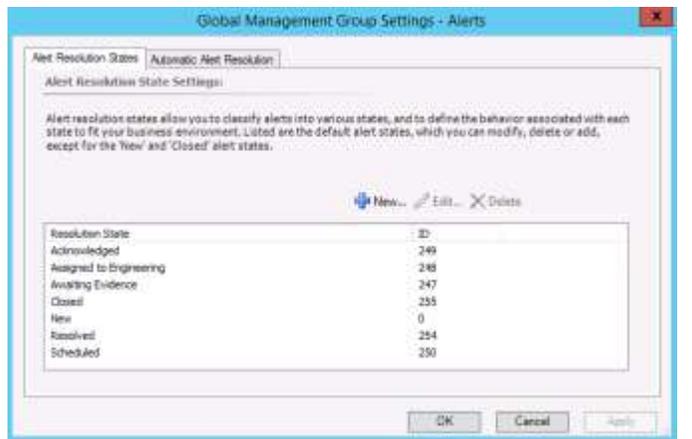


Configure Fault Acknowledgement

In the Operations Manager console, select **Administration**. Scroll to the bottom of the list and select **Settings**. Right-click **Alerts** in the center pane and select **Properties**.



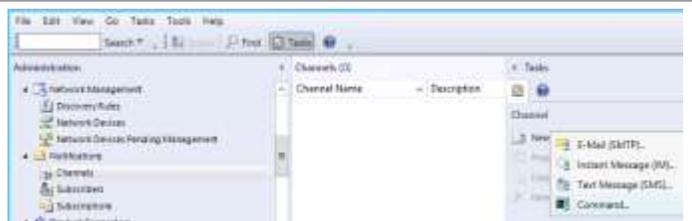
On the **Global Management Group Settings** – **Alerts** page, click **New...**



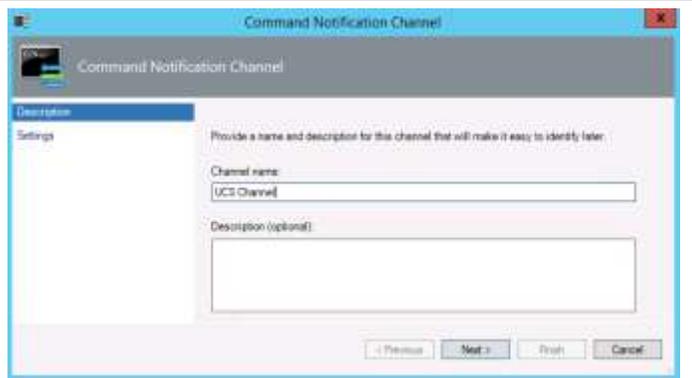
On the **Add Alert Resolution State** page, enter a name for the **Resolution State**. From the **Unique ID** drop-down list, select an available identifier. Click **OK** to return to the Global Management Group Settings window. Click **OK** to continue.



Back in the Operations Manager console, within **Administration**, scroll up to select **Notifications** and then **Channels**. Under **Tasks** click **New** and select **Command...** from the drop-down list.



On the **Command Notification Channel** page, enter a name for **Channel Name**. Click **Next** to continue.



On the **Command Notification Channel** page, enter the following for the **Full path of the command line**.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

In the **Command line parameters** enter:

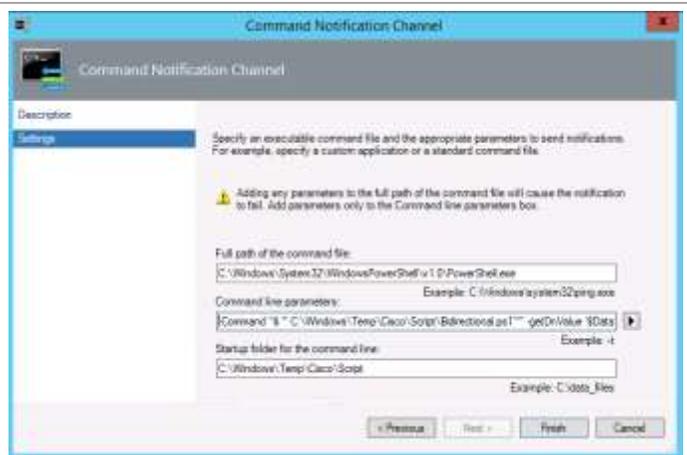
```
-Command "& '"  
C:\Windows\Temp\Cisco\Script\Bidirectional.ps1"'" -getDnValue  
'$Data/Context/DataItem/Custom6$'  
-getFaultID  
'$Data/Context/DataItem/Custom7$'  
-getWebProxyUrl  
'$Data/Context/DataItem/Custom10$'  
-getEntityFullName  
'$Data/Context/DataItem/ManagedEntityFullName$'
```

In the **Startup Folder for the command line** enter:

```
C:\Windows\Temp\Cisco\Script
```

Click **Finish** to continue, and **Close** upon successful completion.

Note: The installation of the Cisco UCS management pack places the Bidirectional.ps1 file into the C:\Windows\Temp\Cisco\Script directory. You can change that location, but be sure to change the values in this setting to reflect any changes.

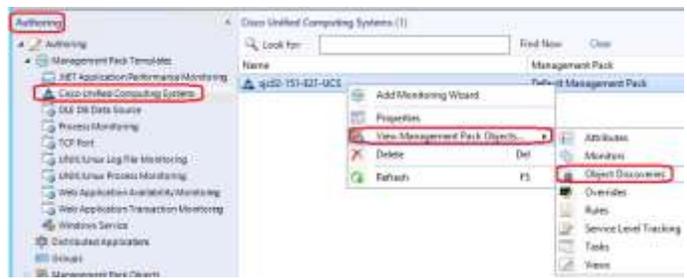


Configure Cisco UCS Management Service

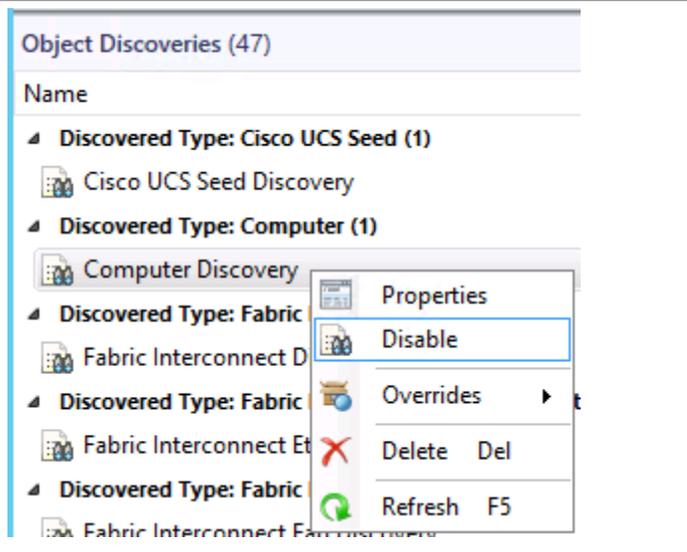
Disable Computer Discovery

It is recommended to disable the Computer Discovery of the UCS management pack. Computer Discovery is an object discovery in the management pack which creates a mapping between the Windows Computer monitored by SCOM and the UCS Domain on which they are hosted. Disabling Computer Discovery in Cisco UCSM SCOM MP will not have any impact on the monitoring of hardware and logical components of UCS Domain, even all Windows Computer will continue to be monitored by SCOM, only mapping between the Windows Computer and the UCS Domain will not be available. This relieves some of the CPU cycles required on the management server.

In the **Operations Manager** console navigate to **Authoring > Management Pack Templates > Cisco Unified Computing System**. Right-click the UCS template and select **View Management Pack Objects > Object Discoveries** from the drop down menus.



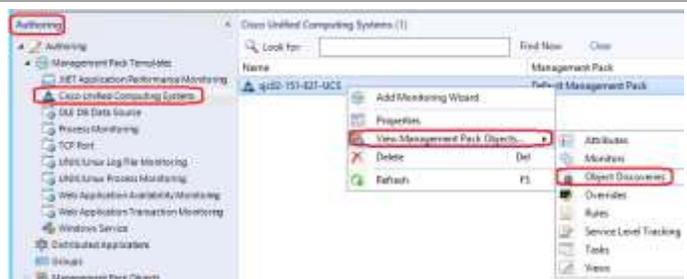
On the **Object Discoveries** window that displays, scroll down to find **Computer Discovery**. Right-click and select **Disable**. Close the Object Discoveries window.



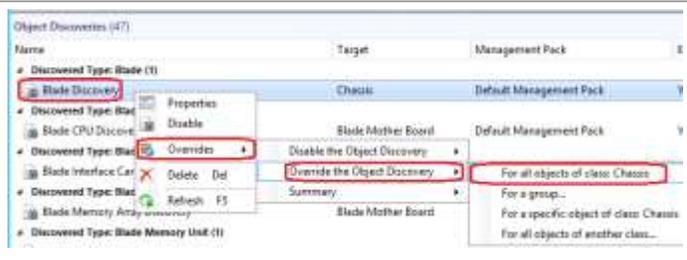
Increasing the Discovery Interval for Physical Inventory

By default the object discoveries are set to run between 1800 to 2000 seconds. Since the physical inventory of the UCS Domain generally will not change in this short period, increasing the discovery intervals by 6 hours will help relieve CPU cycles on the management server.

In the **Operations Manager** console navigate to **Authoring > Management Pack Templates > Cisco Unified Computing System**. Right-click the UCS template and select **View Management Pack Objects > Object Discoveries** from the drop-down menus.



On the **Object Discoveries** window that displays, right-click a discovery and select the **Overrides > Override the Object Discovery > For all objects of class: xxx** from the drop-down menus.



On the **Override Properties** page, select the check box by **Interval Seconds** and modify the **Override Value** according to the following table. Click **OK** to make the change to the default.

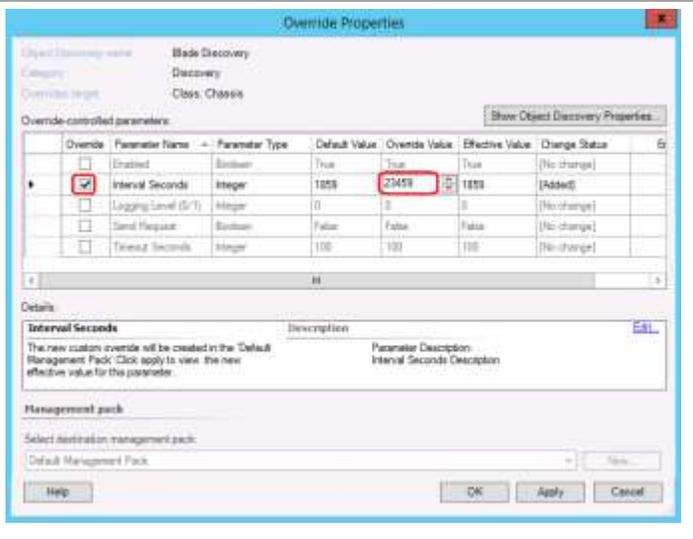


Table 31. Suggested Object Discovery Intervals

Object Discovery	Default Discovery Interval (Seconds)	Suggested Discovery Interval (Seconds)
Blade Discovery	1859	23459
Blade CPU Discovery	1979	23579
Blade Interface Card Discovery	1919	23519
Blade Memory Array Discovery	1979	23579
Blade Memory Unit Discovery	1979	23579
Blade Mother Board Discovery	1919	23519
Blade StorageController Discovery	1979	23579
Blade StorageLocalDisk Discovery	1979	23579
Chassis Discovery	1798	23398
Chassis Fabric Port Discovery	1919	23519
Chassis Fan Discovery	1919	23519
Chassis Fan Module Discovery	1859	23459
Chassis IOModule Discovery	1859	23459
Chassis PSU Discovery	1859	23459
Chassis Server Port Discovery	1919	23519
Cisco UCS Instance Discovery	720	720
Computer Discovery	21600	21600
Fabric Interconnect Discovery	1798	23398
Fabric Interconnect Ethernet port Discovery	1859	23459
Fabric Interconnect Fan Discovery	1919	23519

Fabric Interconnect Fan Module Discovery	1919	23519
Fabric Interconnect Fan Module Fan Discovery	1919	23519
Fabric Interconnect FC Port Discovery	1859	23459
Fabric Interconnect PSU Discovery	1919	23519
FEX Discovery	1798	23398
Fex Fabric Port Discovery	1979	23579
FEX Fan Discovery	1859	23459
FEX IOModule Discovery	1859	23459
FEX PSU Discovery	1859	23459
Fex Server Port Discovery	1979	23579
Operating System Discovery	21600	21600
Organization Discovery	1800	23400
Rack Unit Discovery	1798	23398
RackUnit CPU Discovery	1979	23579
RackUnit Fan Discovery	1979	23579
RackUnit FanModule Discovery	1859	23459
RackUnit InterfaceCard Discovery	1919	23519
RackUnit MemoryArray Discovery	2039	23639
RackUnit MemoryUnit Discovery	2039	23639
RackUnit MotherBoard Discovery	1919	23519
RackUnit PSU Discovery	1859	23459
RackUnit StorageController Discovery	2039	23639
RackUnit StorageDrive Discovery	2039	23639
RackUnit StorageLocalDisk Discovery	2039	23639
Service Profile Discovery	1800	23400
SwitchCard Discovery	1919	23519

When a discovery interval is increased whenever if any hardware/logical component gets added or modified, it will require maximum up to the discovery interval period to reflect the changes in the SCOM Console.

Example: If a memory unit is added to a blade and the discovery interval of Blade Memory Unit is 23579 seconds, it will take maximum of this period to discover the new memory unit hardware in the SCOM Console.

Note: Changing the discovery interval does not impact the fault collection mechanism, hence for the discovered UCS components, faults will still be collected every 720 Seconds (default).

For further information about the various configuration options that can be executed to tailor the monitoring to your environment, download the [Cisco UCS Management Pack User Guide, Release 2.6](#).

System Center 2012 R2 Orchestrator Integration Pack

The Cisco UCS OIP (Orchestrator Integration Pack) is a plug-in for System Center 2012 Orchestrator. It is used to develop runbooks for automating processes that need to read and modify information within UCSM.

Register the Cisco UCS OIP

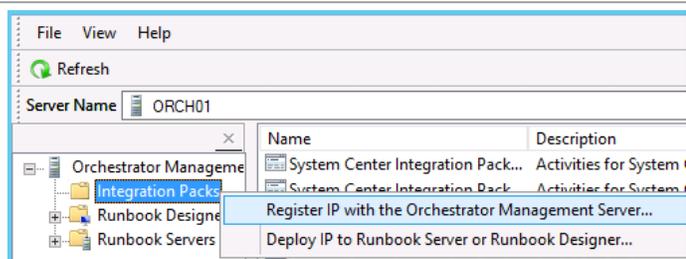
After downloading the Cisco UCS OIP, extract the installation file from the zip file. Then perform the following steps on all Orchestrator management servers to register the integration pack.

- ▶ **Make sure that Cisco UCS PowerTool has been installed on all Orchestrator management servers.**

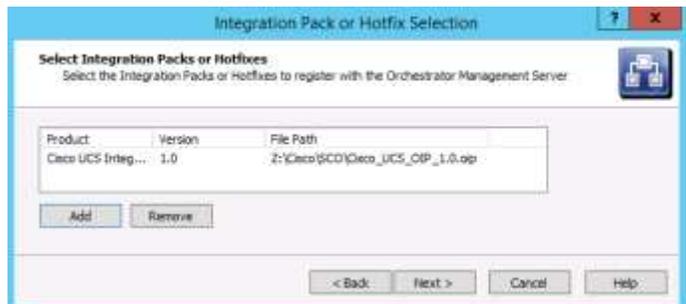
Launch the System Center 2012 R2 Orchestrator Deployment Manager.



Right-click **Integration Packs** and select **Register IP with the Orchestrator Management Server**. Click **Next** on the Welcome page.



On the **Select Integration Packs or Hotfixes** page, click **Add**. Browse to the location you extracted the OIP file and select the file. Click **Next** to continue. Click **Finish** on the **Completing the Integration Pack Wizard** page.

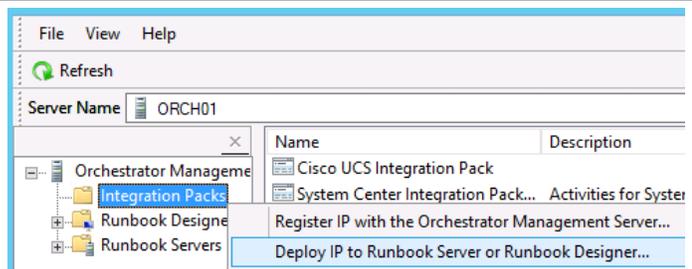


Click **Accept** on the **End User License Agreement** page to complete the installation.

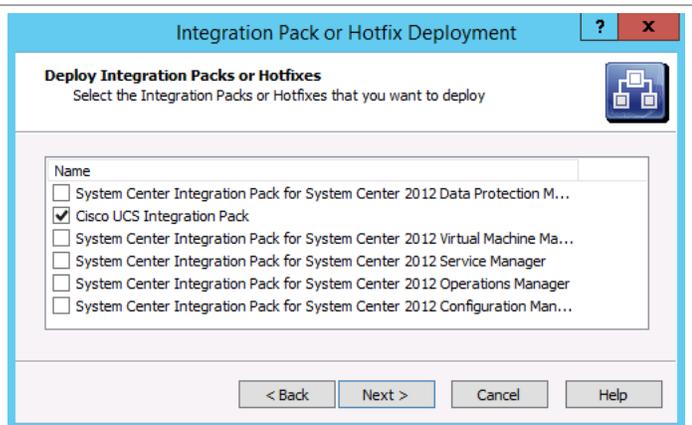


Deploy the Cisco UCS OIP

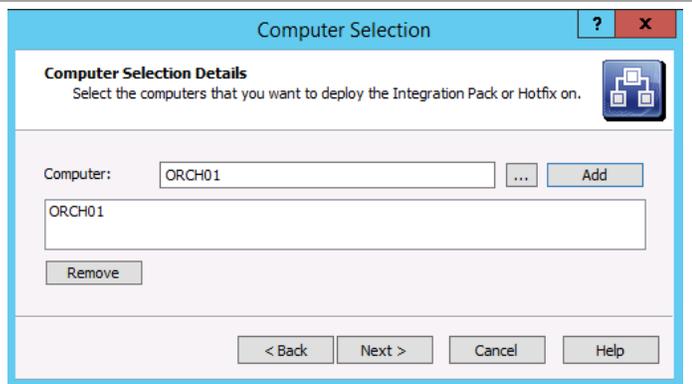
From the Deployment Manager, right-click **Integration Packs** and select **Deploy IP to Runbook Server or Runbook Designer...**. Click **Next** on the Welcome screen.



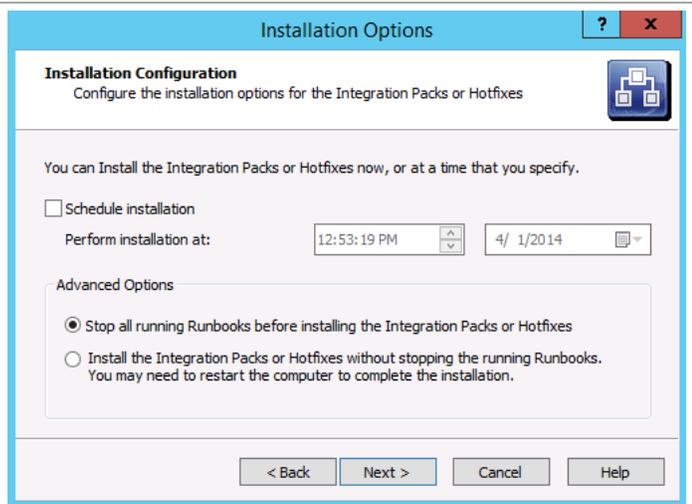
On the **Deploy Integration Packs or Hotfixes** page, select the **Cisco UCS Integration Pack**. Click **Next** to continue.



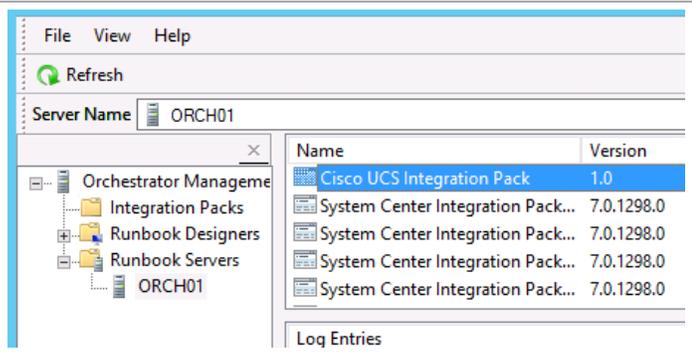
On the **Computer Selection Details** page, enter the name of the Runbook Server. Click **Next** to continue.



On the **Installation Configuration** page, make sure the radio button by **Stop all running Runbooks before installing the Integration Packs or Hotfixes** is selected. Click **Next** to continue. Click **Finish** on the Summary page that comes up. Status windows will display for each server previously entered.



In the Deployment Manager console, expand **Runbook Servers**. Make sure the server is listed. Select the server to validate the integration pack is deployed. Repeat for each Runbook Server.

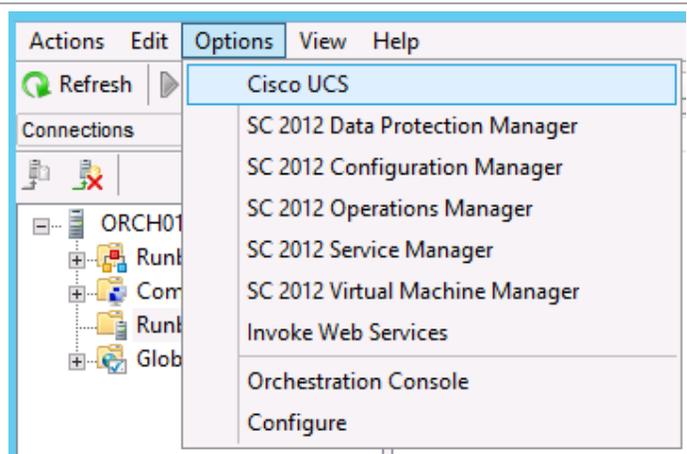


Configure the Cisco UCS OIP

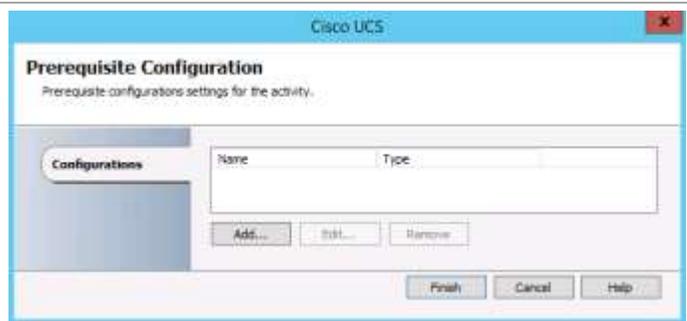
On each system running the Orchestrator Runbook Designer, configure the Cisco UCS OIP.

Launch the Runbook Designer. Select **Options** and then **Cisco UCS**.

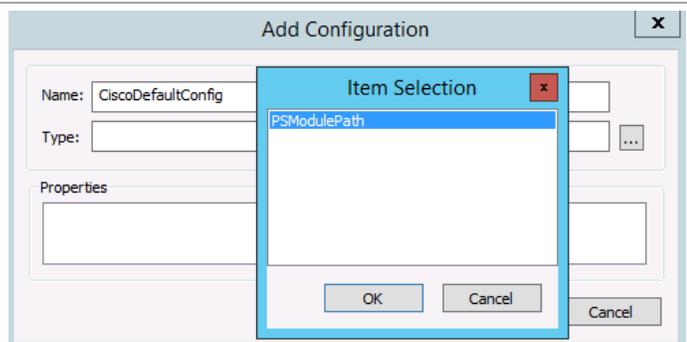
Note: If you do not see Cisco UCS under Options, make sure that you have installed Cisco UCS PowerTool.



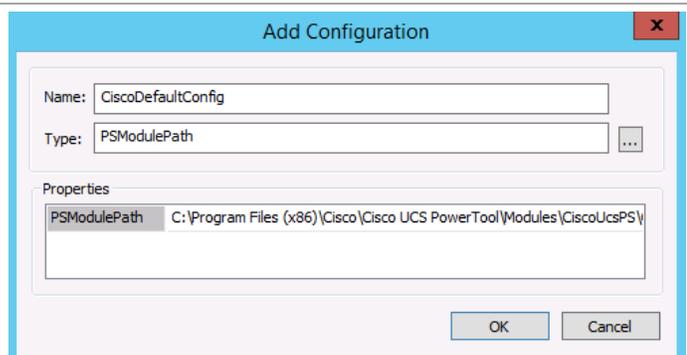
On the **Prerequisite Configuration** page, click **Add...**



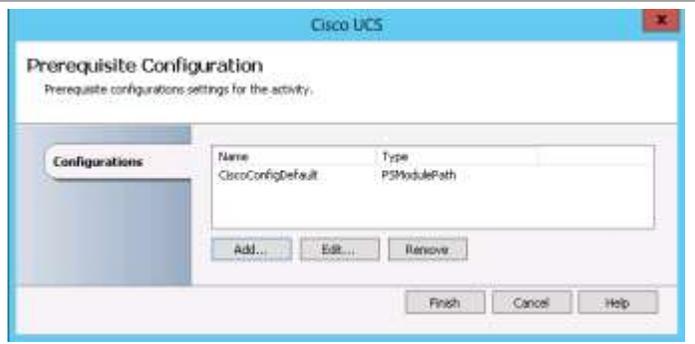
On the **Add Configuration** page, enter a **Name** for this configuration. Click the ... at the end of the **Type** field and select **PsModulePath**. Click **OK** on the **Item Selection** window.



In the **Properties** field of **PsModulePath** field, enter the location where the Cisco UCS PowerTool PowerShell module is installed. By default, this is located at C:\Program Files (x86)\Cisco\Cisco UCS PowerTool\Modules\CiscoUcsPS\CiscoUcsPS.psd1. Click **OK** to continue.



On the **Prerequisite Configuration** page, click **Finish** to complete the configuration.

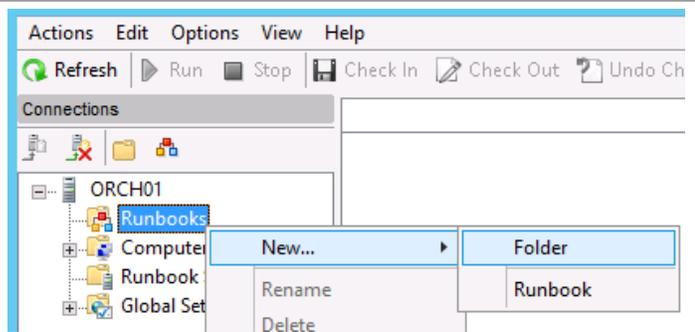


Install Sample Runbooks

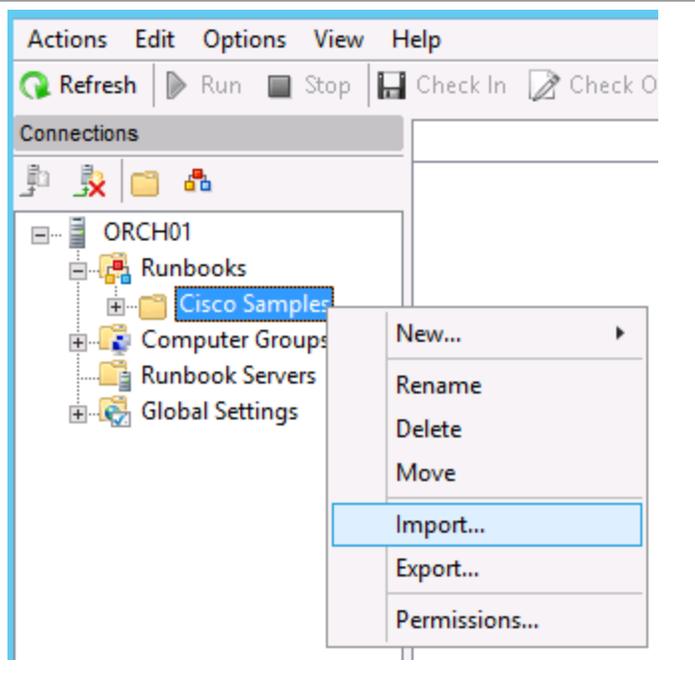
Cisco provides a small set of sample runbooks that assist in learning how to use the various activities available in their Integration Pack. Download the zip file and extract its contents. Perform the import of the sample runbooks on any Runbook Designer system.

In the Runbook Designer, right-click **Runbooks**, then click **New...** and select **Folder** to create a new folder in which to store the sample runbooks. Provide a name for the new folder.

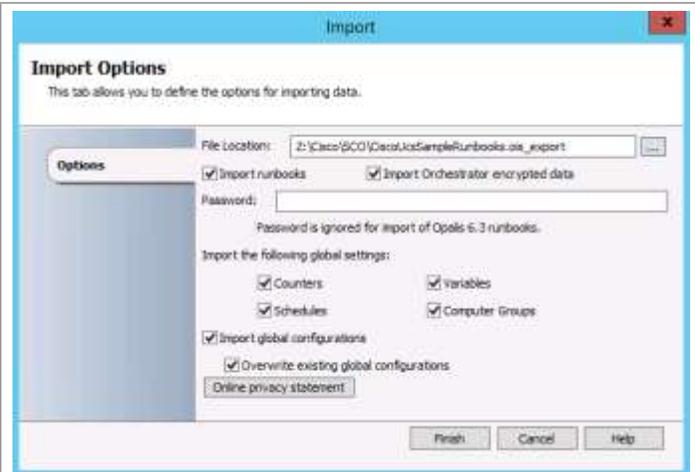
Note: Creating a new folder is optional. By default, the sample runbooks will import into a folder named *Sample Runbooks* under whatever level you import to.



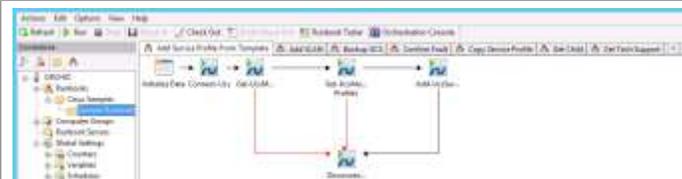
Right-click the newly created folder and select **Import...**



On the **Import Options** page, browse to the **File Location** where you extracted the contents of the sample runbooks zip file. Click **Finish** to complete the import. When the process is complete, click **OK** on the successful completion window.



Open the newly create folder to view the sample runbooks.



Cisco Nexus 1000V

Cisco Nexus 1000V Series Switches provide a comprehensive and extensible architectural platform for virtual machine and cloud networking. The switches are designed to accelerate server virtualization and multi-tenant cloud deployments in a secure and operationally transparent manner for environments like Microsoft's Private Cloud. Download the distribution software from the location specified in the Software Revision table at the beginning of this document and expand it into a temporary directory.

For complete installation documentation, see:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/hyperv/sw/5-2-1-SM-1-5-2a/install-and-upgrade/n1000v_gsg.html.

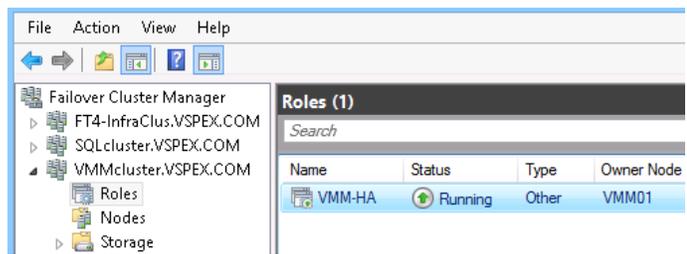
Install SCVMM Components

There are three components that need to be copied or run to initiate the installation of the Cisco Nexus 1000V.

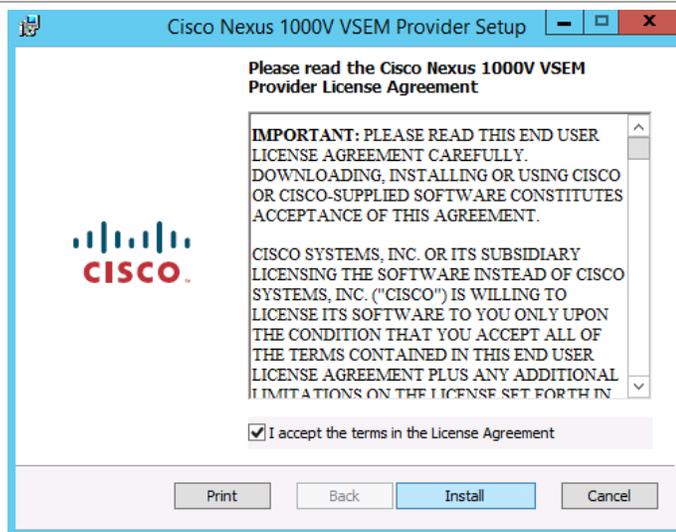
- Switch Extensions
- VSM Template
- VEM Installation File
- VSM ISO File

Install the Virtual Switch Extension Module

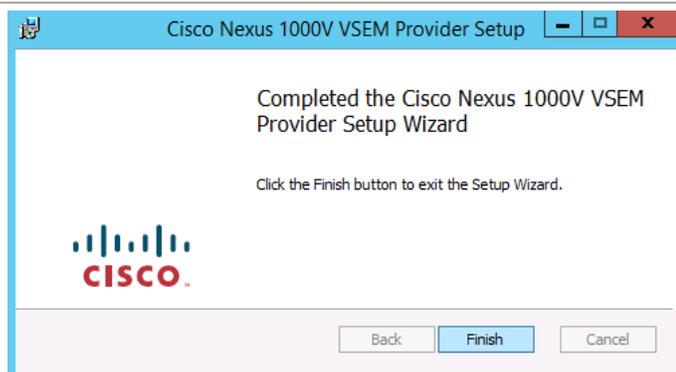
Determine which one of the VMM virtual machines is the owner of the highly available Virtual Machine Manager service by opening the **Failover Cluster Manager**. Expand the VMMcluster and click **Roles**. Log into the **Owner Node** and from an elevated command prompt run the **Nexus1000V-VSEMPProvider-5.2.1.SM1.5.2a.0.msi** installation file (found in the \VMM sub-directory of the extracted files).



On the license screen, select the check box by the **I accept the terms in the Licensing Agreement** statement. Click **Install** to continue.

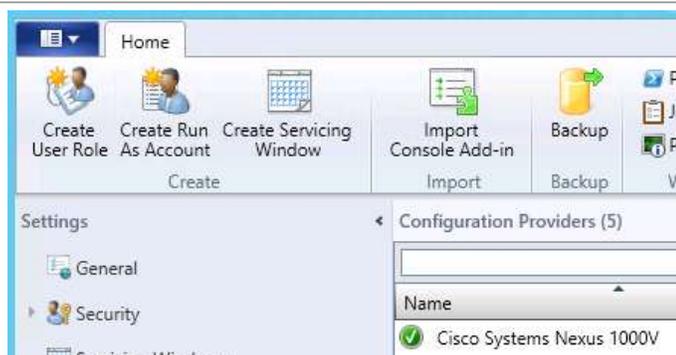


A status screen will show the progress of the installation. Click **Finish** to complete the installation. Restart the server.



Verify the Cisco VSEM Provider is properly installed. You can either wait for the node you restarted to come up or you can go to the other node.

From the **VMM Console**, select **Settings > Configuration Providers** and validate that the Cisco Systems Nexus 1000V is listed.

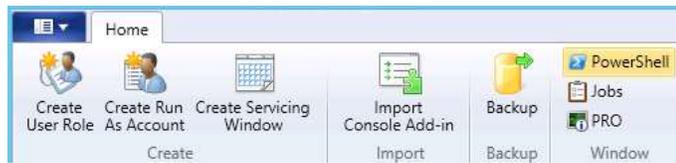


Install VSM Template

From the **VMM Console** of one of the VMM virtual machines, launch a PowerShell window. This must be launched from the VMM Console in order for the proper PowerShell modules to be loaded. Be patient – it takes a little time for the modules to load.

Note: You have to set the PowerShell Execution Policy to allow the execution of scripts. **Set-ExecutionPolicy Bypass -Force** helps ensure it will run.

Note: PowerShell can be launched from any screen. This is the menu ribbon from the Settings screen.



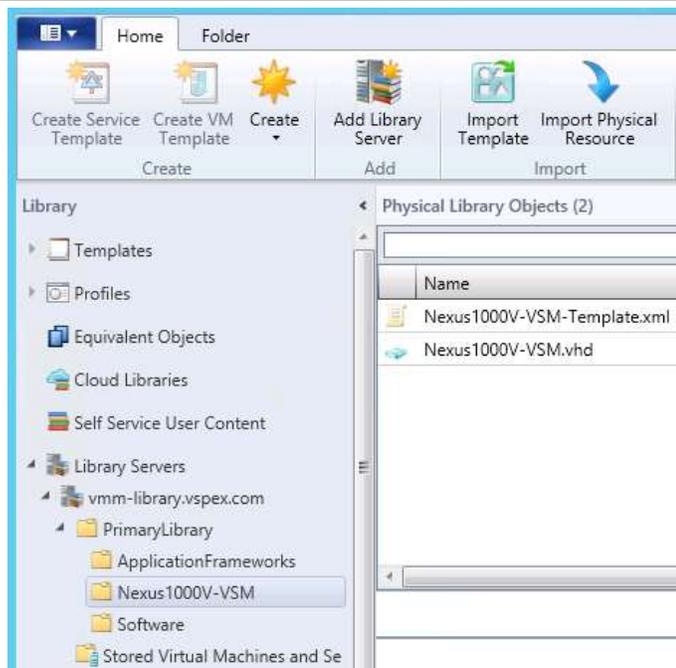
From the PowerShell prompt, enter the command shown to the right.

Note: There is a period (.) at the beginning of this command to tell PowerShell that a script is going to be executed.



```
. "\Program Files\Cisco\Nexus1000V\Nexus1000V-VSMTemplate\Register-Nexus1000VVSMTemplate.ps1"
```

You can verify the success by looking in the VMM Library. You should see a new sub-directory name **Nexus1000V-VSM** and two elements stored in it.

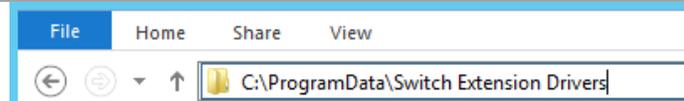


Copy the VEM to the SCVMM repository

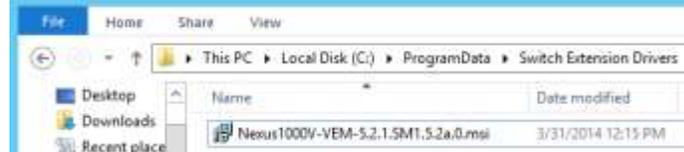
The VEM installation script gets copied to the SCVMM repository on each Virtual Machine Manager management server. That location is C:\ProgramData\Switch Extension Drivers.

► Perform this copy on each VMM management server. DO NOT EXECUTE – JUST COPY.

The destination directory is a hidden directory, so unless you have configured your system to show hidden directories, you need to type its location in the top of the Windows Explorer window.



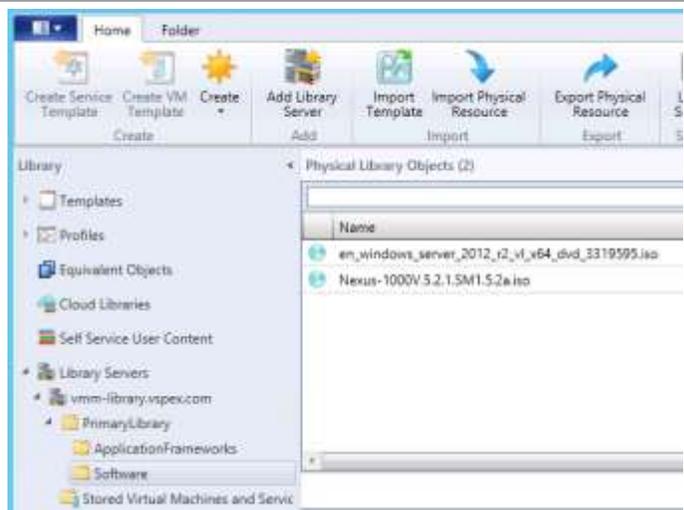
The Nexus1000V-VEM-5.2.1.SM1.5.2a.0.msi file is located in the \VEM subdirectory of the expanded files. Copy it to the Switch Extension Driver directory.



Copy the VSM ISO to SCVMM Library

The destination of this ISO file will vary slightly depending upon how you configured the SCVMM Library. In this example, a sub-directory was created under the main directory in which to store Software Distributions; this is where the file is copied.

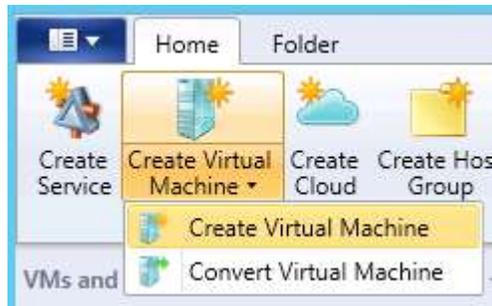
Copy the VSM ISO file to the SCVMM Library. The VSM ISO file is found in the \VSM\Install directory of the expanded files. The SCVMM library is a standard file share, so you just have to copy the file to the appropriate file share.



Create Two VSM Virtual Machines

The Cisco Nexus 1000V is deployed as a pair of highly available virtual machines. Each machine will have its own unique management IP address, and the highly available service will have its own virtual IP address separate from the individual machines. It is necessary to add, at a minimum, the virtual IP address to DNS. SCVMM uses the virtual IP address for communication.

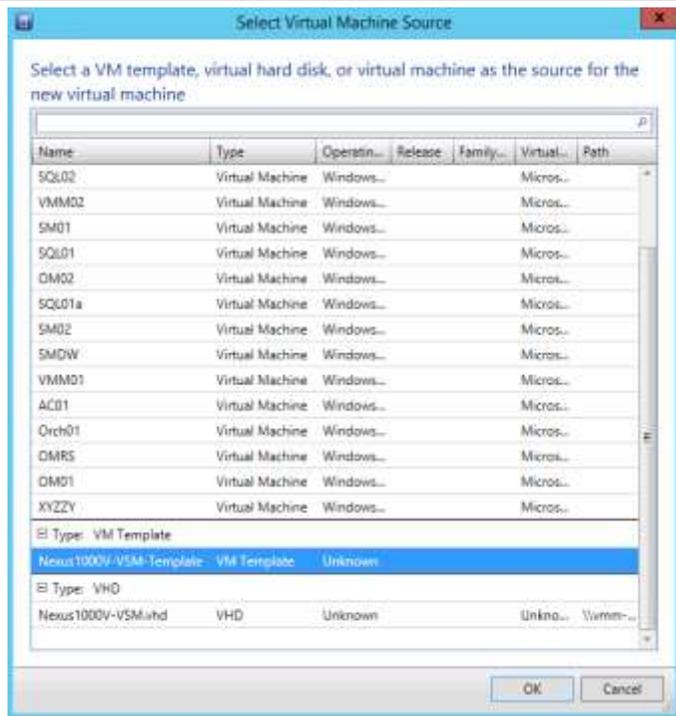
From the VMM console, select **VMs and Services**. Select **Create Virtual Machine** from the menu ribbon, and select **Create Virtual Machine**.



On the **Select Source** page, select the radio button by **Use an existing virtual machine, VM template, or virtual hard disk**. Click the **Browse...** button.



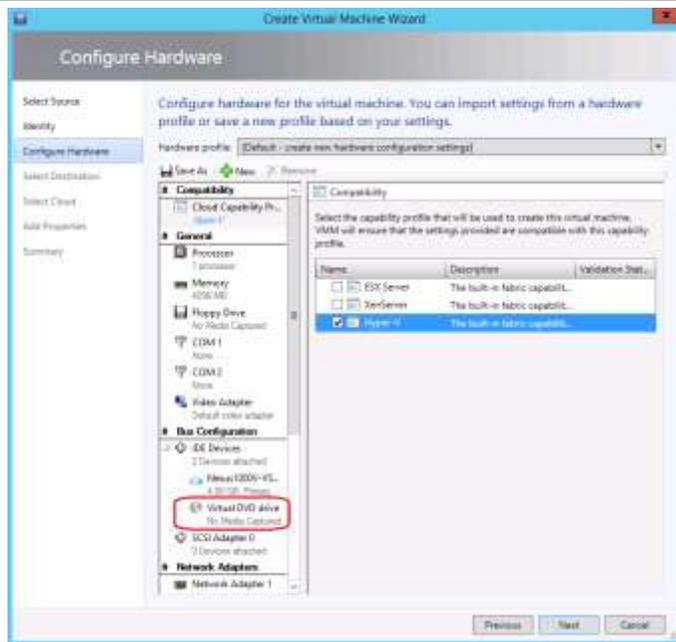
On the **Select Virtual Machine Source** page, scroll to the bottom to find the **Type: VM Template**. Select the **Nexus1000v-VSM-Template**. Click **OK** to continue. Then click **Next** when you are back on the **Select Source** page.



On the **Identity** page, enter a name for the virtual machine you are creating. Click **Next** to continue.

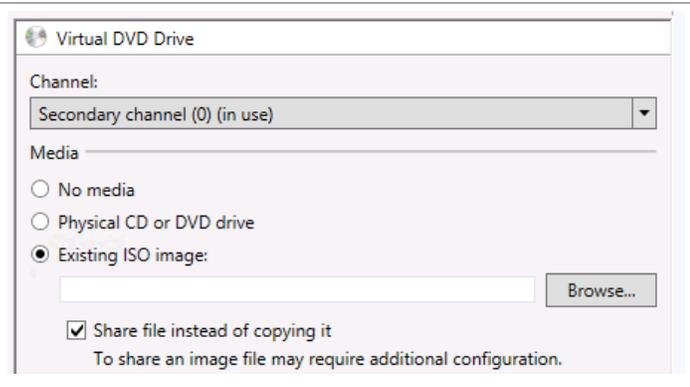


On the **Configure Hardware** page, under Compatibility, select the check box by **Hyper-V**. Almost everything should already be configured from the template. However, you must still assign the ISO file for installation. Click **Virtual DVD drive**.



The right-hand side of the page will change to allow you to configure the **Virtual DVD Drive**. Select the radio button by **Existing ISO image**. Click the **Browse...** button.

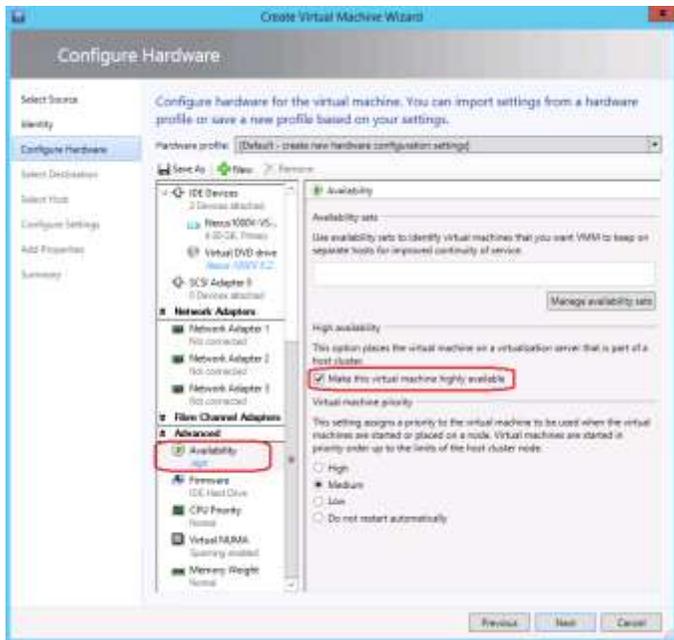
Note: If you have configured your systems for Constrained Delegation, you can also select the check-box by **Share file instead of copying it**.



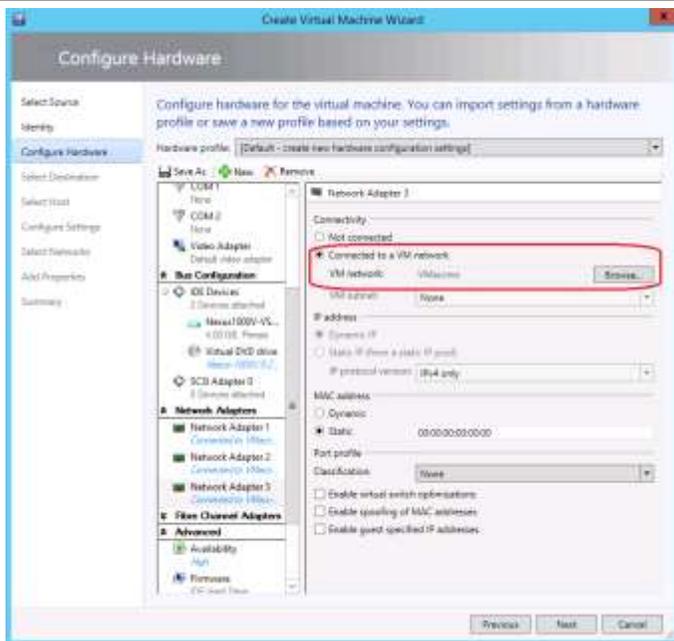
On the **Select ISO** page, select the **Nexus-1000V.5.2.1.SM1.5.2a.iso** file. Click **OK** to continue.



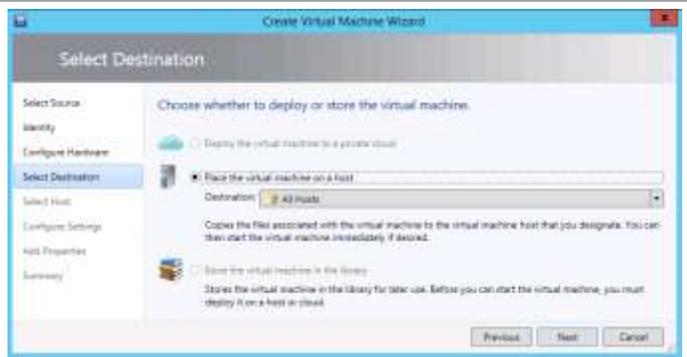
Back on the **Configure Hardware** page, scroll down on the left to find **Advanced**. Under **Advanced**, click **Availability** and select the check box for **High availability**.



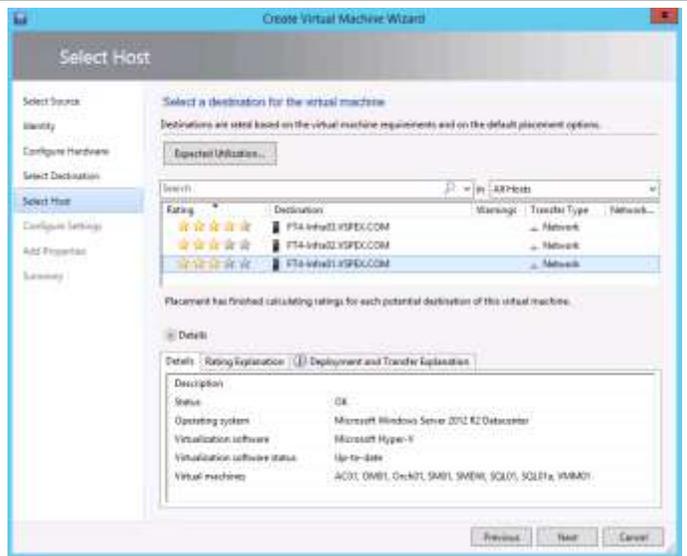
Still on the **Configure Hardware** page, select each of the three **Network Adapters** that were created by the template and assign them to the VM management network. Click **Next** to continue.



On the **Select Destination** page, accept the default of placing the virtual machine on a host with the destination being All Hosts. Click **Next** to continue.



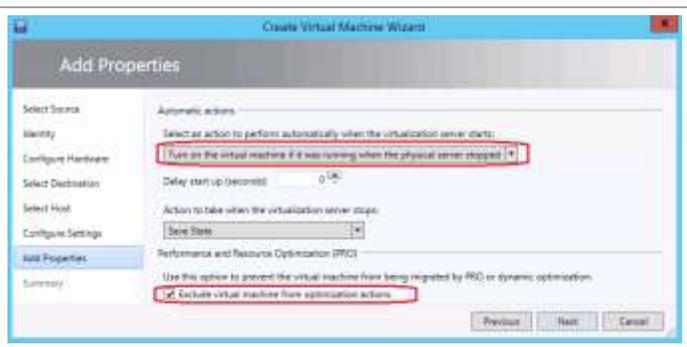
On the **Select Host** page, select a host on which to deploy this VM. After the build of the VMs, you will need to set preferred owners for these VMs just as you set those values for the fabric management VMs. Click **Next** to continue.



On the **Configure Settings** page, make sure the proper location is presented for where to store the VM. Click **Next** to continue.



On the **Add Properties** page, you may want to alter the **Automatic actions**. Determine which actions make sense for your environment. Select the check box by **Exclude virtual machine from optimization actions**. Click **Next** to continue. On the following **Summary** page, review the settings and click **Create** to create the virtual machine.

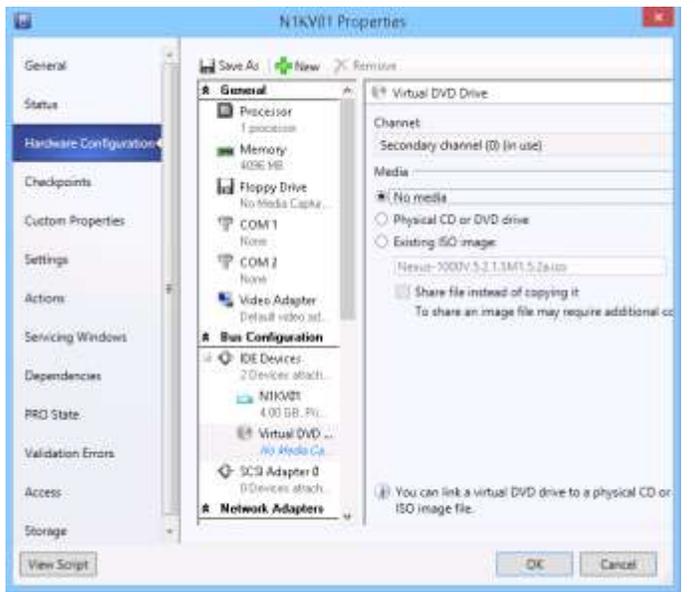


On the **Jobs** page you will be able to track the status of the job creating the VM.

Repeat the procedure to create a second N1KV VM.



When the build of the two VMs is complete, remove the ISO file from the virtual DVD of each VM. Open the **Properties** of the VM and select **Hardware Configuration**. Select the **Virtual DVD Drive** and click the radio button by **No Media**. Click **OK** to accept the change.

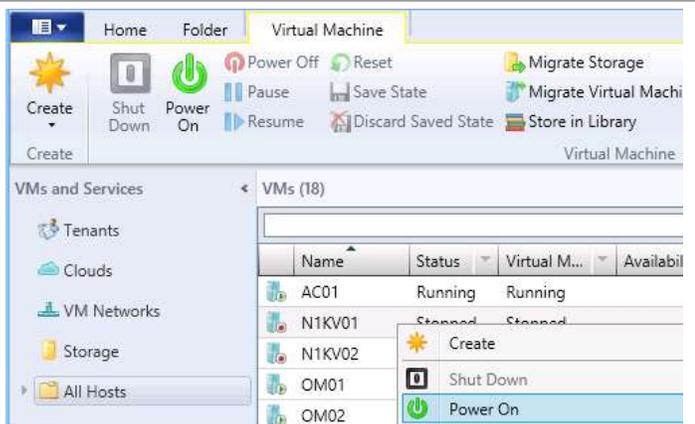


Configure Highly Available VSM

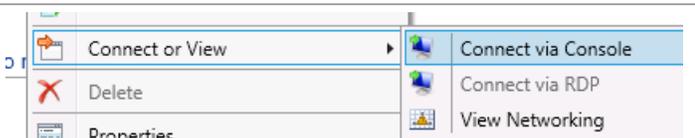
After creating the VMs, they need to be configured to create a highly available solution. The steps are different for the first and second VMs. Most of the configuration is performed when you first run the first VM. When the second VM is started, you basically join it to the first and it picks up most settings from that.

► Perform these actions on the first VSM

Within the SCVMM management console, right-click the first N1KV VM and select **Power On**.



After starting the VM, right-click and select **Connect or View** and **Connect through Console**.

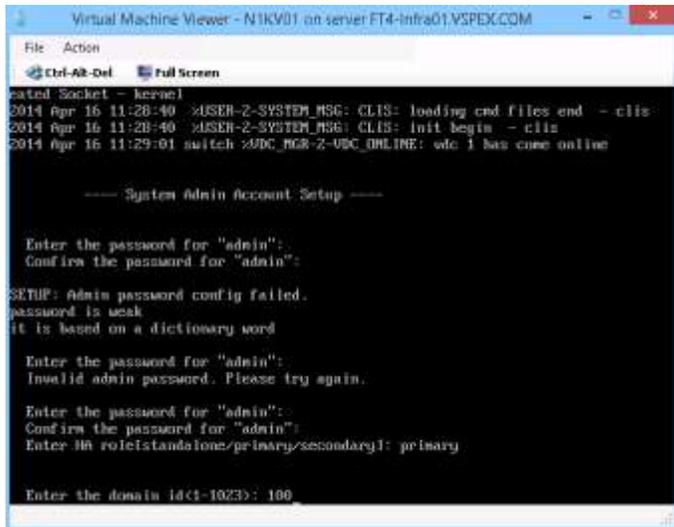


There are three questions asked, all of which have short timers on them. If you do not answer, they take the automatically continue using the defaults. The defaults are the answers you want.

The installation asks for a password for the admin account. Enter the password and confirm it. If the password is not considered 'strong', you will be prompted for a different password.

The next question is the HA role. Enter **primary**.

The next question is the domain ID. Enter a value between 1-1023.

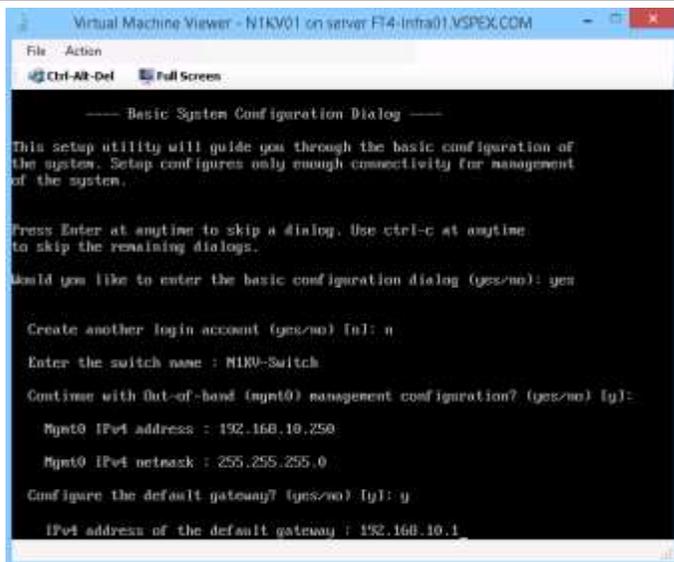


The system saves the configuration and then enters the Basic System Configuration Dialog. The first question is **Would you like to enter the basic configuration dialog (yes/no)**: Enter **yes**.

Answer **n** when it asks to create another login.

Enter the IP address and subnet mask of the switch.

Enter **y** when asked to configure the default gateway. Enter the gateway address.

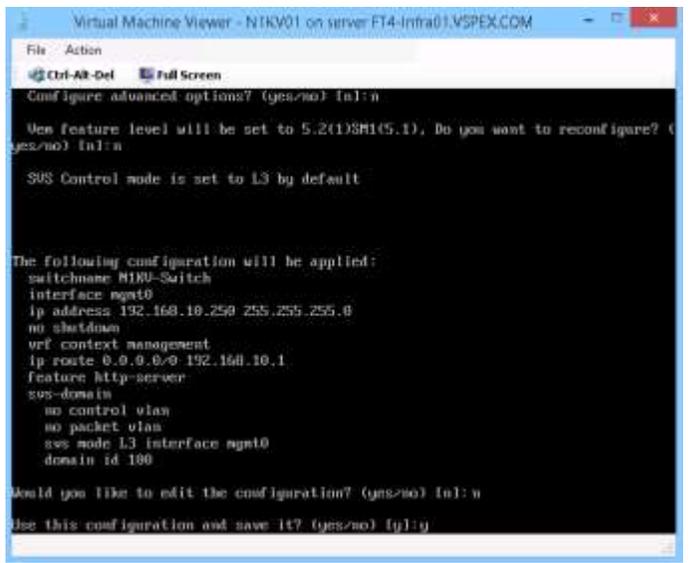


Answer **n** to the question to configure advanced options.

Answer **n** to the question about reconfigure the feature level.

Answer **n** to question to edit the configuration.

Enter **y** to question to save the configuration.



The system will save the configuration and prompt for a login. Login using the previously entered password.



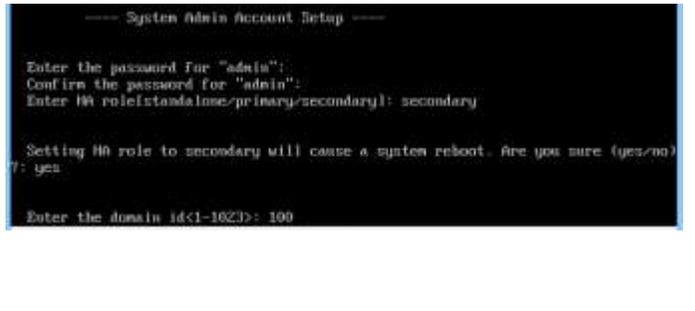
► Perform the following steps on the second VSM

Perform steps 1-4. When the system asks for the HA role, enter **secondary**.

Setting the HA role to secondary will cause a system reboot. Answer **yes** to the confirmation question.

Enter the **domain ID** entered during the installation of the first VSM.

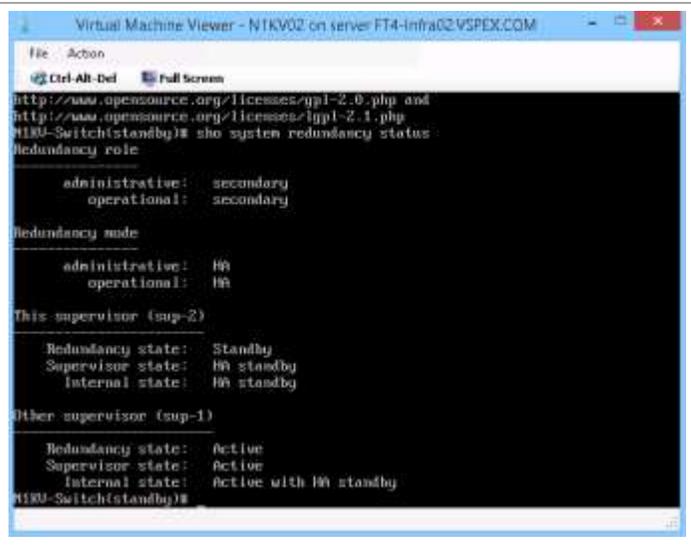
System will save the configuration and reboot.



The system will prompt for a login. Login with the admin account and the password entered previously.

To check the redundancy status, enter the command:

```
show system redundancy status
```



The VSM creates interfaces in an ascending MAC address order of the virtual NIC offered by Microsoft Hyper-V. Currently, Microsoft Hyper V provides no guarantees that this order is the same as displayed at the VSM VM Settings panel. The VSM always uses its first interface as control0 and its second interface as mgmt0. The network profiles for these two interfaces might need different VLANs. Therefore, you should verify that the interfaces are selected by the VSM in the same order that are displayed in the virtual machine Settings panel.

Execute the following CLI on the primary VSM to verify the order of the management and control MAC addresses:

```
NTKV-Switch# show interface mac-address
```

```
-----
Interface          Mac-Address      Burn-in Mac-Address
-----
mgmt0              001d.d8b7.1e61  001d.d8b7.1e61
control0           001d.d8b7.1e60  001d.d8b7.1e60
```

If the order is not the same, you can use the following commands to specify the preferred MAC to control0/mgmt0 interface mappings:

```
system internal control-mac XXXX.XXXX.XXXX
system internal mgmt-mac XXXX.XXXX.XXXX
```

These commands require that you enter the `copy running-config startup-config` command afterwards to make the change persistent and effective after the next VSM reload.

Configure VSM

After ensuring the two VSM virtual machines are configured for HA, and that the proper MAC addresses are allocated to the right function, the following minimal objects need to be created in the VSM.

- Logical Network
- Network Segment Pool
- IP Pool Template
- Network Segment
- Virtual Ethernet Port Profile
- Ethernet Port Profile
- Network Uplink

Log into the primary VSM to perform create these objects. Though not required, you may also want to add the telnet feature to the VSM so it can be managed without the need to connect to the VSM VM through SCVMM.

The following values need to be defined:

- **<FastTrack>** - user-defined name that will be used when defining a logical switch in VMM
- **<Fabric-Mgmt>** - user-defined name of the management fabric. Member of just defined logical network
- **<N1KV-pool-200>** - user-defined name for a fabric management IP pool. Multiple pools can be created when managing multiple networks with N1KV
- **<192.168.200.100 192.168.200.199>** - pool of IP addresses to be managed
- **<192.168.200.0 255.255.255.0>** - pool IP subnet and netmask
- **<192.168.200.1>** - pool default gateway
- **<N1KV-MF-Public>** - user-defined network segment name. Different network segments can be defined using different IP pools
- **<200>** - VLAN tag for management network
- **<AllAccess>** - port profile created for later use in the definition of logical switch in VMM when configuring the virtual port
- **<N1KV-MF-Uplink>** - uplink port profile created for later use in the definition of the logical switch in VMM
- **<N1KV_Uplink_Policy_FastTrack>** uplink port profile for physical NIC

```

configure terminal

feature telnet

nsm logical network <FastTrack>
exit

nsm network segment pool <Fabric-Mgmt>
member-of logical network <FastTrack>
exit

nsm ip pool template <N1KV-pool-200>
ip address <192.168.200.100 192.168.200.199>
network <192.168.200.0 255.255.255.0>
default-router <192.168.200.1>
exit

nsm network segment <N1KV-MF-Public>
member-of network segment pool <Fabric-Mgmt>
switchport access vlan <200>
ip pool import template <N1KV-pool-200>
publish network segment
exit

port-profile type vethernet <AllAccess>
no shutdown
state enabled
publish port-profile
exit

port-profile type ethernet <N1KV_Uplink_Policy_FastTrack>
channel-group auto mode on mac-pinning
no shutdown
state enabled
exit

nsm network uplink <N1KV-MF-Uplink>
import port-profile <N1KV_Uplink_Policy_FastTrack>
allow network segment pool <Fabric-Mgmt>
system network uplink
publish network uplink
exit

copy running-config startup-config

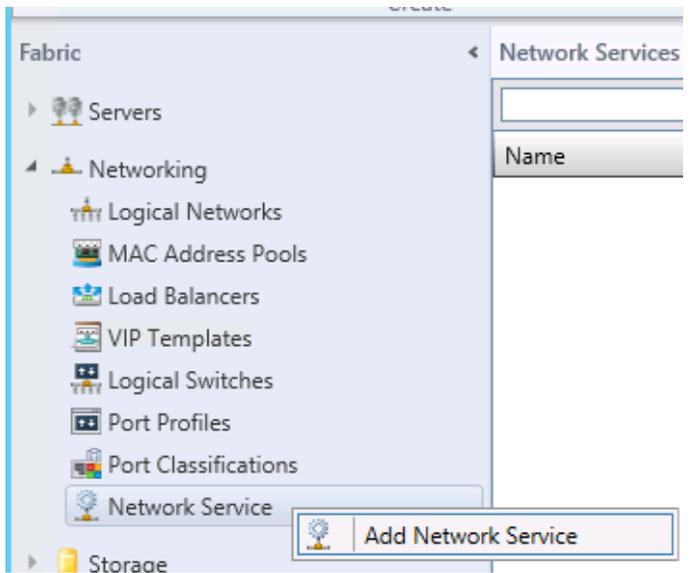
```

Connect SCVMM to VSM

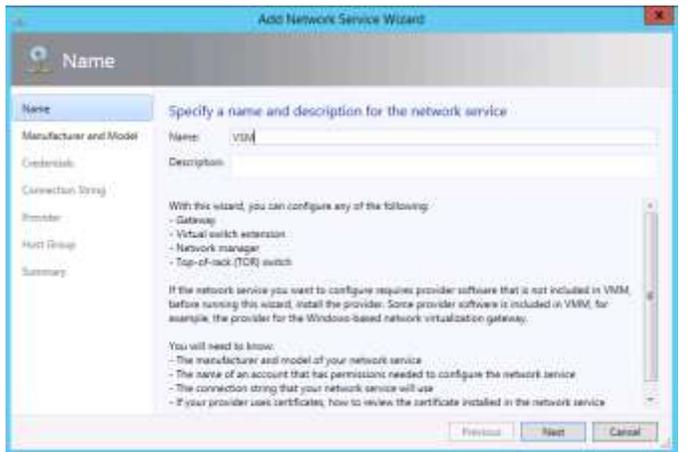
When the VSM is up, configure the SCVMM networking fabric for the Nexus 1000V.

For detailed information on configuring SCVMM, go to the complete documentation: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/hyperv/sw/5-2-1-SM-1-5-2a/install-and-upgrade/n1000v_gsg.html.

In the SCVMM console, select the **Fabric** pane and expand **Networking**. Right-click **Network Service** and select **Add Network Service**.



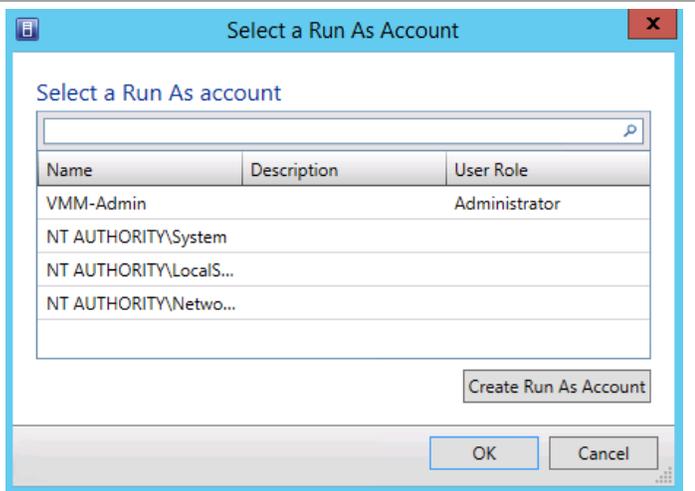
On the **Name** page, enter an appropriate name. Optionally provide a Description. Click **Next** to continue.



Establishing the connection requires a Run As account. On the **Credentials** page, click **Browse...**



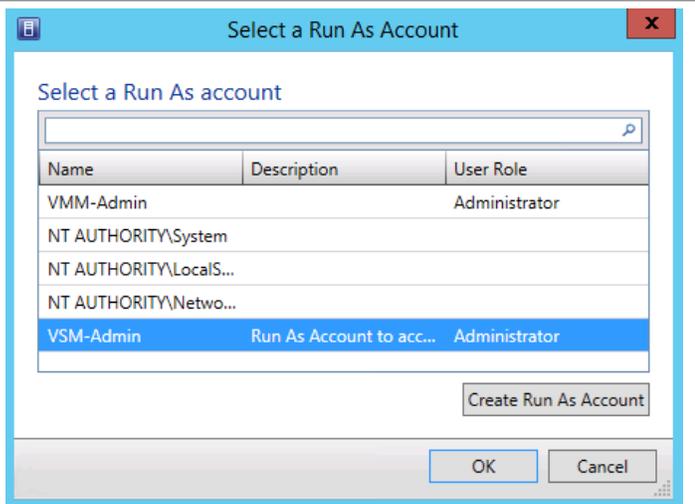
The Run As account for connecting to the VSM requires the username and password of the VSM. Click **Create Run As Account**.



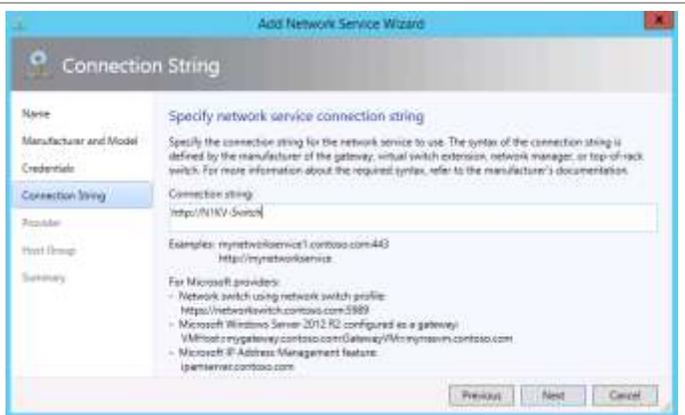
On the **Create Run As Account** page, enter a value for the **Name** of the account. Optionally you can enter a Description. Enter **admin** as the **User name**. For **Password** enter and confirm the password you created for the VSM. Make sure to clear the check box by **Validate domain credentials**. Click **OK** to add this as a Run As account.



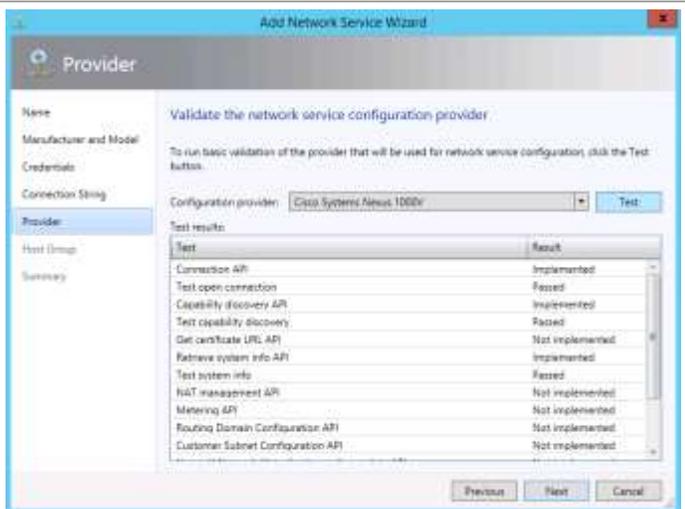
Back on the **Select a Run As Account** page, select the newly created account and click **OK** to continue. That returns you to the **Credentials** page. Click **Next** to continue.



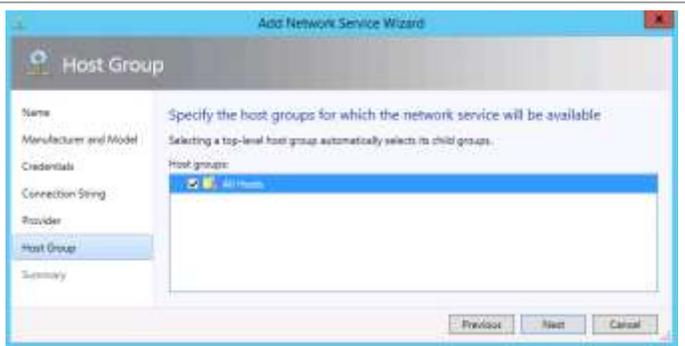
On the **Connection String** page, enter the **IP address** or **DNS name** of the VSM. This solution is not configured with certificates, so it uses an **http** connection. If using certificates, use an **https** connection. Click **Next** to continue.



On the **Provider** page, click the **Test** button to test the connection to the VSM. Make sure there are no **Failed** tests. Click **Next** to continue.



On the **Host Group** page, select the host groups for which you want to make the VSM available. Click **Next** to continue. On the **Summary** page, confirm your settings and click **Finish** to add the network service.



Create a Logical Switch in SCVMM

When the Virtual Switch Extension Manager has been added, create a logical switch on VMM. Define the extensions and port profiles for the logical switch, create classifications that contain the native port profile and a port profile for each extension as outlined in the following steps.

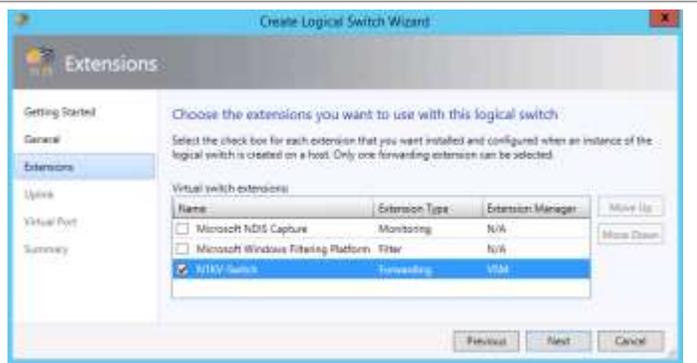
In the **Fabric** pane, select **Networking** and click **Create Logical Switch** from the menu ribbon. Click **Next** on the Getting Started page that displays.



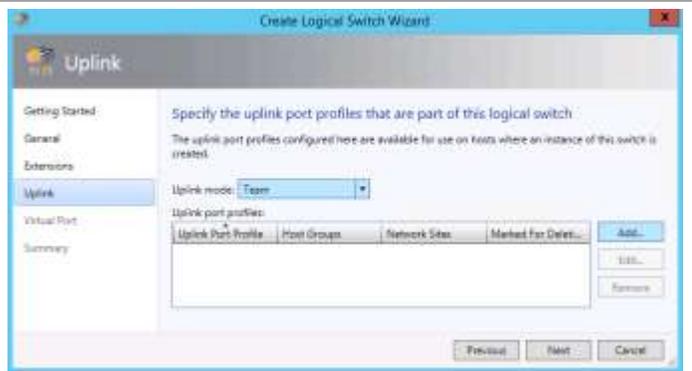
On the **General** page, enter a **Name** for this logical switch. Optionally you may enter a Description. Click **Next** to continue.



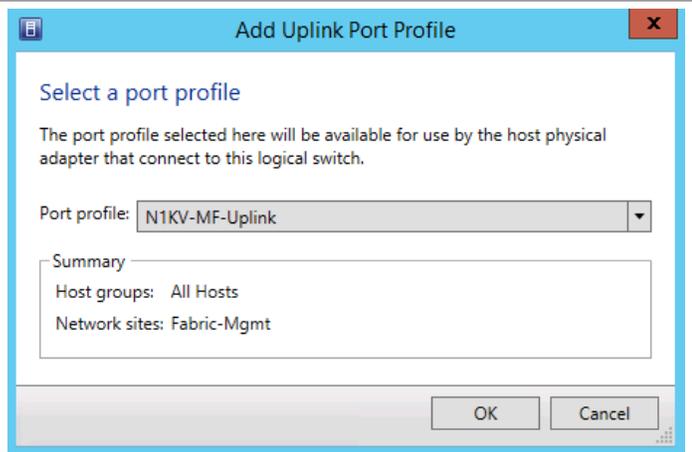
On the **Extensions** page, clear the check box by Microsoft Windows Filtering Platform and select the check box by the extension you created in the previous steps. Click **Next** to continue.



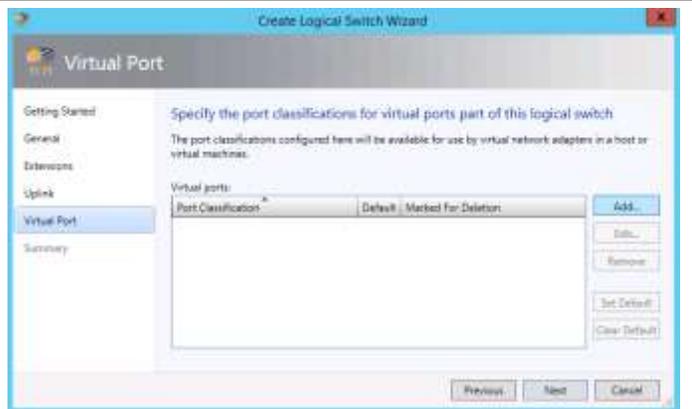
On the **Uplink** page, select **Team** for the **Uplink mode**. Then click **Add...**



On the **Select a port profile** page, select a port profile you created on the VSM. Click **OK** to continue. Back on the **Uplink** page, click **Next** to continue.



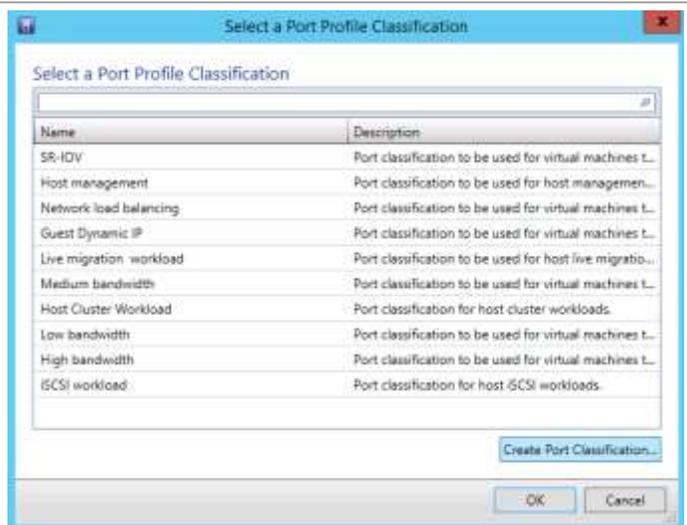
On the **Virtual Port** page, click **Add...**



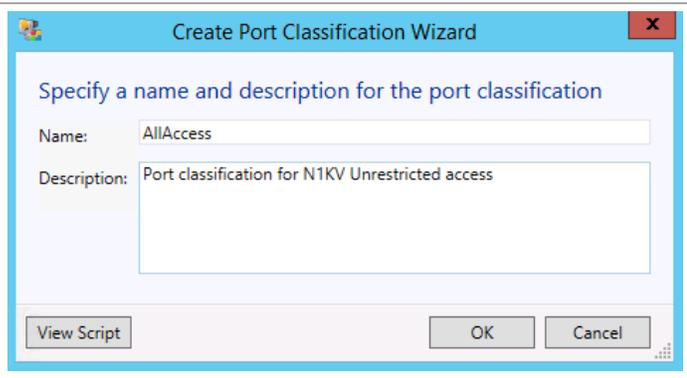
On the **Configure the virtual port** page, select the VSM you created earlier. From the **Use this port profile** drop down list, select the appropriate port profile. Click **Browse...**



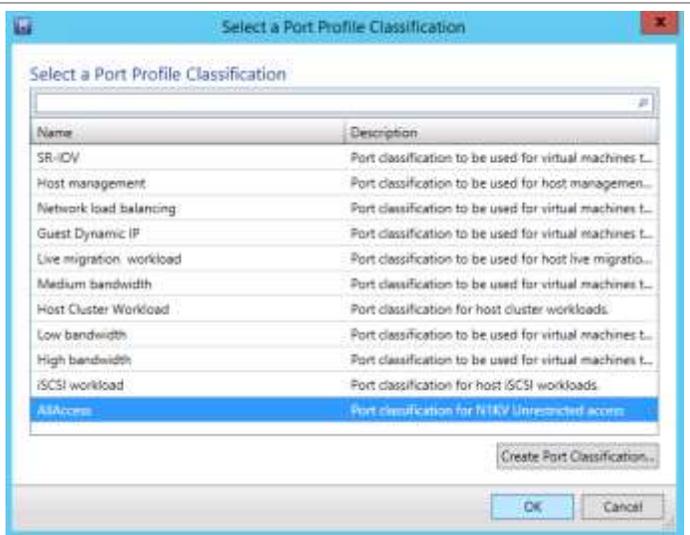
On the **Select a Port Profile Classification** page, click **Create Port Classification**.



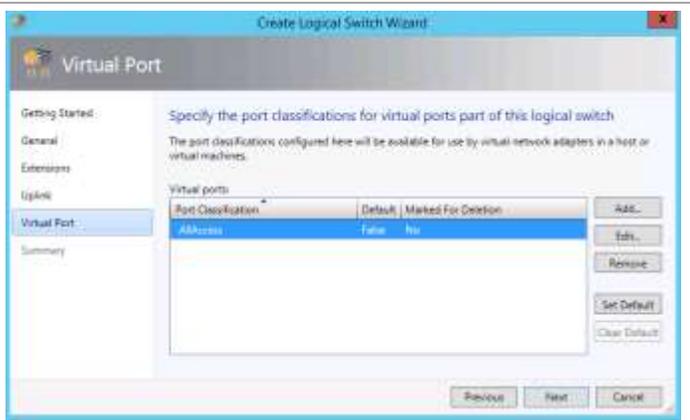
On the **Specify a name and description for the port classification** page, enter a name and, optionally, a description. Click **OK** to continue.



Back on the **Select a Port Classification**, select the newly created classification, and click **OK** to continue. This take you back to the **Configure the virtual port** page. Click **OK** to continue.

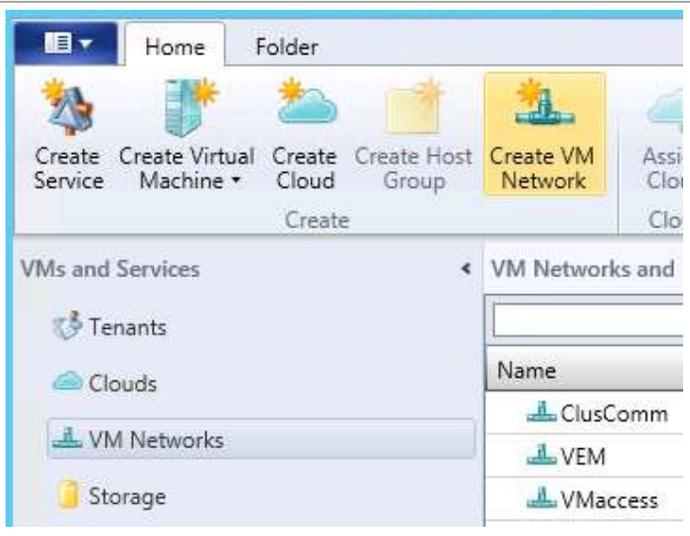


On the **Virtual Port** page, click **Next** to continue. On the **Summary** page, confirm your settings and click **Finish** to create the logical switch.



Configure a VM Network

Select the **VM and Services** page in the SCVMM console. Select **VM Networks** and click **Create VM Network** on the menu ribbon.



On the **Name** page of the Create VM Network Wizard, enter a descriptive **Name** for the network. Optionally, enter a Description. Select the appropriate **Logical network** from the drop down list. Click **Next** to continue.



On the **Isolation** page, the proper selections should already be made. Click **Next** to continue.



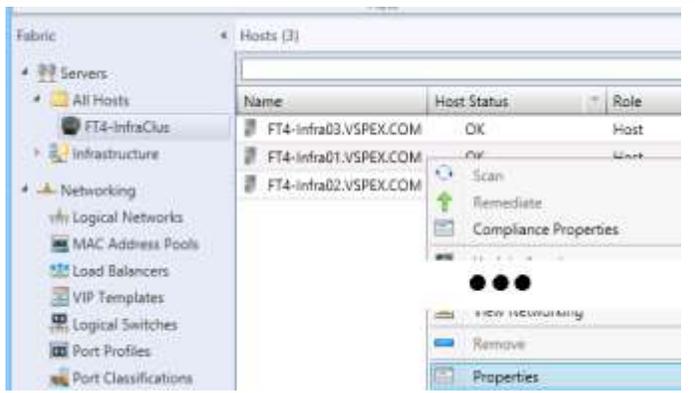
On the **Isolation Options** page, select the radio button by **Specify an externally supplied VM network**. Make sure the proper network is selected from the drop down list. Click **Next** to continue. On the **Summary** page, confirm your settings and click **Finish** to create the VM network.



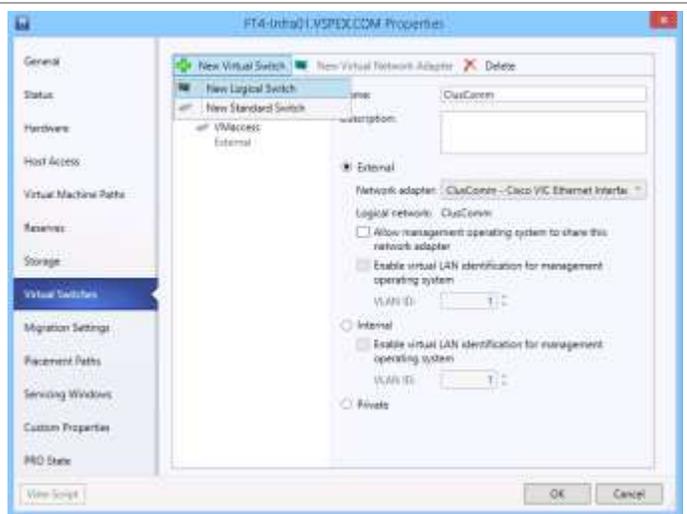
Add Hyper-V Hosts to a Logical Switch

After a logical switch is created, you can update the properties of the logical switch.

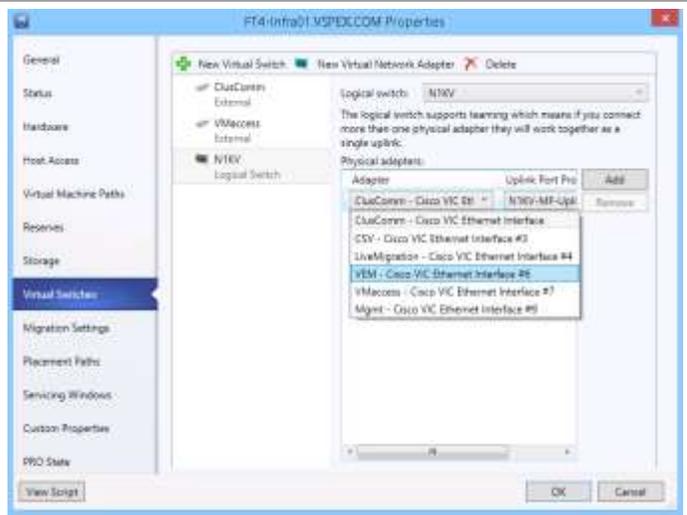
In the **Fabric** pane, select **Servers > All Hosts** and expand it to list the individual servers. Select a server, right-click, and select **Properties**.



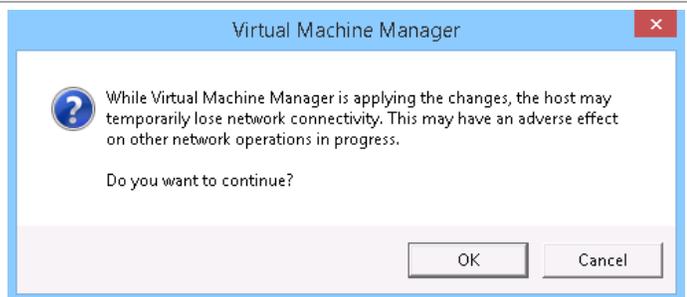
On the server's **Properties** page, select **Virtual Switches**. Click **New Virtual Switch** and select **New Logical Switch**.



From the **Physical adapters** drop down list, select the NIC that is to be used with the logical switch. Select the appropriate **Uplink Port Profile** from its drop down list. Click **OK** to continue.



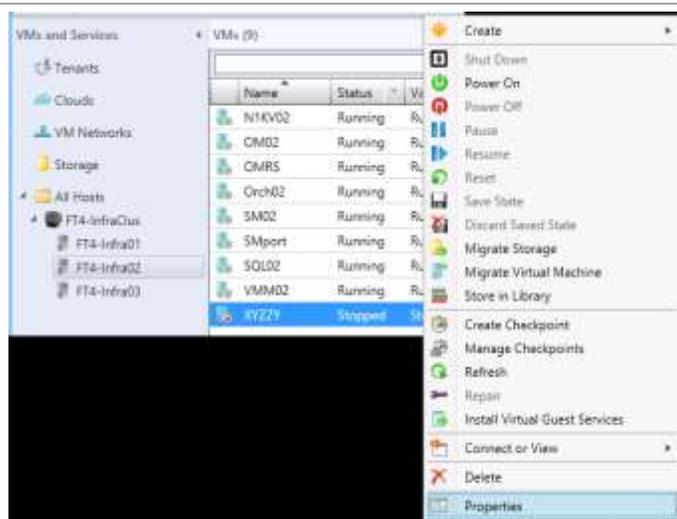
A message displays warning of potential loss of connectivity. You should not be selecting the NIC on which management traffic is occurring, so click **OK** to accept the risk.



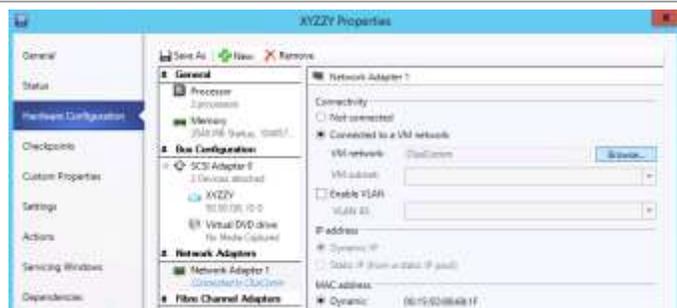
You can monitor the progress of the job in the **Jobs** pane. Repeat this process for each Hyper-V host that needs this logical switch. When using in a cluster, all nodes of the cluster need the same logical switch.

Connect VMs to Cisco Nexus 1000V

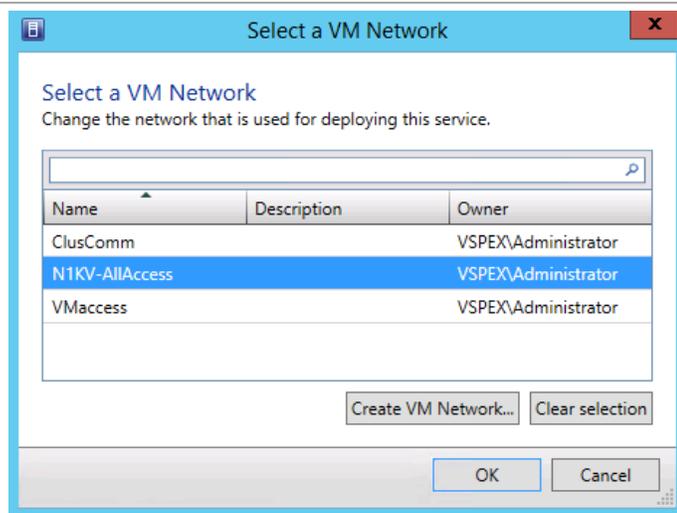
Select a VM that is on a Hyper-V host that has the logical network. Right-click the VM and select **Properties**.



On the **Properties** page for the selected VM, select **Hardware Configuration**. Under **Network Adapters** select the adapter to connect to the logical switch. Under **Connectivity** select the radio button by **Connected to a VM network** and click **Browse...**



On the **Select a VM Network** page, select the previously created logical network. Click **OK** to continue.



Back on the VM's **Properties** page click the radio button by **Logical Switch**. Make sure the proper switch is selected in the **Logical switch** drop down list and then select the associated **Classification** from that drop down list. Click **OK** to accept the changes.

The screenshot shows the 'Network Adapter 1' configuration window. The 'Connectivity' section has 'Connected to a VM network' selected. The 'VM network' is 'N1KV-AllAccess' and the 'VM subnet' is 'N1KV-MF-Public'. The 'IP address' section has 'Dynamic IP' selected. The 'MAC address' section has 'Dynamic' selected with the address '00:15:5D:82:13:0F'. The 'Virtual switch' section is highlighted with a red box and has 'Logical Switch' selected. The 'Logical switch' is 'N1KV' and the 'Classification' is 'AllAccess'. The 'Standard switch' section has 'VMAccess' selected.

Cisco Nexus 1000V PowerShell Cmdlets

Cisco provides a PowerShell module containing cmdlets to invoke the REST APIs on the Nexus 1000V. This can be downloaded from <https://developer.cisco.com/fileMedia/download/8bf948fb-83a5-4c9e-af5c-4faac735c8d3>.

Download the .zip file and expand it. Copy the Cisco-Nexus1000V.psm1 file to the system from which the PowerShell cmdlets will be used. Before using the cmdlets, the module must be imported.

```
PS C:\> Import-Module .\<location>\Cisco-Nexus1000V.psm1
```

Before issuing any other Nexus 1000V cmdlets, you need to establish a link to the virtual supervisory module with the following cmdlet.

```
PS C:\> Connect-VSM -Vsm_IP <IP address>
```

A credentials window will open allowing for the entry of the credentials to connect to the VSM. This cmdlet will create two global variables which must not be overridden during the PowerShell session - \$VSM_IP and \$Credential.

To see all cmdlets available to be used, issue the following cmdlet.

```
PS C:\> Get-Command -Module Cisco-Nexus1000V
```

EMC Integration Components

EMC Software Installation Locations

There are several EMC management software components which are recommended to be installed in the Fast Track environment. Some of the components, specifically ESI PowerShell and Navisphere CLI can be installed on a configuration workstation to assist in the initial setup of the Fast Track infrastructure. After the initial deployment, a management VM can be configured to host all of the EMC software components. The list below outlines the components and their installation locations as tested during the Fast Track validation.

- EMC Storage Integrator Service
 - EMC Management VM
- EMC System Center Operations Manager Management Packs
 - System Center Operations Manager Server
- EMC Storage Integrator PowerShell Toolkit
 - Configuration Workstation
 - ESI requires a Windows Server host for installation. Please see the ESI release notes for supported operating system versions.
 - EMC Management VM
- EMC SMI-S Provider
 - EMC Management VM
- EMC Navisphere CLI (naviseccli)
 - Configuration Workstation
 - EMC Management VM

EMC Storage Integrator v3.1 Overview

EMC Storage Integrator (ESI) for Windows is a set of tools for Microsoft Windows and Microsoft applications administrators. ESI for Windows provides the ability to view, provision, and manage block and file storage for Microsoft Windows, Exchange, and SharePoint sites. ESI supports the EMC Symmetrix VMAX series, EMC VNX series, EMC VNXe series, and EMC CLARiiON CX fourth generation (CX4) series of storage systems. ESI requires that you install the applicable adapter for your specific storage systems. The ESI suite includes the following components:

- ESI for Windows and ESI PowerShell Toolkit
- ESI Service and ESI Service PowerShell Toolkit
- ESI hypervisor support
- ESI Adapter for EMC RecoverPoint
- ESI Integration for Microsoft Exchange
- ESI Adapter for Microsoft SharePoint
- ESI Management Packs for Microsoft System Center Operations Manager
- ESI Integration Pack for Microsoft System Center Orchestrator
- EMC Hyper-V Volume Shadow Copy Service Requestor

In this document, we will concentrate on the following ESI components, which are particularly useful in our Private Cloud environment:

ESI for Windows and ESI PowerShell Toolkit: ESI for Windows has a GUI that is based on Microsoft Management Console (MMC). You can run ESI as a stand-alone tool or as part of an MMC snap-in on a Windows computer. The ESI PowerShell Toolkit provides ESI storage provisioning and discovery capabilities with corresponding PowerShell cmdlets.

ESI Service and ESI Service PowerShell Toolkit: ESI Service is the communications link between ESI and the ESI Management Packs for Microsoft System Center Operations Manager. You can use ESI Service to view and report on registered EMC storage systems and storage system components that are connected to the ESI host system. ESI Service then pushes this data to Operations Manager. You can also use the ESI Service as a stand-alone tool without Operations Manager to collect, view, and report this same system data.

ESI Hypervisor Support: In addition to supporting physical environments, ESI supports storage provisioning and discovery for Windows virtual machines that are running on Microsoft Hyper-V, Citrix XenServer, and VMware vSphere.

ESI Management Packs for Microsoft System Center Operations Manager: The EMC Storage Integrator System Center Operations Manager (ESI SCOM) Management Packs and the ESI Service work in conjunction with Microsoft System Center Operations Manager for centralized discovery and monitoring of supported EMC storage systems and storage-system components. The ESI Service reports information to SCOM regarding all registered EMC storage systems and storage-system components. The ESI SCOM Management Packs integrate EMC storage systems with SCOM by providing the following functionality:

- Consolidated and simplified dashboard view of storage entities
- Health status and events from the storage system
- Alerts for possible problems with disk drives, power supplies, storage pools and other types of physical and logical components in SCOM

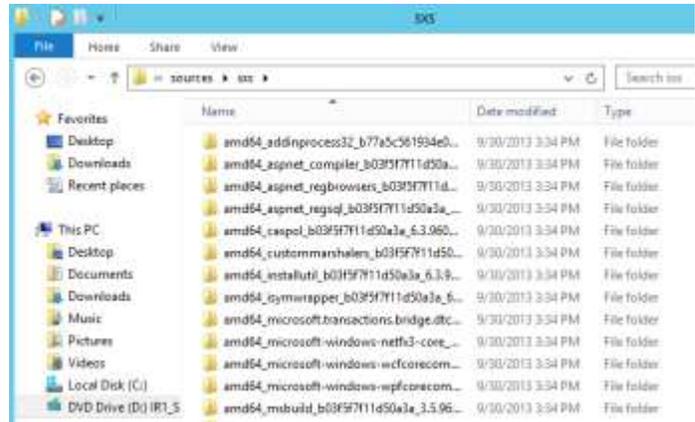
ESI Integration Pack for System Center Orchestrator: Microsoft System Center 2012 Orchestrator is a workflow management system that defines, creates, and manages workflows. The ESI System Center Orchestrator Integration Pack provides workflow automation for ESI storage provisioning tasks. Using the ESI SCO Integration Pack, you can manage and provision storage for interoperable storage management and process consistency across a data center.

Installing ESI v3.1

To use ESI features as documented with the Fast Track architecture, perform the following installation procedure.

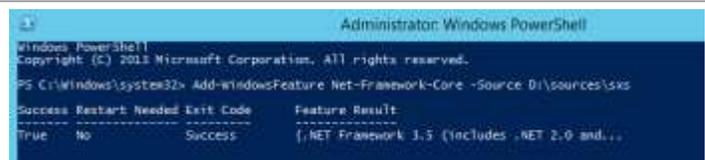
▶ Perform the following steps on the **EMC Management** virtual machine.

Obtain a copy of the Windows Server 2012 R2 source files. The source files can be found on the installation media in the “\sources\sxs” folder



Install .Net Framework 3.5 using the source files from the previous step. From PowerShell run the following command:

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

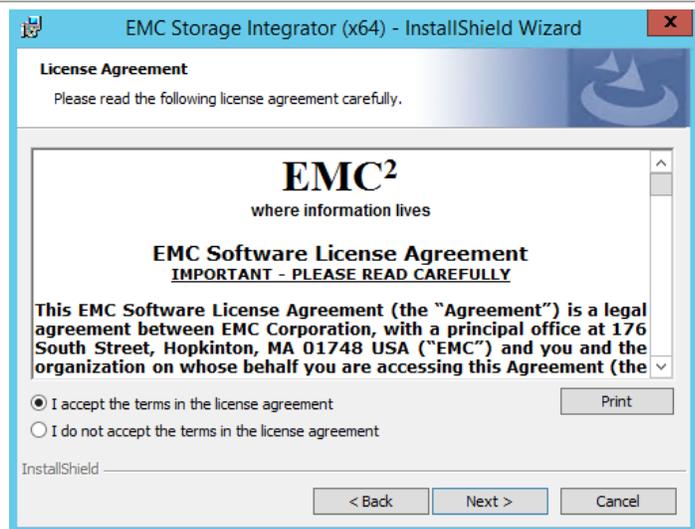


Install the Windows PowerShell 2.0 Engine

```
Add-WindowsFeature PowerShell-V2
```



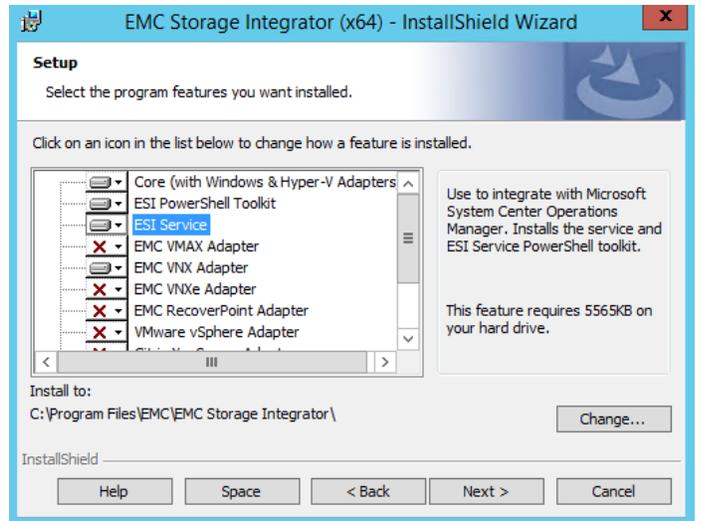
Run the EMC Storage Integrator (x64) installer and accept the License Agreement



Select the following components:

- Core (with Windows & Hyper-V Adapters)
- ESI PowerShell Toolkit
- ESI Service
- EMC VNX Adapter

Click **Next**



Click **Install**



Click **Finish**



Register the VNX for use with the ESI PowerShell Toolkit

► Perform the following steps on the **EMC Management** virtual machine.

From PowerShell command window run:

```
Get-EmcStorageSystemCredential | Connect-EmcSystem
```

When prompted choose the appropriate **System Type**:

- “VNX” for a Unified System
- “VNX-Block” for a block only system

Enter the credentials and IP address information.

If available, select **Add host Key If Missing**

Click **Test Connection** to make sure connectivity

Provide detailed connection information (Fields with * are required):	
Block-Username(*)	UserID
Block-Password(*)	*****
SPA's IP address(*)	192.168.177.113
SPB's IP address(*)	192.168.177.114
Block Port Number	443

Click **OK** following the test connection results

Click **OK** again to register the VNX storage array with ESI

Testing system connection...

Resulting output from PowerShell

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-EmcStorageSystemCredential | Connect-EmcSystem

AdapterType           : StorageSystem
UserFriendlyName      : EnterpriseFastTrack
OperationalStatus     : (OK)
StatusMessages        : (OK)
BlockSoftwareRevision : 05.33.000.5.051
```

Installing and Configuring the EMC Storage Integrator Management Pack for System Center Operations Manager

The installation and configuration of ESI and the SCOM management pack includes several steps outlined below:

Install the ESI Service and ESI Service PowerShell Toolkit as detailed in the

- Installing ESI v3.1 section
- Register the VNX array with the ESI Service
- Create an ESI Service user for the SCOM Management Pack RunAs Account
- Install the ESI SCOM Management Packs
- Import the ESI SCOM Management Packs
- Create an ESI RunAs Account and associating the account with a Profile
- Set Overrides for the EMC SI Service Discovery

Additional information can be found in the EMC Storage Integrator online help file, specifically the “ESI Service and ESI SCOM Management Packs” section.

Register the VNX with the ESI Service

► Perform the following steps on the **EMC Management** virtual machine.

From PowerShell command window run:

`Add-EmcSystem`

When prompted choose the appropriate **System Type**:

- “VNX” for a Unified System
- “VNX-Block” for a block only system

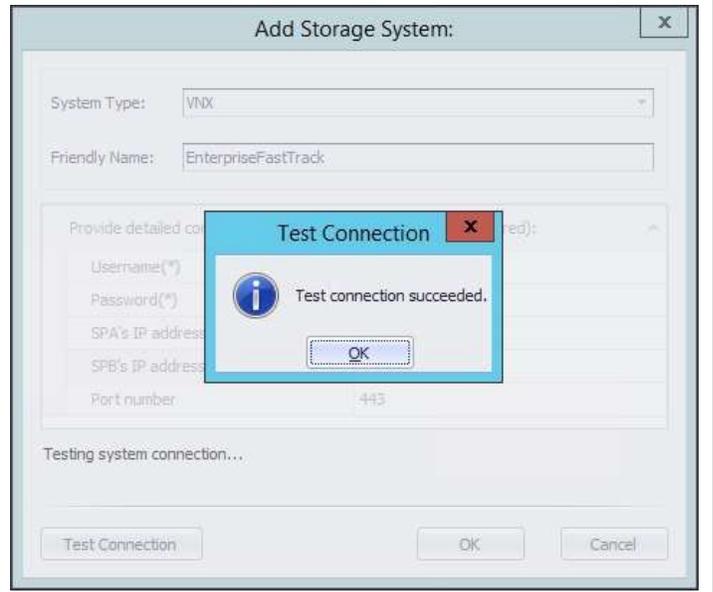
Enter the credentials and IP address information.

If available, select **Add host Key If Missing**

Click **Test Connection** to make sure connectivity

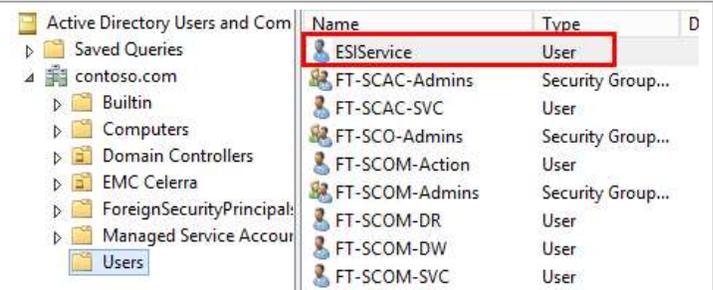
Provide detailed connection information (Fields with * are required):	
Block-Username(*)	UserID
Block-Password(*)	*****
SPA's IP address(*)	192.168.177.113
SPB's IP address(*)	192.168.177.114
Block Port Number	443

Click **OK** following the test connection results
 Click **OK** again to register the VNX storage array with the ESI Service



Create an ESI Service User for the SCOM Management Pack Run As Account

Create an ESI Service user account within the Active Directory domain. The user does not need administrative access to the host running the ESI Service.



From the host running the ESI Service, run the **Add-EMCUser** PowerShell command and give the ESI Service user "Monitor" access:

```
Add-EmcUser "Contoso\ESIService"
Monitor
```



Install the ESI SCOM Management Packs

► Perform the following steps on the **SCOM** virtual machine.

From the SCOM host run the ESI SCOM Management Packs installer and select **Next**



Accept the license agreement to proceed and select **Next**



Select or note the installation location

Select the following component:

- ESI SCOM Management Packs

Select **Next**



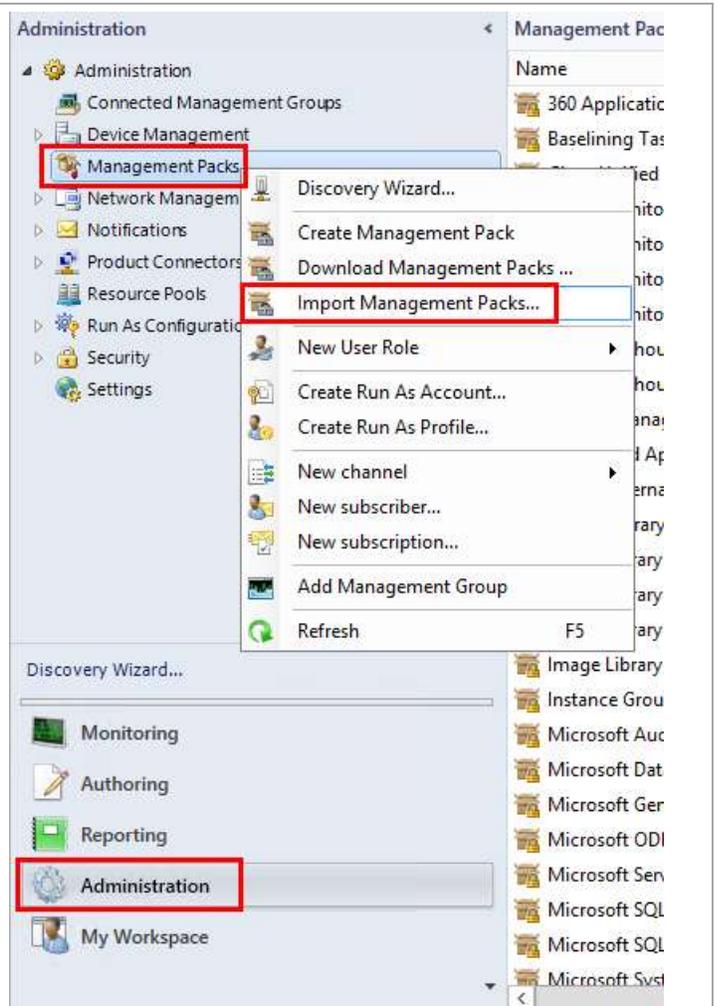
Select **Install** and then **Finish**



Import the ESI SCOM Management Packs

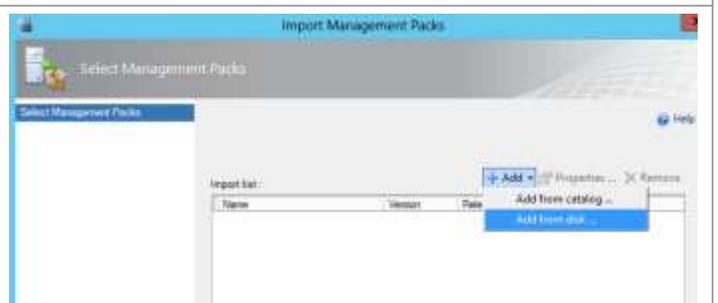
From within the Operations Manager console go to **Administration > Management Packs**

Right-click **Management Packs** and select **Import Management Packs**

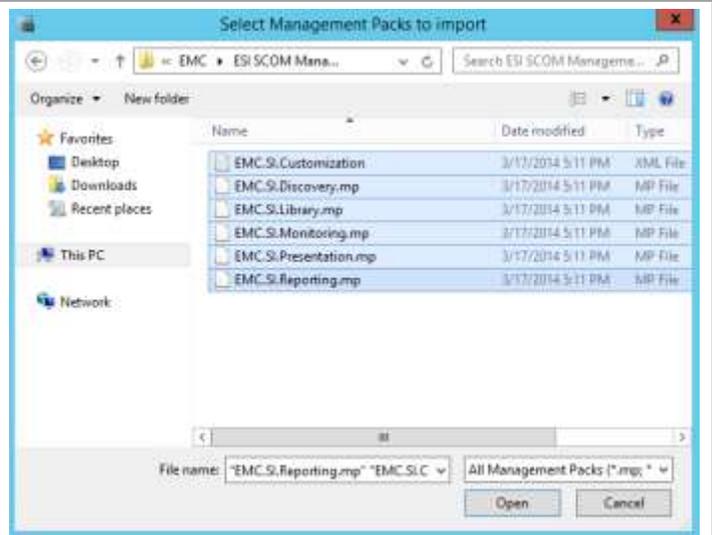


Select **Add** and then **Add from disk ...**

Select **No** if prompted to search the online catalog for dependencies

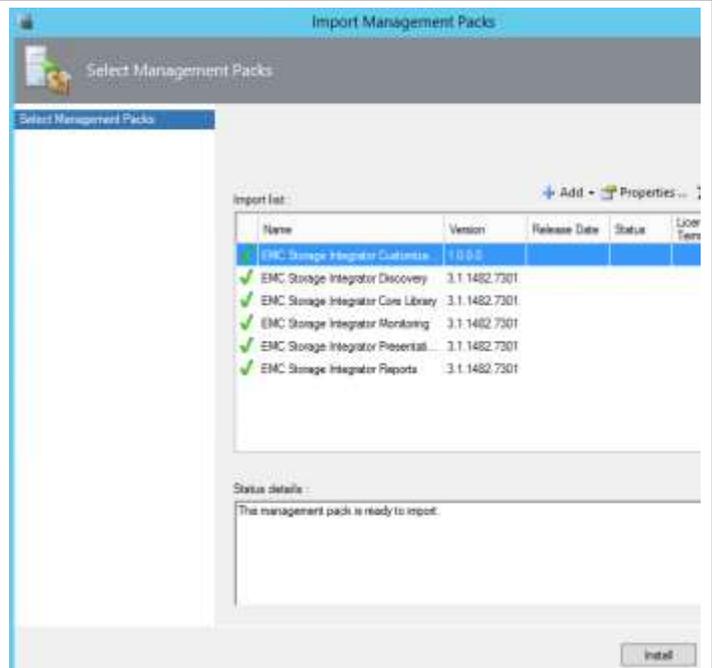


Browse to the management pack installation directory and select the 5 .MP and 1 .XML file in that directory. Select **Open**



Select **Install**

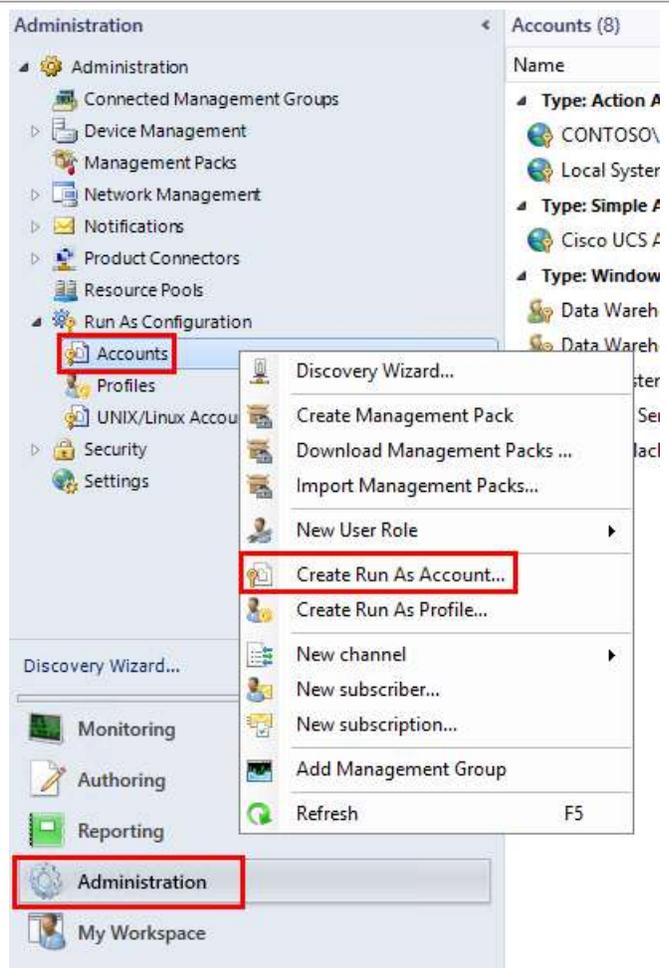
Then **Close** the wizard following successful completion.



Create ESI Run As Account and Associate with a Profile

From within the Operations Manager console go to **Administration > Run As Configuration > Accounts**

Right-click **Accounts** and select **Create Run As Account...**



Select **Next**



Choose a Run As account type of **Windows** and type in the desired Display Name and Description.

Select **Next**

The screenshot shows the 'Create Run As Account Wizard' window at the 'General Properties' step. The left sidebar has 'General Properties' selected. The main area is titled 'Specify general properties for the Run As account'. It contains a dropdown menu for 'Run As account type' set to 'Windows', a text box for 'Display name' containing 'EMC SI Service', and a text box for 'Description (optional)'. At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

Enter the account details for the domain account created in the previous steps that was assigned “Monitor” access to the ESI Service.

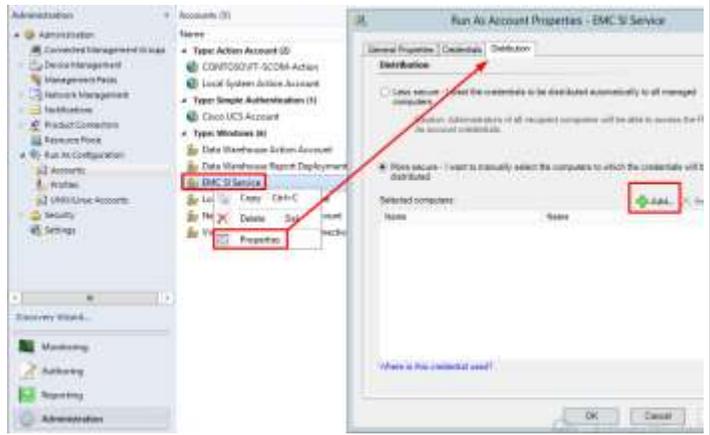
Select **Next**

The screenshot shows the 'Create Run As Account Wizard' window at the 'Credentials' step. The left sidebar has 'Credentials' selected. The main area is titled 'Provide account credentials'. It contains text boxes for 'User name' (containing 'ESIService'), 'Password' (masked with asterisks), and 'Confirm password' (masked with asterisks). There is also a dropdown menu for 'Domain' set to 'XXX.com'. At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

Choose the desired security option and select **Create** and then **Close**.

The screenshot shows the 'Create Run As Account Wizard' window at the 'Distribution Security' step. The left sidebar has 'Distribution Security' selected. The main area is titled 'Select a distribution security option'. It contains a warning message: 'The credentials for this Run As account must be distributed to the agent-managed computers or management servers to perform the monitoring operations that are associated with a Run As profile. Distribution cannot occur until the Run As account is added to a Run As profile.' Below this are two radio button options: 'Less secure - I want the credentials to be distributed automatically to all managed computers.' (unselected) and 'More secure - I want to manually select the computers to which the credentials will be distributed.' (selected). At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

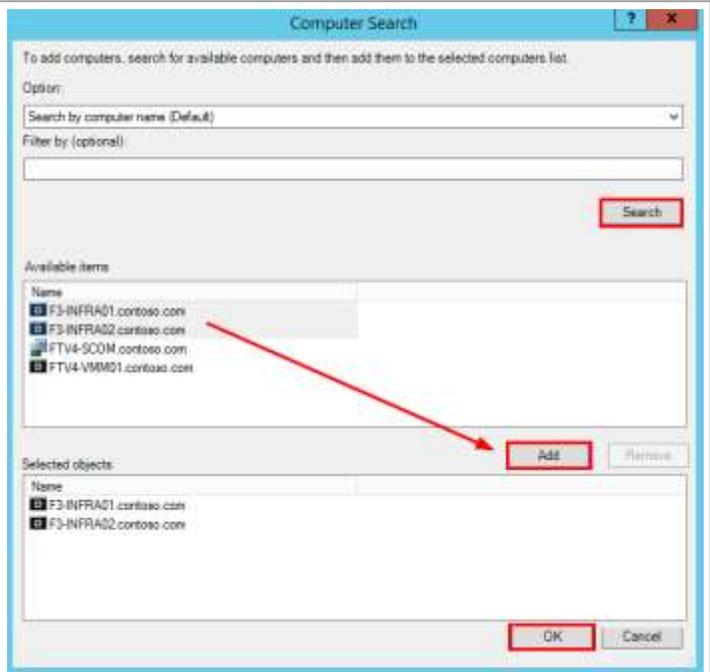
If the **More secure** security option was selected, go to the **Properties** of the Run as account and select the **Distribution** tab



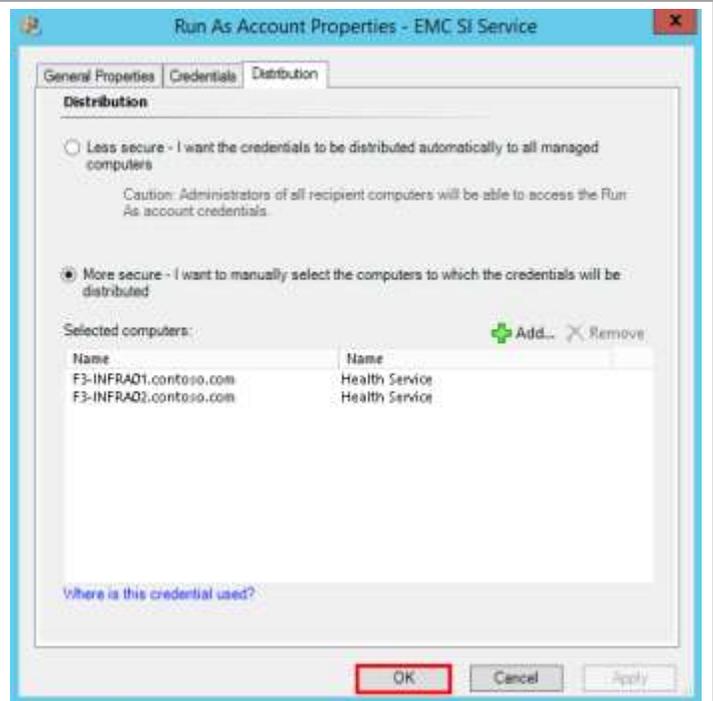
Select **Add**

Select **Search** to get a list of the available hosts, running the SCOM agent which can be used to communicate with the ESI Service.

Add the desired server or VM running the SCOM agent and select **OK**.

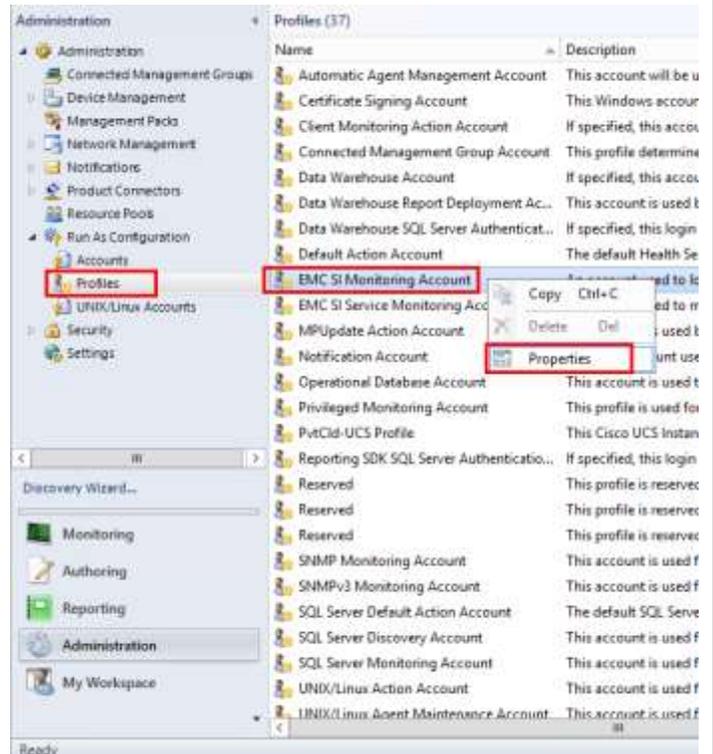


Select **OK** to save the change to the run as account



Go to **Administration > Run As Configuration > Profiles**

Within Profiles find the EMC SI Monitoring Account profile. Right-click that profile and select **Properties**.



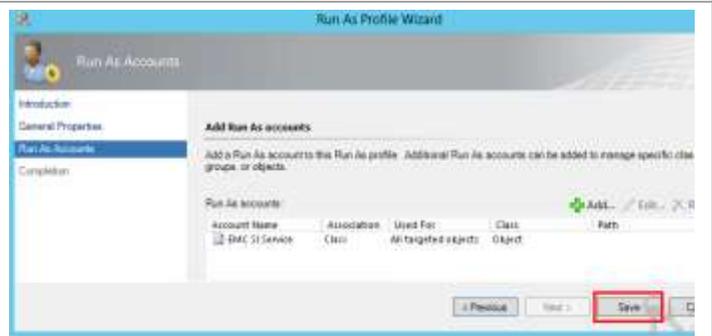
Select **Run As Accounts** and then select **Add...**



Select the run as account created in the previous steps and click **OK**



Select **Save** to commit the change
Select **Close** at the following screen

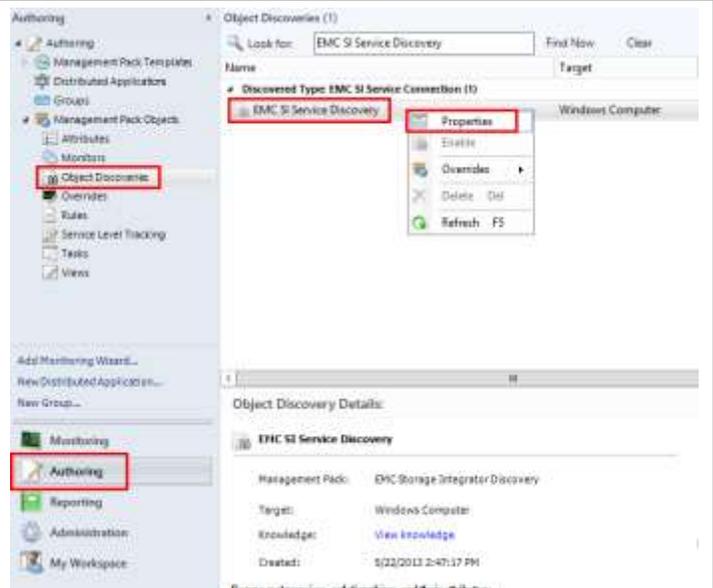


Setting Overrides for the EMC SI Service Discovery

From within the Operations Manager console go to **Authoring > Management Pack Objects > Object Discoveries**

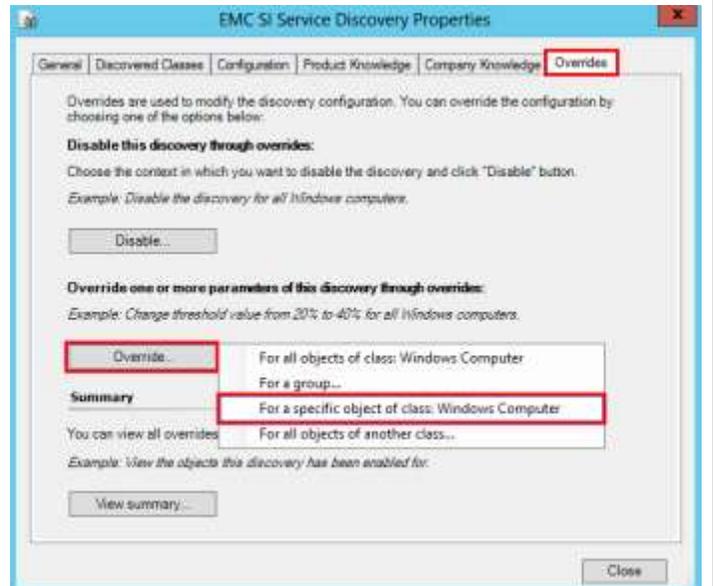
Find the **EMC SI Service Discovery** entry

Right-click EMC SI Service Discovery and select **Properties**



Go to the **Overrides** tab

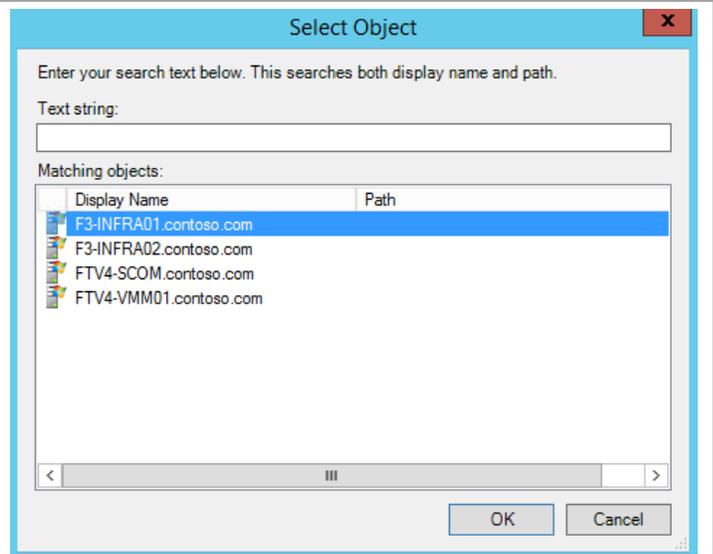
Click **Override...** and select **For a specific object of class: Windows Computer**



Select the desired host that will be used to communicate with the ESI Service.

If the “more secure” run as account option was selected in the previous steps, make sure to use the host where the credentials were distributed.

Select **OK**



Within the override properties the following parameters are required to be changed:

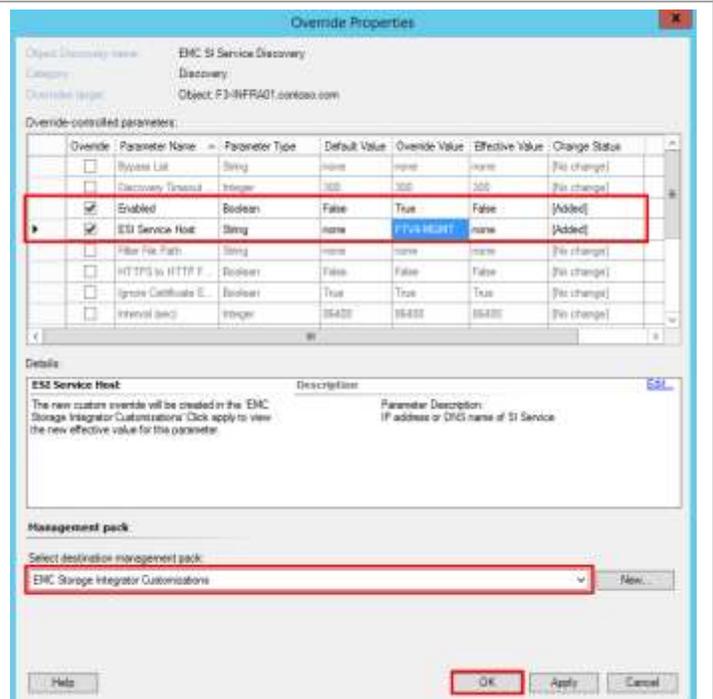
Parameter Name: **Enabled**
Override Value: **True**

Parameter Name: **ESI Service Host**
Override Value: **Name or IP Address of EMC Service Host**

For **Select destination management pack** choose “**EMC Storage Integrator Customizations**”

Select **OK**

For more details on additional parameters that can optionally be modified, see the ESI SCOM Management Pack online help



Install and Configure the EMC SMI-S Provider for System Center Virtual Machine Manager integration

VMM storage integration requires an SMI-S provider instance to communicate with the VNX storage array. The following sections outline the minimum requirements for configuring the SMI-S provider and VMM environment to allow for VMM to manage VNX storage and perform rapid virtual machine deployment. At a high level the required steps include:

- Installing the EMC SMI-S Provider
- Registering the VNX with the Provider

- Creating the SMI-S user for the SCVMM run as account
- Creating the run as account within SCVMM
- Registering the EMC SMI-S provider with SCVMM
- Creating classifications and choosing storage pools for management
- Allocating Storage Pools to Host Groups
- Configuring the Library Server
- Creating a San Copy Capable Template
- Selecting the Rapid Provisioning Deployment Method

Additional information can be found in the document titled “Storage Automation with System Center 2012 and EMC Storage Systems using SMI-S” available at <https://support.emc.com>

Install the EMC SMI-S Provider

► Perform the following steps on the **EMC Management** virtual machine.

From an elevated Command prompt or PowerShell session run the following commands to open the ports required for the SMI-S provider:

Command line

```
netsh advfirewall firewall add rule name="SLP-udp" dir=in protocol=UDP localport=427 action=allow

netsh advfirewall firewall add rule name="SLP-tcp" dir=in protocol=TCP localport=427 action=allow

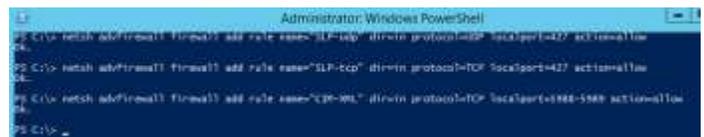
netsh advfirewall firewall add rule name="CIM-XML" dir=in protocol=TCP localport=5988-5989 action=allow
```

PowerShell

```
New-NetFirewallRule -DisplayName "SLP-udp" -LocalPort 427 -Protocol UDP -Action Allow -Direction Inbound

New-NetFirewallRule -DisplayName "SLP-tcp" -LocalPort 427 -Protocol TCP -Action Allow -Direction Inbound

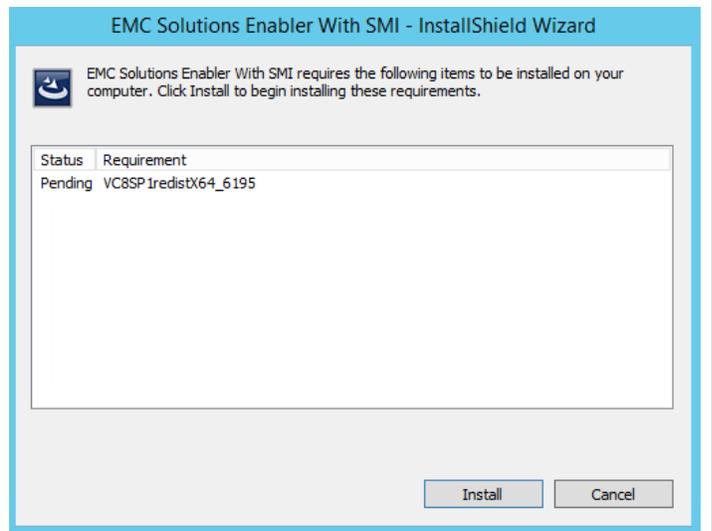
New-NetFirewallRule -DisplayName "CIM-XML" -LocalPort 5988-5989 -Protocol TCP -Action Allow -Direction Inbound
```



If the ESI Service is installed it should be stopped prior to installing the provider.

Run the **se7628-WINDOWS-x64-SMI.exe** installer

If prompted **install** the required Visual C++ runtime components.

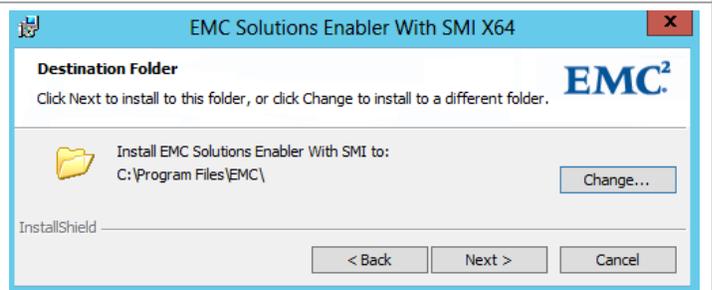


Select **Next** to begin installation

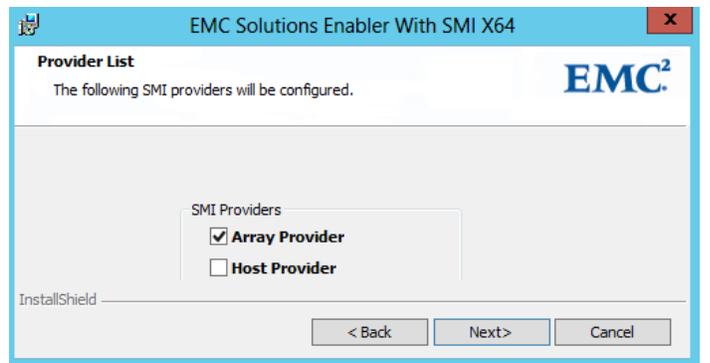


Install to the desired location

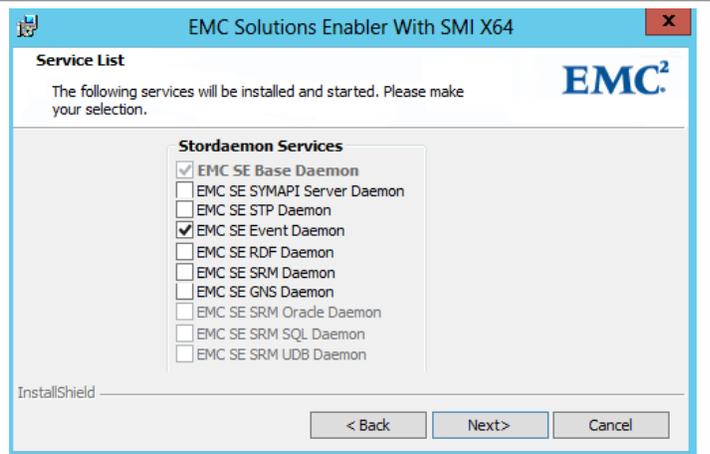
Click **Next**



Make sure **Array Provider** is selected and click **Next**



Accept the default service list and click **Next**
Then select **Install** to start the installation.
Select **Finish** to close the installer upon completion



Register the VNX with the Provider

Perform the following steps on the **EMC Management** virtual machine.

From a command or PowerShell prompt, change directory to C:\Program Files\emc\ECIM\ECOM\bin

Run the **TestSmiProvider.exe** command and accept all defaults by hitting **Enter** when prompted.

```
Administrator: Wind
PS C:\Program Files\EMC\ECIM\ECOM\bin> .\TestSmiProvider.exe
Connection Type (ssl,no_ssl,native) [no_ssl]:
Host [localhost]:
Port [5988]:
Username [admin]:
Password [#1Password]:
Log output to console [y|n (default y)]:
Log output to file [y|n (default y)]:
Logfile path [Testsmiprovider.log]:
Connecting to localhost:5988
Using user account 'admin' with password '#1Password'

#####
##
##          EMC SMI Provider Tester
## This program is intended for use by EMC Support personnel
## At any time and without warning this program may be revised
## without regard to backwards compatibility or be
## removed entirely from the kit.
#####
slp   - slp urls          slpv  - slp attributes
cn    - Connect          dc    - Disconnect
disco - EMC Discover     rc    - RepeatCount
addsys - EMC AddSystem   remsys - EMC RemoveSystem
refsys - EMC RefreshSystem

ec    - EnumerateClasses   ecn   - EnumerateClasses
ei    - EnumerateInstances ein   - EnumerateInstances
ens   - EnumerateNamespaces  miner - Mine classes
```

Run the **addsys** command

For **Add System** enter **y**

For **ArrayType** enter **1**

For **IP address or hostname** enter the IP for **SPA** and hit **enter**

For **IP address or hostname 2** enter the IP for **SPB** and hit **enter**

For **Address Type** enter **2** for each entry

Enter the appropriate **User and Password** with access to run privileged commands to the array

Resulting output should be **0**

Press **enter** to continue

Press **q** to quit

```
#####
Built with EMC SMI-S Provider: V4.6.2
Namespace: root/emc
repeat count: 1
(localhost:5988) ? addsys
Add System {y|n} [n]: y

ArrayType (1=Clar, 2=Symm) [1]:
One or more IP address or Hostname or Array ID

Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 10.1.1.1
IP address or hostname or array id 1 (blank to quit): 10.1.1.2
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/NodeName, 3=Array ID)
Address Type (0) [default=2]:
Address Type (1) [default=2]:
User [null]:
Password [null]:
+++ EMCAddSystem +++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Fail
5=Invalid Parameter
4096=Job Queued, 4097=Size Not Supported
Note: Not all above values apply to all methods - see MOF for t
System : //10.5.177.41/root/emc:Clar_StorageSystem.CreationClas

In 11.731732 Seconds
Please press enter key to continue...
```

Create the SMI-S user for the SCVMM Run As Account

Perform the following steps on the **EMC Management** virtual machine.

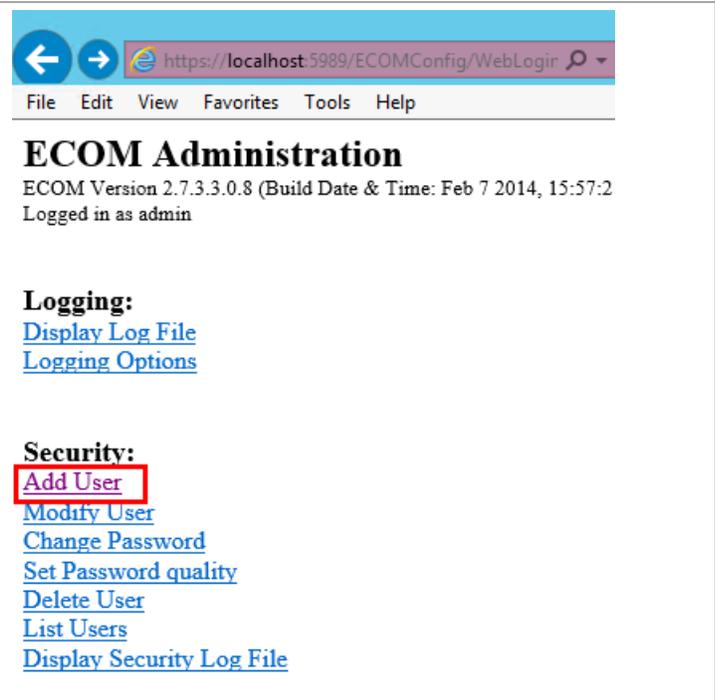
From a web browser go to <https://localhost:5989/ecomconfig>

Note: To access the localhost URL from the Management virtual machine using Internet Explorer, “Protected Mode” may need to be disabled from the Local Intranet security zone.

Log in as:
Username: admin
Password: #1Password



Select **Add User**



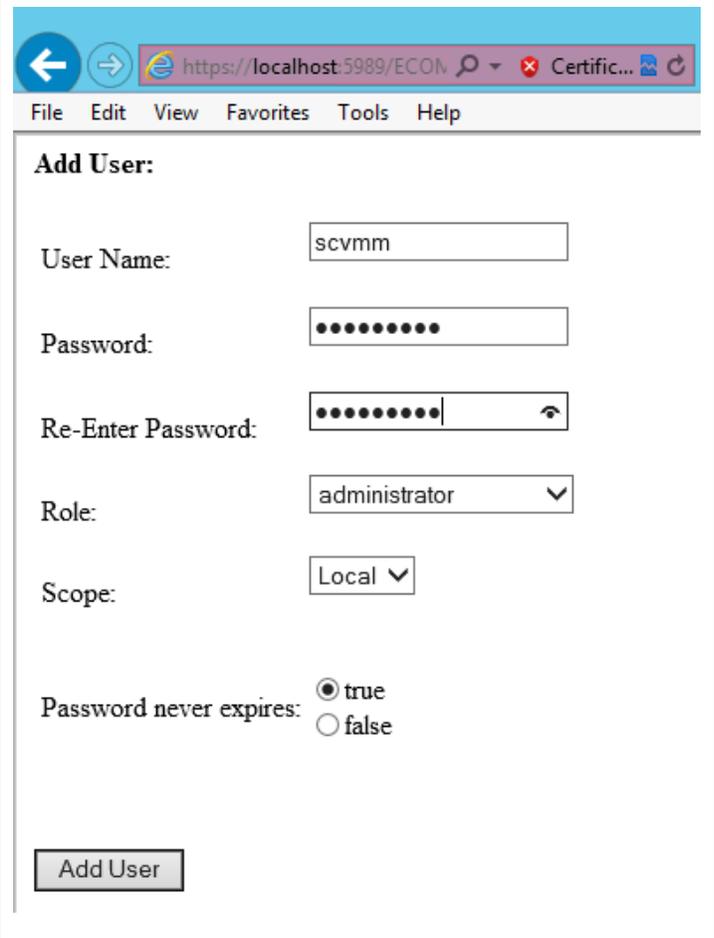
Insert the desired **User Name** and **Password**

For **Role** choose **administrator**

For **Scope** choose Local

If **Password never expires** is set to **false** the password for this user will expire in 90 days.

Select **Add User**



The screenshot shows a web browser window with the address bar displaying `https://localhost:5989/ECOM`. The browser menu includes File, Edit, View, Favorites, Tools, and Help. The main content area is titled "Add User:" and contains the following form elements:

- User Name:** A text input field containing "scvmm".
- Password:** A password input field with 10 dots.
- Re-Enter Password:** A password input field with 10 dots and a small eye icon on the right.
- Role:** A dropdown menu showing "administrator".
- Scope:** A dropdown menu showing "Local".
- Password never expires:** Two radio buttons, with "true" selected.

An "Add User" button is located at the bottom of the form.

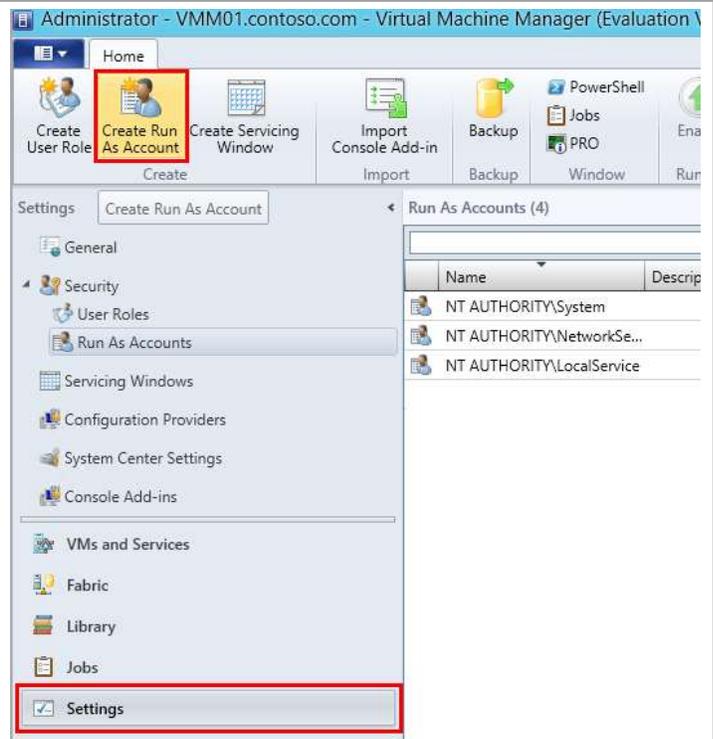
Create the Run As Account within SCVMM

This section assumes that SCVMM has already been installed in the environment

Perform the following steps on the **SCVMM** virtual machine.

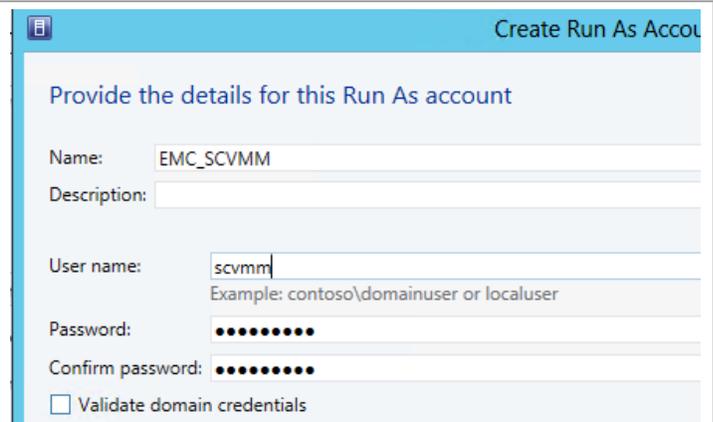
From within the Virtual Machine Manager console, go to **Settings > Security > Run As Accounts**

Select **Create Run As Account**



Enter the appropriate information, including the **User name** and **Password** used when creating the account on the SMI-S provider host.

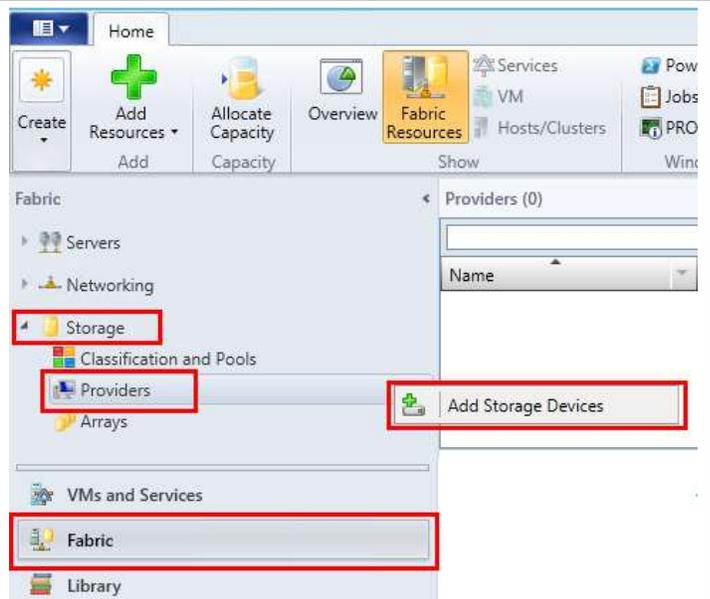
Select **OK**



Register the EMC SMI-S provider with SCVMM

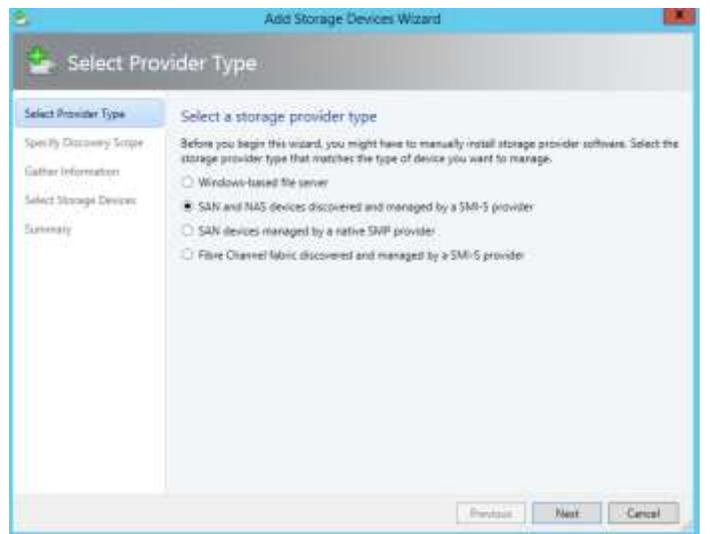
From within the Virtual Machine Manager console, go to **Fabric > Storage > Providers**

Right-click **Providers** and select **Add Storage Devices**



Select **SAN and NAS devices discovered and managed by a SMI-S provider**

Select **Next**



Enter the following information:

Protocol:

Choose “SMI-S CIMXML”

Provider IP address or FQDN:

Enter the IP or Name of the SMI-S provider host

TCP/IP

port:

If SMI-S provider was not modified, keep the default port selection

Use

SSL:

Optionally select SSL

Run

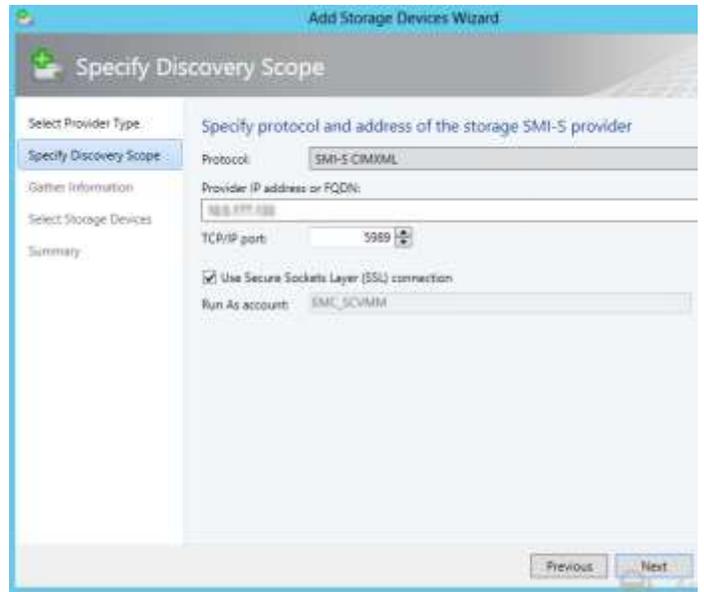
As

account:

Select the Run As account previously created which will connect to the SMI-S Provider host.

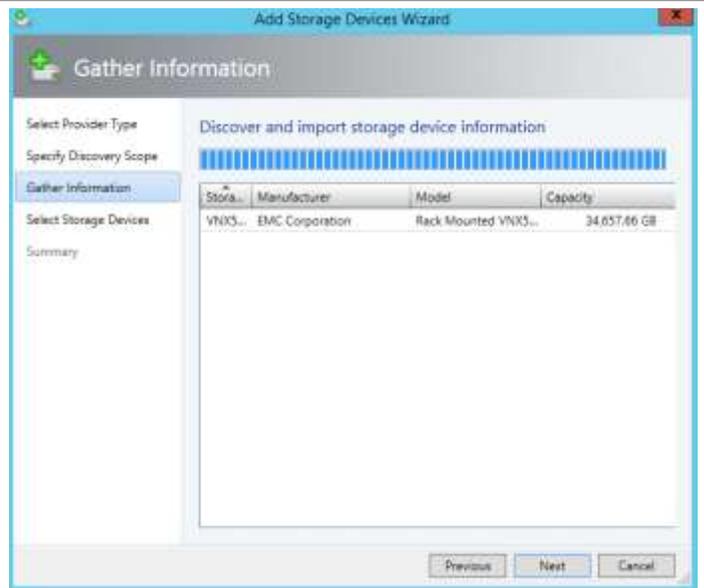
Select **Next**

If SSL was selected, import the certificate when prompted.



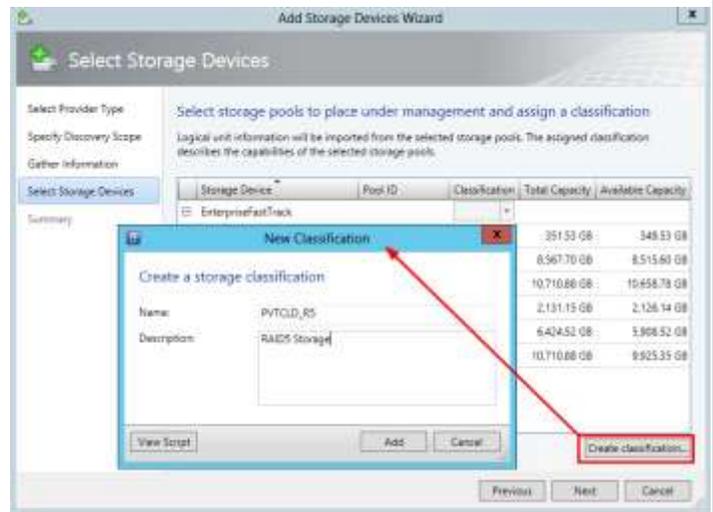
Verify the storage device following a successful discovery operation.

Select **Next**



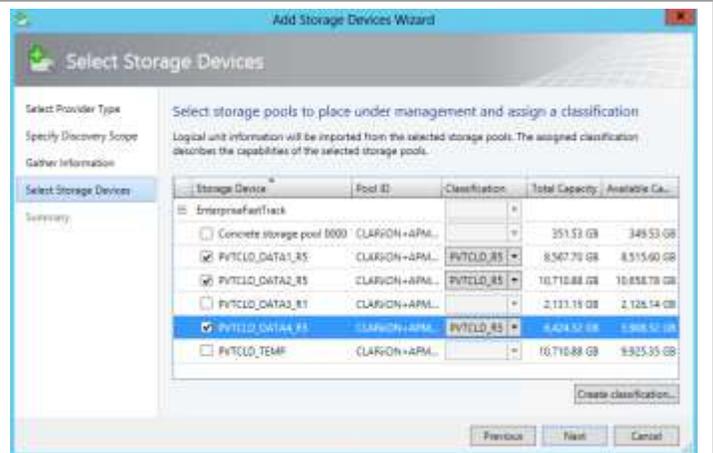
Select **Create classification** and create one or multiple classifications based on the storage types in your environment.

Select **Add**

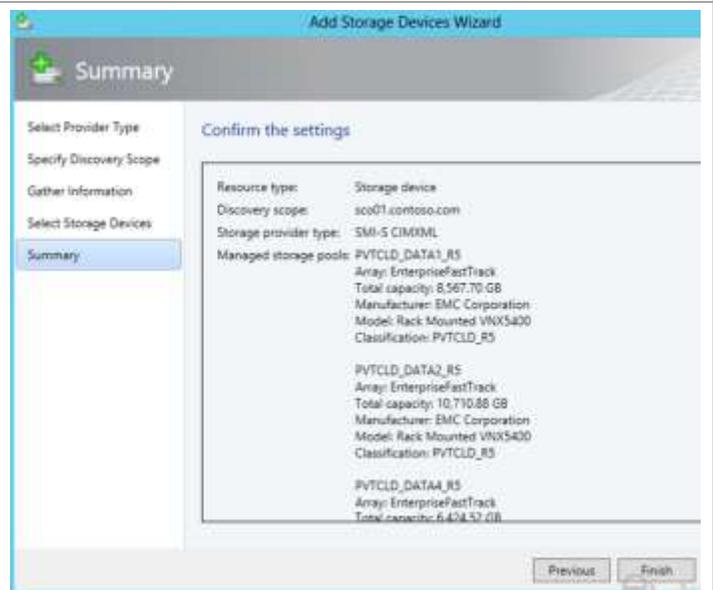


Select the pools to be managed within SCVMM and assign the previously created Classification(s)

Select **Next**



Confirm the settings and select **Finish**



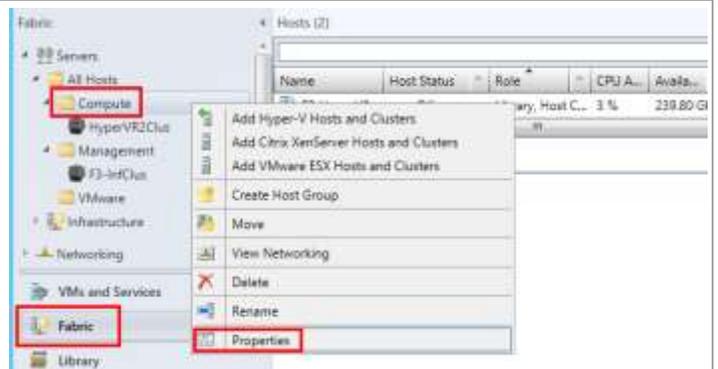
Allocate Storage Pools to Host Groups

This section assumes that SCVMM has already been installed in the environment and physical hosts have been added to host groups within VMM. Allocating a storage pool to a VMM host group makes that storage pool available for use by the hosts or clusters within that group.

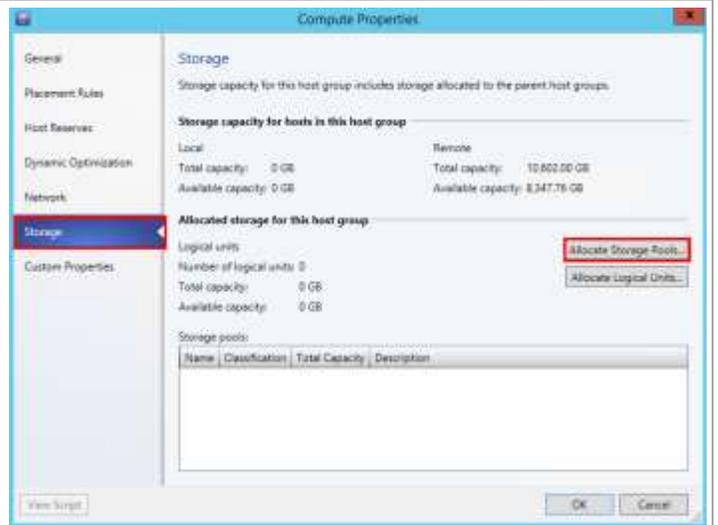
From within the Virtual Machine Manager console, go to **Fabric > Servers**

Expand the **Servers** folder

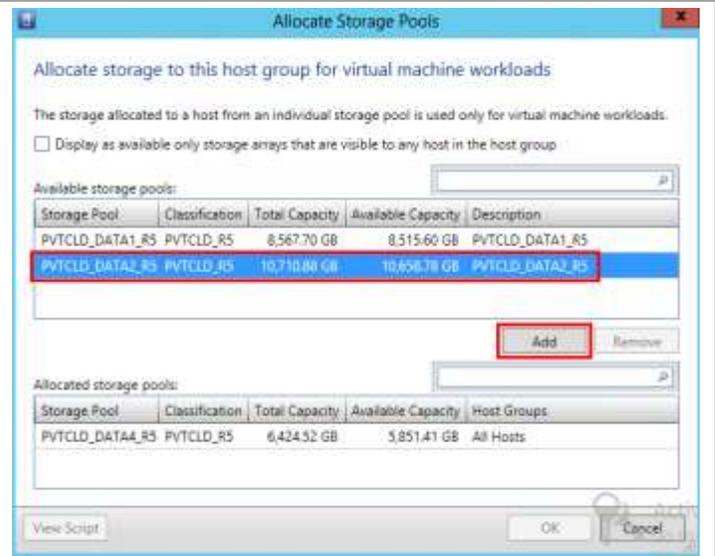
Right-click the appropriate host folder and select **Properties**



Go to the **Storage** menu and select **Allocate Storage Pools....**



Select the desired storage pools and click **Add**
 Select **OK** to commit and exit.



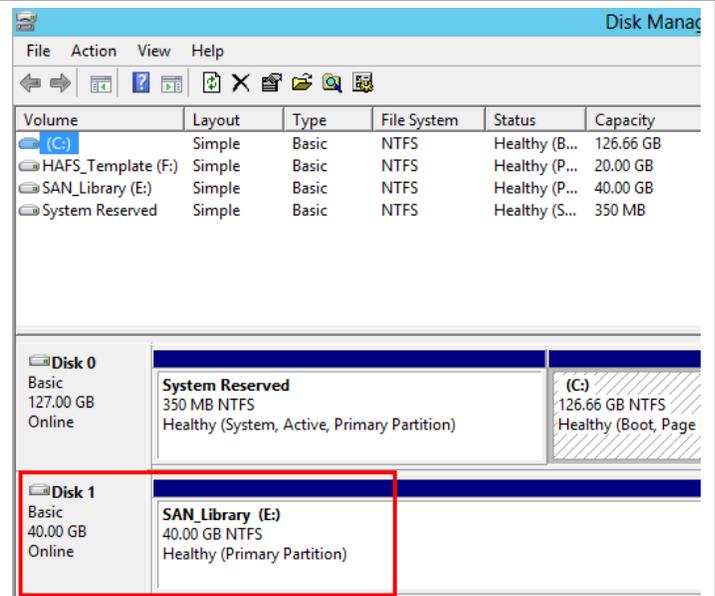
Configure the Library Server

SCVMM supports rapid virtual machine deployment with the use of array snapshots or clones. To support this functionality a library server can be configured to support a “San Copy Capable” template as a source for the replicas. The library server must be hosted by a stand-alone Hyper-V host or VM, with a physical LUN presented over either FC, iSCSI or as a pass through disk. The LUN presented to the library server must contain a single virtual hard disk. If multiple virtual hard disks reside on the template LUN then it will not be considered San Copy Capable.

Note: The LUN presented to the library server must be created in a pool which is managed by VMM. Also, the pool where this LUN resides must also be allocated to the appropriate host group where deployment is planned.

After the appropriate LUN is presented to the planned library server, execute the following steps:

Mount the LUN to the desired mount point or drive letter



Go to the drive letter or mount point in Windows Explorer and create a folder.

Right-click the newly created folder and select **Properties**

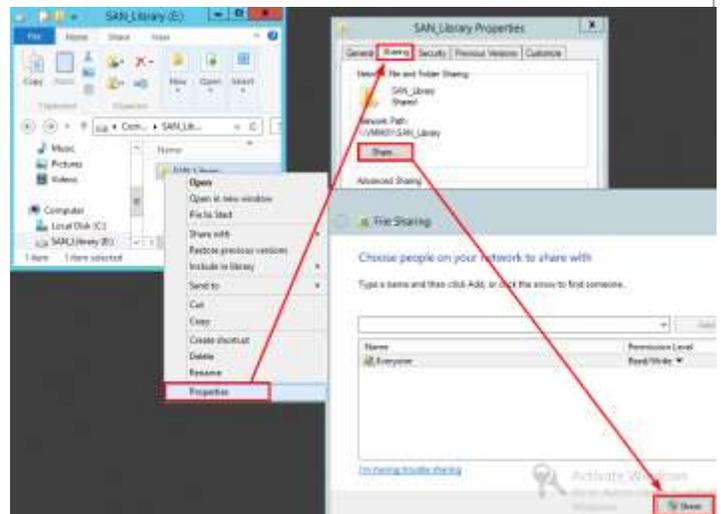
Go to the Sharing tab and select **Share** to share out the folder.

For permissions, Microsoft states the following:

For a library share to function through VMM, the minimum required permissions are that the Local System (SYSTEM) account has full control permissions at both the share and the NTFS file system level. By default, the Local System account has full control permissions when you create a file share and then add the library share to VMM management.

*However, to add resources to a library share, an administrator typically needs to access the share through Windows Explorer. They can do this either outside VMM or through the VMM console, where they can right-click the library share, and then click **Explore**. Because of this, make sure that you assign the appropriate access control permissions outside VMM. For example, we recommend that you assign full control share and NTFS permissions to the Administrators group.*

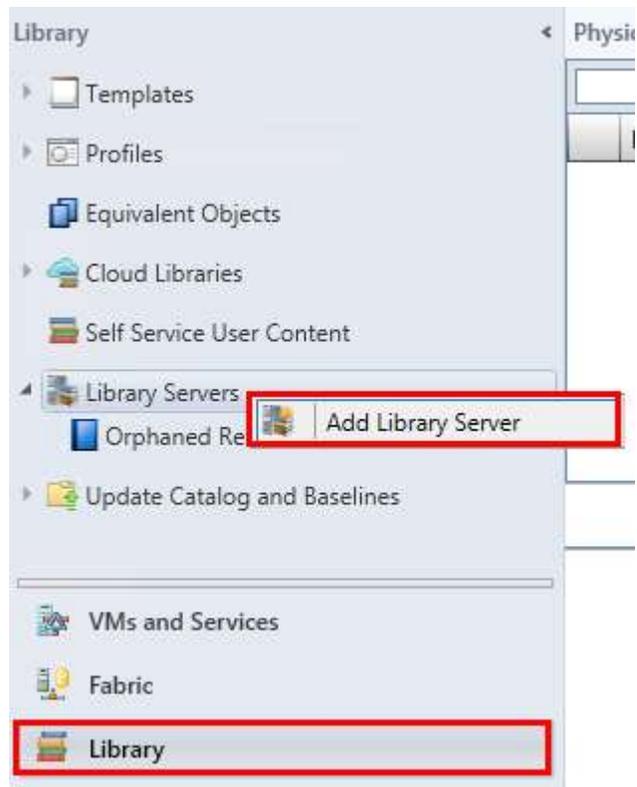
Add the desired virtual hard disk representing a sysprepped operating system image to the share. This virtual hard disk will be used for creating a san copy capable template.



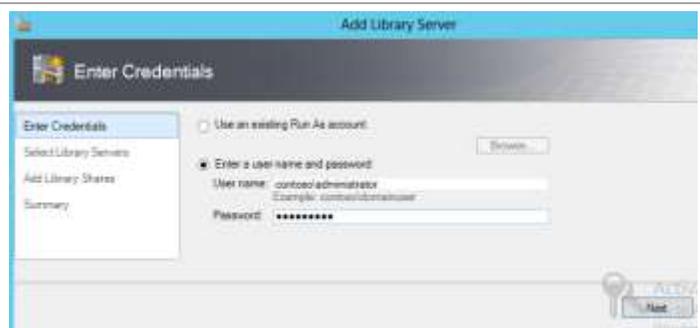
Computer > SAN_Library (E:) > SAN_Library

Name	Date modified	Type	Size
san_template	3/30/2013 4:35 PM	Hard Disk Image File	8,982,528 KB

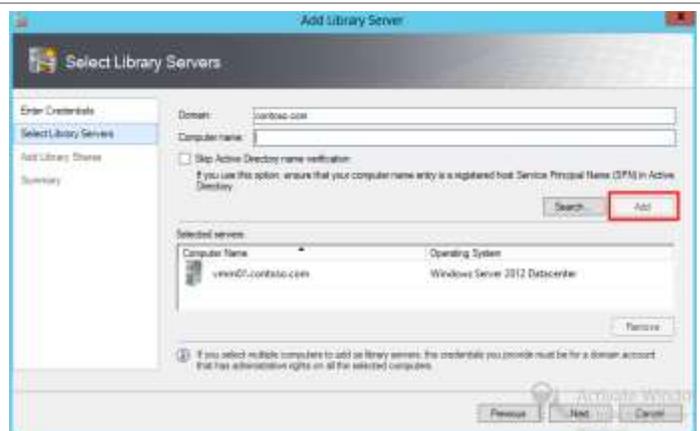
From the **Library** node of the VMM console go to **Library Servers**. Right-click library servers and select **Add Library Server**



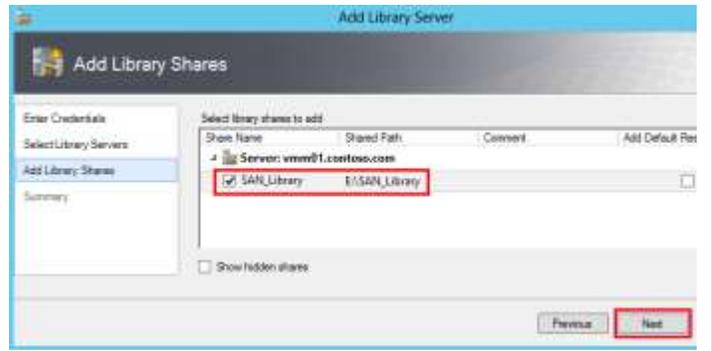
Enter a user which has administrator access to the planned library server and select **Next**



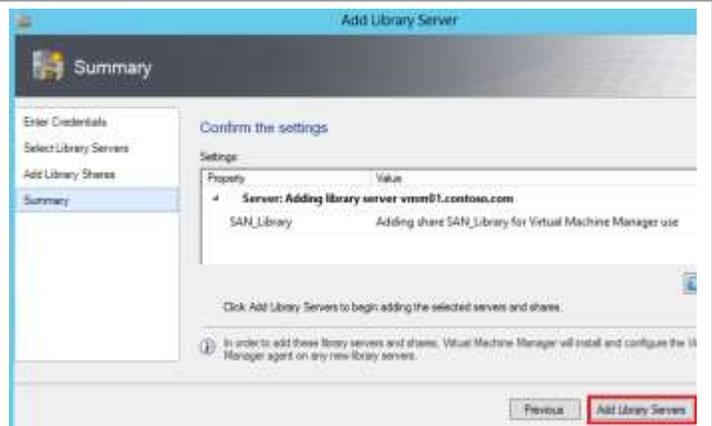
Enter the **Computer name** of the library server and choose **Add**. Then select **Next** to continue.



Select the previously created library share and click **Next**



Select **Add Library Servers** to complete the wizard and start the Add Library Server job.

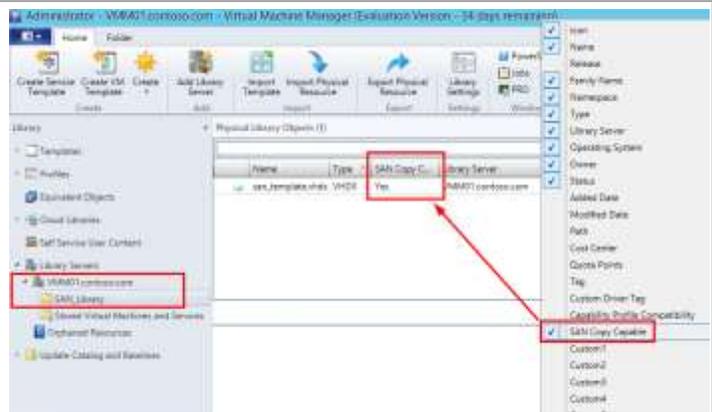


Following the successful add library server job, return to the Library area of VMM and expand the newly added library server

Select the library share and view the virtual hard disk within the share. Right-click a column grouping and find the **“San Copy Capable”** column to add.

Make sure the San Copy Capable column displays **Yes**

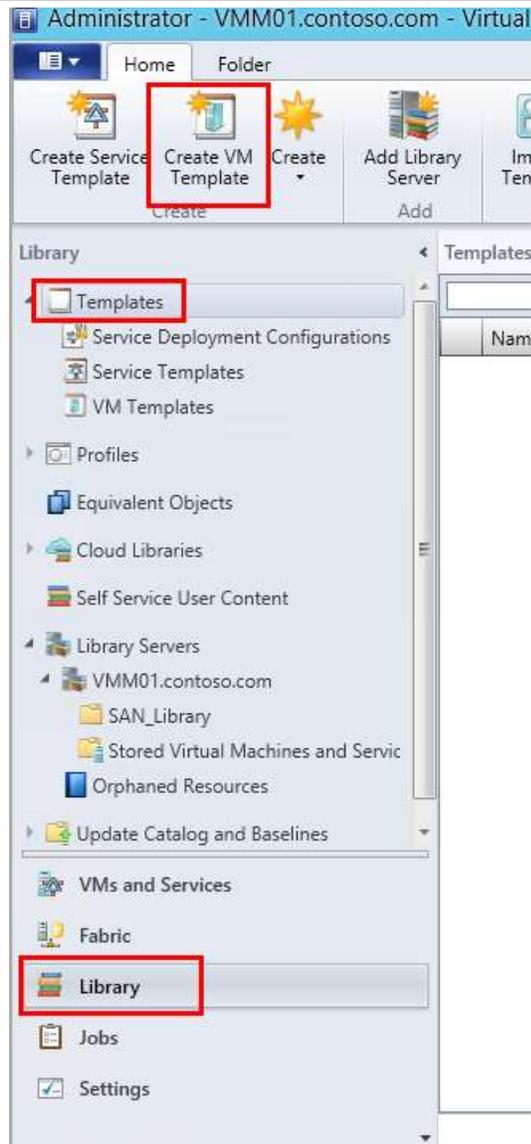
If San Copy Capable displays as “No” make sure the pool where the LUN supporting the .vhdx resides is managed by VMM. Also make sure that the pool is allocated to a host group.



Create a SAN Copy Capable Template

From within the Virtual Machine Manager console, go to **Library > Templates**

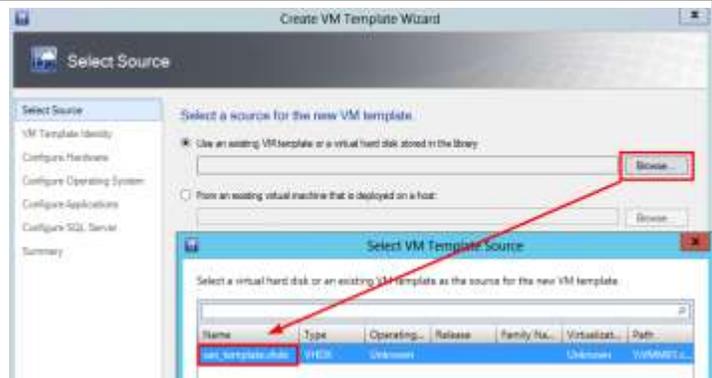
Select **Create VM Template**



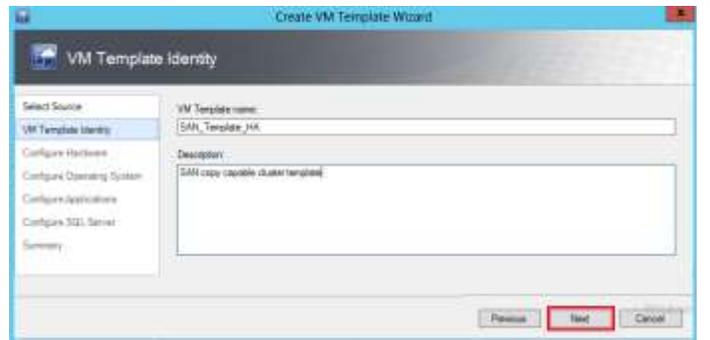
Select **Use an existing VM template or a virtual hard disk stored in the library** and choose **Browse**

Select the **San Copy Capable virtual hard disk** and select **OK**

Select **Next**

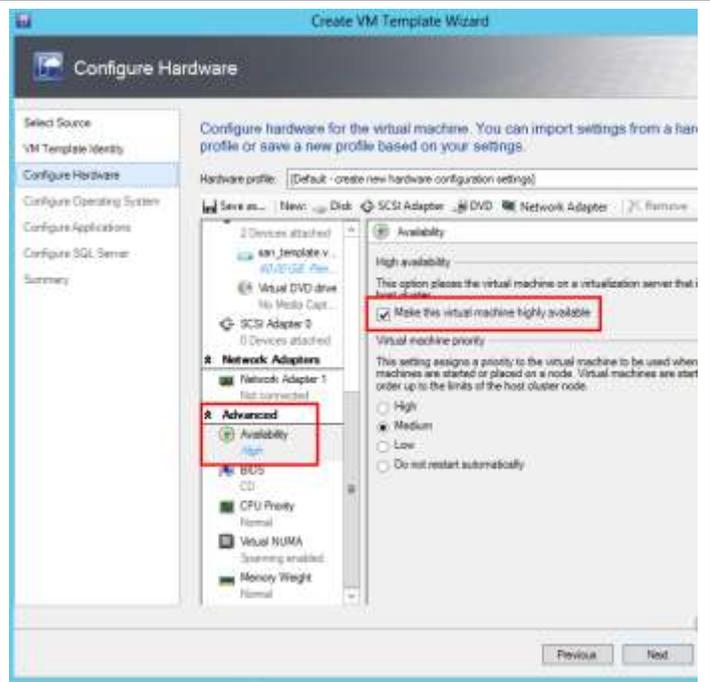


Name the template and select **Next**

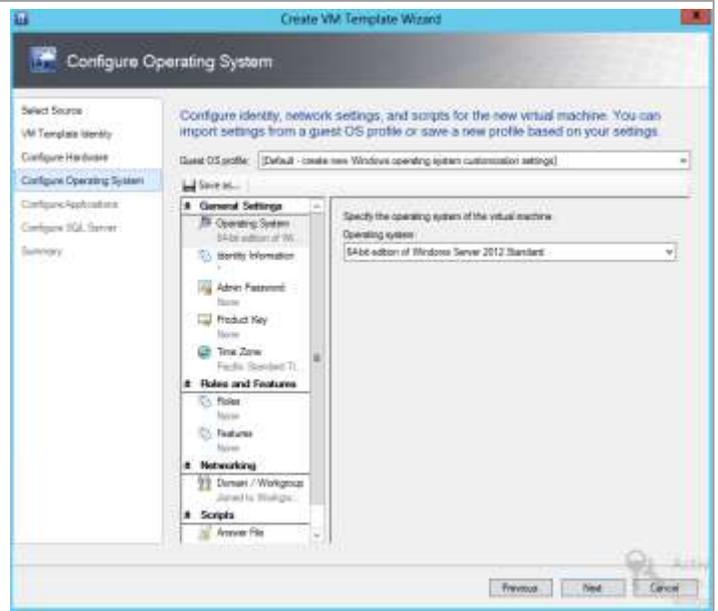


Select the appropriate hardware customizations. If the template is intended for cluster deployment, go to **Advanced > Availability** and select **Make this virtual machine highly available**

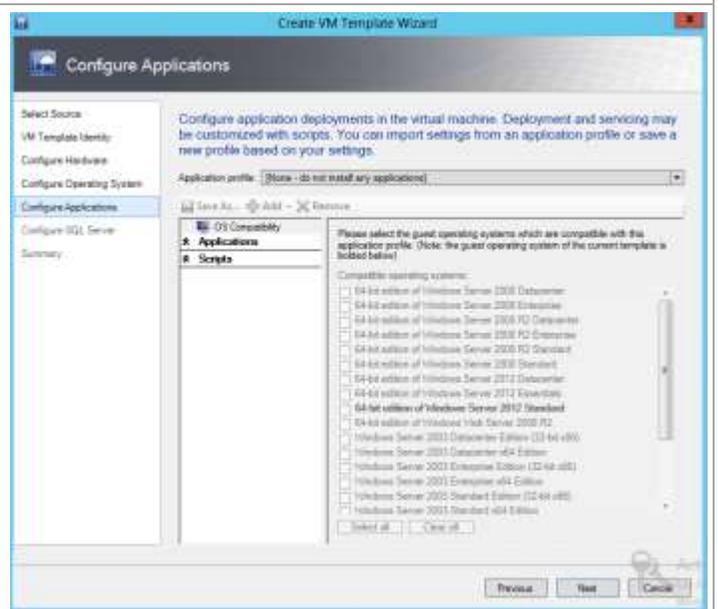
Select **Next**



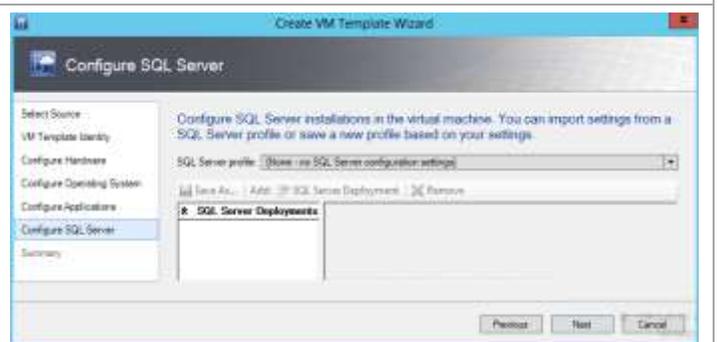
Choose the desired operating system customization and select **Next**



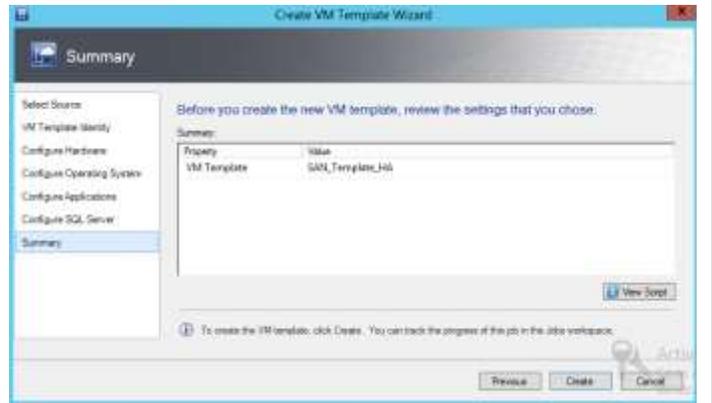
Choose optional application deployments and select **Next**



Optionally choose the SQL Server configuration for the template and choose **Next**



Select create to start the Create template job and complete the wizard.

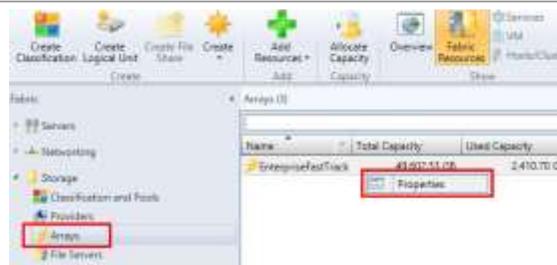


Select the Rapid Provisioning Deployment Method

SCVMM supports both clones and snapshots for SAN Copy based deployments. The copy method can be changed through PowerShell or from the GUI. The following steps detail how to change this setting using either method.

From within the Virtual Machine Manager console, go to **Fabric > Storage > Arrays**

Right-click the VNX entry and select **Properties**

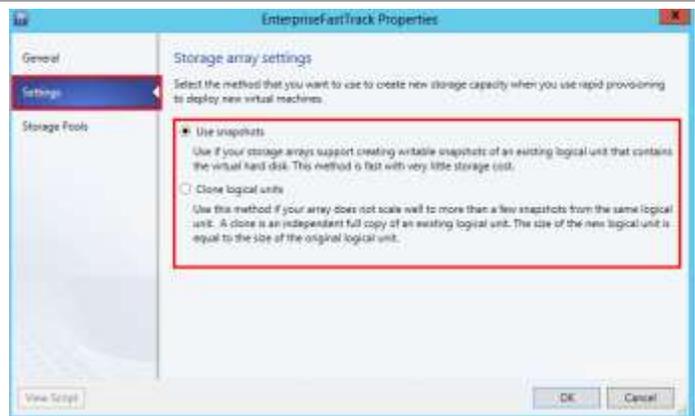


Go to the **Settings** menu

From the Settings menu **Use snapshots** can be selected to use VNX Snapshots, where up to 256 snapshots can be taken per template LUN.

Alternatively **Clone logical units** can be chosen to do full copy clones of the template LUN.

Select **OK** to change the setting.



For scripting purposes, the storage array setting for choosing snapshots or clones can be modified for a particular job. Use the following command to set either “snapshot” or “clone” for the copy method:

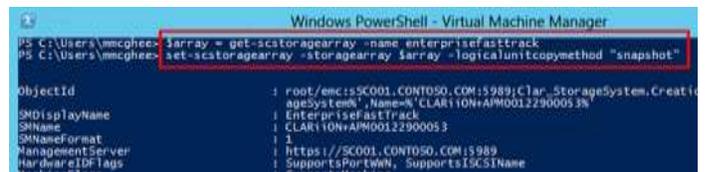
```
$array = get-scstoragearray -name  
enterprisefasttrack
```

#For Snapshots

```
set-scstoragearray -storagearray  
$array -logicalunitcopymethod  
"snapshot"
```

#For Clones

```
set-scstoragearray -storagearray  
$array -logicalunitcopymethod  
"clone"
```



Using ODX for Virtual Machine Deployments

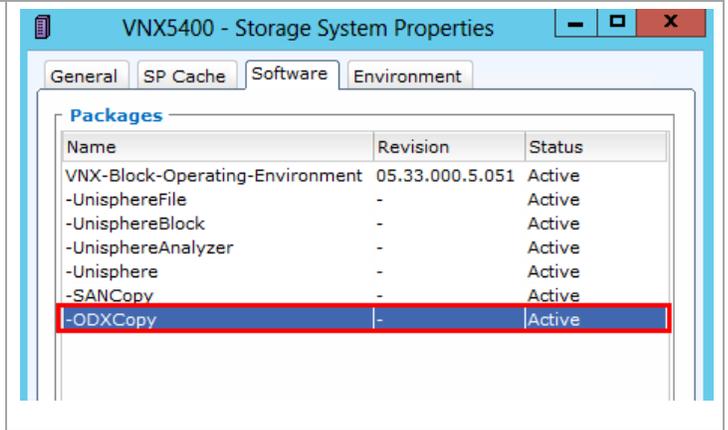
Starting with SCVMM 2012 R2, you can use ODX when deploying virtual machines from templates. When using the “network” transfer type, SCVMM 2012 R2 automatically attempts to use ODX to perform the virtual machine deployments. The VNX supports ODX when copies are performed across LUNs within the same storage array and within a LUN on the storage array. For the purposes of this document, only block based VNX support for ODX is discussed. The following steps can be used to verify if ODX is enabled on the VNX.

From Unisphere

Go to **System > System Properties**



Go to the **Software** tab and make sure **ODXCopy** is listed and active.



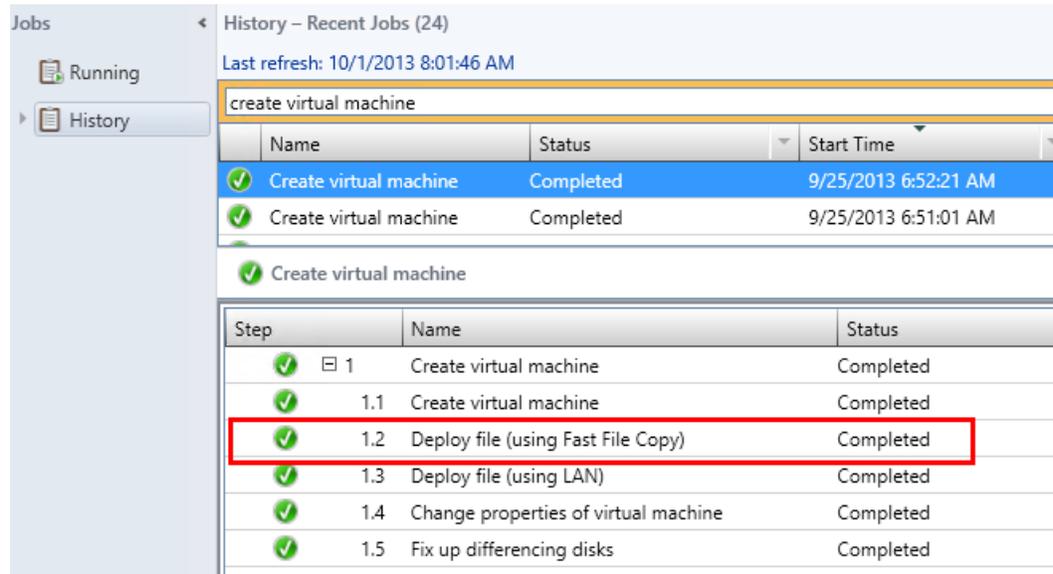
For ODX to be used, the library server, Hyper-V hosts, and clusters need an appropriate run as account for their host management credentials. You can assign the credential by specifying a run as account, which has permissions to the servers to be added, while adding the library server Hyper-V host, or cluster into SCVMM. The run as account is then assigned to the host management credentials.

For clustered hosts previously added to SCVMM, the ability to change the host management credential may be disabled from within the SCVMM console. To change the credential, run the following PowerShell commands:

```
$Cluster = Get-SCVMHostCluster -Name HyperVR2Clus.contoso.com
$RunAs = Get-SCRunAsAccount -Name dcadmin
Set-SCVmHostCluster -VMHostCluster $Cluster -VMHostManagementCredential
$RunAs
```

The library share hosting the virtual hard disk to be used for template deployment can reside in a physical or virtual host or clustered file share. For virtual environments, the storage being used to host the library share can be presented as Pass-through, Virtual Fibre Channel or a VHDX based virtual hard disk.

When ODX is automatically invoked, the create virtual machine job performing the deployment displays a step called Deploy file (using Fast File Copy) as shown below.



If ODX fails or is not used when you create a virtual machine, the deployment continues and completes by reverting to a traditional host based copy. The job displays a status of **Completed w/ Info** which notes the failure to use ODX, as shown in the example below.

Jobs

- Running
- History

History - Recent Jobs (24)

Last refresh 10/1/2013 8:01:46 AM

create virtual machine

Name	Status	Start Time	Result Name	Owner
✓ Create virtual machine	Completed	9/25/2013 6:52:24 AM	VM-578341-4	MSTPM\Administrator
✓ Create virtual machine	Completed w/ Info	9/25/2013 6:52:23 AM	VM-578341-3	MSTPM\Administrator
✓ Create virtual machine	Completed	9/25/2013 6:52:22 AM	VM-578341-2	MSTPM\Administrator

✓ Create virtual machine

Status: Completed w/ Info
Command: New-SCVirtualMachine
Result name: VM-578341-3
Started: 9/25/2013 6:52:23 AM
Duration: 00:04:25
Owner: MSTPM\Administrator

Information (26278)
Information (26278)
VMM could not offload transfer the file \\mstpm3033.mstpm.local\FC_Templates3\template.vhdx to C:\ClusterStorage\Volume3\VMs\VM-578341-3\template.vhdx.